5. Difference between Linear Supply and Switch Mode Power Supply

The **linear power supply** and **Switch mode power supply,** both supplies DC power to electrical and electronic circuits but the similarities end here. The crucial factor which differentiates linear power supply and SMPS is the working procedure. The Linear power supply converts high voltage AC into the low voltage using a transformer and then converts it into DC voltage while the switched mode supply converts AC into DC first then transform that DC voltage into desired voltage.

The Switch mode power supply is also termed as SMPS in abbreviated form. SMPS is most commonly used in **mobile chargers, DC motors** etc. On the contrary, the linear power supply is used in high-frequency application such as **Radio Frequency application etc.**

Another significant factor which creates the difference between these linear power supply and SMPS is size. The linear power supply is bulky while the **SMPS is light in weight.** This makes the SMPS portable and can be easily used anywhere while linear power supply can be used only for laboratory or big electrical and electronic circuit.

We will discuss some more significant differences between linear and switch mode power supply in the comparison chart but before that let’s put light on the roadmap of this article.

Comparison Chart

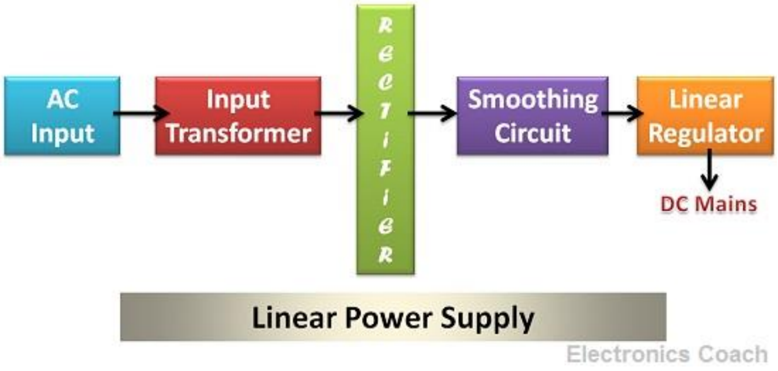
PARAMETERS	LINEAR POWER SUPPLY	SWITCH MODE POWER SUPPLY (SMPS)
Definition	It completes the stepping down of AC voltage first then it converts it into DC.	It converts the input signal into DC first then it steps down the voltage up to desired level.
Efficiency	Low efficiency i.e. about 20-25%	High Efficiency i.e. about 60-65%
Voltage Regulation	Voltage regulation is done by voltage regulator.	Voltage regulation is done by feedback circuit.
Magnetic material used	Stalloy or CRGO core is used	Ferrite core is used
Weight	It is bulky.	It is less bulky in comparison to linear power supply.
Reliability	More reliable in comparison to SMPS.	its reliability depends on the transistors used for switching
Complexity	Less complex than SMPS.	More complex than Linear power supply.
Transient response	It possess faster response.	It possess slower response.

PARAMETERS	LINEAR POWER SUPPLY	SWITCH MODE POWER SUPPLY (SMPS)
RF interference	No RF interference	RF shielding is required as switching produces more RF interference.
Noise and Electromagnetic interference	It is immune to noise and electromagnetic interference.	Effect of noise and electromagnetic interference is quite significant, thus EMI filters are required.
Applications	Used in Audio frequency applications and RF applications.	Used in chargers of mobile phones, DC motors etc.

Definition

Linear Power Supply

The **Linear Power Supply** is power supplying circuit which is used in electrical and electronic circuit to supply the DC power to the circuit. It consists of a step-down transformer, rectifier, a filter circuit and voltage regulator.



The AC is always supplied with high voltage because it is economical to supply AC at high voltage. The frequency of the AC signal is very low, i.e. **50 Hz or**

60Hz. To reduce the voltage of AC, step down transformer is used. The size of the transformer is large for linear power supply.

The transformer which is used to step down the low-frequency AC signal will be bulky. If the AC signal frequency is high, then a small transformer can be used but in this application the AC signal comprised of low-frequency AC thus, the circuit requires a large size and bulky transformer.

The step-down voltage is then passed to the rectifier circuit to convert it into DC. The DC voltage obtained from the rectifier comprises of AC pulses. Thus, a filter circuit is used to remove the AC ripples.

The obtained DC voltage does not remain constant; it changes with the variation in input voltage or the value of load resistor. This variation in the output voltage is undesirable. Therefore, a voltage regulator is used after filtering the signal.

The voltage regulator consists of the variable resistor the value of which changes according to the output required. This variable resistor produces voltage drop when the output voltage required is low.

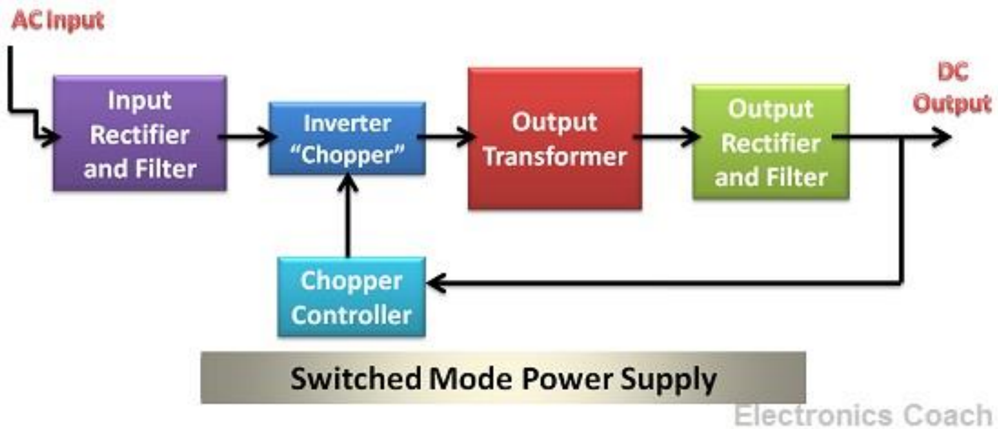
Drawback of Linear Power Supply

The drawback of the linear power supply is that the use of voltage regulator requires sink which increases the size of the power supply. The voltage regulator dissipates power due to which **ohmic losse**s occur this increases the temperature, and thus a heat sink is required.

As a consequence of using heat sink and transformer of large size the size of the linear power supply becomes more and this makes the power supply bulky to use. Moreover, dissipation caused by variable resistor decreases the **efficiency of linear power supply to 25-50%.**

Switched Mode Power Supply

The **Switched Mode Power Supply** operated on the principle of switching using a **MOSFET transistor.** It consists rectifier circuit, a filter circuit, chopper, chopper controller, output transformer and a filter circuit.



The principle of working of Switched Mode Power Supply is based on switching technique. The low-frequency AC is converted first into DC signal. Then this DC signal is chopped using chopper circuit. Chopper Circuit consists of MOSFET switching transistor which switches ON or OFF with the help of chopper controller circuit.

The output obtained by Chopper is high-frequency DC signal. Now again a step-down transformer is used to convert this high voltage high-frequency signal into a low voltage signal. The step-down transformer used in this case will be small in size because the transformer used to operate for high-frequency application is small in size.

This is the advantage of using an SMPS (switched mode power supply) circuit. This configuration power supply is not bulky and thus portable. The voltage regulation in SMPS is obtained by the feedback circuit. The feedback circuit takes input from output DC voltage and gives output to chopper controller. The chopper controller generates the gate pulse according to the output DC.

Therefore, voltage regulation in SMPS does not dissipate power and thus do not require sink. This increase the efficiency of SMPS power supply as there is no ohmic loss and the size is also small.The **efficiency of SMP S lies in the range of 65-75%.**

Key Differences Between Linear Supply and Switch Mode Power Supply

1. The **main difference** between the linear power supply and SMPS is that linear power supply converts the high voltage of AC into low voltage AC first then the rectification procedure takes place. On the contrary, the SMPS

converts the AC signal into DC signal first then the stepping down of voltage signal takes place.

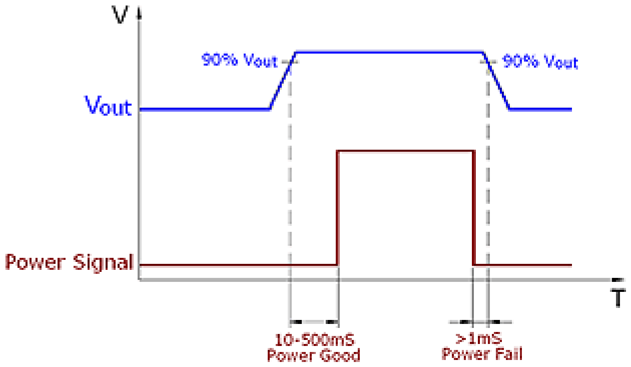
2. Linear power supply use voltage regulator for **voltage regulation** of the output voltage while SMPS uses feedback circuit for voltage regulation.
3. **Power dissipation** also plays a key role in differentiating linear power supply and SMPS. The Linear power supply also dissipates power and thus requires a heat sink, but SMPS do not require **heat sink** as there is no power dissipation.
4. The step-down transformer used in **linear supply is bulky** while in SMPS the step-down transformer is light in weight.
5. The **noise disturbance** is more in SMPS due to switching action; this makes SMPS inappropriate for audio and radio frequency application. The linear power supply is immune to noise disturbance and thus used in audio and radio frequency application.
6. There is the major difference between the **efficiency** of the linear power supply and SMPS. The efficiency of the linear power supply is low about 20-25% due to ohmic losses while that of SMPS is high, i.e. about 65-75%.

Conclusion

The linear power supply steps down the AC voltage first then converts it into DC while SMPS converts into DC first then uses the step-down transformer to obtain the desired voltage. The SMPS has the drawback that it creates noise interference due to switching. Moreover, switching also creates **electromagnetic interferences** and **RF interferences** thus **EMI filters**, and **RF shielding** is also used along with SMPS circuit.

What is Power Good Signal?

The power good signal is a +5 volts signal that is generated by a switching power supply when the supply has stabilized its output voltages and passed all its internal self-tests. The is usually generated after s a period of between 0.1 seconds and 0.5 seconds after turning on the power supply.



The power supply is usually designed with the normal voltage outputs to supply the various circuits and components of the computer. In addition to these voltages, a power good signal is added to ensure that all the required voltages are always stable for the designed computer operation. This ensures that the magnitude of the voltages do not rise or fall to abnormal levels that would risk the proper operation of the delicate computer circuits.

The computer processor is designed to monitor the power and only start operations once all the required power conditions are met. This avoids the possibility of the computer starting on unstable voltages which can damage the mother board components and other computer devices such as hard disks. Once the power supply is turned on and stabilized its designed output voltages with no faults, the power good signal is sent to the processor to inform the computer that the supply is operating well and all required voltages and currents are available for the proper operation.

The motherboard relies on the processor timer chip which manages a reset line to the processor. As long as the power good signal is absent, the timer chip applies a constant reset signal to the processor and the computer cannot turn on. Once the power supply completes its initialization and stabilizes its outputs, the power good signal is sent to the timer chip which in turn stops resetting the processor. The processor now starts the computer boot up process and executes the code at the FFFF:0000 address which is normally the ROM BIOS.

The power supply diagnostics continuously monitors its outputs and stability of the supply, in case a fault or unstable voltages due to brownouts, deteriorated components, or input supply issues, the power good signal is withdrawn. This causes the timer chip to reset the processor continuously and thereby turn off the computer operations. Once the power supply resumes its normal and stable output voltages, the power good signal is again regenerated and sent to the timer chip to restart the computer operation.

Once a bad power situation detected, the computer is permanently reset and stopped quickly to avoid malfunction such as parity errors and malfunction. The power good signal therefore ensures that the computer will only operate when it receives the proper voltages and never receives the bad power which is unstable or have improper voltage levels.

“Power Good Signal” Function of PC Power Supply

This article will discuss about the alert function of pc power supply. The main voltage power supply, which supply the computer is +12 volts. Power supply for this circuit should provide a large output current, especially in computers with lots of drive bays. 12 V is applied also to the fans, who tend to work all the time. Usually, the fan motor consumes between 100 and 250 mA, but with newer computers, this value is less than 100 mA. In most computers, fans operate from a +12, but portable models are used for +5 V (or 3.3).

The purpose of Power Good signal is to tell the computer all is well with the power supply and that the computer can continue to operate normally. If the Power-Good signal is not present at startup, the CPU is held in reset state. If a Power-Good signal goes down during operation, the CPU will shut down. The Power-Good signal prevents the computer from attempting to operate on improper voltages and damaging itself.

Power supply not only produces the necessary sites for computer power, but suspends the operation of the system until long as the magnitude of this voltage reaches a value that is sufficient for normal operation. In other words, the power supply does not allow the computer to work with “abnormal” level of supply voltage. Each power supply before getting permission to run the system, the internal inspection and testing of the output voltage. After that, the system board sends a special signal Power_Good. If this signal is not received, the computer will not work. The mains voltage may be too high (or low) for normal operation the power supply, and it may overheat. In any case, the signal Power_Good disappear, leading to either restart or shutdown to complete the system. If your computer shows no signs of life when switched on, but fans and motors drives work, then perhaps there is no signal Power_Good .

Such a radical method of protection was provided by IBM, based on the consideration that in case of overload or overheating of the power supply output voltage to be go beyond the acceptable limits and work on that computer would be impossible.

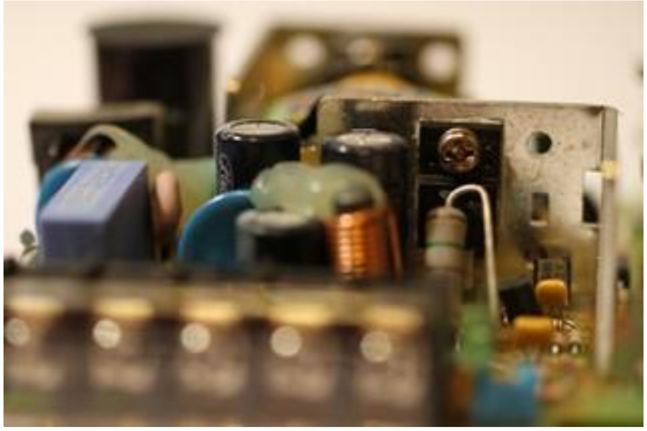
Power_Good Sometimes signal is used to reset manually. He served on chip clock generator. This chip controls the formation of the clock signal and produces the initial restart. If the signal circuit to ground Power_Good any switch, the clock generation ceases and the processor is stopped. After opening the switch produces a momentary output of the processor and the initial installation allowed the normal signal path Power_Good, a result of running a hardware reboot the computer.

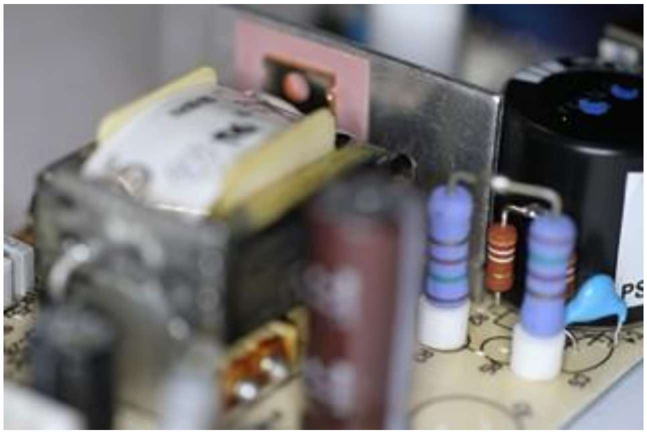
In computers the motherboard form factors (such as ATX, micro-ATX and NLX) provides another special signal. This signal, called PS_ON, the program can be used to turn off the power supply (and, thus, the entire computer). PS_ON signal used by the operating system (eg, Windows 9x), which supports Advanced Power Management (Advanced Power Management – APM). When you select the Shut Down command from the main menu, Windows automatically disables the computer’s power supply. System that does not have this feature, just displays a message stating that you can turn off the computer.

Troubleshooting switch mode power supplies

Introduction

Switch mode power supplies (SMPS) are now standard for the majority of our home appliances. Old fashioned linear power supplies based on mains frequency transformers are disappearing, mainly because of their cost, their large size and weight. We're taking here about mains voltage (say 120 V or 230 V AC) power supplies with power ranging from a few Watts to several hundred Watts.





Switch mode power supplies are everywhere; here are some pictures of their guts. The big high power components and small heat sinks are typical of SMPS.

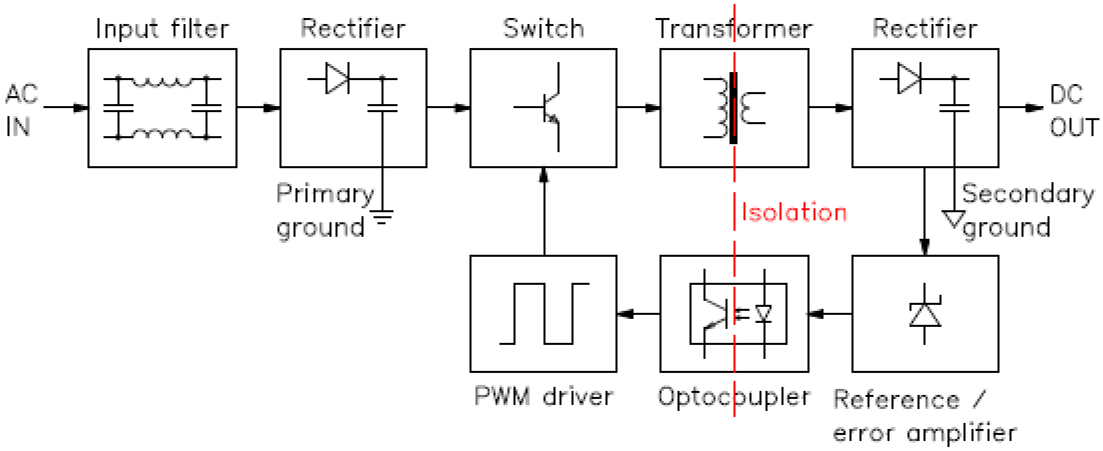
These devices are incredibly reliable, but being very often left powered all the time (even when their load is switched off), they still are the weak link. Components are fed with high voltage, they get warm, they age quickly because of the full time operation and when there is a surge, the SMPS is the first stage concerned. Many problems with our home appliances are due to SMPS faults.

Unfortunately, SMPS are a bit tricky to repair and I often get asked for advice. So, I summarized in this page the basic ideas and the tricks that I use the most.

Here, I suppose you have a perfectly designed circuit that used to work perfectly and suddenly failed. If you're trying to debug your own design, still some of these tricks apply, but you'll probably need much more than just this article.

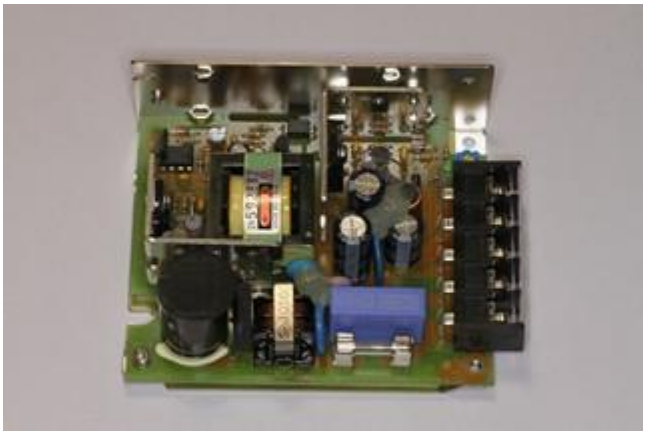
SMPS structure

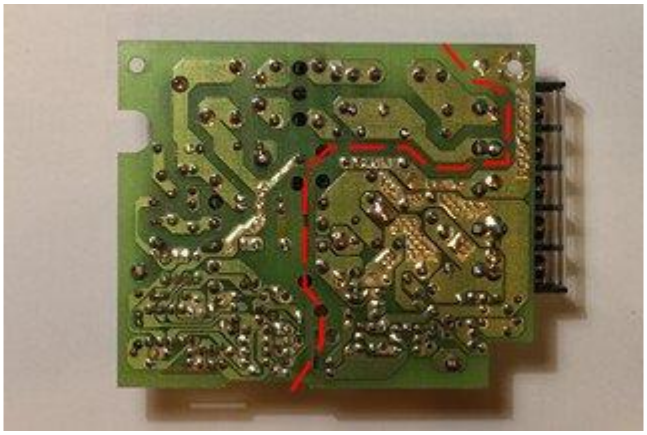
First, let's take a look to the generic block diagram of a SMPS. The mains power enters the circuits through a line filter, it's rectified and smoothed out to obtain a high DC voltage (a few hundreds volts). Some rectifiers have a switch that makes them a voltage doubler when working with 120 V AC mains or just a rectifier when working with 230 V. Some others are designed to work from say 100 to 240 V AC with no switches and the regulator does the rest. This high DC voltage is switched by one or more transistors (or MOSFETs) to drive the primary of a ferrite transformer. On the secondary side, the voltage is rectified and filtered. Switching transistors are driven by a control circuit that senses the output voltage (and input current) and regulates accordingly. This control circuit is very often on the primary side and often powered by an extra winding on the transformer. A sample of the output voltage is fed back via an opto-coupler. In some cases the control circuit is located on the secondary side and drives the transistor(s) via a small additional transformer. All configurations have some additional circuit to allow the controller to start at power-up.



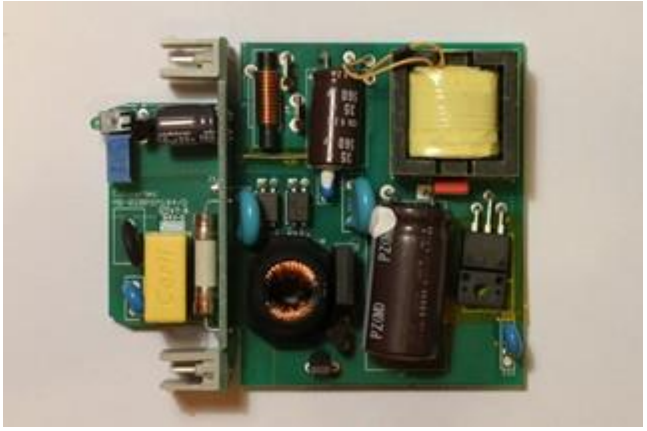
Structure of a SMPS.

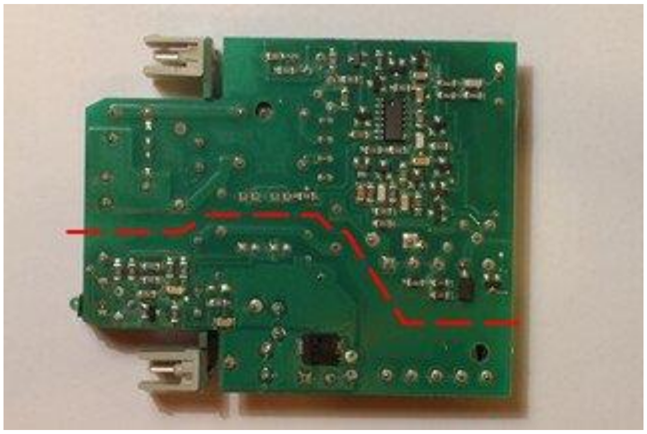
There is always a very clear separation between the high and low voltage sides (primary and secondary sides). You can observe it on the bottom (copper) side of the PCB as a larger spacing in the tracks. Some times the solder mask varnish is removed in this area or there are holes and slots to increase insulations. On the pictures in this page, this separation is often marked with a dashed red line.





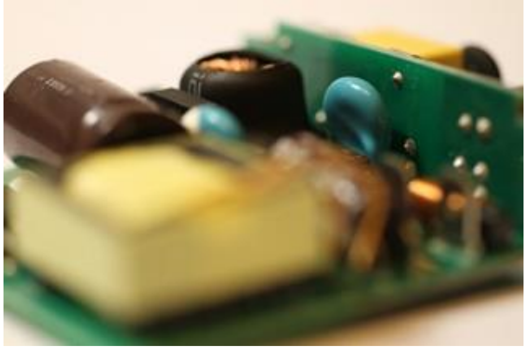
This SMPS uses classic-style (through hole) components. The high voltage side is on the left of the dashed red line.





This SMPS uses modern surface mount (SMD) components. Here, the controller uses SMD technology and is mounted on the bottom side. The large SMD diode is the low voltage rectifier. The high voltage side is above the dashed red line.

The primary and secondary side are fully DC isolated by the transformer. Very often, if the ground of the output is not connected to the mains ground, a small high voltage capacitor connects these two grounds at high frequency.

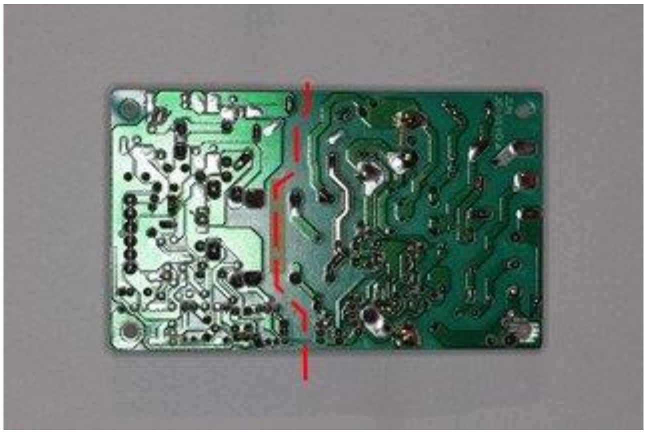


The light blue capacitor in this picture is the high voltage capacitor connecting the low voltage ground with the mains ground. Of course, there is DC insulation.

Safety first

Before starting, I just want to remind that SMPS are dangerous circuits: half of the components are directly connected to the mains voltage. A large storage capacitor is charged at high voltage and can be dangerous even when the mains supply is disconnected. Not all SMPS include bleeding resistors (or they could be broken) so the capacitors could stay charged for a long time. Always make sure all capacitor are completely discharged before touching the circuit. To discharge the capacitors, don't short them with the screwdriver, use a suitable resistor instead (a few kΩ and a few

Watts) connected to two insulated probes like the one of a multimeter. Then, measure the voltage and make sure it's zero before proceeding. Keep also in mind that heat sinks very often are not grounded and they can very well be at mains voltage. Beware of taking measures with an oscilloscope: oscilloscopes are grounded to the mains supply (and it's a bad idea to float them) and you could make a short with your ground lead (this would be dangerous also for your oscilloscope). In summary, SMPS repair is for experienced and skilled technicians; if you don't know exactly what you're doing, stay away from SMPSs.

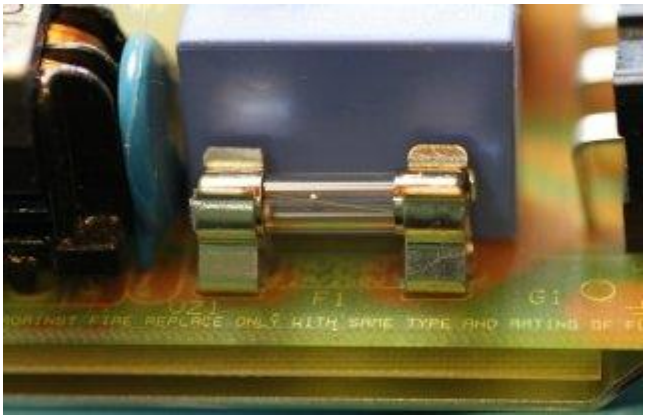


This SMPS has no bleeder resistor on the high voltage filter capacitor. Please remark the 330 kΩ resistor tack soldered on the bottom side of the PCB during the repair operation to automatically discharge the capacitor in a reasonable time and avoid potential shocks. The high voltage side is on the right of the dashed red line.

Visual inspection

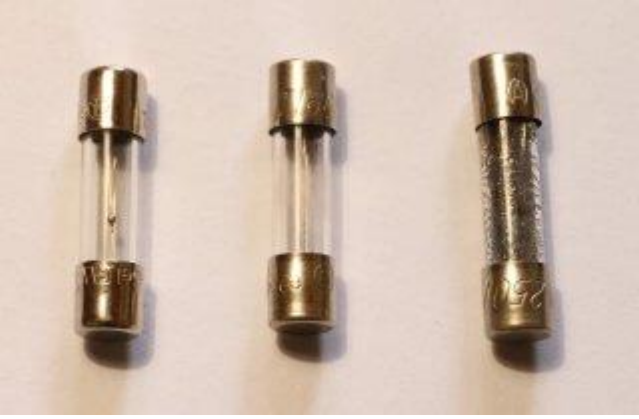
I usually start with a visual inspection to get an idea. Of course, first I disconnect the SMPS and I make sure all capacitor are discharged. Many faulty electrolytic capacitors, when not exploded, can easily be spotted because they "inflate" and their top (or bottom) side becomes dome-shaped (see below). Burned resistor can also be spotted by their black colour and bad smell. A look to the ferrite transformer is very important: if it looks burned out and smells badly, I generally give up because it may have shorted turns and it's a nightmare to repair or find a replacement part. If the transformer is faulty, I prefer to replace the whole SMPS and save a lot of time. Some components are warm and as time goes by they tend to get a little brownish (the same is true for the board near them): this is not necessarily a problem; a little brown is ok, black and smelly is not.

If your SMPS has a regulator IC, try to find it's datasheet on the internet: many SMPS have a schematic diagram very similar to the examples reported in the datasheets. If it does, you'll save a lot of time.



Start by looking at the SMPS mains line fuse (this one is good).

Start by looking at the mains fuse: this will give you good clues on the origin of the failure. A blown fuse usually means many faulty semiconductors; a healthy one is probably just a single component.



Three Ø5 × 20 mm fuses: the one on the left is good, the one in the middle blew up with a moderate current and the one on the right blew up with a large current.

Also look at how the fuse looks like: if it only slowly burned the failure was not catastrophic, but if the fuse almost "exploded", there was a big current when it blew up and you can expect a lot of damaged components (especially semiconductors). It doesn't mean you can't fix it, but just that you'll have many components to replace: if you find just a faulty one, you should check again. Unfortunately some fuses are filled with sand and you cannot see what happened.

No output, good fuse

SMPS can fail in many different ways, the most common being no output power at all. In this case, I start by checking the input fuse. If the fuse is good but there is no output, probably all the semiconductors are good and it could be easy to fix. Keep in mind that usually semiconductors blow up shorted and resistors (and often capacitors) blow up open.

A good candidate is the inrush current limiter (an NTC). Than I check for high power rating resistors, particularly on the primary side: I measure their resistance one by one, in circuit. If the value doesn't match what written (or colour coded) on the component, I unsolder one terminal and measure again: if the value is wrong, I replace it with a new one.

The first resistors to check are the one in series with the power transistors, usually less than one Ohm. Sometimes the regulator is powered by a high value high wattage resistor in series with a Zener diode: if the resistor is good, maybe the Zener is shorted, so I check all diode junctions with the diode function of the multimeter (most of the times, you can do this in circuit). Than I check the capacitors (see below). Faulty regulators IC can happen but it's not very common.

No output, blown fuse

On the other hand, if the fuse is open, than something went really wrong in the circuit. Don't replace the fuse yet, it would just blow again: there is a short circuit somewhere that you have to fix first. Typical problems are blown up power transistors or rectifier diodes, especially on the primary side. Just use the diode function of a multi-meter and check the junctions: shorts are easy to spot. More components can be faulty at the same time and if you don't replace them all, they may blow again, so be careful. Than, I also check for faulty resistors as above and faulty capacitors (see below).

If the power transistor (or one of them) is dead, chances are that many other components are dead too. Often SMPS include protection components such as additional resistor or Zener diodes to reduce damages in case of failure, but not always. Before going to far in replacing, make sure you check all the parts. For example, check if the controller IC still works. Powering it off-line with a small external DC power supply and checking for pulses on the transistor base (or gate) is a good idea. But some IC won't work if there is no high voltage to switch: check the datasheet first. If too many components are dead, it’s probably easier to replace the whole SMPS.

When replacing semiconductors I first try to source the exact same part. If it's unavailable (or too expensive) I look for alternatives. Of course the new semiconductor must show at least the same voltage, current and power characteristics, or be even better. For diodes also check the switching time: you want a diode that is at least as fast as the old one, or faster. For transistor, check the gain and the cut-off frequency: you want a similar gain (not too low and not too high) and a cut-off frequency at least ten times higher than the switching frequency. For MOSFETs check the gate capacitance that should not exceed the one of the old component and the gate threshold voltage that has to be similar to the old device.

After replacing the faulty components, it's a very good idea to use the light bulb trick (see below) for the very first power on test: this will limit the damages in case the problem isn't completely fixed.

SMPS partially working

Sometimes the SMPS is only partially working: it may start for a fraction of a second and than shut down, or it may pulsate trying to start every few seconds and shutting down after a fraction of a second, or it may produce a wrong output voltage. Here, probably all power semiconductors are good, so the first thing to check are the capacitors (see below).

Than, there may be something wrong with the feedback circuit: a good trick is to apply an external adjustable DC voltage to the SMPS output (the SMPS being not connected to the mains). When gradually increasing the DC voltage, you should see the feedback circuit working when you cross a threshold near the nominal output voltage. Since, while doing this test there are no dangerous voltages involved, you can easily use an oscilloscope to diagnose the feedback circuit. You may also have to supply the controller IC (on primary side) with the same low voltage source to see what happens on the other side of the optocoupler.

A SMPS being powered on its output by an external laboratory DC power supply to check the feedback circuit.

Capacitor check

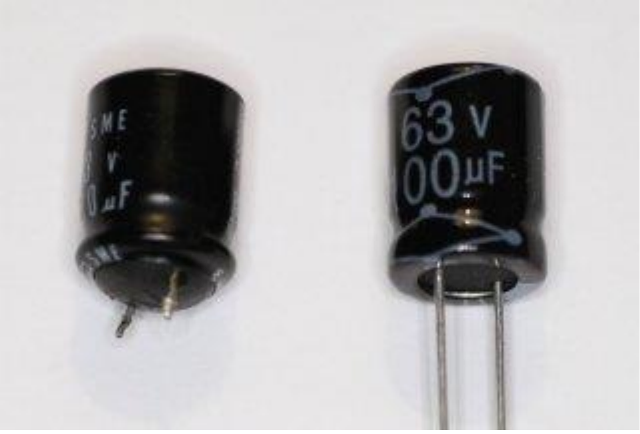
Electrolytic capacitors are very often the cause of SMPS problems. In cheap designs, where thermal dissipation is a bit too close to the limit, and a choice of components a bit too cost-oriented, electrolytic capacitors are real time-bombs that will eventually fail (sometimes by literally exploding)... The liquid electrolyte inside these components tends to evaporate and dry out completely altering the characteristics.

The two blue electrolytic capacitors in this picture are the low voltage filter capacitors. These ones are in good shape.

The big brown electrolytic capacitor in this picture is the high voltage filter capacitor. This one is in good shape.

When electrolytic capacitors explode, they throw out corrosive (and bad smelling) projections. The exploded components are easy to spot, but before going any further, one should check the status of the rest of the circuit: if it cannot be cleaned or is already too corroded, replacing the whole SMPS is the best option since corroded components or copper PCB tracks will eventually fail.

Fortunately, only very few electrolytic capacitors explode, the majority of them just fail silently. Look at all the capacitors, their shape and their neighbourhood. If they are not cylindrical anymore, are "inflated", have a dome-shaped top or bottom side (instead of being flat) or have leaked they're faulty. Don't bother measuring them: if it's visually bad it's 100% faulty and needs replacement.



Two electrolytic capacitors: the one on the left is "inflated" compared to a new one on the right. No need to measure: an inflated capacitor must be replaced.

But some electrolytic capacitors can be bad and still look decent. The only way of finding the faulty ones is by measuring them. Just measuring the capacitance may help, but it's not enough. It's much better to measure the equivalent series resistance

(ESR) and compare it with the one of a known good capacitor. The bad news is that you need an ESR meter (or an RLC bridge); the good news is that it works most of the times in the circuit without removing the capacitors (unless you have several in parallel).

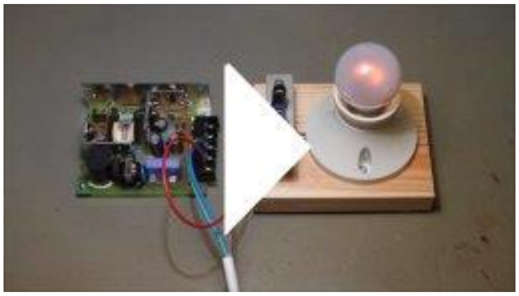
For replacement, use only new capacitors. Choose a good brand and keep in mind that good capacitors are expensive, but fixing a SMPS is hard enough and completely justifies the extra cost. Electrolytic capacitors exist in two flavours: 85 °C and 105 °C. I always choose the higher temperature because they last longer.

The light bulb trick

After replacing all the faulty parts, there is still a reasonable risk of blowing them again, especially if the fuse was initially blown. So, for the first test, I replace the fuse with a 100 W or so light bulb (or I put the bulb in series with the mains line). About the same bulb power of the SMPS is a good starting point, but it's not critical at all. This limits the power in case the short isn't fixed yet, prevents more catastrophic failures, and don't make me nervous in replacing fuses again and again. Wearing safety glasses is also a very good idea.

Put a light bulb in series with the AC mains line to prevent damage when first powering up a SMPS.

When you switch the power on (with no load) you'll see the bulb flash for a fraction of a second and than goes off (or glows slightly). If you still have a short circuit the bulb will glow bright and steady: just switch quickly the power off, discharge all the capacitors and start to look for the problem again.



Watch a movie showing this trick on a healthy SMPS: lightbulb-trick-video.mp4 (3,215,292 bytes, 4 s, H264, 854 x 480, 24 fps).

In the above video, in order to make the light bulb glow with this low power SMPS, a 15 W bulb has been used, since a 100 W one wasn't glowing at all. The bulb is initially off; the flash is due to the inrush current when switching the SMPS on (charging of the high voltage filter capacitor), than the brightness goes down showing little current. Of course, if you load the output the bulb will glow brighter.

Conclusion

Several ideas for fixing SMPS have been explained, not with the intent of being an exhaustive troubleshooting manual, but more as a collection of tricks that you may find useful. I tried to summarize the way I usually proceed and share some of my experience; other people may very well have a different approach. Since SMPS can fail in a lot of different ways, you may still not find the right hint in this page, but I truly hope you'll find here useful information and that your SMPS will be back in business soon.

CTM NOTES

1. Concept of servicing & maintenance

Maintenance is a partial or total renewal of an item. **Maintenance** reduces the physical age of an item or can even "zero time" the item by rejuvenating some or all of its components. By contrast, Nowlan and Heap describe "**service**" as "activities necessary for achieving the design life of the asset".

Service vs. maintenance

There is a noteworthy distinction between the activities of "maintenance" on one hand and "service" on the other. Maintenance is a partial or total renewal of an item. Maintenance reduces the physical age of an item or can even "zero time" the item by rejuvenating some or all of its components. By contrast, Nowlan and Heap describe "service" as "activities necessary for achieving the design life of the asset". Service is something that we have to do, operationally, if we wish to achieve the item's inherent reliability. Service should not, generally speaking, in RCM(realibility centered maintenance) or LRCM (living rcm), be the object of intense debate or scrutiny by reliability or maintenance engineers.

We note the difference between service and maintenance, primarily to address a frequent confusion of priorities for reliability engineering studies. Generally speaking, maintenance engineers should not spend significant energy second guessing the manufacturers' service recommendations. Those are usually a good starting point and can be taken at face value. Rather, reliability engineers should target their reliability studies towards the improvement of *maintenance* strategies. To this end, they should spend the bulk of their time in the following activities:

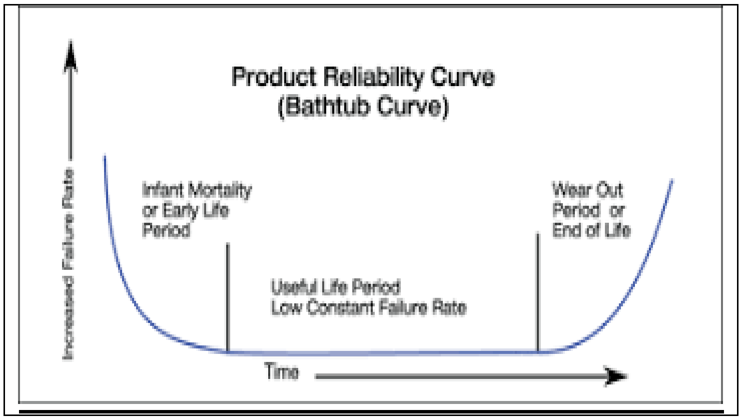
1. managing the RCM knowledge base,
2. managing the relationships (reference links) between the RCM knowledge base and the work order database,
3. generating samples for reliability analysis,
4. performing reliability analysis,
5. reporting the recommendations derived from their analyses,
6. monitoring the performance of all of the above (low level or "leading" KPIs), and
7. monitoring the results of implementing those recommendations (high level or "lagging" KPIs).

Service tasks often represent opportunities for effective CBM measurements. In this respect they justify scrutiny by the RCM analysts.

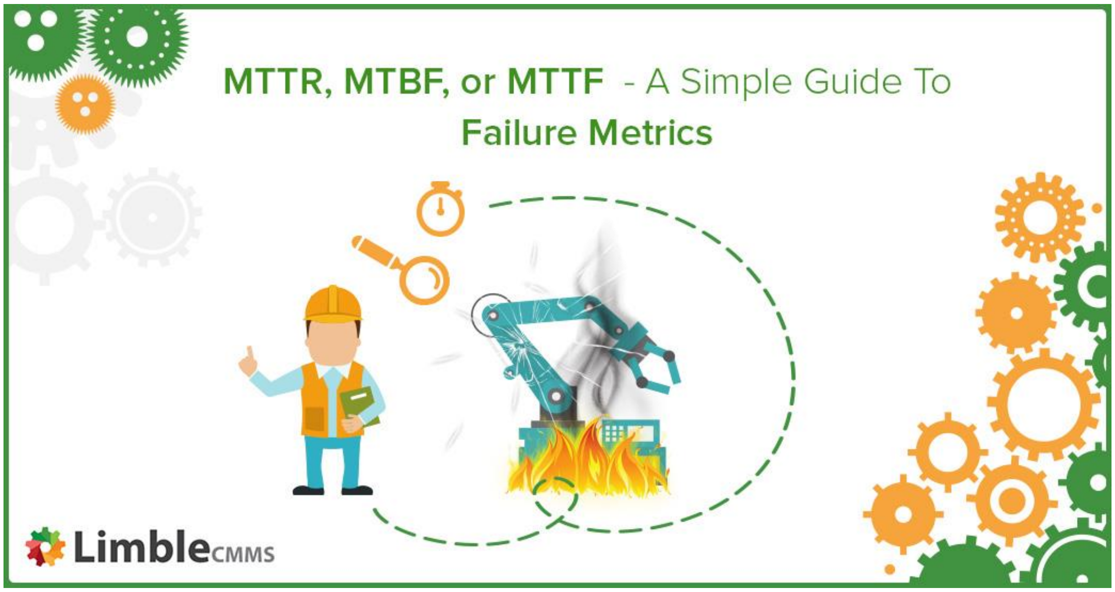
Reliability centred **maintenance** (**RCM**) is a corporate-level **maintenance** strategy that is implemented to optimize the **maintenance** program of a company or facility. The final result of an **RCM** program is the implementation of a specific **maintenance** strategy on each of the assets of the facility.

Featured snippet from the web

MTBF. Mean time between failures is calculated in hours and is a prediction of a power supply's **reliability**. **MTBF** = 1/λ (failure rate). ... **Reliability** is further defined as the probability that given a certain failure rate, that a certain number of units will pass (or fail) within a specified period.



MTTR, MTBF, or MTTF? – A Simple Guide To Failure Metrics



Asset performance metrics like MTTR, MTBF, and MTTF are essential for any organization with equipment-reliant operations. Only by tracking these critical KPIs can an enterprise maximize uptime and keep disruptions to a minimum.

Tracking the reliability of assets is one challenge that engineering and maintenance managers face daily. While failure metrics can be very useful in this context, to use them effectively, you need to know what meaning hides behind their acronyms, how to distinguish between them, how to calculate them, and what does that tell you about your assets.

That's why we decided to create a simple to follow guide to failure metrics that will help you avoid costly mistakes and successfully monitor equipment performance.

Introduction to Failure Metrics

Even the most efficient maintenance teams experience equipment failures. That's why it's critical to plan for them.

But first, what does equipment failure look like?

Failure exists in varying degrees (e.g. **partial or total failure**) but in the most basic terms, failure simply means that a system, component, or device can no longer produce specific desired results. Even if a piece of manufacturing equipment is still running and producing items, it has failed if it doesn’t deliver the expected quantities.

Managing failure correctly can help you to significantly reduce its negative impact. To help you effectively manage failures, several critical metrics should be monitored. Understanding these metrics will eliminate guesswork and empower maintenance managers with the hard data they need to make informed decisions.

Which failure metrics should be tracked? Across industries and applications, we’ve found that those are **MTTR, MTBF, and MTTF**. We’ll discuss what each of those acronyms means and how you can use them to improve your operations.

But before that, we need to discuss one thing that is often overlooked – the importance of having **reliable** data behind your failure metrics.

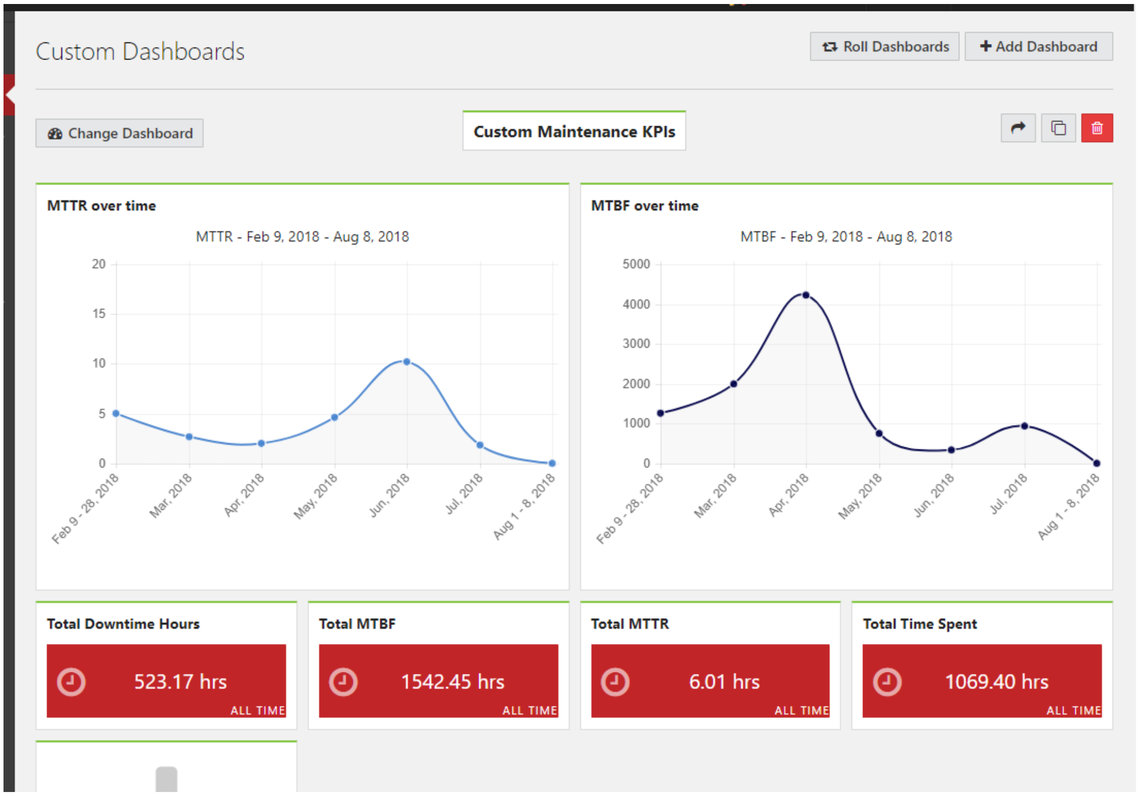
The Importance of Reliable Data

To make data-backed improvements in equipment failure, it’s crucial for the right data to be collected and for that data to be accurate.

High-level failure statistics require a significant amount of meaningful data. As we’ll show in the failure metrics calculations below, the following inputs must be collected as part of your maintenance history:

- **Labor hours spent on maintenance**
- **Number of breakdowns**
- **Operational time** (can be calculated from total expected operating hours per week – total equipment downtime)

As tedious as recording maintenance figures can be, it’s an essential part of improving operations. This process can be painfully time-consuming when done manually, but it’s made simple with a mobile CMMS like Limble that lets you quickly and easily log reliable data for labor hours and downtime on your phone while you’re performing maintenance tasks. Additionally, Limble runs all the calculations of MTTR and MTBF automatically for you, as seen below.



Total Downtime Hours: 523.17 hrs ALL TIME

Total MTBF: 1542.45 hrs ALL TIME

Total MTTR: 6.01 hrs ALL TIME

Total Time Spent: 1069.40 hrs ALL TIME

Collecting inaccurate data can cause a lot of issues. Maintenance technicians might occasionally write down the wrong figure is just one example. A potentially much bigger problem is neglecting to record tasks, which leads to incomplete data.

If data is missing or inaccurate, your failure metrics will be useless in informing decisions on improving operations. Worse still, if you are unaware that the data is unreliable, you might end up making operational decisions that could be counterproductive and harmful.

Did you know that MTTR can mean both “Mean Time To Repair” and “Mean Time To Recovery”?

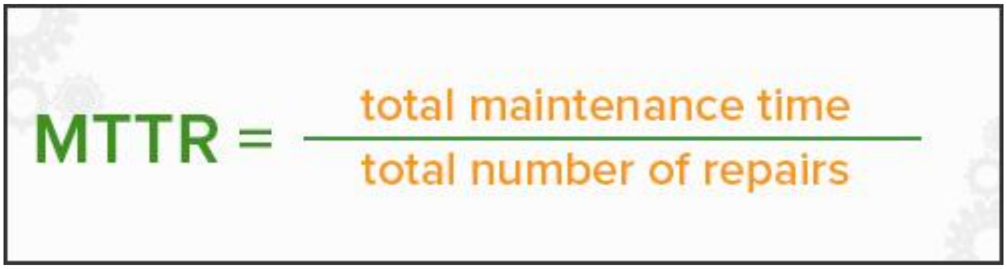
What is Mean Time To Repair (MTTR)?

Mean Time To Repair (MTTR) refers to the amount of time required to repair a system and restore it to full functionality.

The MTTR clock starts ticking when the repairs start and it goes on until operations are restored. This includes **repair time, testing period, and return to the normal operating condition**.

How do you calculate MTTR?

To calculate MTTR, divide the **total maintenance time** by the **total number of maintenance actions over a given period of time**.



$$\text{MTTR} = \frac{\text{total maintenance time}}{\text{total number of repairs}}$$

Imagine a pump that fails three times throughout a workday. The time spent repairing each of those breakdowns totals one hour. In that case, MTTR would be 1 hour / 3 = 20 minutes.

A couple of things to note:

- Typically, every instance of failure will vary in severity. So while some incidents will require days to repair, others could take mere minutes to fix. Hence, MTTR gives an average of what to expect.
- To obtain reliable results, every repair must be handled by competent and trained personnel that can follow well-defined procedures.

Every efficient maintenance system always needs to look at how to reduce MTTR as much as possible. That can be done in a few different ways.

One approach is through tracking spare parts and inventory levels (thereby saving on downtime while sourcing for parts).

Another way is to implement proactive maintenance strategies like predictive maintenance. Predictive maintenance (PdM) will, among other things, allow you to better monitor the condition of in-service equipment and predict potential failure more accurately by using condition-monitoring sensors mounted directly on those components that are prone to failure.

These sensors can alert them well in advance when to expect failure. At this point, the repair is no longer reactive but predictive, as the manager has enough time to arrange for all the resources needed to execute the job.

Why is MTTR helpful?

Taking too long to repair a system or equipment is not desirable as it can have a highly unpleasant impact on business results. This is especially the case for processes that are particularly sensitive to failure. It often results in production downtime, missed deadlines, loss of revenue, and so on.

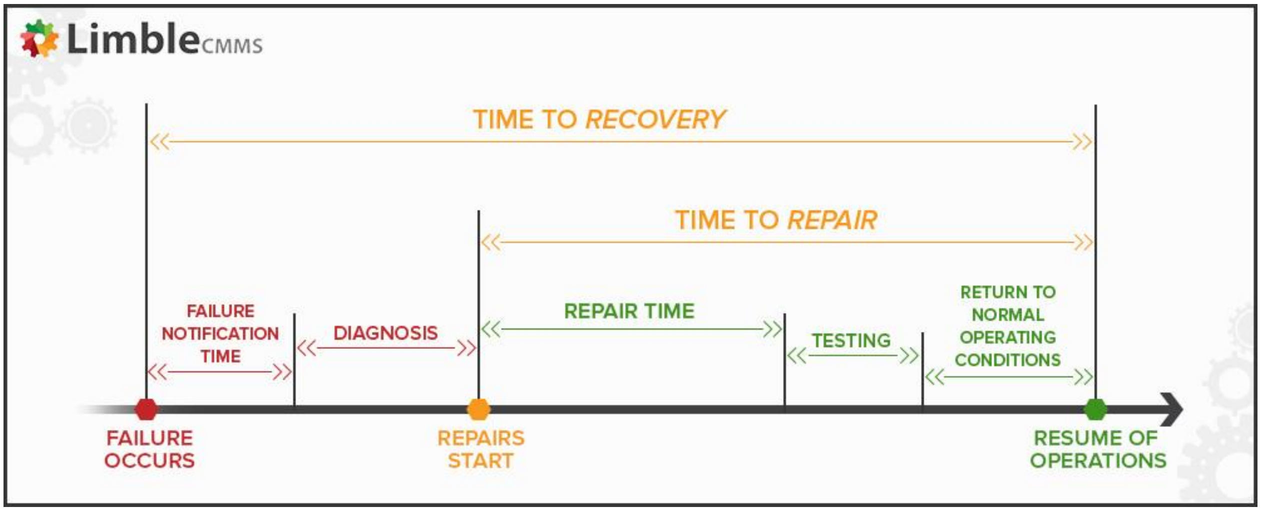
Understanding MTTR is an important tool for any organization because it tells you how efficiently you can respond to and repair any issues with your assets. Most organizations seek to decrease MTTR with an in-house maintenance team supported with the necessary resources, tools, spare parts, and CMMS software.

Maintenance managers can use MTTR to inform maintenance decisions such as:

- when to repair or replace assets
- quantity of parts and inventory to have on hand
- whether to lease or buy equipment

Mean Time To Repair vs Mean Time To Recovery

There are several commonly used terms for the acronym "MTTR." The two most common are "mean time to repair" (discussed above) and "mean time to recovery."



Mean Time To Recovery is a measure of the time between the point at which the failure is first discovered until the point at which the equipment returns to operation. So, in addition to repair time, testing period, and return to normal operating condition, it captures **failure notification time and diagnosis**.

Although both terms are often used interchangeably, the need for distinction becomes important in the context of Service Level Agreements (SLAs) and maintenance contracts.

Hence, all parties to such contracts will need to agree on what exactly are they measuring.

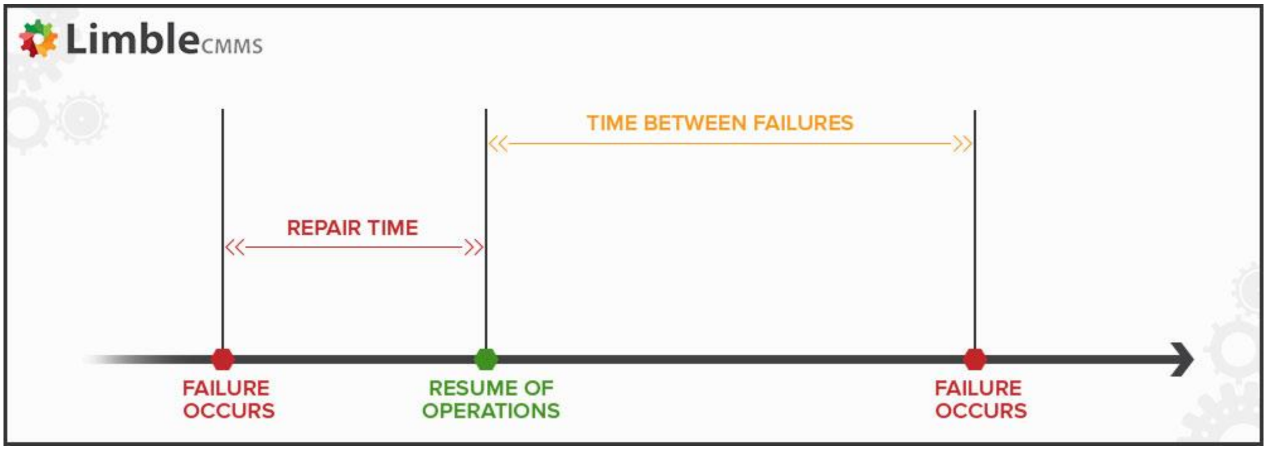
What is Mean Time Between Failures (MTBF)?

The second failure metric we'll cover is Mean Time Between Failures. MTBF measures the predicted time that passes between one previous failure of a mechanical/electrical system to the next failure during normal operation. In simpler terms, MTBF helps you predict how long an asset can run before the next unplanned breakdown happens.

The expectation that failure will occur at some point is an essential part of MTBF.

The term MTBF is **used for repairable systems**, but it **does not take into account units that are shut down for routine scheduled maintenance** (re-calibration, servicing, lubrication) or routine preventive parts replacement. Rather, it captures failures that occur due to design conditions that make it necessary to take the unit out of operation before it can be repaired.

So, while **MTTR measures availability, MTBF measures availability and reliability**. The higher the figure of the MTBF, the longer the system will likely run before failing.



How do you calculate MTBF?

Expressed mathematically, the lapses of time from one failure to the next can be calculated using the **sum of operational time** divided by the **number of failures**.

$$\text{MTBF} = \frac{\text{total operational time}}{\text{total number of failures}}$$

Looking at the example of the pump we mentioned under MTTR, out of the expected runtime of ten hours, it ran for nine hours and failed for one hour spread over three occasions. So, MTBF = 9 hours / 3 = 3 hours.

As you can see from the example above, **the repair time is not included in the calculation of MTBF**.

Apart from the design conditions mentioned earlier, other common factors tend to influence the MTBF of systems in the field.

A major one of these factors is human interaction. For instance, low MTBF could either indicate poor handling of the asset by its operators or a poorly-executed repair job in the past.

Why is MTBF helpful?

MTBF is an important marker in reliability engineering and has its roots in the aviation industry, where airplane failure can result in fatalities.

For critical assets such as airplanes, safety equipment, and generators, MTBF is an important indicator of expected performance. Therefore, manufacturers use it as a quantifiable reliability metric and as an essential tool during the design and production stages of many products. It is commonly used today in mechanical and electronic systems design, safe plant operations, product procurement, and so on.

Even everyday decisions like buying a particular brand of car or computer are affected by the buyer’s desire for a product with a higher MTBF than what the next brand has to offer.

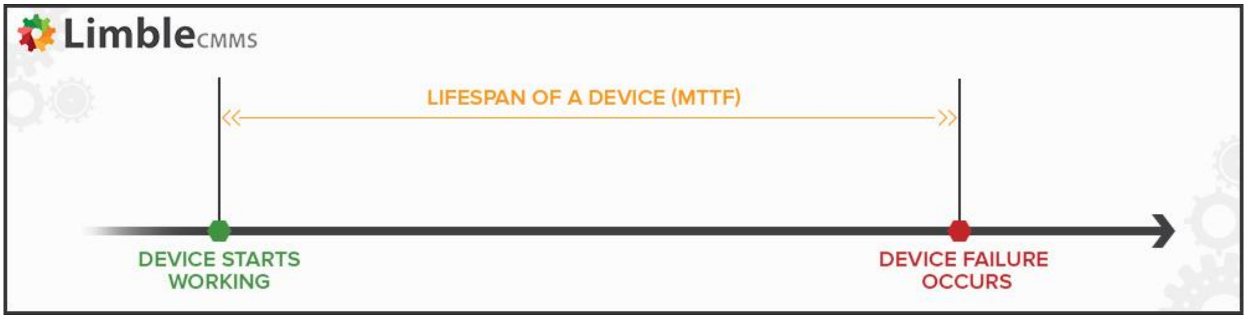
Although MTBF does not consider planned maintenance, it can still be applied for things like **calculating the frequency of inspections for preventive replacements**.

If it is known that an asset will likely run for a certain number of hours before the next failure, introducing preventive actions like lubrication or recalibration can help keep that failure to the minimum and extend the uptime of the asset.

What is Mean Time To Failure (MTTF)?

Mean Time To Failure (MTTF) is a very basic measure of reliability **used for non-repairable systems**. It represents the length of time that an item is expected to last in operation until it fails.

MTTF is what we commonly refer to as the lifetime of any product or a device. Its value is calculated by looking at a large number of the same kind of items over an extended period and seeing what is their mean time to failure.



In the manufacturing industry, MTTF is one of the many metrics commonly used to evaluate the reliability of manufactured products. However, there is still a lot of confusion in differentiating between MTTF and MTBF because they are both somewhat similar in definition. The good news is that this is easily resolved by remembering that while **MTBF is used only when referring to repairable items, MTTF is used to refer to non-repairable items**.

When using MTTF as a failure metric, repair of the asset is not an option.

How do you calculate MTTF?

MTTF is calculated as the total hours of operation, divided by the total number of items being tracked.

$$\text{MTTF} = \frac{\text{total hours of operation}}{\text{total number of units}}$$

Let’s assume we tested three identical pumps until all of them failed. The first pump system failed after eight hours, the second one failed at ten hours, and the third failed at twelve hours. MTTF in this instance would be (8 + 10 + 12) / 3 = 10 hours.

This would lead us to the conclusion that this particular type and model of the pump will need to be replaced, on average, every 10 hours.

The only surefire way to increase MTTF is to look for higher-quality items made from more durable materials.

Why is MTTF helpful?

MTTF is an important **metric used to estimate the lifespan of products that are not repairable**. Common examples of these products range from items like fan belts in automobiles to light bulbs in our homes and offices.

In particular, MTTF is important to reliability engineers when they need to estimate how long a component would last as part of a larger piece of equipment. This is especially true where the entire business process is sensitive to the failure of the equipment in question.

In such cases, MTTF becomes the primary indicator of the equipment’s reliability, intending to maximize asset lifetime. Shorter MTTF means more frequent downtime and disruptions.

Reduced Reactive Maintenance by 73.2%

Final thoughts

One of the top priorities of maintenance managers is to ensure maximum operational availability of their equipment, as well as keeping equipment operations safe and efficient.
Understanding the calculations and use of failure metrics will enable maintenance professionals to determine, with greater accuracy, when a critical asset is most likely to fail.

Based on their findings, they can proceed to develop better asset management strategies and improve their overall maintenance processes.

By calculating failure metrics and planning maintenance based on those results, they can also **reduce their organization's dependence on reactive maintenance** in favor of planned (predictive) maintenance, which can be just the thing they need to spark their business's growth.

If you are one of the many managers and technicians that are looking to improve these metrics by implementing a CMMS into their organization, you can **start a free trial of Limble CMMS here** or **contact us** for more information.

Preventive maintenance refers to regular, routine maintenance to help keep equipment up and running, preventing any unplanned downtime and expensive costs from unanticipated equipment failure. It requires careful planning and scheduling of maintenance on equipment before there is an actual problem as well as keeping accurate records of past inspections and servicing reports. Preventive management can be very complex, especially for companies with a lot of equipment. For this reason, many companies rely on preventive maintenance software to help organize and carry out all their preventive maintenance needs.

What Does Preventive Maintenance Include?

Preventive maintenance involves the systematic inspection of equipment where potential problems are detected and corrected in order to prevent equipment failure before it happens.

In practice, a preventive maintenance schedule may include things such as cleaning, lubrication, oil changes, adjustments, repairs, inspecting and replacing parts, and partial or complete overhauls that are regularly scheduled.

The exact preventive maintenance required will vary based on operation and type of equipment. Recommended standards of the American National Standards Institute (ANSI) are used to help determine the type of inspections and maintenance needed and how often they should be performed. ANSI helps ensure the health and safety of consumers by creating and overseeing the use of thousands of guidelines and norms for nearly every industry, and ANSI standards can be used like a preventive maintenance checklist to define requirements and instructions for maintaining equipment.

Preventive maintenance includes much more than simply performing routine maintenance on equipment. It also involves maintaining accurate records of every inspection and servicing, as well as knowing the lifespan of each part to understand the replacement frequency. These records can help maintenance technicians anticipate the appropriate time to change parts and can also help diagnose problems when they occur. Preventive maintenance software helps collect and organize this information so it is readily available to maintenance technicians.

What Are the Benefits of Preventive Maintenance?

Preventive maintenance offers companies a number of important benefits including

- Prolonged life of company equipment
- Less unplanned downtime caused by equipment failure
- Less unnecessary maintenance and inspections
- Fewer errors in day-to-day operations
- Improved reliability of equipment
- Fewer expensive repairs caused by unexpected equipment failure that must be fixed quickly
- Reduced risk of injury

Ideally, a preventive maintenance schedule will prevent all equipment failure before it occurs. It will save time, reduce costs, and keep an operation running efficiently and productively.

How Can Preventive Maintenance Software Help?

Many companies choose preventive maintenance software to coordinate all their preventive maintenance tasks because it simplifies what is otherwise a complex process. Preventive maintenance software stores a company's maintenance data on a computer (or in the cloud) to easily keep track of all inspections, repairs and replacements. With all data conveniently stored in one place, preventive maintenance software can be used to effectively manage work orders, purchase orders, inventory and maintenance records. Preventive maintenance software even prioritizes maintenance tasks and gathers information a technician needs to perform maintenance work.

Preventive maintenance software offers a number of key benefits. It helps manage all maintenance tasks (and the records of those tasks) so maintenance operations will run smoothly. It can also save on maintenance costs because the system can plan and prioritize maintenance tasks based on operations, therefore minimizing the disruption to the work schedule when maintenance is performed. Finally, preventive maintenance software takes the burden of administrative duties off technicians' shoulders so they can better focus on their job.

Preventive maintenance is designed to keep equipment running and operations productive. By staying on top of maintenance tasks, maintenance professionals can prevent unplanned downtime that in turn saves a company time and money. The coordination of a preventive maintenance schedule can be very complex, but the use of preventive maintenance software simplifies the process, making preventive maintenance attainable for any business wanting to improve their overall maintenance operations.

CMMS stands for Computerized Maintenance Management System and is software designed to simplify and improve maintenance operations for a business.

Factors affecting computer performance

You may be wondering why you computer is slow at times and there are other times when it is fast in processing. This could be caused by a number of factors. They include: the speed of the CPU, the space on the hard disk, the size of the RAM, the type of the graphics card, the speed of the hard disk,, if the computer is multitasking, the defragmenting files.

1) The speed of the CPU
The speed of the CPU is also known as the clock speed of the CPU. The clock speed of the CPU is the frequency of which the processor executes instructions or the frequency by which data is processed by the CPU. It is measured in millions of cycles per second or megahertz (MHz). If the Clock speed of the CPU is fast then definitely the performance of the computer will be affected positively, in other words the computer will carry out processing functions at a faster

pace.

2) The size of the RAM (Random Access Memory)
The RAM is referred to as the active part of the computer. This is because the RAM has the capability of storing data that the computer is currently using, because of the fact that it is fast to retrieve data stored in the RAM. With the definition above, a large RAM size will mean a faster computer performance and a smaller RAM size will result to slower computer performance.

3) The speed of the hard disk
The hard disk speed is defined as the rate at which material and content can be read and written on it. The hard disk speed of different hard disks is not consistent because they vary by manufacturer, drive type and the use of the hard disk. It therefore means that the higher the speed of the hard disk the
faster the performance of the computer and vice versa.

4) Hard disk space
The bigger the space on the hard disk will result to faster performance of the computer. The smaller the space on the hard disk will result in a slower performance of the computer. The hard disk is filled with data this will use most of the memory leaving less memory for the operations of the processor.

5) Multiple applications running on the computer
Multi-tasking tends to slow down the performance of the computer because memory is used to support more than one applications compared to when one application has all the memory to itself. This means that the more applications that are running the slower the computer will perform. Likewise if less or one application is running the performance of the computer will be faster.

6) Type of graphic card
When it comes to quality of pictures and animations graphic cards are the main factors. So if a machine processes many graphics and it has a weak graphic card it will perform slower. This means that the more powerful the graphic card is the faster the performance of the computer.

7) Defragmenting files
Files that are broken or it takes long to read them will mean that the computer will have to defragment them first. This will slow down the performance of the computer.

There may be several reasons behind poor performance of a pc below i am listing some of them

1. Virus,worms,trojans infections
2. Lack of free disk space
3. Insufficient memory
4. many Unnecessary programs installed
5. Errors on harddisk
6. Operating system curruption
7. improper device drivers installed

8. Same frequency ram not installed if multiple rams are installed
9. Processor is heating - no proper ventillation/Dust accumulated near cpu fan
10. Harddisk is heavily fragmented

It depends a lot on what type of computer that you are starting with but these would be my recommendations:

- If your computer still has a spinning hard disk as the boot drive replace it with an SSD, any SSD. Spinning hard disks are no match for solid state storage that has far lower latency and far higher write speeds.
- If you have less than 8 GB of RAM (or especially less than 4 GB of RAM) upgrade that right away. On many newer laptops the RAM is soldered to the motherboard so there may not be much you can do in this area
- If you have an underpowered processor get a faster one. Like with RAM this may be difficult to upgrade on a laptop
- Remove any background processes that you aren’t finding useful. Open Task Manager (on a PC) or Activity Monitor (on a Mac) and take a look at any programs that might be using a lot of resources and research them before ending the process

There are many factors that affect your performance:

1. Amount of programs running: Running many programs at the same time can affect the performance of your computer. It takes up storage and RAM, which will slow your device down.
2. Age of the computer: The older your computer is, the more worn out its battery and its processing power gets.
3. Battery: The more battery your computer has, the more likely it is to prioritize performance over battery life. Some computers have a setting to switch this.
4. Processor: This one is obvious. If you have a good processor and CPU, then your computer is going to be able to perform better than one with a worse drive.

There may be much more smaller factors, but these are the main reasons that performance is affected.

What does a Preventive Maintenance Program Requires?

An effective preventive maintenance program requires careful planning and scheduling of maintenance on an asset before an actual breakdown. Also, it requires tracking data related to past inspections and maintenance. But it's always worth the investment. A good program delivers:

- Reduced Costs
- Reduced probability of failure
- Increased productivity

"Preventive maintenance (PM) is a routine for periodical inspections, with the goal of noticing small problems, and fixing them before major ones develop. Ideally, nothing breaks down."

It can be a bit confusing, because in other circles, PM is also used to mean project management. And to make it even tricker, a PM is used to mean a task that's a part of a preventive maintenance program.

So, someone might say, "I have five PMs scheduled for this week." The good news is not matter what you call it, you still get all the benefits.

What are the steps to setting up the perfect preventive maintenance program?

A large part of keeping a company running efficiently and profitably is ensuring that all equipment is functioning optimally.

To do so, routine preventive maintenance needs to be conducted. Unfortunately, regular equipment checks often go overlooked in certain areas of a company's operations mainly because attention is usually directed toward more pressing issues.

However, when small tasks go overlooked for long periods of time, problems often follow; production errors, work injuries, and asset damage can all occur if careful tracking and maintenance aren't followed.

A breakdown in critical equipment is costly both regarding repairs as well as downtime and delays in a company's productivity.

The problems outlined can be avoided with a computerized maintenance management software (CMMS) system that offers preventative maintenance as one of its key functions.

With CMMS software in place, companies can get a birds-eye-view of all their facilities and locations to ensure that effective preventative maintenance schedule is a part of all standard operating procedures.

Preventive maintenance software provides tools such as automatic triggers, email integration, set reminders, equipment information, and auto-assigned task which can streamline a company's entire maintenance process.

Here are the steps in creating an effective preventative maintenance plan:

1. Create a preventive maintenance plan

Before any preventive maintenance (PM) procedures are put in place, it is important first to establish who will be involved in the preventative maintenance project.

Depending on the company size, likely choices may include maintenance managers, maintenance techs and/or people from accounting or finance departments.

Additionally, it is critical that staff members are fully invested in developing the program so that the PM maintenance implementation can be successful.

A final aspect of creating a preventative maintenance plan is determining a goal for the project.

Examples of PM maintenance project goals are: reducing reactive or corrective maintenance costs by X% or decreasing equipment downtime by X%.

2. Inventory facility equipment/assets

The most time-consuming aspect of setting up a preventive maintenance program involves going through a facility and creating an inventory of all relevant equipment.

Although a time consuming exercise, it is a critical one as it ensures that preventive checks are routinely be made on key operational equipment.

As part of this task, it is important to take note of equipment make/model, serial numbers, specifications, asset identification numbers and fixed locations.

Finally, documenting the current condition of the equipment can help prioritize its importance as part of a preventive maintenance program.

EAM software offers ways for users to digitally track the location of assets that have been physically tagged.

It also stores asset information and inventory data, and can alert managers when spare parts stock is low.

3. Create preventive maintenance procedures

Once a list of equipment has been made, the next step is to determine the tasks or jobs required to maintain each piece of equipment as well as the frequency with which these tasks should occur (i.e., weekly, monthly, quarterly, semi-annually, annually).

There may be times when preventive maintenance is best suited to be scheduled around run-time hours while for other assets, other meter based triggers are more appropriate.

Whichever is the case, it is important to make note of these different scheduling scenarios while also estimating how much time may be needed to perform the PM with work order software.

Most preventive maintenance programs accommodate schedules based on run-time hours, but having prior knowledge of how often these may occur will assist in a company’s scheduling process.

Preventive maintenance procedures can be determined based on prior corrective maintenance experiences or by referencing owner’s manuals and manufacturer recommendations and documented industry standards.

An important part of creating preventive maintenance checklist is making a list of tools and internal and external resources needed to complete each job. In summary, a preventive maintenance plan should include the following: a parts list, standard operating procedures (SOPs), safety/lockout procedures and estimated time to complete the PM tasks.

4. Create preventive maintenance schedules

Preventative maintenance scheduling is critical to company operations since these occur regularly and involve time, energy and staff resources to complete.

In creating a preventive maintenance schedule, it is important to make a list of high priority items; these will be the starting points.

Preventative maintenance programs take time to be created and it is best to schedule the highest priority maintenance before overloading staff with tasks that rank lower on priority.

The initial preventive maintenance goals established will direct which assets should be prioritized.

For example, it is important to identify which equipment is most costly to a company regarding repairs, downtime and value to operations.

Once high priority items have been identified, it is recommended to begin by scheduling preventive maintenance tasks with longer intervals first (i.e. annual, semi-annual, quarterly).

Equipment requiring preventive maintenance on longer intervals generally require the most time and resources, and because of this, scheduling may be best during specific times during the year (i.e., plant shutdown, at the beginning of heating/cooling season.)

Once high priority long term preventive maintenance is completed, scheduling tasks with shorter intervals and more frequent cycles (i.e., weekly, monthly, etc.) and low priority items should follow.

Since these preventive maintenance tasks generally require less time, they can also easily fill the gaps between the long term and high priority preventive maintenance.

It is important to realistically plan preventative maintenance schedules by striking a balance between preventative maintenance and the time needed to address corrective or emergency maintenance as well as other projects that will likely surface.

Setting up a preventive maintenance schedule

Setting up a customized preventive maintenance schedule is aimed at achieving the above outcomes. Here are five tips to make this happen:

a. Get a Handle on Your Assets

Since company assets are unique and vary by industry and sector, size of the organization and production activities, there is no “cookie cutter” method to developing an inventory list for the purpose of developing a preventive maintenance schedule.

At the outset, determinations need to be made about which assets require routine checks and which do not.

In general, company assets that will benefit most from a preventive maintenance schedule are those that have a critical operational function, failure modes that can be prevented with routine maintenance and a likelihood of failure that increases with time or use.

Assets less amenable to preventive maintenance scheduling may be better handled using spreadsheet systems.

b. Use Architectural Drawings to Locate Assets

An architectural drawing is a rendering of an architectural design as plan and/or elevation views of a building or structure.

Many CMMS software systems have the capability of integrating architectural drawings with preventive maintenance programs. Using these drawings make it possible to view supply levels visually rather than in a spreadsheet format alone.

Most important, exact locations of equipment can be highlighted on the drawings.

Knowing the locations of critical equipment in need of preventive maintenance system can facilitate efficient preventive maintenance scheduling because technicians can be deployed to service several pieces within close proximity in a shorter time frame as opposed to the time required to service items spread throughout a facility.

This approach results in better time and resource utilization management.

c. Gather Operating and Maintenance Manuals and Serial Codes

An important aspect of establishing maintenance schedules is becoming familiar with equipment O&M manuals which among other things, set out recommended maintenance schedules and procedures as well as troubleshooting information.
Serial codes are important to ensure that when replacement parts are needed, the correct ones are ordered.
An efficient preventive maintenance will benefit from technicians who are knowledgeable about the assets they are servicing as well as having the appropriate parts on hand, when needed.

d. Review Equipment Repair Histories

Apart from setting preventive maintenance schedule based on O&M manual recommendations alone, gaining additional information about asset use and repair histories can be helpful.
Since no two operations are identical, O&M manual recommendations are just that – recommendations. They do not replace a thorough review of repair and inspection histories.
This added information is beneficial in fine tuning preventive maintenance schedules to reflect the actual usage and performance of a particular piece of equipment.
Equally important, a review of the repair histories will provide valuable information about prior downtime and serve as a baseline upon which improvements can be targeted.

5. Train your maintenance team

While developing a preventive maintenance program takes time, proper CMMS implementation and adoption of the program is crucial.

It is essential that companies prioritize the training of its maintenance staff as they are the core users of the system.

Having staff members trained to use a program is a key determinant of successful outcomes. Do not scale back on training. Having staff that buy in to the software, adopt it and use it will ensure the highest ROI.

6. Analyze – adjust - improve

Businesses are dynamic and so are its equipment assets. Because of this, it is important always to analyze the results of a preventative maintenance program and adjust or improve it as needed.

Preventive maintenance programs help companies identify equipment that require more time and money than others, leading to adjustments in the preventive maintenance procedure/schedule.

Companies often seek the assistance of consultants or CMMS implementation experts to assess and adjust preventive maintenance programs.

It's not a bad idea to assess and adjust your PM plan every couple of years.

Without a doubt, developing and implementing a preventative maintenance program takes time and energy.

However, once in place with staff trained to use it, the benefits of automated preventive maintenance far outweigh the costs associated with reactive or emergency maintenance that often results in unforeseen downtime, equipment replacement, and operation disruption.

Having facility management software in place that monitors company assets makes it possible for flexible maintenance scheduling saving time, money and energy.

How do I know if my preventive maintenance program is working?

It is essential to ensure that all plant and facility equipment is covered by a cost-effective overall preventive maintenance program. An effective preventive maintenance program will reduce the amount of unplanned work to less than 80% of the total man-power expanded for all equipment maintenance activities.

But it's not enough to just have a plan. The effectiveness of a maintenance program depends on execution of the plan.

What are the key performance indicators for preventive maintenance?

- **Productivity**
  More specifically, this refers to emergency man-hours. An effective Preventive Maintenance

Schedule should see a significant drop (almost negligible) in emergency hours put and therefore an increase in overall productivity.

- **Equipment downtime**
  The total breakdown downtime for an equipment, a plant or even an entire facility indicates the level of effectiveness of a PM program.
- **Equipment costs**
  The cost of repairs includes the cost of labor, materials, extra labor hours as well as any direct or indirect maintenance cost. This plays a major role in indicating improvements after implementing a PM program.
- **Preventive maintenance efficiency**
  This would go over the amount of work orders generated from a preventive maintenance program. These should see a rise when a preventive maintenance program is installed since it would highlight whether the developing equipment problems are being identified more proactively.

What are the benefits you should be looking for with your preventive maintenance program?

If you know the benefits, one way to check your program is by working backward. If you see these benefits, you know the program is working. Preventive maintenance should deliver:

- Reduced unplanned downtime due to asset failure.
- Better margins and profits due to less downtime
- Prolonged life of the assets and less unnecessary maintenance and inspections
- Less injury risk and increased safety
- Fewer interruptions to vital operations as timely, routine repairs ensures fewer large-scale repair

Increased safety also ensures that organizations are in compliance with the rigorous OSHA standards.

An effective preventive maintenance program, if implemented properly, will help with a boost in profit margins as assets last longer, use less time and energy for repairs, and are responsible for fewer interruption to your processes.

If you don't see these benefits, it's time to start rechecking your program. One problem area could be the types of PMs you're performing.

What are the types of preventive maintenance tasks?

PM tasks vary upon the need of the users. The three main types include:

- Mandatory or Non-Mandatory
- Pyramiding or Non-Pyramiding
- Inspections or Task Oriented:

Mandatory PMs are ones that must be performed at all costs when they are due. They may involve OSHA, safety, EPA, and license inspections, among others.

Non-mandatory PMs are inspections or service PMs that can be postponed for a short time period or even eliminated for the present cycle without resulting in immediate failure or performance penalty.

Each PM task should be designated in one of these categories.

Pyramiding PMs are generated each time they come due. When there is already a PM due and the next one comes due, the first one should be canceled, with a note written in the equipment history that the PM was skipped.

The new PM should have a due date from the canceled PM written in, so that it is understood how overdue the task is.

Some companies, however, choose to make their PMs floating or non-pyramiding. They follow the same scenario as described above, except there is no notification that the PM was missed.

The previously uncompleted PM is thrown away and the new one (without any carry over information) is issued and placed on the schedule.

Inspections will involve only filling out a check sheet and then writing work orders to cover any problems discovered during the inspection.

Task-oriented PMs allow the individual performing the PM to take time to make minor repairs or adjustments, eliminating the need to write some of the work orders when turning in the inspection sheet.

Preventive maintenance programs

Preventive maintenance system streamlines every aspect of preventive maintenance programs, including development, scheduling, and tracking.

By helping maintenance departments find small issues before they grow into large problems, the software cuts costly downtime, increases profits.

Why should you use preventive maintenance system? Because without it, you're only ever reacting to problems, never getting out ahead of them.

Without a structured PM program, you're stuck relying on run-to-failure and on-demand work orders. Scheduling resources and controlling inventory are challenging when you can never plan beyond the next surprise breakdown.

As critical facility and production equipment gets overlooked, downtime and repair costs rise.

Preventive maintenance system, a core module of EAM software, helps you develop, schedule, and track a PM program that cuts downtime and boosts asset and equipment life cycles.

Data-packed preventive maintenance work orders include everything technicians needs to close out efficiently, including customizable step-by-step instructions, associated parts and materials, digital copies of O&M manuals, images, and schematics.

Preventive Maintenance Subsystem - Planning Ahead to Avoid Costly Problems

With the Finesse preventive Maintenance subsystem, you can schedule maintenance and repair for all plant equipment while recording all associated costs. And you can be confident that you have complete control over these critical functions.

Maintain Order
Preventive Maintenance is all about staying on top of things. Make a plan. The subsystem lets you establish your service budget and cover all the bases...personnel, equipment and materials.

Schedule It
The same flexibility we built into our other Finesse modules shows here with the ability to schedule maintenance and repair services by project, company, department, plant, warehouse, work center, equipment groups or other categories you define. And because Shop Floor is fully integrated with Projects, Master Scheduling and CRP, you'll know ahead of time when a workcenter will be down for maintenance or repair and can plan and schedule work accordingly.

Track It All
The subsystem automatically records the resources you actually use. Maintenance control has never been easier.

Module Highlights

GENERAL FEATURES

- Multi-company, plant and warehouse capabilities
- Multi-project capability
- User-defined fields, screens and reports
- Handle multiple shifts

ANALYSIS

- Analyze defects
- Actual begin and end date and time
- Quantity and percent variances
- Actual materials and labor

REPORTING

- Billing, unbilled and cost status reports
- Labor, expense and machine cost and billing reports
- Machine activity reports
- Maintenance due reports by procedure and machine

SCHEDULING

- Schedule equipment and/or equipment groups
- Schedule by hour, days and units lapsed
- Schedule personnel, materials, work centers and operations
- Schedule set-up time and downtime

STATUS AND TRACKING

- Track serial number, purchase date and warranty status
- Machine characteristics
- Record comments
- Last and/or next service date

The word auxiliary can be used to describe any optional component, such as a subsystem. Windows 10 supports the “Windows Subsystem for Linux (WSL)”, which is an optional Windows feature allowing for the direct execution of many native Linux binaries. WSL does **not** aim to support GUI desktops or applications (e.g. Gnome, KDE, etc.) Also, even though you will be able to run many popular server applications (e.g. Redis), Microsoft does not recommend WSL for server scenarios.

Preventive maintenance for this subsystem is done in two parts.

1. Perform typical Microsoft Windows maintenance and patches; these will include patches to WSL itself.
2. To maintain Linux packages which you may install using the WSL subsystem, you will typically execute a bash command such as “apt-get upgrade”, to ensure that these packages receive security upgrades.

An auxiliary emergency system is an equipment that provides support to meet the energy needs of a given location or infrastructure, can function as a primary or complementary source.

Auxiliary emergency system presupposes design, development, and installation tailored to the needs and conditions of the infrastructures which will assist. To achieve this, the assembly teams must use all their experience to implement a reliable solution corresponding to the demanding levels of the final application.

When faced with types of large installations and high need for energy supply, it is essential to ensure that the network outage or failure rate is very low. This is because all the components involved in emergency energy support are the main pillar, that is, the most critical part of the entire installation.

In the auxiliary emergency systems solutions are included such as:

- Auxiliaries for turbine generation plants: Single cycle thermal power plants, Combined cycle thermal power plants, Hydroelectric or Solar thermal plants;
- Black Start systems: are systems for power generation and auxiliary subsystems intended for turbine startup and for operation even in the absence of any external power supply;
- Emergency groups for auxiliary subsystems, fluid storage tanks, fire-fighting systems, recirculation pumps, refrigeration systems, where the facilities are adapted and implemented according to the specifics of each client;
- Emergency systems for hospitals, airports and data centers.

Learn about the most common options for auxiliary emergency systems:

- *Supervisory Control and Data Acquisition and Control* (**SCADA**): control and communication system with a plant control system (DCS or distributed control);
- *Human Machine Interfaces* (**HMI**): touch screens in the control panel, mobile devices with internet access;
- Integrated circuit breakers and integrated medium voltage cells;
- Integrated fuel systems from the containers;
- Independent Fire Protection Systems (PCI): detection and extinction;
- Pneumatic and redundant double start-up;
- Ventilation, heating and air conditioning (HVAC) system, capable of operating at very high or very low temperatures;
- Systems for explosive atmospheres (ATEX);
- Large capacity main tanks and fuel pumping system;
- Engine’s optimized emissions;
- Remote cooling systems using air-coolers;
- Containers with IP54;
- Dust filters;
- External power take-offs sockets panels.

Bet on auxiliary emergency systems that meet all legal requirements and standards in terms of features, dimensions and the facility itself. Correct installation and adaptation of these systems is essential to ensure network availability and thus ensures maximum efficiency and continuous supply of energy.

Grupel over the years has been developing several projects of different dimensions and for various professional applications. Get to know some of our projects and works already done in 5 continents and in more than 40 countries.

2. Breakdown maintenance

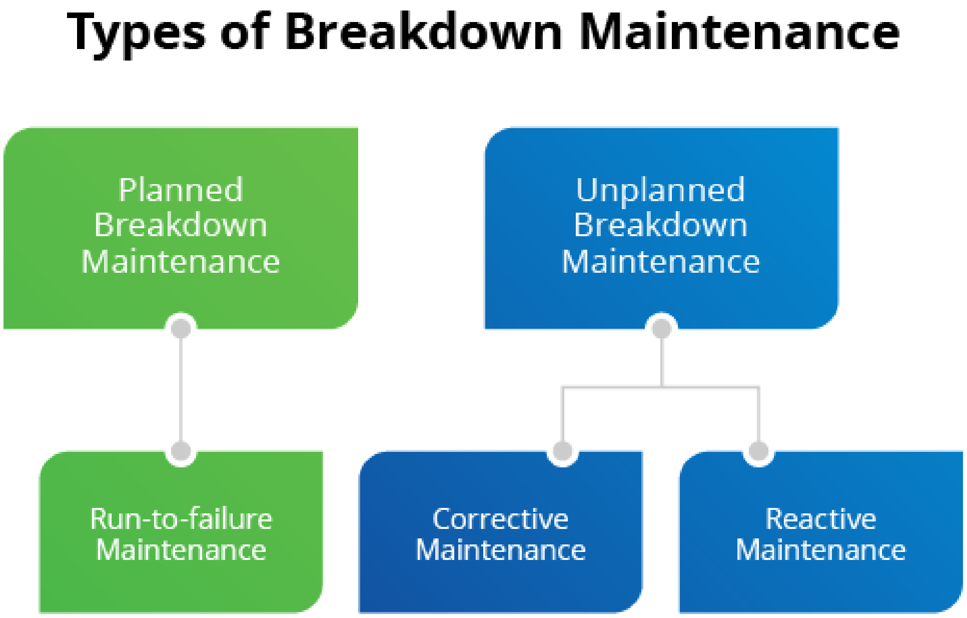
What is breakdown maintenance?

Definition

Breakdown maintenance is maintenance performed on equipment that has broken down and is unusable. It is based on a breakdown maintenance trigger. It may be either planned or unplanned.

Examples of breakdown maintenance

An example of planned breakdown maintenance is run-to-failure maintenance, where an organization has decided that letting a piece of equipment break down before servicing is the most cost-effective and least disruptive option.
Examples of unplanned breakdown maintenance include corrective maintenance and reactive maintenance. Corrective maintenance is performed when a breakdown occurs between scheduled preventive maintenance occurrences. Reactive maintenance is performed if a breakdown occurs because a maintenance strategy has not yet been put in place.


Types of Breakdown Maintenance
Planned Breakdown Maintenance
Unplanned Breakdown Maintenance
Run-to-failure Maintenance
Corrective Maintenance
Reactive Maintenance

Advantages of breakdown maintenance

Using breakdown maintenance when it makes sense can help organizations focus on optimizing PM programs for critical equipment.

Disadvantages of breakdown maintenance

Unplanned breakdown maintenance can be more costly than preventive maintenance, because it typically causes downtime and interrupts production. It can also be difficult to find the root cause of a breakdown when no maintenance strategy is in place. Finally, breakdown maintenance can raise health and safety issues if technicians are rushing to fix a problem and taking risks to do so.

The bottom line: Breakdown maintenance can be a good thing—when it's planned

Though the term "breakdown maintenance" sounds catastrophic, if it's part of a planned maintenance strategy, it can often make a lot of sense for certain pieces of machinery. When breakdown maintenance is unplanned, though, it can lead to costly downtime, health and safety risks, and halted production.

Field service management (FSM) refers to the management of a company's resources employed at or en route to the property of clients, rather than on company property. Examples include locating vehicles, managing worker activity, scheduling and dispatching work, ensuring driver safety, and integrating the management of such activities with inventory, billing, accounting and other back-office systems. FSM most commonly refers to companies who need to manage installation, service or repairs of systems or equipment. It can also refer to software and cloud-based platforms that aid in field service management.

Industry examples

Field service management is used to manage resources in several industries.

- In telecommunications and cable industry, technicians who install cable or run phone lines into residences or business establishments.
- In healthcare, mobile nurses who provide in-home care for elderly or disabled.
- In gas utilities, engineers who are dispatched to investigate and repair suspected leaks.
- In heavy engineering, mining, industrial and manufacturing, technicians dispatched for preventative maintenance and repair.
- In property maintenance, including landscaping, irrigation, and home and office cleaning.
- In HVAC industry, technicians have the expertise and equipment to investigate units in residential, commercial and industrial environments.

Requirements

Field service management must meet certain requirements:

- Customer expectations: Customers expect that their service should not be disrupted, and should be immediately restored
- Underutilized equipment: Expensive industrial equipment in mining or oil and gas can cost millions when sitting idle
- Low employee productivity: Managers are unable to monitor field employees, which may reduce productivity
- Safety: Safety of drivers and vehicles on the road and while on the job site is a concern both for individuals and their employers
- Cost: Rising cost of fuel, vehicle maintenance, and parts inventory
- Service to sales: Increasingly, companies expect their services department to generate revenues.
- Dynamic environment: Continuously balancing between critical tickets, irate customers, productive employees and optimized routes makes scheduling, routing and dispatching very challenging
- Data and technology: Many times, the data for analytics is missing, stale or inaccurate.

Software

FSM software has significantly evolved in the past 10 years, however the market for FSM software remains fragmented. The software can be deployed both on-premises or as a hosted or cloud-based system. Typically, FSM software is integrated with backend systems such as service management, billing, accounting, parts inventory and other HR systems.

The large majority of FSM companies are fee-for-service and offer differing features and functionality that vary from one company to the next.[1] Whereas one company will provide most, if not all, of the desirable features in field service management, another will be missing one or up to several functions. Pricing is dependent on several factors: a company's size, business needs, number of users, carrier selection and planned data usage. Some popular fee structures are pay-per-franchise, pay-per-use/administrators, and pay-per-field technician/employee. Costs can range from $20.00 per month for an unbundled solution that does not include carrier data charges to upwards of $200.00. It is not uncommon, although not always the case, for there to be other fees incurred with the use of the FSM platform; namely, fees for software, extra technical support, and additional training.[2]

For the enterprise market, Gartner estimates that market penetration for field service applications has reached 25% of the addressable market. Software sales in the FSM market can only be approximated. Gartner research puts the revenue for packaged field service dispatch and workforce management software applications, not including service revenue, at approximately $1.2 billion in 2012, with a compound annual growth rate of 12.7%.[3]

Companies are using mobile computing to improve communication with the field, increase productivity, streamline work processes, and enhance customer service and loyalty.[4] Field service software can be used for scheduling and routing optimization, automated vehicle location, remote vehicle diagnostics, driver logs and hours-of-service tracking, inventory management, field worker management and driver safety. Mobile software may use databases containing details about customer-premises equipment, access requirements, and parts inventory. Some field service management software integrates with other software such as accounting programs.

Mobility can

- Provide real-time analysis of mobile work status
- Increase first-time-fix rate
- Reduce overhead or administration costs of paper-based field service management and data entry
- Preserve e-audit trail for full regulatory compliance
- Increase productivity
- Shorten billing cycles

Computer Service Technicians ensure that both the hardware and software equipment of an enterprise are well-secured so that they function uninterruptedly. Known also as PC technicians, they have experience with a variety of tools to effectively troubleshoot problems of computer systems.

Computer service technicians are either employed in large organizations or on-site at client locations or service repair firms. The individual repairs and maintains computers. Technicians also install, support, and repair computer hardware, in addition to addressing networking, software or Internet issues. Typically, they replace or reinstall computer equipment, instead of repairing them because this solution is more cost-efficient. Technicians also work on help desk as technical support specialists. Importantly they should have excellent communication and analytical skills.

Computer Service Technician’s Job Description

Computer Service Technicians are responsible for resolving problems such as hard drive crashes, obsolete hardware, infected files, spyware, malware, viruses, and otherwise compromised operating systems. Since service technicians have to handle clients' problems, who sometimes may not be tech-savvy, they should demonstrate the ability to stay calm in trying situations.

PC technicians need to stay abreast of the latest trends in the information technology arena. Along with the ability to troubleshoot issues, they should possess superior interpersonal skills as they will interact with many customers. It would be beneficial to specialize in PCs, servers or laptops and ideally to specialize in more than one computer hardware types.

Computer Technicians remove viruses and other harmful programs, such as adware, malware, spyware, etc., from computers in order to secure them. For home PCs, they use free antivirus software, including avast!, and AVG Free Antivirus, among others, but for enterprise users, they use commercial antivirus software of Kaspersky or McAfee.

Technicians also repair a motherboard by checking monitors, graphics hardware, battery, RAM, and internal hardware. If a motherboard is not working well, it could be because the keyboard or mouse is not working properly, making the computer start in BIOS mode.it can stop functioning even if a cable is disconnected. Sometimes, they reformat the hard drives to set them right. Before they go about repairing a motherboard, technicians diagnose the problem by identifying the symptoms.

It is recommended that Computer Service Technicians have with them several tools, such as range of screwdrivers and torx drivers, USB keyboard and mouse, network cable testers, ADSL filters, portable labelers, hard disk to USB adapters, cable ties, 1TB USB hard disk drive, variety of blank DVDs and CDs, pre-made OS DVDs, Cage nuts and screws, USB DVD RW drives, cans of compressed air, crimping tools, tone, and probe kits, punch down tools, RJ45 connectors, spools of network cable, BT extension cables, network cables of varying lengths, wireless VDSL routers, RJ11 to RJ45 cables, and RJ11 cables.

Technicians must have the ability to upgrade customer's system software and hardware readily and to test computer devices to ensure they are in fit condition. They also determine prices for new installations and carry out the servicing of all on-site computer equipment.

These technicians develop and assemble servers and PCs or install LANs or other equipment. They promptly respond to requests from employees or customers by addressing their issues whenever they arise. It is essential that technicians practice efficient time management. Finally, they undertake help desk support responsibilities.

Additionally, technician's job entails having knowledge of the latest operating system versions of Windows and macOS. Technicians should also have experience in configuring servers, PCs, laptops, and other computer hardware.

It would be advisable for technicians to learn a programming language. Although it would be advantageous if they learn HTML or CSS, which are for web pages, it is not adequate. If technicians learn a language, they will understand how programming and coding work so that they can fix websites or mobile apps. It will also help them change their jobs and let them become database administrators or software developers, in case they find these roles more interesting.

Lastly, technicians also provide remote computer support to workstations or PCs via the Internet by using the remote-controlled software. This allows them to check and fix issues, perform repairs and maintaining the systems. They do this by staying put in their workstations, and, at times, users may not even have to reboot their systems. Here, clients need to purchase initial software only. Technicians, meanwhile, troubleshoot the issues online, making it a cost-effective solution for clients. Remote support is gaining in popularity, as it saves time for users.

Finally, technicians also prepare cost estimates for new installations

Analysis of customer call reports in locating faults

1. Identify the problem

The first step in problem solving is to identify the problem. This may seem simple, but as any seasoned call center agent knows, sometimes isn't so straightforward.

To help with this first step, ask yourself the following questions:

- What is the customer calling about?
- Is there another issue that is causing the problem that they are not aware of?
- What would the customer like us to improve?
- Is their issue being compounded by a known bug?
- Is this issue specific to this customer, or have other customers called in about the same issue?

Once you have clearly identified the problem, summarize the problem to the customer and get verbal confirmation that they agree that the problem you identified is the problem they called in about. This will make your job much more efficient and will also go a long way to improving the quality of service you provide.

2. Find out why the problem exists

Once you have identified the problem and confirmed this with the customer, find out why the problem exists. To accomplish this, **you should**:

- Understand how this customer perceives the problem and try to gain a better understanding of their needs.
- Ask them what they have already tried to resolve the issue.
- Check your systems, ask other agents if they have fielded calls about the same issue and analyze your data to see if the problem really exists.
- Decide whether or not the benefits of solving the problem will be worth the effort that you'll put into solving it (to adequately accomplish this, you must move on to step 3).

3. Find out how the problem impacts the customer

As a call center agent aiming to provide top-notch service, you must have an understanding of how the issue impacts the customer. For example, if a bug in your software is causing your customer to manually enter information after hours, you might feel sorry for them and say so (e.g., “I am really sorry for all of the extra effort. I can understand that you are frustrated.”), and tag their issue as normal priority. However, if that same bug is causing them to miss a work event and their job is on the line, their frustration with the bug should clearly be addressed and their ticket priority set to urgent. Understanding how the issue impacts the customer will help you to prioritize tasks and also connect better with your customers.

4. Clearly define the problem

Once you have completed steps 1-3, it is time to not only clearly define the problem but also to define what the customer wants or needs. At this stage you should already have a comprehensive understanding of both, but you should check in with the customer to make sure you are on the same page as them. If the problem they would like solved is still too broad (i.e., “better product”), it might take some more effort on your part to whittle it down to a concrete problem that you can work towards resolving.

5. Generate possible solutions

Once you have identified a concrete problem, it is time to brainstorm possible solutions. To help with this, ask yourself the following:

- What have other agents done to solve similar problems?
- What have our competitors done to resolve similar problems?
- Can someone from another department (i.e., tech, marketing, sales, support) help me resolve this issue?
- Does management have insight that might be helpful?

While going through this brainstorming process, generate a list of possible solutions.

6. Evaluate each solution and select the most appropriate

Once you have identified possible solutions, evaluate each one. Ask yourself the following:

- Do we have the resources to attack the problem from this angle?
- How much is this going to cost to implement?
- How long is this going to take to implement?
- Is there a cheaper, quicker, more effective way to do this?
- Will resolving the issue using this method adequately address the customer’s needs?
- Is this solution in-line with our company policy, culture and ethics?
- Would management agree with this solution?
- What could go wrong by implementing this solution?
- What would be the impact on other customers, the company, other agents and my team if we implement this solution?

Once you have evaluated each possible solution, select the most appropriate and move on to the next steps.

7. Plan the implementation of the solution

Some solutions are very straightforward to implement. For those that are not, think about the following:

- Who – who from our team will implement the solution?

- What – what will the implementation entail, cost, etc.?
- When – when will we start the implementation process and when should it be completed?
- Where – are we going to the customer to implement the solution or can we do it remotely?
- Why – why are we implementing this solution, what are the benefits of doing so, how is this going to impact the customer?
- How – how are we going to execute?

8. Pitch the solution to the customer

Once you have nailed out the details of the implementation process, you must pitch your plan to the customer. You should walk through the details of your solution and be open to their feedback. It is important to go into the pitch with an open mind, ready to make adjustments to your well-thought out plan. After all, the customer comes first!

9. Implement the solution

Once you, your customer and your team are all on the same page about the solution, it is time to execute. During this time it is important to continually check in on your progress to ensure that you are meeting your deadlines and are within your budget. If you need to re-work you plan, make sure that you appropriately manage the expectations of all parties involved.

10. Analyze the results

Once you have finished the implementation process, you should analyze the results. Do this by collecting quantitative and qualitative data. Ask the customer how they feel about the solution, if it met their expectations, if it has improved the way they use your product or service, etc. Analyze the metrics pre- and post-implementation to see if there has been a significant improvement. If there is room for improvement, start from step one with an open mind and an eager attitude.

VIRUSES

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

How does a computer virus attack?

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.

This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do.

While some viruses can be playful in intent and effect, others can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disk. Worse yet, some viruses are designed with financial gains in mind.

How do computer viruses spread?

In a constantly connected world, you can contract a computer virus in many ways, some more obvious than others. Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links. Your mobile devices and smartphones can become infected with mobile viruses through shady app downloads. Viruses can hide disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files.

To avoid contact with a virus, it’s important to exercise caution when surfing the web, downloading files, and opening links or attachments. To help stay safe, never download text or email attachments that you’re not expecting, or files from websites you don’t trust.

What are the signs of a computer virus?

A computer virus attack can produce a variety of symptoms. Here are some of them:

Frequent pop-up windows. Pop-ups might encourage you to visit unusual sites. Or they might prod you to download antivirus or other software programs.

Changes to your homepage. Your usual homepage may change to another website, for instance. Plus, you may be unable to reset it.

Mass emails being sent from your email account. A criminal may take control of your account or send emails in your name from another infected computer.

Frequent crashes. A virus can inflict major damage on your hard drive. This may cause your device to freeze or crash. It may also prevent your device from coming back on.

Unusually slow computer performance. A sudden change of processing speed could signal that your computer has a virus.

Unknown programs that start up when you turn on your computer. You may become aware of the unfamiliar program when you start your computer. Or you might notice it by checking your computer's list of active applications.

Unusual activities like password changes. This could prevent you from logging into your computer.

How to help protect against computer viruses?

How can you help protect your devices against computer viruses? Here are some of the things you can do to help keep your computer safe.

Use a trusted antivirus product, such as Norton AntiVirus Basic, and keep it updated with the latest virus definitions. Norton Security Premium offers additional protection for even more devices, plus backup.

Avoid clicking on any pop-up advertisements.

Always scan your email attachments before opening them.

Always scan the files that you download using file sharing programs.

What are the different types of computer viruses?

1. Boot sector virus

This type of virus can take control when you start — or boot — your computer. One way it can spread is by plugging an infected USB drive into your computer.

2. Web scripting virus

This type of virus exploits the code of web browsers and web pages. If you access such a web page, the virus can infect your computer.

3. Browser hijacker

This type of virus “hijacks” certain web browser functions, and you may be automatically directed to an unintended website.

4. Resident virus

This is a general term for any virus that inserts itself in a computer system’s memory. A resident virus can execute anytime when an operating system loads.

5. Direct action virus

This type of virus comes into action when you execute a file containing a virus. Otherwise, it remains dormant.

6. Polymorphic virus

A polymorphic virus changes its code each time an infected file is executed. It does this to evade antivirus programs.

7. File infector virus

This common virus inserts malicious code into executable files — files used to perform certain functions or operations on a system.

8. Multipartite virus

This kind of virus infects and spreads in multiple ways. It can infect both program files and system sectors.

9. Macro virus

Macro viruses are written in the same macro language used for software applications. Such viruses spread when you open an infected document, often through email attachments.

How to remove computer viruses

You can take two approaches to removing a computer virus. One is the manual do-it-yourself approach. The other is by enlisting the help of a reputable antivirus program.

Want to do it yourself? There can be a lot of variables when it comes to removing a computer virus. This process usually begins by doing a web search. You may be asked to perform a long list of steps. You’ll need time and probably some expertise to complete the process.

If you prefer a simpler approach, you can usually remove a computer virus by using an antivirus software program. For instance, Norton Antivirus Basic can remove many infections that are on your computer. The product can also help protect you from future threats.

Separately, Norton also offers a free, three-step virus clean-up plan. Here’s how it works.

Run a free Norton Security Scan to check for viruses and malware on your devices. Note: It does not run on Mac OS.

Use Norton Power Eraser’s free virus and malware removal tool to destroy existing viruses. Need help? A Norton tech can assist by remotely accessing your computer to track down and eliminate most viruses.

Install up-to-date security software to help prevent future malware and virus threats.

Computer virus examples

Sometimes to understand what something is, we have to examine what it isn't. Keeping that in mind, let's play: *Is It a Virus*?

In the *Is It a Virus* game we're going to take a look at examples of things people on the Internet commonly believe to be a virus and explain why it is or isn't. What fun!

Is a Trojan a virus? Trojans can be viruses. A Trojan is a computer program pretending to be something it's not for the purposes of sneaking onto your computer and delivering some sort of malware. To put it another way, if a virus disguises itself then it's a Trojan. A Trojan could be a seemingly benign file downloaded off the web or a Word doc attached to an email. Think that movie you downloaded from your favorite P2P sharing site is safe? What about that "important" tax document from your accountant? Think twice, because they could contain a virus.

Is a worm a virus? Worms are not viruses, though the terms are sometimes used interchangeably. Even worse, the terms are sometimes used together in a strange and contradictory word salad; i.e. a "worm virus malware." It's either a worm or a virus, but it can't be both, because worms and viruses refer to two similar but different threats. As mentioned earlier, a virus needs a host system to replicate and some sort of action from a user to spread from one system to the next. A worm, conversely, doesn't need a host system and is capable of spreading across a network and any systems connected to the network without user action. Once on a system, worms are known to drop malware (often ransomware) or open a backdoor.

Is ransomware a virus? Ransomware can be a virus. Does the virus prevent victims from accessing their system or personal files and demands ransom payment in order to regain access à la ransomware? If so, then it's a ransomware virus. In fact, the very first ransomware was a virus (more on that later). Nowadays, most ransomware comes as a result of computer worm, capable of spreading from one system to the next and across networks without user action (e.g. WannaCry).

Is a rootkit a virus? Rootkits are not viruses. A rootkit is a software package designed to give attackers "root" access or admin access to a given system. Crucially, rootkits cannot self-replicate and don't spread across systems.

Is a software bug a virus? Software bugs are not viruses. Even though we sometimes refer to a biological virus as a "bug" (e.g. "I caught a stomach bug"), software bugs and viruses are not the same thing. A software bug refers to a flaw or mistake in the computer code that a given software program is made up of. Software bugs can cause programs to behave in ways the software manufacturer never intended. The Y2K bug famously caused programs to display the wrong date, because the programs could only manage dates through the year 1999. After 1999 the year rolled over like the odometer on an old car to 1900. While the Y2K bug was relatively harmless, some software bugs can pose a serious threat to consumers. Cybercriminals can take advantage of bugs in order to gain unauthorized access to a system for the purposes of dropping malware, stealing private information, or opening up a backdoor. This is known as an exploit.

How Anti-Virus Software Works

Anti-virus software today is fairly sophisticated, but virus writers are often a step ahead of the software, and new viruses are constantly being released that current anti-virus software cannot recognize. The key to anti-virus software is detection. Once an infected file has been detected, it can sometimes be repaired. If not, the file can at least be quarantined so that the viral code will not be executed. The difficulty here is that generic virus detection is inadequate for current and new viruses, and so anti-virus software must be constantly updated with new lists of viruses. Currently, when a new virus is discovered (unfortunately only through execution,) samples are sent to virus analysis centers. These centers analyze the virus, and extract a unique string from the virus that will identify it. This and other information about the virus is added into a database that users can then download. However, should generic virus detection ever become 100% effective, then the other steps (removal/repair) should be greatly simplified.

Virus Detection Methods Top

There are four major methods of virus detection in use today: scanning, integrity checking, interception, and heuristic detection. Of these, scanning and interception are very common, with the other two only common in less widely-used anti-virus packages. Unfortunately, while scanning is very effective against known viruses, it is completely incapable of dealing with new viruses, forcing anti-virus analysis centers into a reactive stance.

Scanning

Definition: A scanner will search all files in memory, in the boot sector (the sector on disk that specifies where boot information is,)

and on disk for code snippets that will uniquely identify a file as a virus. Obviously, this requires a list of unique signatures that will be found in viruses and not in benign programs. To prevent false alarms, most scanners also will check the code of a suspected file against either the virus code itself or a checksum of it. (A checksum is a method frequently used to determine if data has been changed, and involves summing all of the bits in a file.) This is the most common method of virus detection available, and is implemented in all major anti-virus software packages. There are two types of scanning: on-access and on-demand. On-access scanning scans files when they are loaded into memory prior to execution. On-demand scanning scans all of main memory, the boot sector, and disk memory as well, and is started by a user when he/she wishes. On-access scanning has become more aggressive recently, with virus scans occurring even if files are selected, but not loaded.
Advantages: Scanners can find viruses that haven't executed yet - this is critical for e-mail worms, which can spread themselves rapidly if not stopped. Also, false alarms have become extremely rare with the software available today. Finally, scanners are also very good at detecting viruses that they have the signatures for.
Disadvantages: There are two major disadvantages to scanning-based techniques. First, if the software is using a signature string to detect the virus, all a virus writer would have to do is modify the signature string to develop a new virus. This is seen in polymorphic viruses. The second, and far greater disadvantage is the limitation that a scanner can only scan for something it has the signature of. The Maltese Amoeba virus was a very destructive virus that activated on November 11, 1991, and was able to spread rapidly before its activation without being detected. According to the 1991 Virus Bulletin: "Prior to November 2nd, 1991, no commercial or shareware scanner (of which VB has copies) detected the Maltese Amoeba virus. Tests showed that not ONE of the major commercial scanners in use ... detected this virus." Although virus updates occur more frequently today because of the Internet, viruses still cannot be detected until one has executed.

Integrity Checking

Definition: An integrity checker records integrity information about important files on disk, usually by check summing. Should a file

change due to virus activity or corruption, the file will no longer match the recorded integrity information? The user is prompted, and can usually be given an option to restore the file to its pre-corrupted/infected state. This is an extensive process, and few virus checkers today utilize it. Norman Virus Control, however, is one.
Advantages: Integrity checking is the only way to determine whether a virus has damaged a file, and it's fairly foolproof. Most integrity checkers today also have the benefit of detecting other damage to data, such as corruption, and can restore that as well.
Disadvantages: The major problem with integrity checking is that not enough companies offer comprehensive integrity checking software. Most anti-virus suites that do offer it don't protect enough files, and those that they do may not be damaged at all with newer viruses. Simpler integrity checkers won't be able to differentiate between damage done via corruption and damage done via a virus, thus giving the user unclear information as to what's going on. Finally, this process is simply rather cumbersome - in today's computers, many important files are changed by as little as booting up and shutting down, so integrity checkers need to be coupled with scanners for maximum efficacy in detecting viruses.

Heuristic Virus Checking
Definition: This is a generic method of virus detection. Anti-virus software makers develop a set of rules to distinguish viruses from non-viruses. Should a program or code segment follow these rules, then it is marked a virus and dealt with accordingly. This allows detection of any virus, and theoretically, should be sufficient to deal with any new virus attacks. F-secure virus software uses this method in addition to scanning, although not very many software packages available today utilize heuristic virus checking.
Advantages: Generic virus protection would make all other virus scanners obsolete and would be sufficient to stop any virus. The user doesn't need to download weekly virus updates anymore, because the software can detect all viruses.
Disadvantages: Although these are huge benefits to heuristic virus checking, the technology today is not sufficient. Virus writers can easily write viruses that don't obey the rules, making the current set of virus detection rules obsolete. Changes to these rules must be downloaded, and thus these virus checkers must be updated and

won't stop many new viruses, which gives them similar characteristics to scanners. In addition, the potential for false alarms and not detecting a known virus is greater with heuristic checkers than with scanners.

Interception
Definition: Interception software detects virus-like behavior and warns the user about it. How to detect virus-like behavior? Use heuristics again. Many viruses will perform some suspicious action, like relocating themselves in memory and installing themselves as resident programs. Many software packages have this as an option, although most people usually disable it.
Advantages: Interception is a good generic method to stop logic bombs and Trojan horses. Logic bombs will trigger a (usually destructive) sequence given an event, such as the date being set to a certain date. When not detected by scanners, interception software will usually detect the destructive and unusual sequences of events caused by logic bombs and Trojan horses.
Disadvantages: Unfortunately, interceptors aren't very good at detecting anything else. Interceptors also have all the drawbacks of heuristic systems - difficulty differentiating virus from non-virus, and easy to program around. Also, most interceptors are very easy to disable, and so many viruses frequently disable them before launching. Due to the nature of an interceptor, this software is unable to detect viruses before they launch, and a lot of damage could already have been done. Lastly, interceptors are a nuisance and frequently prompt the user to allow/disallow activity during software installations and system upgrades, making the above very tedious. Combined with their limited usefulness, most software packages disable or strongly limit interception by default.

Upcoming Improvements to Software Top
Symantec has recently released something called the "Digital Immune System" with the Norton AntiVirus Corporate Edition. Currently only available to corporations, this system automates much of the virus detection/vaccine process. A sample is automatically uploaded to an analysis center when the system detects virus-like activity. If the virus matches a known virus, then a vaccine is downloaded to the infected computer and the software

cleans it out. If this is a new virus, the sample is sent to analysts to develop a vaccine. This greatly speeds up the time it takes to clean a virus off of a computer, thus greatly decreasing the ability the virus has to infect other computers. Unfortunately, virus activity is detected using heuristics, which, as mentioned above, are not totally accurate. Network Associates has a similar process in its Virus Scan software. Unfortunately, not many other improvements to virus software are foreseen, and improvements in this area rely wholly on improved AI to detect viruses.

Ways to Defeat Anti-virus Software Top

Because the same anti-virus software methods are in use all over the world, virus writers have attempted to defeat the software in their viruses, either by disabling the software or getting around the detection algorithms. This section will briefly examine the techniques that virus writers use to get around the software and how effective they are in doing so.

Polymorphic viruses attempt to neutralize virus-scanning techniques by changing the code every time the virus infects a new computer. Even if the virus signature remains unchanged, the checksum of the virus will, ensuring that anti-virus software won't pick it up. However, all of the viruses today that use such a technique are fairly ineffective, because the code that is generated is too similar to the original virus. "Toolkits" have been developed by virus writers - some with excellent user interfaces and even help files - to generate polymorphic viruses, but even so, the similarities between the viruses generated by these toolkits makes it easy for anti-virus software to detect the virus. Nevertheless, the possibility exists that a polymorphic virus will be developed that can evade virus scanners; such a virus would be extremely difficult to contain.

Tunneling viruses attempt to get around anti-virus software by loading themselves underneath the scanner, closer to the hardware. Such viruses aim to gain access to interrupt handlers and thus have direct access to the operating system. Most anti-virus software can detect this. When detected, the anti-virus software installs itself underneath the virus. Smarter viruses then try to install themselves underneath the anti-virus software, leading to a battle over the interrupt handlers and system problems as no one is allowed access to the interrupt handlers.

Stealth viruses rely on being loaded before the anti-virus software, which could occur should the virus infect the boot sector or a system file that is loaded before anti-virus software is. These viruses then disguise the changes that they make, and thus get around any virus detection schemes. Cleaning such viruses off isn't that difficult - booting with a clean diskette will prevent the virus from being loaded into memory, and a scanner should be able to clean it off then.

Fast infecting viruses work similarly to stealth viruses - they rely on being invisible to the virus scanner to infect computers. These viruses usually piggyback on anti-virus scanners, and infect files whenever they are accessed. If not found before the virus scanner begins scanning files, the virus will quickly infect every file on disk. Because of on-access scanning, this type of virus will spread even without an on-demand scan. However, the virus still needs to infect its first file, and most scanners will block the virus before it can latch onto the virus scanner.

Other methods: Many viruses being developed today use a combination of the above techniques and add a few more of their own. For example, the MTX worm loads itself into memory before anti-virus software and prevents the software from functioning correctly. In addition to that, the virus uses a technique that's becoming more and more common - blocking access to anti-virus vendor websites. The MTX virus blocks access to Symantec, McAfee, and several other companies that provide virus scanner updates so that the user is prevented from retrieving an update. Other viruses will attack the software more directly, damaging and corrupting library or code files that a virus scanner needs to function properly. Finally, many viruses will download updates and plugins, allowing the virus writer to stay one step ahead of the anti-virus software writers.

Virus recovery & removal Top

Once a virus is detected, how do anti-virus programs undo the damage that the virus has done? Anti-virus programs are fairly bad at restoring data - viruses that attempt to damage files instead of merely infecting them will succeed unless those files have been backed up. Virus scanners repair files by deleting the virus code from the file, which in most cases restores the file to its pre-infected state. However, for viruses that damage system files (e.g. viruses that block access to anti-virus software vendors irreparably changes a network library,) the anti-virus program is incapable of repairing all the damage. The only foolproof method of restoring damage done by a virus is to clean all infected files and restore everything else from backups.

Problems with anti-virus software Top

Anti-virus software suffers from more problems than not being able to detect cutting edge viruses. Many copies of anti-virus software are unable to detect even old viruses, because end users frequently forget or simply don't update their virus scanner's virus databases until it's too late. On-demand scans are rarely performed because they're slow and hog resources while running, so dormant viruses tend to have a rather long life. On-access scanners aren't free of troubles, either - some consume too many resources, so many users are tempted to disable them if they're on a slower machine. Finally, while anti-virus software may become extremely good at sensing virus activity, there are always new security holes to exploit in operating system and networking software that would give viruses another entry point that bypasses the anti-virus software. Finding a security hole and getting reported on one of these sites is considered to be an honor among the virus writing community. An example of one of these sites is SANS, which has bulletins about hacker and virus attacks.

The bottom line? Anti-virus software in use today is fairly effective - but only if it's kept updated and the user takes precautions (such as not opening unfamiliar documents or programs.) Despite all this, anti-virus software cannot protect against brand new viruses, and few users take the necessary precautions. A survey was done of corporate computer users, finding that many users still get infected even if they are required to take all the necessary precautions. (Source: ICSA Labs Computer Virus Prevalence Survey 2000.)With the Internet daily growing larger, it is unlikely that anti-virus software will be able to protect all of the users connected; however, with proper care and attention, people should be able to deal with all but the most unusual viruses.

What is Antivirus Software?

Antivirus software, at its most basic, **helps you detect and manage infected files on your computer**. More advanced versions of antivirus will help you uncover infections before they occur, from email scanning to scanning online files and more.

A few common types of infections that a file can have are:

Malware

Ransomware

Spyware

Trojans

Worms

Viruses

Adware

Antivirus software **helps you "quarantine"** infected files, which means they are sent to a dedicated place on your computer. There, these files can be cleaned and then placed back in their original locations or deleted.

Don't worry if you have an infection. The more digitally connected we are, the more vulnerable we are. **Infected files can usually be cleaned**, and you can continue your business online and offline like nothing ever happened…if you've installed an antivirus program.

What is a Virus?

A computer virus is a **type of software that replicates itself**. To remove a computer virus, run a scan through your antivirus software. Once the scan is done, any infected files can be cleaned and removed. In the worst case scenario, you will need to back-up your data and perform a factory (hard) reset on your system.

Common Symptoms of an Infected Computer

If you really want to understand computer viruses, it helps to know what to look for. **Here are a few common symptoms related to viruses:**

Slower speeds on your computer

Random error codes popping up

Popups ads, warnings, and other unwanted material

Browser pages redirecting to a website you've never interacted with

Password locked out of important files or the system itself

Delayed network speeds

The Basics of Your Antivirus

Antivirus programs aren't perfect. With viruses constantly evolving, development teams have to always be ready to solve the next virus.

When your antivirus program scans your files, it compares them to known viruses or malware. There are three types of detection that are used:

Specific Detection – looking for known viruses using a set of characteristics that are specific to a type of virus.

Generic Detection – looking for viruses based on variants assigned to a typical virus family.

Heuristic Detection – searching for odd file structures and behaviors. These types of viruses are usually unknown and identified by the strange behavior they showcase.

Most antivirus programs come with several scanning options. A full-system scan will take the longest to complete, but it **will scan every single file on your computer**. This scan is **best completed when you don't need your computer** as it will require extensive system resources.

In contrast, partial system scans are **great if you want to scan a specific section of your computer**, but they are less thorough.

False Positives

Any antivirus software title is bound to make a few mistakes. Usually, these false positives are nothing more than an annoyance, but in rare cases, they can actually damage system files. For example, AVG once damaged vital system files in 64-bit Windows 7 and Microsoft Security Essentials by classifying Google Chrome as a virus.

The heuristic detection method tends to cause the most false positives because it is a pro-active scanning method. It compares the characteristics of malicious programs to existing programs on your computer to look for a match.

If the results of a virus scan report are confusing, check online to see if other users have had the same problem.

How Updates Work for Antivirus Programs

Antivirus programs rely on updates about the latest threats. Just like any software, your antivirus program needs to be updated regularly.

Updates for antivirus programs are typically called “definitions.” These definitions include **new information discovered by an antivirus**. Once the information is verified for accuracy, these definitions are downloadable across the platform.

The definition system lets antiviruses detect new viruses with reliable accuracy. Antivirus programs are **“trained” by the millions of computers that run the software**, allowing it to collect new information, improve its efficiency against known viruses, and more.

Do All Antiviruses Software Detect All Viruses?

There are many different types of antivirus software, just like there are many different types of computer viruses. Both are improving every day. Depending on your antivirus software and the scans, you may find different infected files on your system than another computer.

Computer viruses are **often tailored to their victims**. Hackers might target Windows over Mac, or Mac over Linux, or online users over offline users. You cannot predict when or where you will get a virus. The best solution is to **have an updated antivirus active on your computer.**

Some software will only scan files on your computer, while other options will scan the cloud. Your AV software might exist in the cloud; this may not be ideal if you are a majority-offline user, while **cloud-based antivirus is perfect for a Chromebook user**. Some AV software work both ways: it's installed, but receives regular updates from an online company server, which routinely improves the virus definitions that it looks for.

What is the Simplest Way to Protect My Computer and My Data?

To protect your computer, never download files that you are unsure of. If you are downloading a file from the Internet or accessing a file from a flash drive, make sure that you **scan the file before opening** it and accessing its contents. A virus can be hiding in any type of file, from an .exe file, to a .docx file, to a .pdf file.

It's always **easier to stop a virus before it's embedded in your system**. A quick scan can detect the virus and snuff it out before it becomes a serious problem.

This doesn't mean that you should avoid sharing and receiving information online or offline, just that you should understand the risks of doing so and make sure you have the right virus program in place.

And as an added security measure, **you should always back up your data**. Whether you use an external hard drive or the cloud, make sure you can access a copy of your data should a file become infected.

Also, do your research regarding antivirus software. Make a list of your priorities concerning your computer usage. Find an antivirus software that **works for you**

and your goals. Some prefer additional premium features, while others love basic, straightforward titles.

I Have a Virus. Now What?

Don't panic. If your antivirus software reported the issue to you, it has most likely quarantined the file. Quarantined files cannot harm your data or your system.

Simply **access the quarantine location where your file is located, clean the file, and purge the infection**. Your file should be good to use again.

Here's my take on it.

I've been using computers for decades. In that time, the only malware that wouldn't leave my computer was a browser cookie that was, for some reason, classified as malware. I had accessed a reputable news website that installed this browser cookie to use my computer resources (i.e. CPU) to mine for Bitcoin while I was accessing the site. After running a few antivirus scans and tracing the location of this "malware," **I simply deleted my cookies and never accessed the site again. Problem solved.**

What did I learn from this?

Even the most innocent websites can be threats. In this case, a reputable news site was the target. That experience taught me to never take anything for granted. Hackers have their own motives and they will accomplish them however they see fit.

Should I Have Multiple Antivirus Programs on My Computer?

There is no limit to the amount of antivirus software programs that you can have on your computer. However, for the sake of hard drive space and sanity, **you should limit the number of antivirus software you use to no more than two**. Typically, **this means running Windows Defender with at least one other program**. Running scans once per week is more than enough for most people.

When running multiple antivirus programs, **you may have conflicting scans** and certain programs **can hog vital system resources**.

Will My Antivirus Work Forever?

Whether your antivirus will work forever is a whole different matter. Free antivirus may not expire, but you will need a regular Internet connection to install patches and updates. The same applies to cloud software. **Like any virus (real or digital), computer viruses evolve over time and you'll need an updated antivirus.**

If you pay for your antivirus, you may be able to install a complete program, either for a restricted amount of time (like a one-year subscription) or for life. Keep in mind, you will need to keep the program updated.

Malware, Antivirus, and the Cloud

Antivirus now exists in the cloud in order to combat malware it finds there. Like most computing networks, the cloud was built with a focus on access, not security. As such, while the cloud is incredibly freeing in terms of what we can do from anywhere, **a virus could appear on our computers**. You don't have to panic if you keep your antivirus up to date.

Updates will provide your antivirus software with the tools it needs to discover infected files and clean them properly.

Being Prepared Is Half the Battle

The key to dealing with an infected file is having reliable antivirus software and understanding how it works. **Scan your system regularly and practice good end-user security measures.** Antivirus is simple to use, and thanks to the many options and configurations available, protecting your data has never been easier.

Virus, Worm, Malware: What's the Difference?

Because these terms are often used interchangeably, you may wonder what the difference is between a virus, worm and malware if your computer is having issues. Let's begin with basics:

Virus – a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting a system or destroying data on an individual computer. A computer virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code.

Worm – a malware computer program that replicates itself so it can spread to other computers, often, via a network. Almost always causing harm to the network, worms rely on security failures on the target computer in order to initially gain access.

Malware – also known as malicious software, is a broad term used to refer to viruses, worms, ransomware, Trojan horses, keyloggers, rootkits, spyware, adware and other malicious software. Malware is designed to disrupt normal computer or mobile operations, gather sensitive information, get access to private computer systems and even to show unwanted advertising.

Symptoms of an Infected Computer

When unprotected devices are infected, they:

Run slower than normal.

Show popups both online and/or offline.

Have programs that do not open, run slow or close unexpectedly.

Have browser(s) that do not display some or any website at all.

Show the 'FBI' or 'Department of Justice' screen, it comes up shortly after loading the computer's operating system.

Present problems when trying to recognize external hardware.

Show a blue screen with the error code.

Once your device exhibits the above symptoms, chances are good that it has been affected by a virus, worm or other type of malware and likely needs immediate attention from someone trained in the identification and removal of such.

What is Antivirus Software? How does Antivirus Software Work?

Antivirus software, sometimes known as anti-malware software, is designed to detect, prevent and take action to disarm or remove malicious software from your computer such as viruses, worms and Trojan horses. It may also prevent or remove unwanted spyware and adware in addition to other types of malicious programs. The first versions of antivirus software can be traced as far back as the 1980s.

Antivirus software will begin by checking your computer programs and comparing them to known types of malware. It will also scan your computer for behaviors that may signal the presence of a new, unknown malware. Typically, antivirus software uses all three scanning detection processes:

Specific Detection – This works by looking for known malware by a specific set of characteristics.

Generic Detection – This process looks for malware that are variants of known "families," or malware related by a common codebase.

Heuristic Detection – This process scans for previously unknown viruses by looking for known suspicious behavior or file structures.

Although the detection tools are highly effective, no antivirus software is failsafe. If you suspect your device has been infected, you should take action to remedy the problem quickly.

What is a computer virus?

A **computer virus** is a type of malware (malicious software or code) that is designed to spread from computer to computer and perform harmful activities such as corrupting and disrupting systems or destroying data. (1)

Computer viruses can also copy (duplicate) themselves.

Computer virus types

A list of well-known computer virus types:

Memory Resident Virus (2) - stays in memory after it executes and after its host program is terminated. In contrast, non-memory-resident viruses only are activated when an infected application runs.

Overwriting Virus (3) - will copy its own code over the host computer system's file data, which destroys the original program.

Direct Action Virus (4) - is considered to be “non-resident” and functions by selecting one or more files to infect each time the code is executed. The primary intentions of this virus is copying itself and to spread infection whenever the code is executed.

Boot Sector Virus (5) - infects computer systems by copying code either to the boot sector on a floppy disk or the partition table on a hard drive. During startup, the virus is loaded into memory. Once in memory, the virus will infect any non-infected disks accessed by the system.

Cluster Virus (6) - associates itself with the execution of programs by modifying directory table entries to ensure the virus itself will start when any program on the computer system is started. If infected by this virus it will look like every program on your PC is infected; however, this virus is only in one place on the system.

Macro Virus (7) - is written in a macro language and infects Microsoft Word or similar applications (e.g., word processors and spreadsheet applications) and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.

Computer virus symptoms (signs)

A few computer virus symptoms are:

Computer and/or internet suddenly slower

Computer behaves weird

PC freezes and crashes a lot

Unusual error messages appear

Files have been automatically deleted or added

Unwanted advertisements appear

Emails have been sent from your account to your contacts (which you know you didn't sent)

Sudden hardware problems (e.g., display acting weird)

Antivirus software and/or its shields are turned off automatically

PC automatically restarts (reboots) by itself

Empower Your Imagination with
Filmora
A video editor for all creators.
CLICK HERE

Computer virus protection

The BEST protection against computer viruses is YOU.

Look:

You can have the best protection there is, but even the best antivirus software can fail to detect new malware (e.g., computerviruses, ransomware, spyware, etc.). (8)

Malware threats grow so fast, that antivirus programs take too long to catch up with malware (even the best free or paid ones). (9)

Therefore, the best protection is yourself.

If you do any of the following:

Ignore Windows and software updates

Don't use antivirus software

Use pirated software

Install free software without checking if it's reliable

Click on every link you see

Ignore security warnings from Windows or antivirus software

Click on buttons in pop-up windows that appear

Then there's a good chance that your PC will get infected one day.

Antivirus software

It's recommended to always use an antivirus program on your PC – even when antivirus software can't protect your computer against all viruses.

It's better to have some protection than no protection at all.

You should only use one antivirus program on your computer.

The free antivirus programs I recommend are:

Bitdefender Antivirus Free

Kaspersky Free Antivirus

Kaspersky Security Cloud Free

If you need more functions (e.g., multi-layer ransomware protection) and settings, then you can try a paid antivirus program.

Most antivirus companies offer the option to download and try their paid antivirus programs for free for 30 days.

The paid antivirus programs I recommend are:

Bitdefender Antivirus

Kaspersky Antivirus

ESET Antivirus (one of the lightest antivirus programs there is)

Free second opinion virus scanners

It's also recommended to use second opinion virus scanners to get more complete detection coverage, because some programs may detect viruses that others might miss.

The free virus (malware) scanners I recommend are:

Malwarebytes (**note:** to download the free version, you will have to scroll down to the bottom of the page and then click on **DOWNLOAD 14 DAY TRIAL**. You will get the Premium version for the first 14 days and after the 14 days it will turn into the free version – which is an on-demand malware scanner)

Zemana Antimalware

Emsisoft Emergency Kit

HitmanPro (I use the free version only for scanning for malware. Visit the product page and click on the **Free 30-Day Trial** button to download it. You can try the premium version for free for 30 days. After the trial period, you can only use it for scanning for malware)

If you think that your PC has a virus (malware) infection, then you can also try the following free virus (malware) scanners:

Kaspersky Virus Removal Tool

ESET Online Scanner

Norton Power Eraser

You can use these virus (malware) scanners alongside your current antivirus software.

You can use these scanners to scan your PC periodically (e.g., once a week) or when you think your PC is infected with a virus or another type of malware.

Computer virus prevention tips

Keep your operating system and software always up-to-date

Use a firewall

Use antivirus software

Don't ignore security warnings from Windows or your antivirus software

Don't install and use pirated software

If you don't use Java, then remove or disable it

Don't click on *OK*, *Yes* or *Run* when a pop-up window appears and ask you to install unknown software. Here's one example: “Your windows computer could be at risk! Install this repair tool to protect and clean your system by clicking Secure Now as soon as possible” Don't fall for this trick!

Before you want to install free software (freeware) first check if its reliable by reading reviews about it

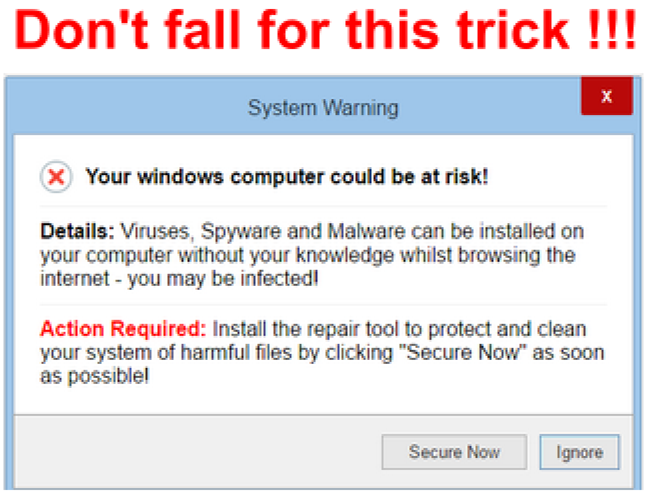
Always download software from the official link or from a trusted website

Don't click on a link (in emails or web pages) if you don't trust it.

Use a secure and safe web browser like Google Chrome or Mozilla Firefox and keep it updated

When installing software, always pay attention and always read everything clearly before clicking *Next*, *OK*, *Install*, *Continue*, etc.

Microsoft recommends that you disable SMB1 on Windows for security reasons.



Don't fall for this trick !!!

System Warning

Your windows computer could be at risk!

Details: Viruses, Spyware and Malware can be installed on your computer without your knowledge whilst browsing the internet - you may be infected!

Action Required: Install the repair tool to protect and clean your system of harmful files by clicking "Secure Now" as soon as possible!

Computer virus detection and removal

I will show you how to detect and how to get rid of a computer virus for free.

But first:

The first thing you want to keep in mind when your PC is infected by a computer virus is whether or not you want to clean it. Because sometimes it may be a better idea to back up any data that you might have and reinstall Microsoft Windows or restore a system image backup that's 100% clean.

Why?

Well, if your antivirus (antimalware) software detected a computer virus or other malware, then you will never know for sure if that's the only piece of malware that has infected your system.

Malware can nestle itself deeper into your system and hide so that it can't be discovered by your security software and it can also open doors to other malware.

And:

You also may end up with a damaged Windows installation.

Considering time and effort, sometimes it's better to wipe everything and start all over again. But, if you wanted to do that, you probably wouldn't be reading this article, so, follow the steps below.

With the following steps, I assume that you have access to your system or at least can boot Windows into “Safe Mode with Networking”.

But:

If you cannot access your computer then I recommend Kaspersky Rescue Disk (located in the “Free Tools” section).

Once you have the ISO file you can install it on a USB flash drive with the help of a free tool called Rufus and then you can boot from the USB drive and use the rescue disk.

Let's continue with the next step.

Step 1: Find out if your files are affected by Ransomware

If you cannot open some files on your computer or you see files with missing or weird file extensions (e.g., .cry, .crypto, .locked, .kraken, etc.), your system is probably infected by Ransomware.

If your system is infected by Ransomware, the first thing you should do is to check if your files can be decrypted.

But to do this, you first need to find out which Ransomware has infected your PC.

To find out which Ransomware has infected your PC, look at the ransom note, or look at any messages on the screen or look at the encrypted files and the extension they have.

If you cannot find out which Ransomware infected your PC you can visit ID Ransomware by MalwareHunterTeam and upload the ransom note or an encrypted file.

You can also visit a cybersecurity forum like BleepingComputer.

On this forum, you can find a lot of malware analysts that you can talk to.

You can post something in the forums and upload one of your encrypted files.

They might be able to tell you whether or not you can decrypt your files.

You can also download the Bitdefender Ransomware Recognition Tool to find out which ransomware has encrypted your data and then get the appropriate decryption tool if it exists.

You can visit NoMoreRansom.org or the free ransomware decryptors page on Kaspersky.com and check if they have a decryptor tool for the ransomware that infected your PC.

Step 2: Make a backup of your files

If your files were not affected by ransomware or you were able to decrypt your files, then you should make a backup of your files.

You can use a free backup program like AOMEI Backupper Standard or copy your files to a USB flash drive or external hard drive.

Step 3: Disable startup programs in Windows

1. Open Windows Task Manager.

Three ways to open Task Manager:

Press the [ctrl] + [alt] + [delete] (del) keys on your keyboard and then click on **Task Manager**.

Press the [Windows] + [R] keys on your keyboard, type **taskmgr** and then click on the **OK** button or press [Enter].

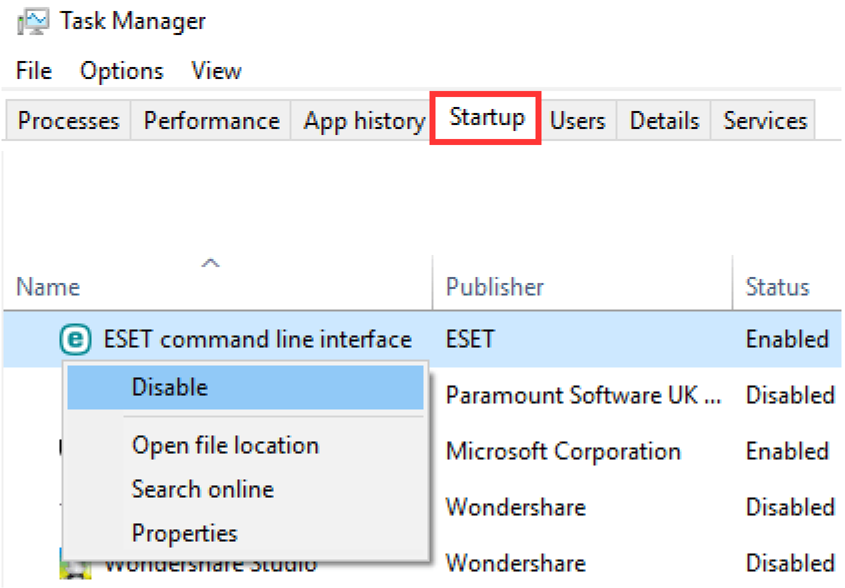
In Windows 10, you right-click on the taskbar or start menu button and then click on **Task Manager**.

2. Click on the **Startup** tab.

Note: if you don't see the **Startup** tab then click on **More details** located at the bottom left of the Taskmanager window.

3. Disable everything that you see here, including your antivirus software.

To do this, right-click on the program and then click on **Disable**.



Name	Publisher	Status
ESET command line interface	ESET	Enabled
	Paramount Software UK ...	Disabled
	Microsoft Corporation	Enabled
	Wondershare	Disabled
Wondershare Studio	Wondershare	Disabled

Step 4: Disable services in Windows

1. Open Windows **System Configuration**.

Three ways to open **System Configuration**:

Press the [Windows] + [R] on your keyboard, type **msconfig** and press [Enter].

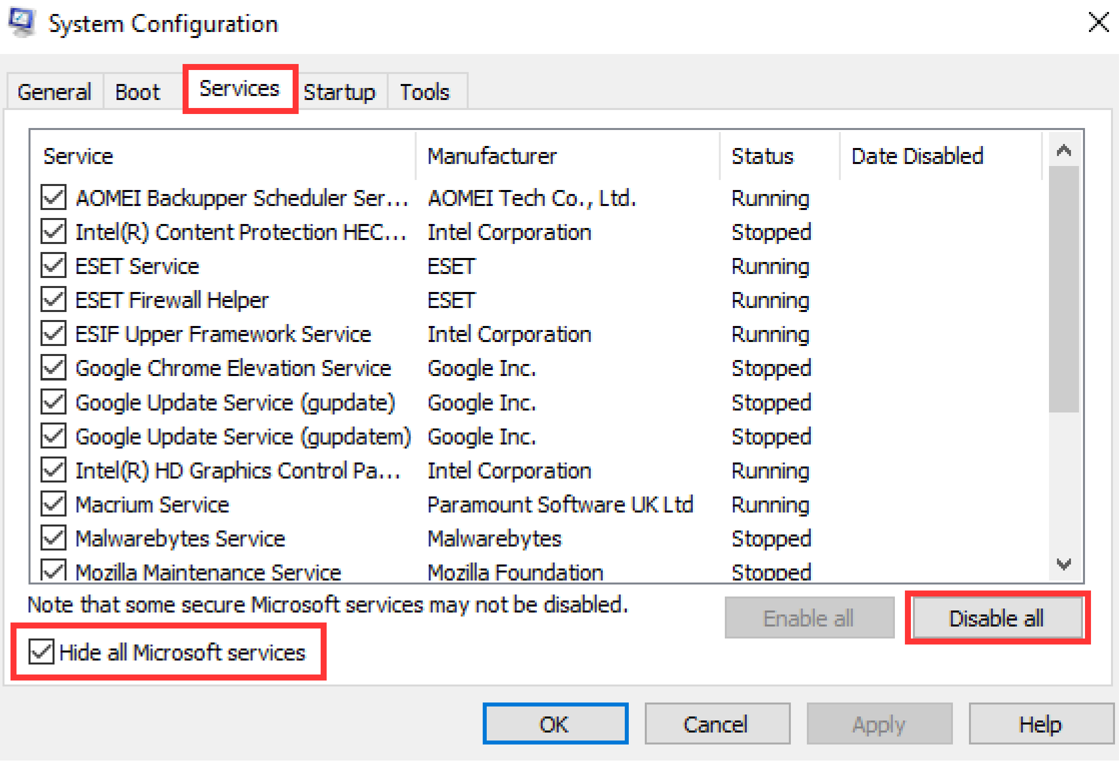
Search for **msconfig** using the Windows search box and then click on **System Configuration** when it appears.

Click on the start menu button, click on **Windows Administrative Tools** and then click on **System Configuration**.

2. Click on the **Services** tab.

3. Check (select) the **Hide all Microsoft services** option located below the list.

4. Click on the **Disable all** button.



Service	Manufacturer	Status	Date Disabled
☑ AOMEI Backupper Scheduler Ser…	AOMEI Tech Co., Ltd.	Running	
☑ Intel(R) Content Protection HEC…	Intel Corporation	Stopped	
☑ ESET Service	ESET	Running	
☑ ESET Firewall Helper	ESET	Running	
☑ ESIF Upper Framework Service	Intel Corporation	Running	
☑ Google Chrome Elevation Service	Google Inc.	Stopped	
☑ Google Update Service (gupdate)	Google Inc.	Stopped	
☑ Google Update Service (gupdatem)	Google Inc.	Stopped	
☑ Intel(R) HD Graphics Control Pa…	Intel Corporation	Running	
☑ Macrium Service	Paramount Software UK Ltd	Running	
☑ Malwarebytes Service	Malwarebytes	Stopped	
☑ Mozilla Maintenance Service	Mozilla Foundation	Stopped	

Note that some secure Microsoft services may not be disabled.

☑ Hide all Microsoft services

5. Click on the **Apply** button.

6. Click on **OK**.

7. Click on **Restart** to restart your computer.

Step 5: Scan your computer with malware scanners

You can use malware scanners to scan your computer for malware, and hopefully, also remove malware.

Malware scanners can run alongside your antivirus without any problems.

The free malware scanners I recommend are:

Kaspersky Virus Removal Tool

Emsisoft Emergency Kit

ESET Online Scanner

Norton Power Eraser

Malwarebytes (**note:** to download the free version, you will have to scroll down to the bottom of the page and then click on **DOWNLOAD 14 DAY TRIAL**. You will get the Premium version for the first 14 days and after the 14 days it will turn into the free version – which is an on-demand malware scanner)

3. Fault location & its identification

Visual Inspection, or Visual Testing (VT), is the oldest and most basic method of inspection. It is the process of looking over a piece of equipment using the naked eye to look for flaws. It requires no equipment except the naked eye of a trained inspector.

USE Visual inspection can be used for internal and external surface inspection of a variety of equipment types, including storage tanks, pressure vessels, piping, and other equipment.

ADVANTAGES Visual inspection is simple and less technologically advanced compared to other methods. Despite this, it still has several advantages over more high-tech methods. Compared to other methods, it is far more cost effective. This is because there is no equipment that is required to perform it. For similar reasons it also one of the easiest inspection techniques to perform. It is also one of the most reliable techniques. A well-trained inspector can detect most signs of damage.

A term used to describe a person who is not an expert. For example, Computer Hope is a site dedicated to helping all users with computers in **layman** terms, making it easy for everyone to read and understand.

Computer Troubleshooting Tutorial

Troubleshooting computers can be a little frustrating and a little tricky. With so many parts and software installed, any number of things can go wrong. But when (not if) something happens, this is the best opportunity for you to learn-of course provided that you have a few basics under your belt. Nothing beats experience. The more you do it, the better you become, and the more your confidence grows. And the best part, you will save yourself a lot of money.

There are many things that can go wrong with a computer. Here, I try to cover the basics to get you going in the right direction.

Well let's start with an important tip: When troubleshooting computers always start with the simple stuff. By that I mean there's a tendency to assume that when something happens it's always due to a major problem, when all it could be is a loose cable or something else minor. I have been guilty of this myself. Check the easy things first!!!

Now the real challenge is deciding whether a symptom is hardware or software related. A lot of times this comes through trial and error. Don't be afraid of misdiagnosing a problem. It's going to happen. Just keep at it.

1. Issues During POST:

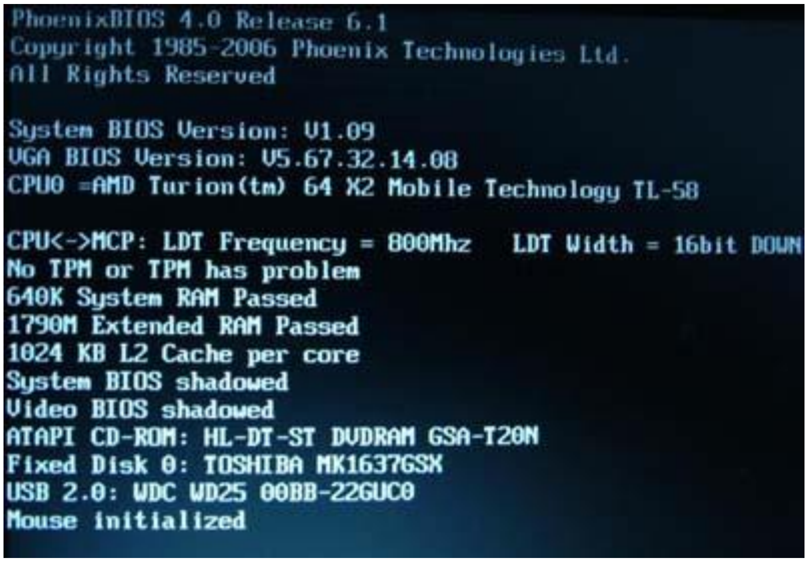
When you power on your system, the power supply sends a signal to the CPU, which receives instructions to go to the BIOS to start the boot process. Part of this process is the POST (Power On Self Test). Problems arising at this stage are almost always hardware. During the POST, devices are found and checked for errors. If everything is fine the motherboard speaker will usually sound a single, short beep and move on to loading the operating system. If something occurs you will hear some type of beep or see an error message on the screen. BIOS manufacturers have different beep codes so you will have to know which BIOS your system is using. Phoenix and AMI are the two primary makers. Award BIOS was bought out by Phoenix in 1998. You can find the type of BIOS you have by either turning on your computer (assuming of course it comes on) and looking at the top left of the screen, opening the case and looking at the BIOS chip, consulting the motherboard manufacturer or the company that built your computer.

Whichever BIOS you have, if the beep code indicates a memory or video card problem the usual solution is to check to see if they are fully seated in their slots or to replace the part. If using built-in video then it could be the motherboard. If it's a CPU beep code your processor might be overheating. Some BIOS setups are set to shut the computer down if the processor is too hot. A malfunctioning processor fan can could be the culprit. Turn off the computer and remove the case door. Turn the computer back on and see if the fan is working or running slowly. If it's the fan, replace it. If not, remove the processor and see if there's any physical damage to it. Keep in mind that you will not always see physical damage on a bad CPU.

If you don't hear a beep at all, more than likely it's a failing power supply or motherboard.

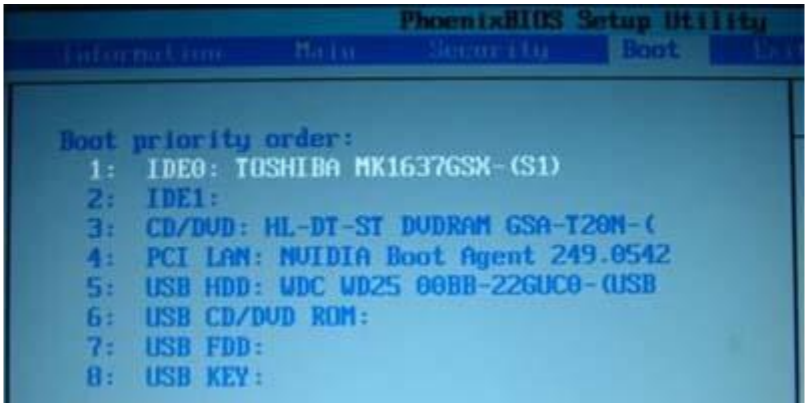
2. Devices Not Listed in BIOS:

Immediately after the POST is performed information about your computer is listed on the screen, including your drives. If you don't see a drive listed, go back and make sure they are installed properly and that cables are firmly connected.



```
PhoenixBIOS 4.0 Release 6.1
Copyright 1985-2006 Phoenix Technologies Ltd.
All Rights Reserved

System BIOS Version: V1.09
VGA BIOS Version: V5.67.32.14.08
CPU0 =AMD Turion(tm) 64 X2 Mobile Technology TL-58

CPU<->MCP: LDT Frequency = 800Mhz   LDT Width = 16bit DOWN
No TPM or TPM has problem
640K System RAM Passed
1790M Extended RAM Passed
1024 KB L2 Cache per core
System BIOS shadowed
Video BIOS shadowed
ATAPI CD-ROM: HL-DT-ST DVDRAM GSA-T20N
Fixed Disk 0: TOSHIBA MK1637GSX
USB 2.0: WDC WD25 00BB-22GUC0
Mouse initialized
```

No Operating System Found or Similar Message:
After the POST and listed information the BIOS checks the boot device for the master boot record (MBR), which tells where the operating system (OS) is. A drive set to boot with no operating system will produce an error, so make sure your system is set to boot from the right device. Go into CMOS and look under the BOOT menu to see if the proper boot order is listed. (Again, depending on the BIOS, there are various ways to enter CMOS. It's listed at the bottom of the screen soon after you turn on the computer. Most of the time it's by pressing DEL, F1, or F2). In many cases the DVD drive is first on the list followed by the hard drive(s). That's OK. If the DVD drive is empty, the BIOS skips it and starts looking at the hard drives. If there is a non-bootable DVD in the drive, remove it. Your boot drive should be the first option or second (If DVD drive is first). Once found, the OS begins to load.



```
Boot priority order:
  1:  IDE0: TOSHIBA MK1637GSX-(S1)
  2:  IDE1:
  3:  CD/DVD: HL-DT-ST DVDRAM GSA-T20N-(
  4:  PCI LAN: NVIDIA Boot Agent 249.0542
  5:  USB HDD: WDC WD25 00BB-22GUC0-(USB
  6:  USB CD/DVD ROM:
  7:  USB FDD:
  8:  USB KEY:
```

Another cause for this message is that the master boot record itself can become corrupted. There is a link to a quick tutorial on how to fix a damaged MBR with an XP or Vista CD located here.

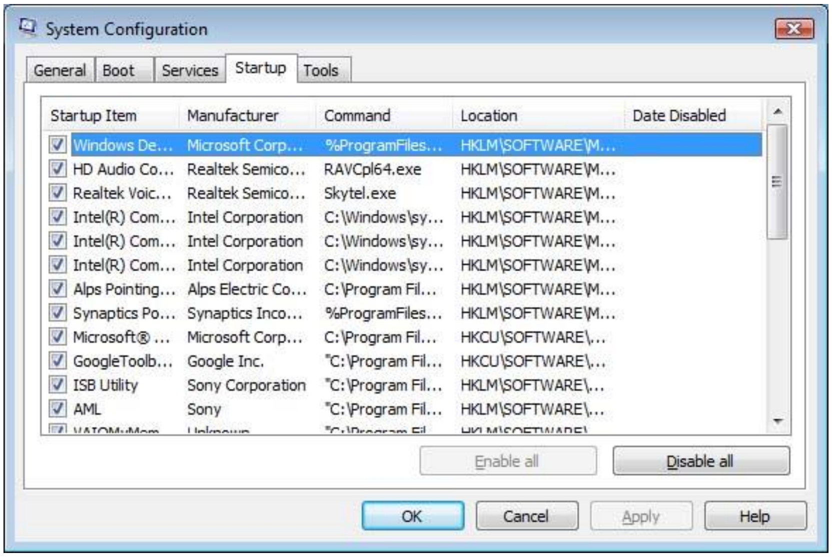
3. Computer is Slow:

A computer that runs at a snail's pace is quite annoying, especially when you have a lot of work to get done. Fortunately, many of the common causes are easily fixable.

A slow running computer is often due to viruses and spyware which are discussed below. Another cause can be programs running in the background. Many times when installing new software, by default they're designed to run when Windows starts. You can look in the tray at the bottom right of the screen to see all the installed software that's running. You can usually stop these from starting with Windows by either right-clicking on the program's icon in the tray and select its properties or options and choose not to have it begin at startup. Or open the entire program and go to the options/properties menu.

Another way to prevent programs from running at startup is to run msconfig.

To open msconfig in XP click start, run, type msconfig. In Vista click start, type msconfig in the "start search" text box right above the task bar (the program icon should appear in the white area above the text box), then either double click the icon or press enter. Go to the startup tab. There you will see the same programs that are in your tray. You have the choice of disabling them all (not wise, there is certain software that needs to run when Windows starts such as anti-virus) or individually selecting the ones you don't want to start by unchecking the box next to them. After making your selection(s) click apply. Your choices will go into effect the next time you start your computer.



Startup Item	Manufacturer	Command	Location	Date Disabled
☑ Windows De...	Microsoft Corp...	%ProgramFiles...	HKLM\SOFTWARE\M...	
☑ HD Audio Co...	Realtek Semico...	RAVCpl64.exe	HKLM\SOFTWARE\M...	
☑ Realtek Voic...	Realtek Semico...	Skytel.exe	HKLM\SOFTWARE\M...	
☑ Intel(R) Com...	Intel Corporation	C:\Windows\sy...	HKLM\SOFTWARE\M...	
☑ Intel(R) Com...	Intel Corporation	C:\Windows\sy...	HKLM\SOFTWARE\M...	
☑ Intel(R) Com...	Intel Corporation	C:\Windows\sy...	HKLM\SOFTWARE\M...	
☑ Alps Pointing...	Alps Electric Co...	C:\Program Fil...	HKLM\SOFTWARE\M...	
☑ Synaptics Po...	Synaptics Inco...	%ProgramFiles...	HKLM\SOFTWARE\M...	
☑ Microsoft® ...	Microsoft Corp...	C:\Program Fil...	HKCU\SOFTWARE\...	
☑ GoogleToolb...	Google Inc.	"C:\Program Fil...	HKCU\SOFTWARE\...	
☑ ISB Utility	Sony Corporation	"C:\Program Fil...	HKLM\SOFTWARE\...	
☑ AML	Sony	"C:\Program Fil...	HKLM\SOFTWARE\...	
☑ VAIOMyMom	Unknown	"C:\Program Fil	HKLM\SOFTWARE\	

Another common reason for a slow computer is not having enough RAM. Installing more can often help the problem.

4. Viruses/Spyware:

Viruses and spyware can not only slow down your computer, they can render it unusable. Furthermore, certain types of viruses and spyware can transmit your personal information to the attackers. You should always have antivirus running on your system. If you are looking for a good free option, I recommend Avast.

5. Limited Hard Drive Space:

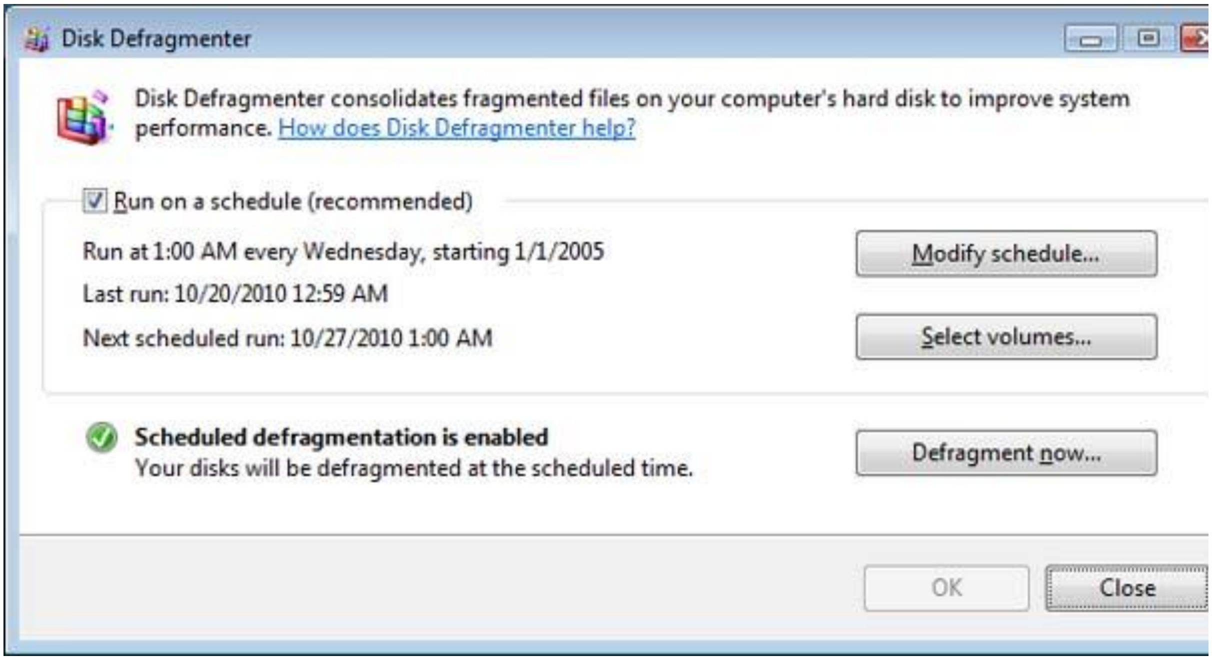
After a long period of time, most of our hard drives contain data we no longer need or that is left over by software not completely uninstalled eventually leading to a messy drive. Given the size of modern hard drives, this is rarely an issue anymore. In any event, if you are a clean freak like me, you may want to periodically clean house. Windows built-in Disk Cleaner tool is a good way to get rid of unwanted files, although there's plenty of other software available too. And of course, you can always add an additional hard drive if you need more storage space.

To open Disk Cleanup in XP or Vista click start -> Programs -> Accessories -> System Tools -> Disk Cleanup and follow the instructions.

6. Fragmented Hard Drive:

When a hard drive is brand new and you begin installing software or saving data, Windows tries to keep all the individual files intact, resulting in them being read extremely fast. But after a while you start deleting things. Well, each time something is deleted, it leaves "gaps" in your drive. Then when another program is installed or data saved, individual files are broken up and placed in these gaps all over the drive. This is what is known as a fragmented hard drive. When opening a file or program, the operating system has to scan the entire drive to find parts of files and put them back together, reducing read time. This why it can seem like forever for a file to open.

Defragmenting a hard drive is easy with Windows Disk Defragmenter. It scans your drive for split up files and reassembles them. To open In XP or Vista click -> Start -> Accessories -> System Tools -> Disk Defragmenter. Before using Disk Defragmenter I would suggest running Disk Cleanup first to eliminate unwanted data. As with Disk Cleanup, there are many other 3rd party defragmenting programs available.



Disk Defragmenter consolidates fragmented files on your computer's hard disk to improve system performance. How does Disk Defragmenter help?

☑ Run on a schedule (recommended)

Run at 1:00 AM every Wednesday, starting 1/1/2005

Last run: 10/20/2010 12:59 AM

Next scheduled run: 10/27/2010 1:00 AM

Scheduled defragmentation is enabled
Your disks will be defragmented at the scheduled time.

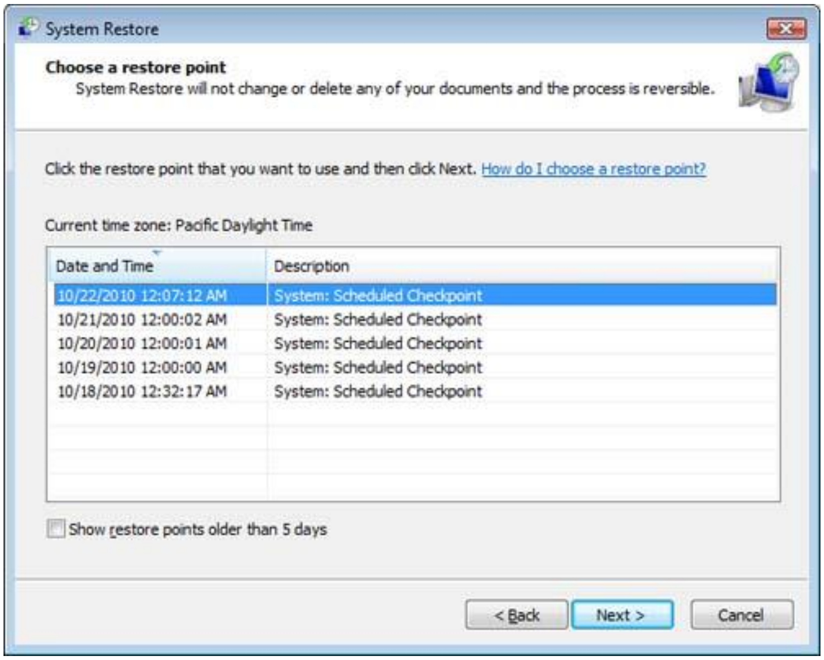
7. Non-Working Devices/Device Not Recognized:

If a device has stopped functioning or isn't recognized by Windows, remember to first check the simple things. Make sure cables and power are plugged in. With an internal component, turn off and unplug the machine. Remove the case door and make sure cables are firmly connected to the device and that add-on cards are seated in their slots. If all is OK, there may be a device driver issue. Device drivers are little pieces of software that allow hardware to work. Reinstall the device driver or download the latest version. Either go the manufacturer of the device or the company where you bought your computer. If still no success try uninstalling and reinstalling the device.

If the above doesn't produce any results, it is probably the device itself.

8. Problems After Installing New Software or Device Driver:

Of course you should first uninstall the software or driver. Or use System Restore to return your system to a previous working state. To open System Restore in XP or Vista click Start -> Programs -> Accessories -> System Tools -> System Restore.



System Restore

Choose a restore point

System Restore will not change or delete any of your documents and the process is reversible.

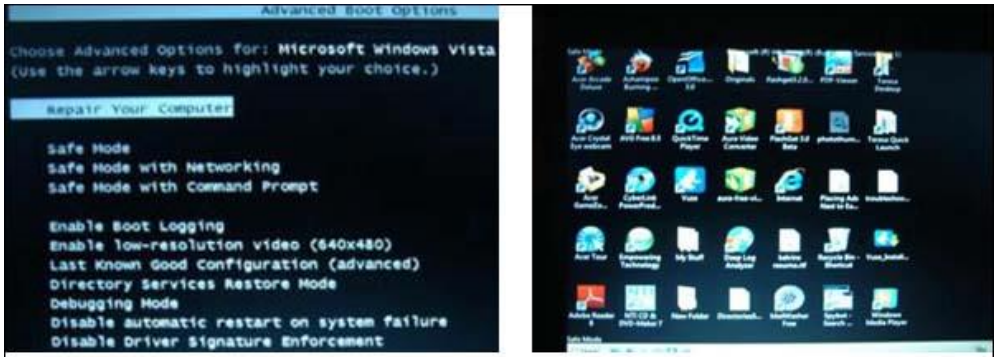
Click the restore point that you want to use and then click Next. How do I choose a restore point?

Current time zone: Pacific Daylight Time

Date and Time	Description
10/22/2010 12:07:12 AM	System: Scheduled Checkpoint
10/21/2010 12:00:02 AM	System: Scheduled Checkpoint
10/20/2010 12:00:01 AM	System: Scheduled Checkpoint
10/19/2010 12:00:00 AM	System: Scheduled Checkpoint
10/18/2010 12:32:17 AM	System: Scheduled Checkpoint

☐ Show restore points older than 5 days

There are times when new programs might freeze up your system. In this case try to see if you can boot to Safe Mode and then perform a restore. Safe Mode only loads the very basic devices and drivers needed for your system. To get to Safe Mode restart your system. When it begins to boot, continuously press the F8 key. A menu should appear that looks similar to the one on the left. Choose Safe Mode and press enter. After Windows loads you should get the screen on the right with a black desktop. Start System Restore like described above.



```
                    Advanced Boot Options
Choose Advanced Options for: Microsoft Windows Vista
(Use the arrow keys to highlight your choice.)

   Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement
```

Advanced Boot Options - Select Safe Mode

9. No Power:

The main culprit is usually the power supply unit (PSU). Make sure the power cord is securely plugged into the supply and the wall outlet. If so, you can buy a tester to see whether your PSU is putting out enough voltage.

Another cause could be a malfunctioning device. Turn off the computer and disconnect all devices. Reinstall each device one by one, turning on the computer after each device. Should your system not come on after installing a particular component, replace it.

If your system doesn't come on after reinstalling every device, you may have a motherboard or CPU problem.

Spontaneous Reboots:
A computer that reboots often (while you're in Windows or other operating system) is another indication of a bad power supply. See the first couple of sentences under No Power above.

Time Keeps Changing:
If you constantly have to set the time/date clock, that's the main symptom of a bad CMOS battery. Replace it. But just like any other battery it has to be the same size. Look at the number on your battery and buy one with the same number.

A **diagnostic program** is a software tool used to diagnose problems with a particular set of hardware devices. It can be used by a trained technician or by the owner of the device, to identify and resolve hardware issues.

Software

Sometimes abbreviated as **SW** and **S/W**, **software** is a collection of instructions that enable the user to interact with a computer, its hardware, or perform tasks. Without software, most computers would be useless. For example, without your Internet browser software, you could not surf the Internet or read this page. Without an operating system, the browser could not run on your computer. The picture shows a Microsoft Excel box, an example of a spreadsheet software program.

Hardware

Abbreviated as **HW**, **hardware** is best described as any physical component of a computer system that contains a circuit board, ICs, or other electronics. A perfect example of hardware is the screen on which you are viewing this page. Whether it be a monitor, tablet, or smartphone, it is hardware.

Without any hardware, your computer would not exist, and software could not be used.

The picture is a Logitech webcam, an example of an external hardware peripheral. This hardware device allows users to take videos or pictures, and transmit them over the Internet.

External hardware examples

Below is a list of external hardware or hardware found outside a computer.

- Flat-panel, monitor, and LCD
- Gamepad
- Joystick
- Keyboard
- Microphone
- Mouse
- Printer
- Projector
- Scanner
- Speakers
- USB thumb drive

Internal hardware examples

Below is a list of internal hardware or hardware found inside a computer.

- CPU (central processing unit).

- Drive (e.g., Blu-ray, CD-ROM, DVD, floppy drive, hard drive, and SSD).
- Fan (heat sink)
- Modem
- Motherboard
- Network card
- Power supply
- RAM
- Sound card
- Video card

What is the most common hardware included with a computer?

Below is a list of the most common hardware you'd likely find inside a computer or connected to a computer today (desktop computer or laptop).

- Processor (CPU)
- One or more fans and heat sink
- Motherboard that most likely has an integrated video card, sound card, and network card.
- For most desktop computers (especially gaming computers), a separate video card is used.
- RAM
- Hard drive

- Power supply
- Cables that connect internal components and external peripherals.
- Keyboard
- Mouse or touchpad with a laptop.
- Flat-panel, monitor, or TV for desktop computers and LCD as part of a laptop.

Error Log

Definition - What does *Error Log* mean?

In computer science, an error log is a record of critical errors that are encountered by the application, operating system or server while in operation. Some of the common entries in an error log include table corruption and configuration corruption. Error logs in many cases serve as extremely useful tools for troubleshooting and managing systems, servers and even networks.

Error logs for different applications, operating systems, networks or servers are set up in different ways. Some error logs are configured to capture every single error which occurs in the system, whereas some are designed to selectively store error information pertaining to specific error codes. Some error logs only capture certain information about the error, whereas others are programmed to capture all available information such as timestamp, system information, user location and user entry. In many cases, access to error logs need special administrative rights, as these would help as a security measure against providing access to unauthorized resources or users from seeing the error documentation or details.

Error logs are useful in many respects. In the case of servers and office networks, error logs track issues faced by users and help in root causes analysis of those issues. A network or system administrator can resolve errors more quickly and easily with the information available from the error logs. For webmasters, error log analysis provides information about the issues users encounter and can proactively resolve issues without anyone reporting on them. Error logs also could provide insights on hacking attempts, as most hacking attempts on systems and servers result in error or have a high probability of being captured in error logs as the hackers attempt to compromise the system.

Are you experiencing problems with PC-attached peripherals, such as your mouse, keyboard, webcam, or another accessory? Whether you’re using legacy or USB peripherals, problems could arise at some point. In some cases, peripherals stop working following an update. The good news is that fixing these common problems with PC peripherals is often simple. A shortcut is to use the Windows troubleshooter. The

interface may vary from one Windows operating system to another, but the purpose is the same.
Click the Start button, open the Hardware and Devices troubleshooter, and then select Troubleshooting. This will automatically check your computer for any problems with hardware and other devices.

Common PC Peripheral Problems and How to Solve Them

The first step is to always check the hardware. The cables may be damaged or the USB hub you're using between your PC and the peripheral may not have power.

#1: Problems with a port

If the attached peripherals suddenly stop working, check the Device Manager to see if the port itself is to blame. A red exclamation mark (!) means there's an error with the port.
Delete a device from the Device Manager and then reboot your computer. Once your PC is up and running again, install the device driver.

#2: Problems with the port connectors

Especially with PS/2 ports, one or two of those holes could be clogged with dust, causing a loss in connection with the pins. The same thing could happen when the pins on the peripheral connector are damaged.
A USB port can get damaged, too, resulting in no power or connection. A solution would be to use another USB port.

#3: USB standards don't match

Newer USB devices may not run on old USB ports. Most of them would need a 3.0 cable for high-speed processing. If the USB port and device are incompatible, attached peripherals will not work.

#4: Error with wireless keyboard or mouse

Common Problems with PC Peripherals

Wireless peripherals often rely on the IR or RF controller to work and communicate with a computer. If it doesn’t work the first time you use it, you could be using an old operating system. Most wireless PC peripherals need a newer OS Service Pack. So, if you’re still using Windows 95 OS or older, an upgrade will fix the problem.

If you’re using the current operating system and the wireless keyboard and mouse still don’t work, the problem may be an interference with the line of sight or a weak battery. Use the peripherals on other PCs to help identify the cause of error.

If the wireless device has a reset button, use it to reset the device and refresh the connection. It would also help if you unplug the USB wireless receiver and leave it off for about 10 seconds. This will help reestablish the wireless connection once you plug the receiver back into the port.

#5: PS/2 keyboard and mouse not working

See that the device is plugged in the correct port. If the port and cable are color-coded, the keyboard cable should go into the purple-colored port and the mouse into the green-colored port. Color coding can vary. Try to switch them up and see if doing so helps fix the problem. Follow the same process if the PS/2 connectors are identical in color and you need to identify which one is designated for the keyboard and the mouse.

If the cables are on the right parts and the peripherals still don’t work, try to use other devices. The keyboard or mouse may need replacement.

#6: Blocked keys or sensors

Dirt blocking the keys or sensors prevents PC peripherals from responding to commands. Regardless of how much you click on a mouse or press a key, nothing will happen if contact is not established.

#7: Input devices stop working after updates

Following an operating system or software update, one or two of your attached PC referrals may no longer work. There are several ways to restore a device's functionality.

- **Switch USB ports**

Doing so will force your computer to recognize a device. A computer system usually recognizes a device based on their location or the specific USB port where the device was attached before any updates were made. If the system thinks nothing has changed, it will not reload drivers, resulting in peripherals not working. Thus, the need to switch USB ports.

- **Start in safe mode**

In some cases, a driver in the cache will not load properly after an update. The result is a broken mouse and keyboard … or so it might appear. With a bit of a system purge in safe mode, the boot will reload drivers and load them properly.

- **Reset the PRAM**

During a firmware update, the PRAM settings of your computer, which include peripheral devices, video settings, startup disk, and audio volumes, may be reconfigured. Reset the PRAM to fix the problem.
Reboot the system and then press and hold down the option-command-P-R keys at the same time. Wait for your computer to reset and chime a couple of times at reboot before you release the keys.

- **Power cycle the entire system**

Faulty settings may occur after an update. Remove a peripheral device from your computer and leave it off for a few minutes. For better results, shut down your computer as well and power cycle it. After 5 to 10 minutes, turn the computer back on and then plug the attached peripherals back in.

#8: Mouse and keyboard stopped working when the printer is turned on

- **Ensure efficient power**

This could happen when the USB ports for the keyboard and mouse receive too little power to work because the printer is hogging all of it. Make sure not to connect the printer to a USB hub that is shared by the keyboard and mouse.

Another solution is to plug the devices into different USB ports. Attached peripherals can go at the back of the computer while the printer is plugged in at the front.

- **Fix interference**

Do your keyboard, mouse, and printer all use a wireless connection? They could be interfering with one another, even if one is using radio frequency while the other relies on Bluetooth.
To avoid conflict and establish different frequencies for different devices, switch off the keyboard and mouse. When you switch them back on, they will be forced to reconnect to your computer using a free frequency.

- **Check driver compatibility**

Conflicts between drivers could cause problems with different devices. Communication with your operating system will be effected and will result in devices not working properly. Open Device Manager and check that drivers for peripherals and the printers are updated.
Double click on a device and open the Properties windows. Under Driver tab, check if the option to Update Driver is available. This means a newer version of a driver is available.

- **Reinstall devices**

If you've done all the steps above and the problem persists, you may need to reinstall devices to resolve the issue.

1. Remove the PC-attached peripherals from Device Manager.
2. Any related software must be uninstalled from your computer.
3. Restart the system.
4. Switch on the printer and see that it is connected to your computer and working properly.
5. Reconnect the keyboard and mouse like you're using them for the first time. This reinstalls the peripherals and ensures there are no conflicts.

If you're still having issues with these common problems with PC peripherals, check out our guide on how to reset your Windows 10 computer here.

An Ultimate Guide to Hard Drive Problems, Solutions and Tips

"Something is wrong with my computer's hard drive and I can't seem to boot the system properly. How can I fix this hard disk problem and access my files again?"

It doesn't matter if you use a Windows or a Mac: your system's hard drive is certainly one of the most important parts of it. A corrupt or malfunctioning hard disk can affect the entire functioning of your computer and cause several other issues. The hard disk can fail after accumulating bad sectors over a long period of time or crash suddenly. Gradual failure of a hard disk is hard to detect since its symptoms mimic those of other computer issues like viruses and malware. These symptoms usually are file corruption and deterioration of PC speed. Corruption of hard disk usually results from the increase in the number of bad sectors that pile up and eventually disable the hard disk.

Hard disk failure can be sudden, complete, gradual, or partial in nature, and most times data recovery is a possibility. If you have also encountered a hard disk error like this, then don't worry. We are here to help you with a complete guide on hard drive problems and solutions that will help you resolve all kinds of unwanted situations. Let's get it started from the basics and gradually unravel the common hard drive problems faced by users these days.

Part 1: A Brief Overview of Hard Drives on Computers

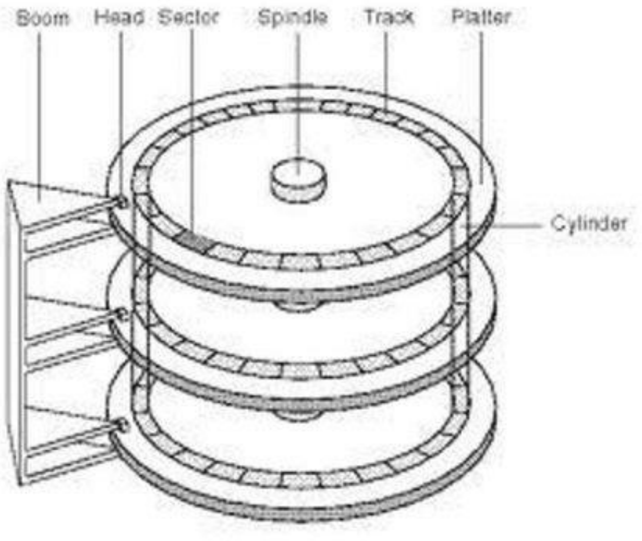
Before we get into the details and troubleshoot hard drives, it is important to cover the basics. For instance, in order to work on computer problems and solutions, you need to know what a hard disk is and how it functions.

1. What is a hard drive?

The history of hard drives is probably as old as computers as they were first introduced by IBM in 1956. Ideally, a hard drive is used to store all kinds of information on a system (if it is an internal drive). It is considered as non-volatile storage, which is different from a computer's primary memory (RAM). An internal drive is connected to the system's motherboard as well as a power socket. Nowadays, external hard disks based on flash memory are extensively used as well.

2. How does a hard disk work?

Since magnetic hard disks are still the most commonly used variety of drives, we will consider its example to explain how it works. Ideally, it is a cylindrical unit that consists of various magnetic plates. Each plate is divided into numerous tracks and sectors. The plate consists of minute units that are used to store data in a binary form (0 or 1). A spindle is located in the middle of the disk that rotates the unit.

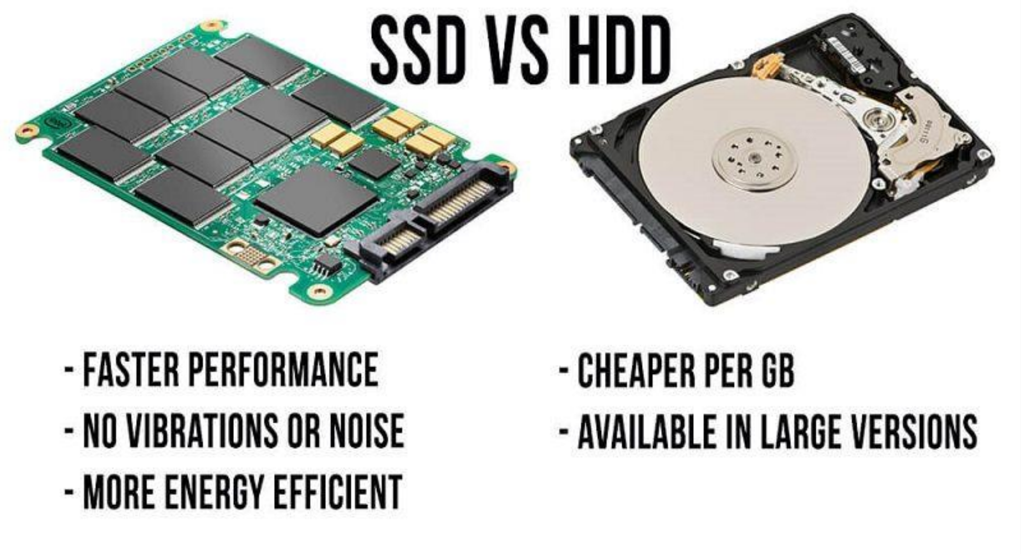


Now, whenever we wish to access or store data, a read/write head is moved to a particular area. The spindle rotates the drive and the head either reads or writes the data on it.

3. What are the different types of hard disks?

Ideally, hard disks can be distinguished into different categories on the basis of numerous parameters like these:

On the basis of technology: Mostly, hard disks can either be HDD (Hard Drive Disk) or an SSD (Solid State Drive). HDDs are based on magnetic disks, have slow processing, and are cheaper. Since they have a read/write head, they produce a sound while operating. On the other hand, SSDs are based on flash memory and does not produce any sound. They are safer, faster, and more expensive.



On the basis of use: Hard disks can also be categorized as internal or external. An internal drive is the native storage of the system which is placed inside the unit. An external drive is an extended storage unit that is used to take a backup or transfer data. It can be connected to the system via a USB cable.

On the basis of size and format: Needless to say, hard disks can be of different sizes ranging from gigabytes to terabytes and of various disk formats.

4. Which type of hard drive is the best?

Since Solid State Drives (SSDs) are newer and more advanced, they are considered better than HDDs. Not only are they faster, but they are also more secure than a magnetic disk. This is because the data stored in an HDD can't be tampered with using a magnet. Also, its speed and overall performance are better than an HDD.

Part 2: How to tell if a Hard Drive is failing?

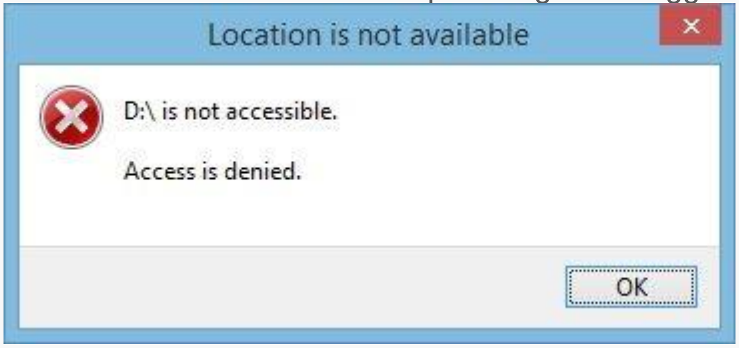
Before a hard drive fails entirely, it gives us certain signs that we should not ignore. Here are some of the major symptoms of hard drive problems that we should take seriously.

Sign 1. Hard drive clicking sound

A lot of times, users complain of a peculiar clicking sound made by the hard drive's head. It usually happens when there is an inconsistent power supply for the disk or physical damage on one of the plates.

Sign 2. Access Denied

When users try to access the disk or a partition, they often get the access denied prompt. This means that the system can't locate the hard disk or a particular partition in it. A loose connection or corrupt storage can trigger this event.


Location is not available

D:\ is not accessible.

Access is denied.

Sign 3. Repeated crashing

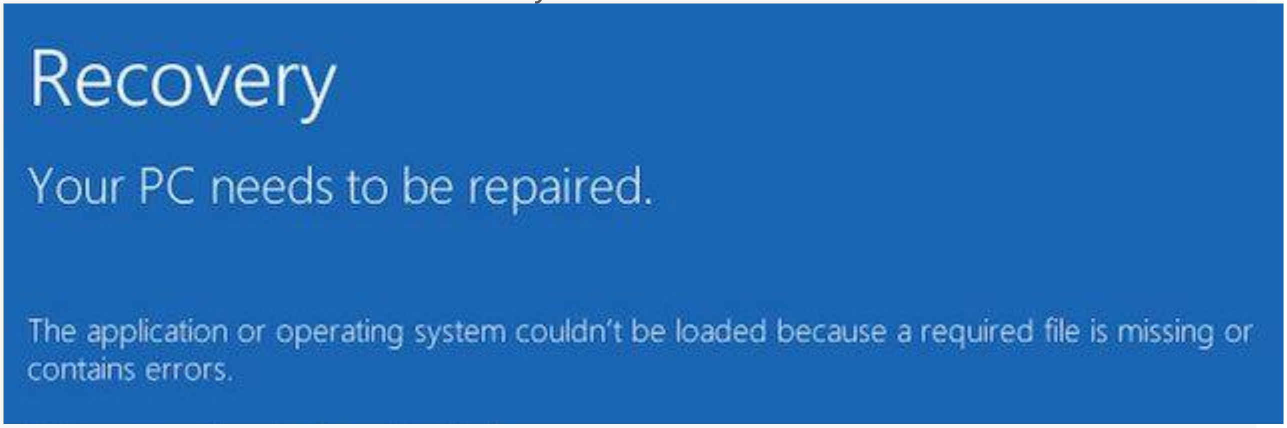
If the computer or the hard drive crashes repeatedly, then consider it as one of the vital symptoms of a bad hard drive. The disk can stop working out of the blue anytime.

Sign 4. Inaccessibility of data

There are times when the data stored in the disk is lost or inaccessible. This is both, a hard drive problem as well as a symptom for further issues.

Sign 5. OS can't be loaded

While booting the system, you might get a recovery screen stating that the system can't load/locate certain files. This is directly related to a hard drive malfunction.



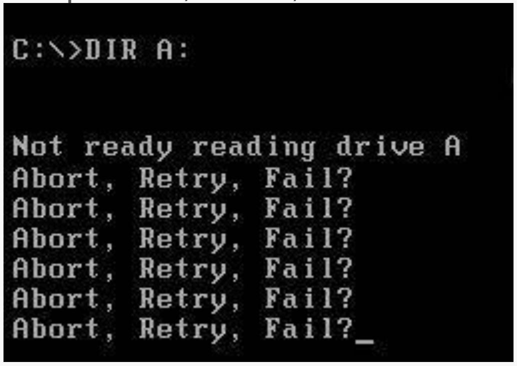
Recovery

Your PC needs to be repaired.

The application or operating system couldn't be loaded because a required file is missing or contains errors.

Sign 6. Abort, Retry, Fail?

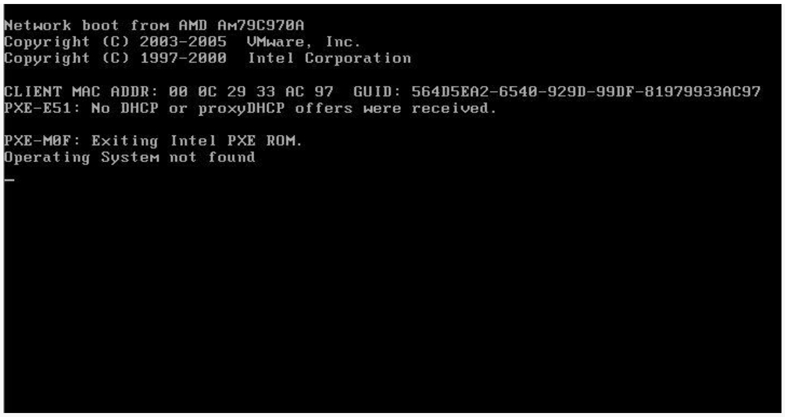
This is again one of the common hard disk failure symptoms as it occurs when the system can't locate the entire OS or some crucial files. It means the system has aborted an operation, retried, and failed.



```
C:\>DIR A:


Not ready reading drive A
Abort, Retry, Fail?
Abort, Retry, Fail?
Abort, Retry, Fail?
Abort, Retry, Fail?
Abort, Retry, Fail?
Abort, Retry, Fail?_
```

Sign 7. Sector not found

Sometimes, the hard disk can have a bad sector or two. In this case, your computer will inform you the same by displaying a similar warning message. This can be major **hard drive problems symptoms** that you should not ignore.



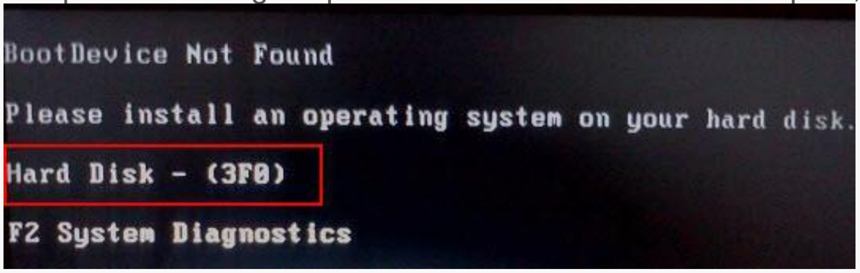
```
Network boot from AMD Am79C970A
Copyright (C) 2003-2005  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 33 AC 97  GUID: 564D5EA2-6540-929D-99DF-81979933AC97
PXE-E51: No DHCP or proxyDHCP offers were received.

PXE-M0F: Exiting Intel PXE ROM.
Operating System not found
_
```

Part 3: Top 10 Hard Drive Problems and Solutions

There are different hard drive problems that users can encounter, resulting in its malfunction in numerous ways. Let's uncover some of these common hard drive issues here.

Disk Error 1. Hard Drive Not Found

Chances are that while turning on your system, you might get the "Hard Drive Not Found" error on the screen. This makes your system standstill as it will not respond to most of the usual commands. The hard disk problem occurs when the internal cable connecting it has been damaged or is loose. Water or physical damage can also lead to this problem. A logical partition can also be lost or corrupted, in this case.



```
BootDevice Not Found

Please install an operating system on your hard disk.

Hard Disk - (3F0)

F2 System Diagnostics
```

Solution 1: Perform a hard reset

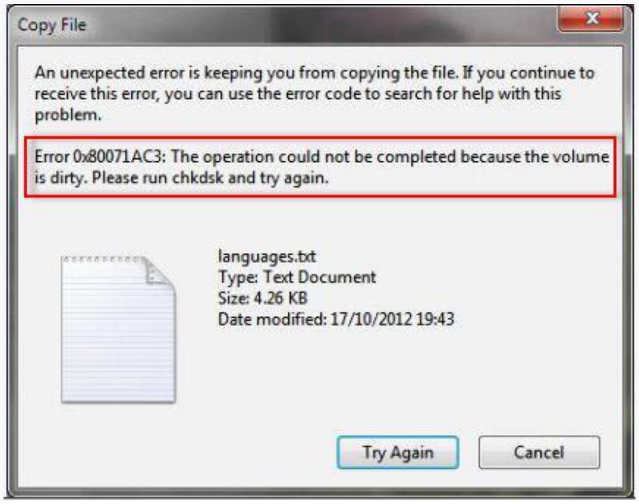
This is the easiest way to fix this hard drive malfunction issue. Simply turn your system off and remove its power cord or battery. Also, disconnect all kinds of peripheral devices from it and press the Power button for 15 seconds. After waiting for a while, connect the battery/power cord (not the peripheral device) and turn it on.

Solution 2: Check for physical damage

While this might be a tedious job, you can consider opening up your system and checking the hard drive connection. If the connection is loose, then you can visit a professional as it would require soldering.

Disk Error 2. Volume is Dirty (Hard Drive Error 0x80071ac3)

As the name suggests, this error depicts that either the entire disk or a volume has been corrupted. When the problem occurs, users get an error like this with a hexadecimal code. The problem can happen with the internal as well as the external hard drive. A bad sector on your hard drive or an unexpected shutdown is the two primary causes of this hard disk problem. If it is an external drive, then an unsupported file system or driver can also be a reason for this.



Copy File

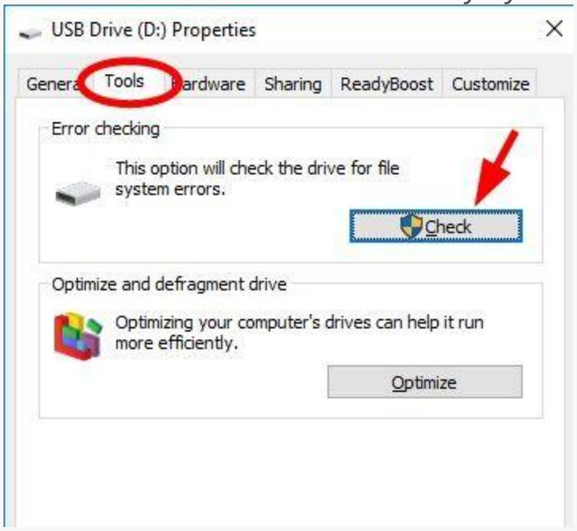
An unexpected error is keeping you from copying the file. If you continue to receive this error, you can use the error code to search for help with this problem.

Error 0x80071AC3: The operation could not be completed because the volume is dirty. Please run chkdsk and try again.

languages.txt
Type: Text Document
Size: 4.26 KB
Date modified: 17/10/2012 19:43

Solution 1: Check System Errors

If a disk is not functioning in an ideal manner, then you should perform an automatic system check. To do this, just right-click its icon and go to its Properties. Under the Tools tab > Error Checking section, click on the "Check" button. Follow the simple on-screen instructions to resolve any system error.



This option will check the drive for file system errors.

Optimizing your computer's drives can help it run more efficiently.

Solution 2: Reconnect the external device

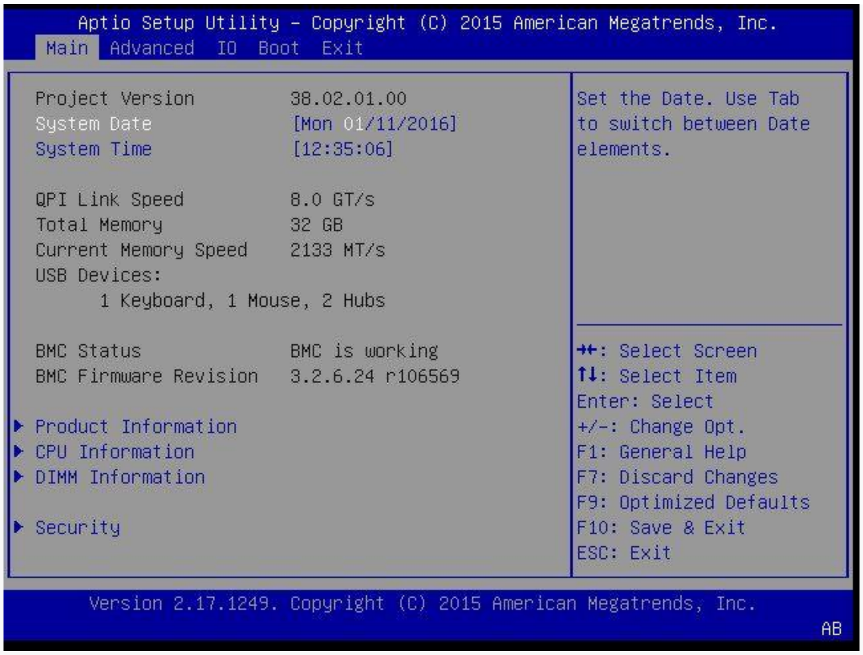
Most of the people get this error while using an external hard drive, USB drive, or an SD card. In this case, simply remove the external drive and turn off your system. Restart it and connect the drive again to check whether you get the error back or not.

Disk Error 3. Can't Boot the System

Since the internal hard drive also stores the firmware and the operating system, its failure can also result in the booting of your system. There are all kinds of prompts that users get in this case when the system can't boot. It happens when there is a change in the BIOS settings or the essential system files have been lost. The partition where the operating system has been installed can also get corrupt, resulting in this computer problem.

Solution 1: Restore default BIOS settings

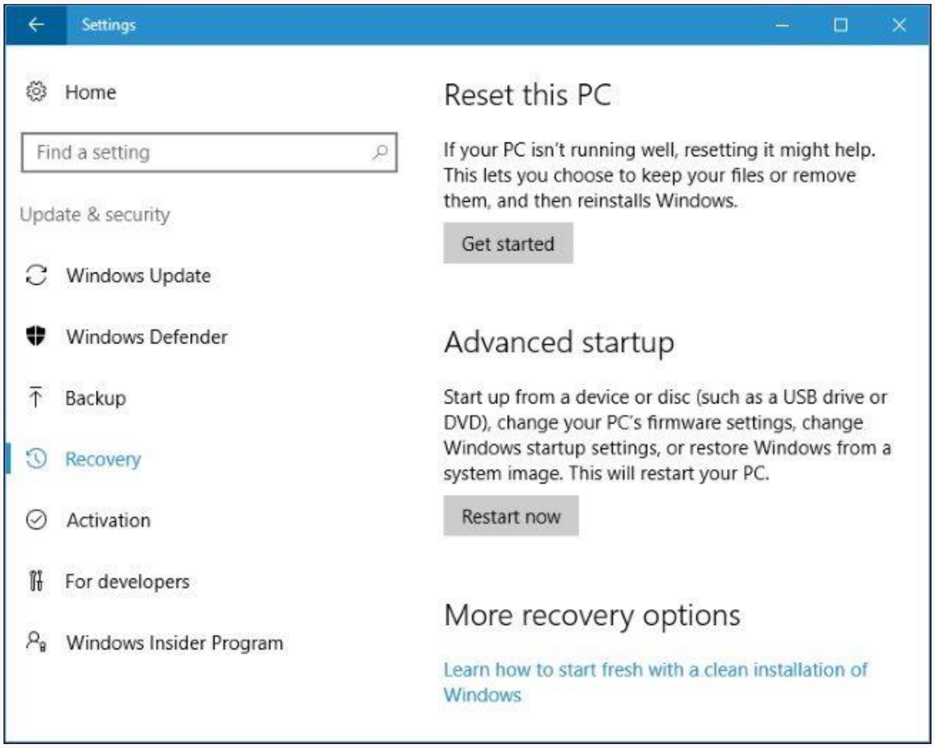
If there is an issue with your system's BIOS settings, then this will fix it. Turn on your computer and keep pressing the BIOS key, which can be F10, F12, F2, DELETE, etc. Once you enter the BIOS window, press F9 to restore the default settings. Exit it and **restart your system** now.



```
      Aptio Setup Utility – Copyright (C) 2015 American Megatrends, Inc.
   Main  Advanced  IO  Boot  Exit

   Project Version         38.02.01.00              Set the Date. Use Tab
   System Date             [Mon 01/11/2016]         to switch between Date
   System Time             [12:35:06]               elements.

   QPI Link Speed          8.0 GT/s
   Total Memory            32 GB
   Current Memory Speed    2133 MT/s
   USB Devices:
         1 Keyboard, 1 Mouse, 2 Hubs

   BMC Status              BMC is working           →←: Select Screen
   BMC Firmware Revision   3.2.6.24 r106569         ↑↓: Select Item
                                                    Enter: Select
 ▶ Product Information                              +/-: Change Opt.
 ▶ CPU Information                                  F1: General Help
 ▶ DIMM Information                                 F7: Discard Changes
                                                    F9: Optimized Defaults
 ▶ Security                                         F10: Save & Exit
                                                    ESC: Exit

        Version 2.17.1249. Copyright (C) 2015 American Megatrends, Inc.
                                                                        AB
```

Solution 2: Perform an advanced startup

You can also take the assistance of a bootable media or a Windows installer to startup your system. Firstly, go to Windows Settings > Recovery > Advanced Setup and click on the "Restart Now" button. Also, connect a Windows CD/DVD or a bootable media to your system. This will let you reinstall Windows on the system or boot it from another media.



Settings

Home

Find a setting

Update & security

Windows Update

Windows Defender

Backup

Recovery

Activation

For developers

Windows Insider Program

Reset this PC

If your PC isn't running well, resetting it might help. This lets you choose to keep your files or remove them, and then reinstalls Windows.

Get started

Advanced startup

Start up from a device or disc (such as a USB drive or DVD), change your PC's firmware settings, change Windows startup settings, or restore Windows from a system image. This will restart your PC.

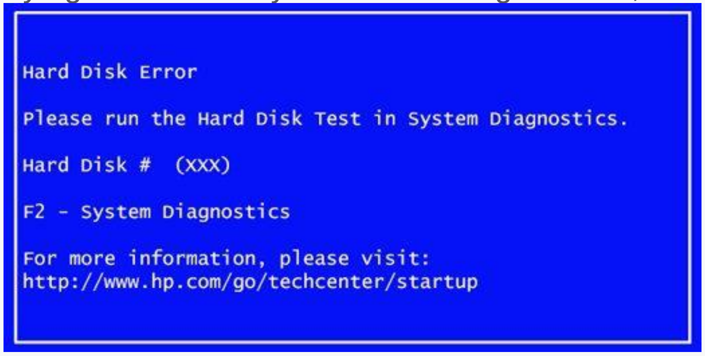
Restart now

More recovery options

Learn how to start fresh with a clean installation of Windows

Disk Error 4. Corrupted Hard Disk (Hard Disk #(XXX) Error)

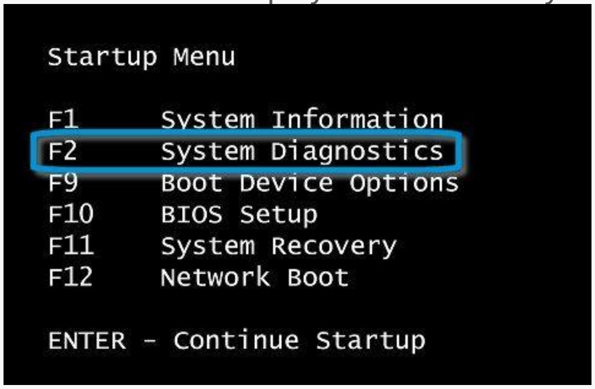
As much as you try to avoid it, chances are that your hard disk can get corrupt unexpectedly. The error mostly occurs in HP systems, but even PCs from other manufacturers can also undergo the same. A malware attack on the system, a corrupted sector, or a bad program can be a major trigger for this. Also, if your system is trying to access any file that no longer exists, it can lead to this error.



```
Hard Disk Error

Please run the Hard Disk Test in System Diagnostics.

Hard Disk #  (XXX)

F2 - System Diagnostics

For more information, please visit:
http://www.hp.com/go/techcenter/startup
```

Solution: Perform a Hard Drive diagnostic test

Since this hard disk error is mostly associated with HP systems, we will consider its example to troubleshoot hard drives. In other systems, the respective key would be different. To fix this, just restart your system and press F2 to run System Diagnostics. The screen will display the relevant key to do it.

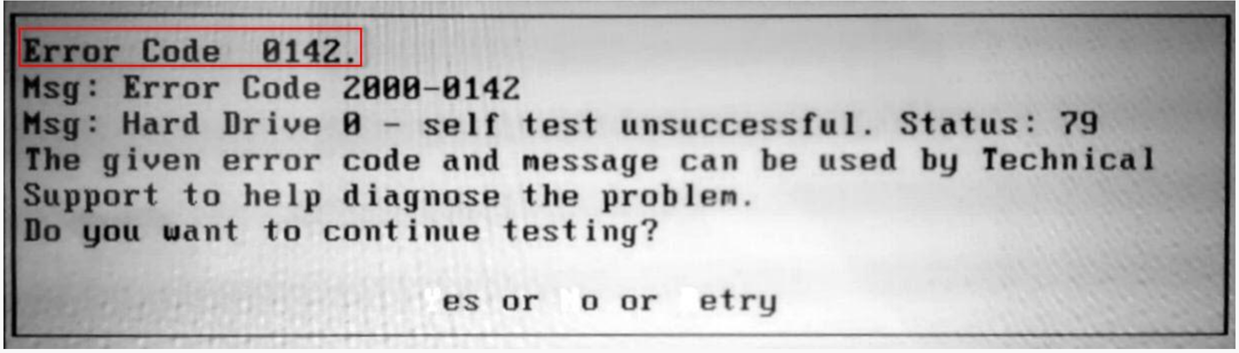


```
Startup Menu

F1      System Information
F2      System Diagnostics
F9      Boot Device Options
F10     BIOS Setup
F11     System Recovery
F12     Network Boot

ENTER - Continue Startup
```

As the diagnostic window will open, choose to perform Component Tests and select your Hard Drive from the available options. Confirm your choice and wait for a while as the system will run a thorough diagnostic and tries to fix this problem.

Disk Error 5. Hard Drive Error 0142

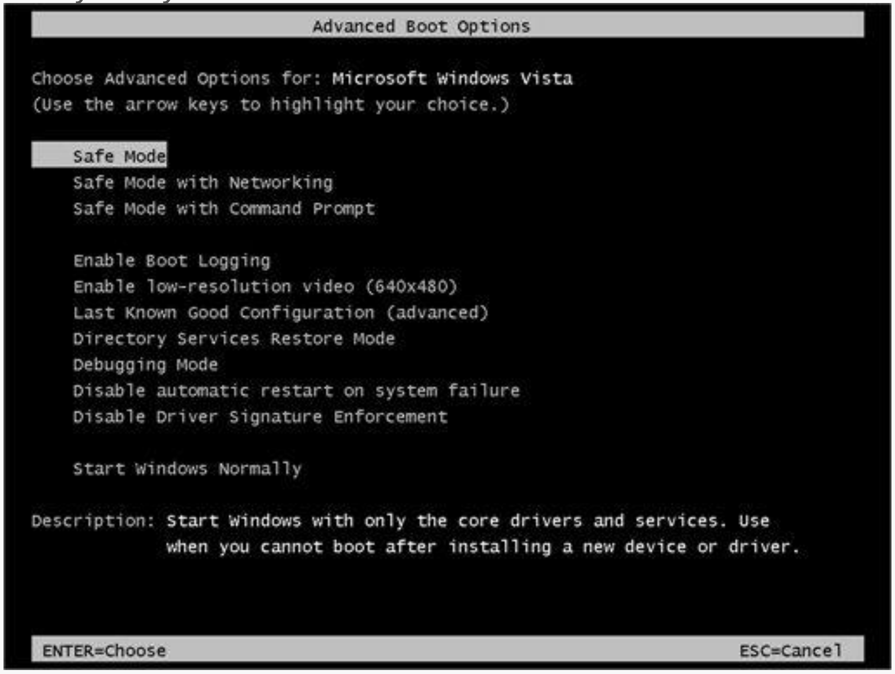
This is categorized as a major hard disk error as it depicts that the disk has failed to load the booting or system files. You might have to run a thorough diagnostic to fix this. If not, then you can consider resetting the system. The hard drive error mostly occurs due to a corrupted sector or a firmware related issue. You might have accidentally deleted a crucial system file as well, leading to the inaccessibility of certain OS components.



```
Error Code  0142.
Msg: Error Code 2000-0142
Msg: Hard Drive 0 - self test unsuccessful. Status: 79
The given error code and message can be used by Technical
Support to help diagnose the problem.
Do you want to continue testing?

                    es or  o or  etry
```

Solution 1: Restart system in safe mode

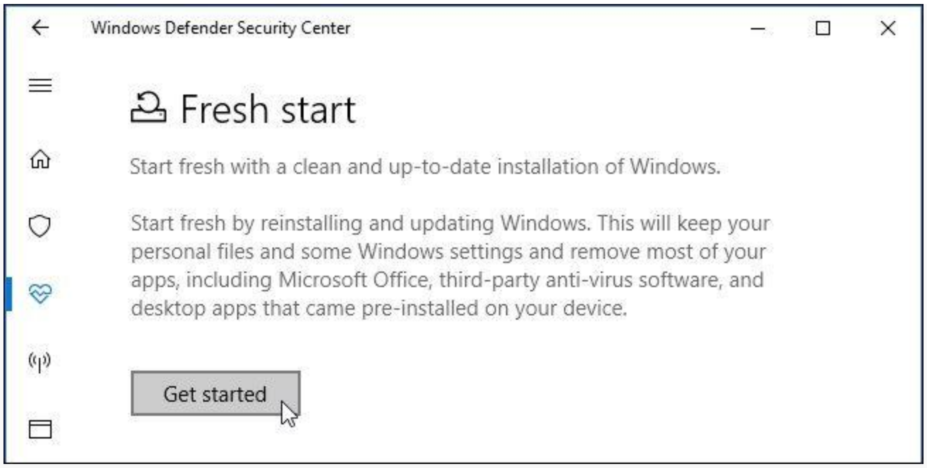
If a particular program or application has caused this hard disk problem, then you can consider restarting it in the safe mode. To do this, just restart your system and press F8 a few times to enter its advanced boot options. The key might differ from one version to another. Use the arrow keys to select the "Safe Mode" option and press enter. This will boot your system in the safe mode.



```
                        Advanced Boot Options

Choose Advanced Options for: Microsoft Windows Vista
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video (640x480)
    Last Known Good Configuration (advanced)
    Directory Services Restore Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement

    Start Windows Normally

Description: Start Windows with only the core drivers and services. Use
             when you cannot boot after installing a new device or driver.


 ENTER=Choose                                              ESC=Cancel
```

Solution 2: Give your system a fresh start

This is relatively a newer feature that is available in Windows 8 and 10. Ideally, it is equivalent to resetting a computer and will automatically remove all the installed programs and applications from it. Simply go to Windows Settings > Windows Defender & Security Settings > Device Performance and health. Go to the "Fresh Start" option here and get things started. Follow a simple click-through process to reset your system and get rid of any malicious entity.



Fresh start

Start fresh with a clean and up-to-date installation of Windows.

Start fresh by reinstalling and updating Windows. This will keep your personal files and some Windows settings and remove most of your apps, including Microsoft Office, third-party anti-virus software, and desktop apps that came pre-installed on your device.

Disk Error 6. Data Loss from a Corrupt Hard Drive

The hard drive is capable of storing a large amount of data which can be accessed at any time. However, sometimes you risk losing the important data contained in them because of failure or corruption of the hard disk. If an entire drive or a partition/sector has been corrupted, then it will automatically delete your saved files.

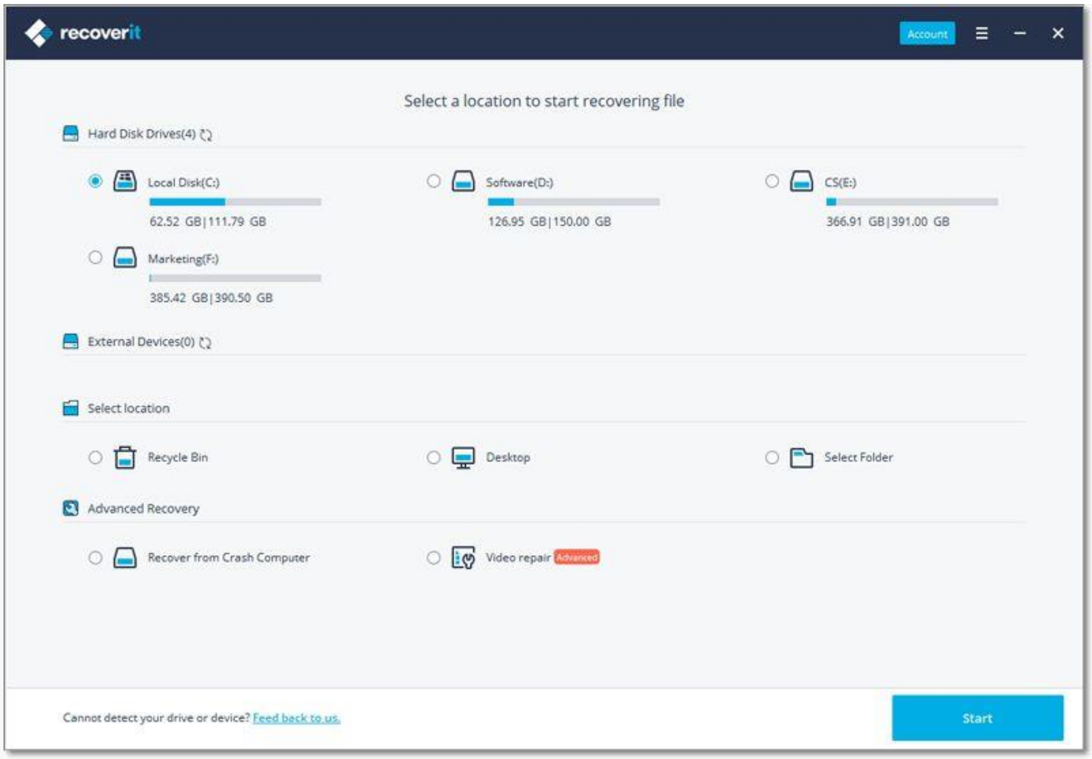
There can be numerous reasons for causing data loss on your system. Corrupt storage, a faulty program, bad sector, malware attack, or any other disk-related issue can trigger it. You can also accidentally format or delete your data as well. While there are hardly any native solutions for this, you can try a dedicated third-party data recovery tool.

Solution: Use Recoverit Data Recovery

It doesn't matter what kind of data loss scenario you are facing, you would be able to move past it using **Recoverit Data Recovery**. It is one of the most advanced data recovery tools available for both Windows and Mac. The application is easy to use and has the highest recovery rates in the industry. You can recover your lost data not only from Windows/Mac's internal hard disk but also from external sources like USB drive, SD card, etc. All you need to do is follow these steps after downloading Recoverit on your system.

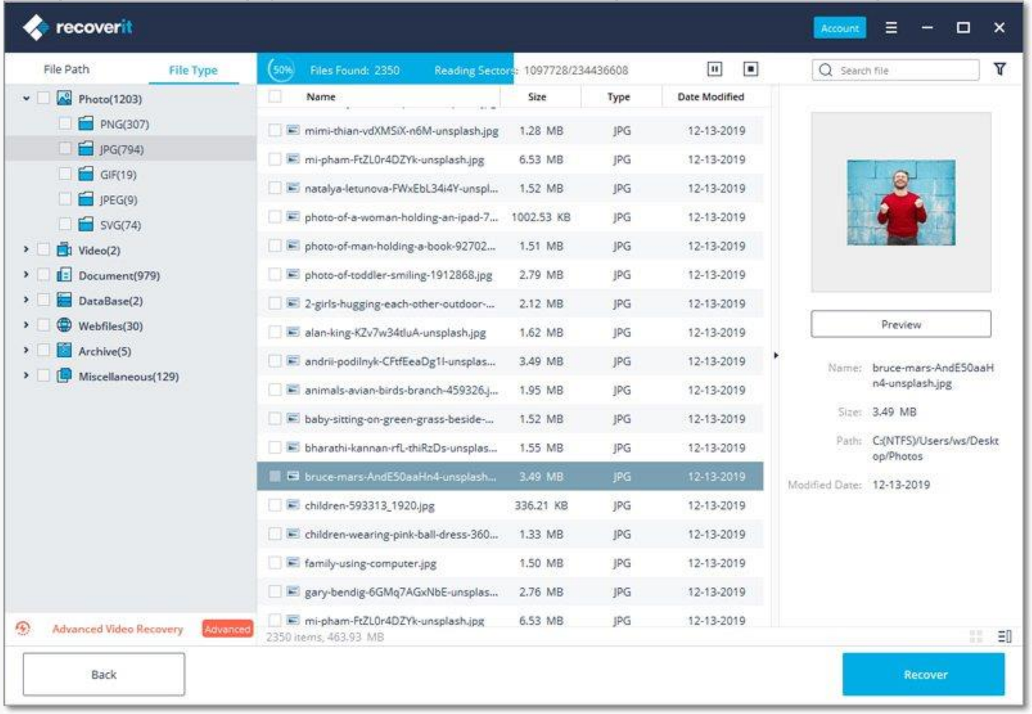
Step 1: Select where to scan

Firstly, launch the Recoverit Data Recovery application on your system and select a location to scan. This can be your entire drive or a partition/folder in it.



Step 2: Scan the hard drive

As soon as you click on the "Start" button, the application will scan the selected drive or the partition. Simply wait for a while for the process to be completed successfully.



50% Files Found: 2350 Reading Sectors: 1097728/234436608

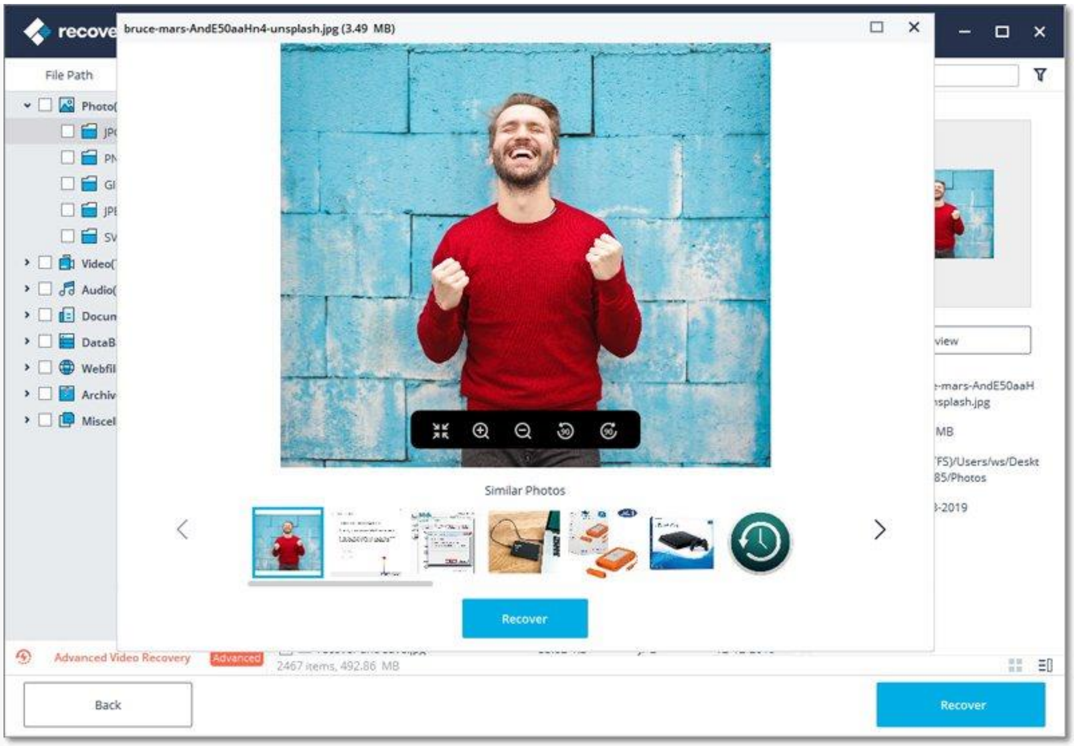
Name	Size	Type	Date Modified
mimi-thian-vdXMSiX-n6M-unsplash.jpg	1.28 MB	JPG	12-13-2019
mi-pham-FtZL0r4DZYk-unsplash.jpg	6.53 MB	JPG	12-13-2019
natalya-letunova-FWxEbL34i4Y-unspl...	1.52 MB	JPG	12-13-2019
photo-of-a-woman-holding-an-ipad-7...	1002.53 KB	JPG	12-13-2019
photo-of-man-holding-a-book-92702...	1.51 MB	JPG	12-13-2019
photo-of-toddler-smiling-1912868.jpg	2.79 MB	JPG	12-13-2019
2-girls-hugging-each-other-outdoor-...	2.12 MB	JPG	12-13-2019
alan-king-KZv7w34tluA-unsplash.jpg	1.62 MB	JPG	12-13-2019
andrii-podilnyk-CFtfEeaDg1I-unsplas...	3.49 MB	JPG	12-13-2019
animals-avian-birds-branch-459326.j...	1.95 MB	JPG	12-13-2019
baby-sitting-on-green-grass-beside-...	1.52 MB	JPG	12-13-2019
bharathi-kannan-rfL-thiRzDs-unsplas...	1.55 MB	JPG	12-13-2019
bruce-mars-AndE50aaHn4-unsplash...	3.49 MB	JPG	12-13-2019
children-593313_1920.jpg	336.21 KB	JPG	12-13-2019
children-wearing-pink-ball-dress-360...	1.33 MB	JPG	12-13-2019
family-using-computer.jpg	1.50 MB	JPG	12-13-2019
gary-bendig-6GMq7AGxNbE-unsplas...	2.76 MB	JPG	12-13-2019
mi-pham-FtZL0r4DZYk-unsplash.jpg	6.53 MB	JPG	12-13-2019

2350 items, 463.93 MB

Name: bruce-mars-AndE50aaHn4-unsplash.jpg
Size: 3.49 MB
Path: C:(NTFS)/Users/ws/Desktop/Photos
Modified Date: 12-13-2019

Step 3: Restore your data

In the end, the application will let you preview the files that it has extracted during the process. You can select the date of your choice and click on the "Recover" button to save it. Make sure you save it to a trusted location (and not the corrupt hard disk again).



Disk Error 7. Corrupted Files

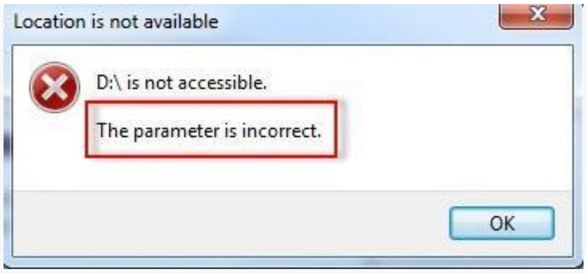
Corruption of system files usually occurs when the system shuts down suddenly, making it impossible for you to access your hard drive and thus your system. Some of the reasons for the corruption of the system files include power surges, use of malicious programs, accidental closure of a running program, and improper shutting down of the PC.

Solution: Close programs before PC shutdown

The solution to this problem is to make sure that you close down all programs that are running before commencing to shut down your computer. Moreover, when shutting down the computer, you must do so in a standard manner. In addition to this, you should avoid installing malicious programs on your hard drive and keep cleaning it regularly so that no unwanted programs remain there for long.

Disk Error 8. The Parameter is Incorrect

If you are trying to connect an external hard drive to your system, then you might get this error message. Subsequently, it won't let you access the data that is stored in your connected disk. An incompatible file system on the hard drive or physical damage can trigger this. If the disk is damaged, then it can also display the hard drive error.


Location is not available

D:\ is not accessible.

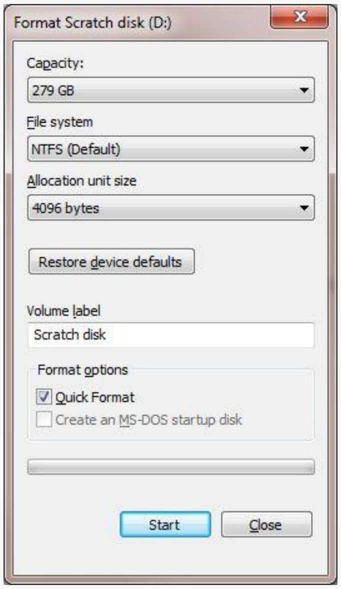
The parameter is incorrect.

Solution 1: Check USB port and drive

Mostly, a damaged port, cable, or the drive can cause these hard drive issues. Make sure that the device is in a working condition and the USB port is not damaged. Clean it thoroughly of any debris or dirt and reconnect the external hard disk to check its connection.

Solution 2: Format the drive

If the hard drive's disk format or file system is not compatible with your system, then it can also trigger this hard disk problem. To fix this, you can just format the drive. Simply connect it to your system, open My Computer, and right-click the hard drive's icon. Go to the "Format" option and select the file system to a compatible format (like NTFS). Click on the "Start" button to wipe the existing data on the drive and reset its file format.


Format Scratch disk (D:)

Capacity: 279 GB

File system: NTFS (Default)

Allocation unit size: 4096 bytes

Volume label: Scratch disk

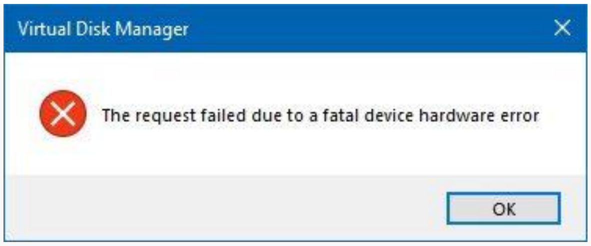
Format options

☑ Quick Format

□ Create an MS-DOS startup disk

Disk Error 9. The Request Failed Due to Fatal Device Hardware Error

This is a fatal error that users get while working on an internal or external hard drive. While it is mostly linked to a hardware issue related to a device, sometimes even a logical error can also trigger this situation. If you are trying to access or copy a file that is no longer available, then you will get a hard disk error like this. Apart from a loose connection, a corrupt configuration, or incompatible driver can also be a trigger.



Virtual Disk Manager

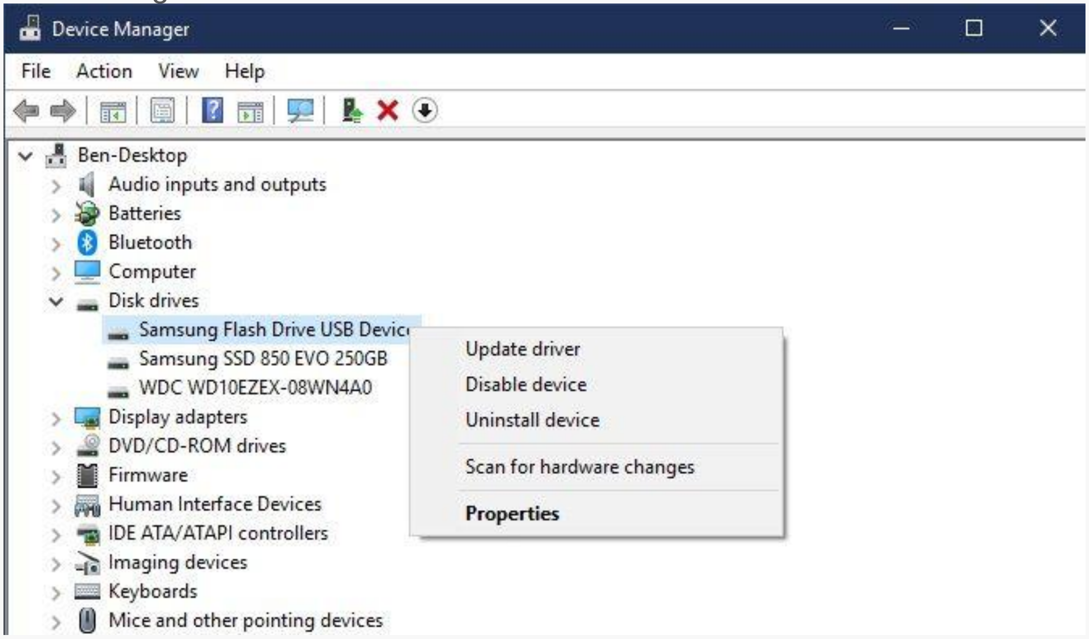
The request failed due to a fatal device hardware error

Solution 1: Reconnect the disk

If these drive problems have occurred due to a loose connection, then you should consider this approach. Disconnect the external hard drive and restart your computer. Now, try to connect it again and check if the system detects the drive. You can consider disassembling the system and check if the internal hard drive has been connected properly or not.

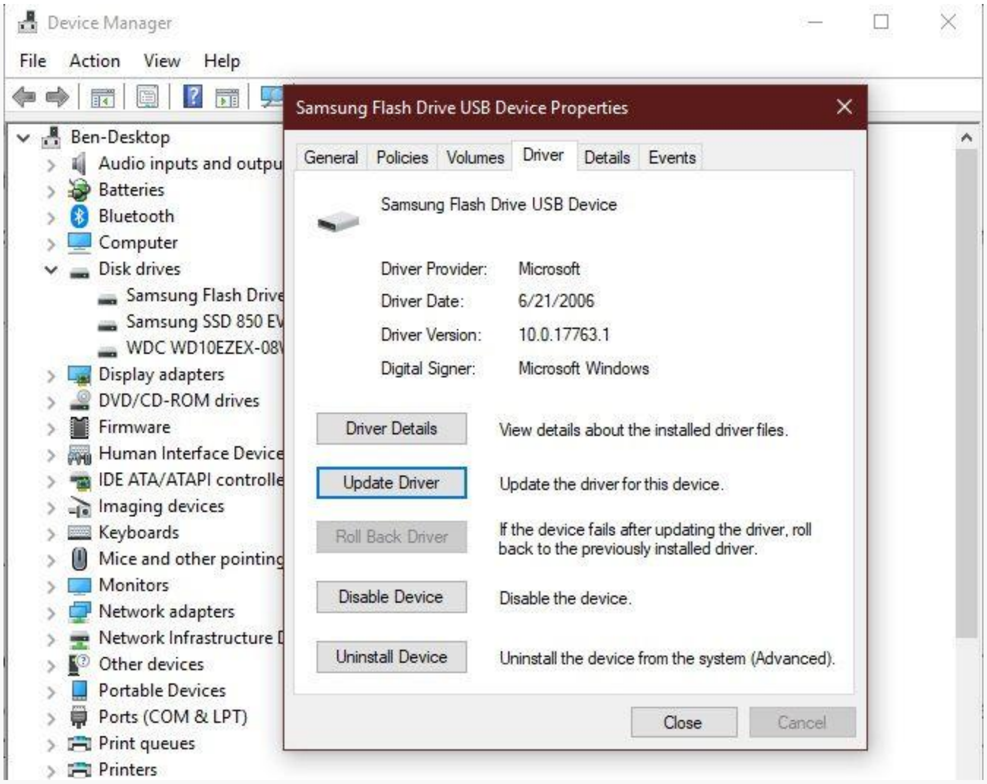
Solution 2: Reset the driver

There are times when the hard drive malfunctions due to a driver related issue. In this case, you can consider resetting the driver to resolve this hard disk problem. Go to the Device Manager from the Start menu and expand the "Disk Drives" option. Select and right-click the driver option. From here, you can disable the device. Wait for a while and enable it again to resolve this hard drive issue.



Solution 3: Update the driver

Apart from resetting the driver, you can also consider updating it as well. Simply launch the Device Manager option and select the driver listed under the "Disk Driver" feature. Go to its Properties > Driver tab and click on the "Update Driver" button. Now, you can just follow on-screen instructions to update the disk drivers on your system.



Samsung Flash Drive USB Device

Driver Provider: Microsoft
Driver Date: 6/21/2006
Driver Version: 10.0.17763.1
Digital Signer: Microsoft Windows

View details about the installed driver files.

Update the driver for this device.

If the device fails after updating the driver, roll back to the previously installed driver.

Disable the device.

Uninstall the device from the system (Advanced).

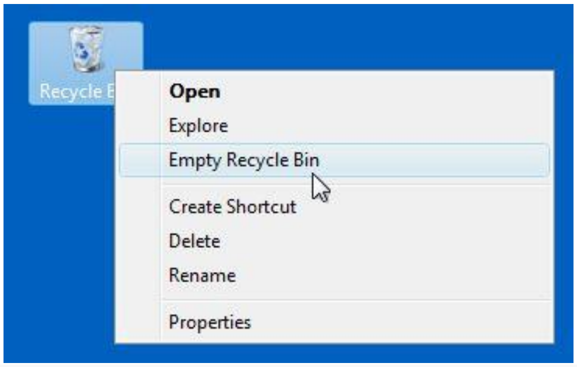
Disk Error 10. The Disk is Full

This is certainly one of the most common hard drive problems that users face. If you have accumulated a lot of data on your disk, then it can run out of space. Not only can it corrupt your hard drive or cause it to malfunction, but it would also make your **system run slow**. The accumulation of tons of photos, videos, documents, and other unwanted files. You could have installed numerous unwanted applications as well. The frequent partitioning of the disk can also lead to its fragmentation.

The disk is full.

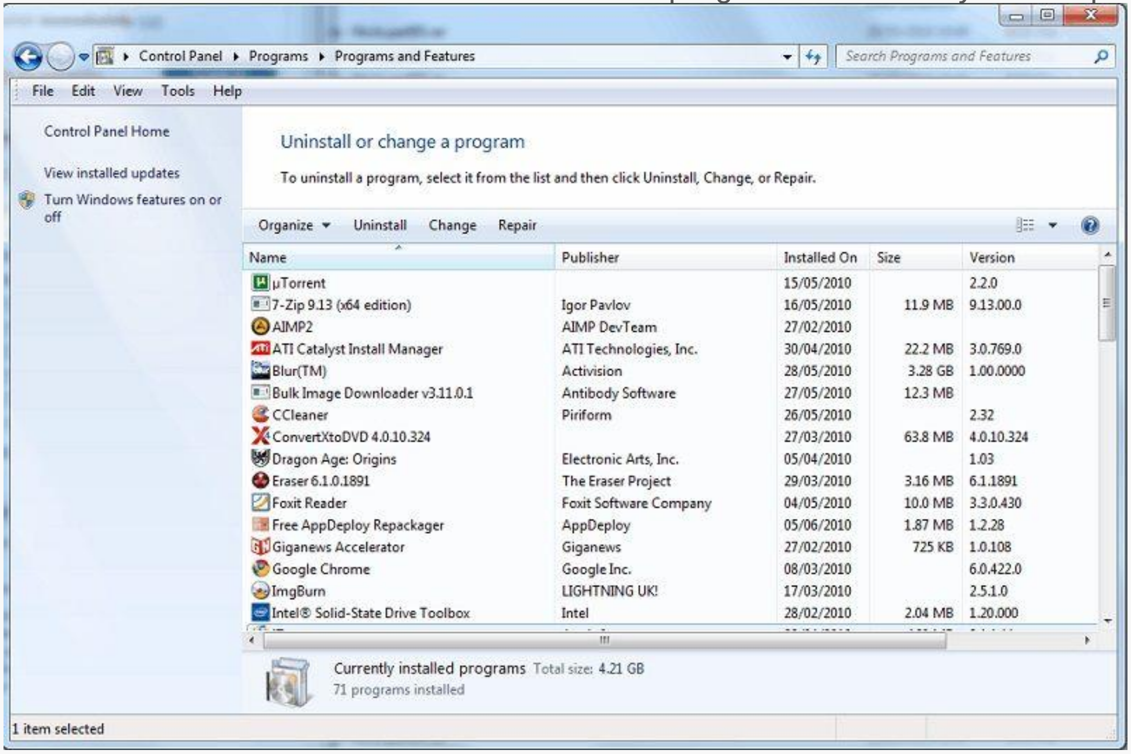
Solution 1: Deleting unwanted content

The easiest fix for this hard disk error is the deletion of any unwanted content. Just go to your disk's partition and start removing the videos, photos, documents, etc. that you no longer want. Just make sure that you don't remove any important system files in the process. Also, visit the Recycle Bin and empty it to make more free space on the disk.



Solution 2: Uninstall unimportant applications

If you have installed lots of applications and programs on your system, then consider getting rid of them. To do this, go to Control Panel > Programs > Programs and Features. In the newer Windows versions, go to Applications under Settings. Now, just select the program you want to remove and click on the "Uninstall" button. Follow the on-screen instructions to uninstall the selected program and restart your computer.


Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
File Edit View Tools Help
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾ Uninstall Change Repair

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

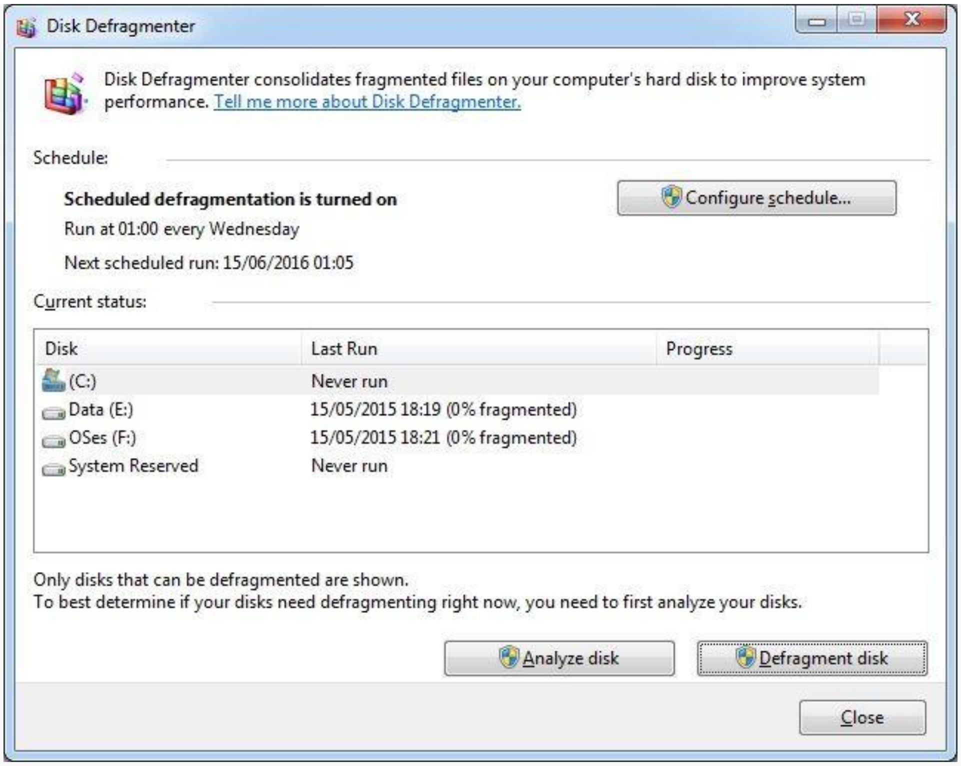
Name	Publisher	Installed On	Size	Version
µTorrent		15/05/2010		2.2.0
7-Zip 9.13 (x64 edition)	Igor Pavlov	16/05/2010	11.9 MB	9.13.00.0
AIMP2	AIMP DevTeam	27/02/2010		
ATI Catalyst Install Manager	ATI Technologies, Inc.	30/04/2010	22.2 MB	3.0.769.0
Blur(TM)	Activision	28/05/2010	3.28 GB	1.00.0000
Bulk Image Downloader v3.11.0.1	Antibody Software	27/05/2010	12.3 MB	
CCleaner	Piriform	26/05/2010		2.32
ConvertXtoDVD 4.0.10.324		27/03/2010	63.8 MB	4.0.10.324
Dragon Age: Origins	Electronic Arts, Inc.	05/04/2010		1.03
Eraser 6.1.0.1891	The Eraser Project	29/03/2010	3.16 MB	6.1.1891
Foxit Reader	Foxit Software Company	04/05/2010	10.0 MB	3.3.0.430
Free AppDeploy Repackager	AppDeploy	05/06/2010	1.87 MB	1.2.28
Giganews Accelerator	Giganews	27/02/2010	725 KB	1.0.108
Google Chrome	Google Inc.	08/03/2010		6.0.422.0
ImgBurn	LIGHTNING UK!	17/03/2010		2.5.1.0
Intel® Solid-State Drive Toolbox	Intel	28/02/2010	2.04 MB	1.20.000

Currently installed programs Total size: 4.21 GB
71 programs installed

1 item selected

Solution 3: Defragment the disk

When we keep on partitioning a disk or join different components, it leads to its fragmentation. Thankfully, with the help of the disk fragmenting tool, you can reclaim this lost space on your hard disk. To do this, just go to the Start Menu and look for "Disk Defragmenter". You can also access it from System Tools > Disk Defragmenter. Authenticate your account by entering the admin password and select the drive you wish to defragment.



Disk Defragmenter consolidates fragmented files on your computer's hard disk to improve system performance. Tell me more about Disk Defragmenter.

Schedule:

Scheduled defragmentation is turned on

Run at 01:00 every Wednesday

Next scheduled run: 15/06/2016 01:05

Current status:

Disk	Last Run	Progress
(C:)	Never run	
Data (E:)	15/05/2015 18:19 (0% fragmented)	
OSes (F:)	15/05/2015 18:21 (0% fragmented)	
System Reserved	Never run	

Only disks that can be defragmented are shown.
To best determine if your disks need defragmenting right now, you need to first analyze your disks.

Disk Error 11. Data inaccessibility on a non-booting system

When a hard drive is crashed, a lot of users end up losing their important files since the system is not able to boot correctly. While the data is still there on the disk, it becomes inaccessible. To get it back, you need to create a bootable media and run data recovery on your system.

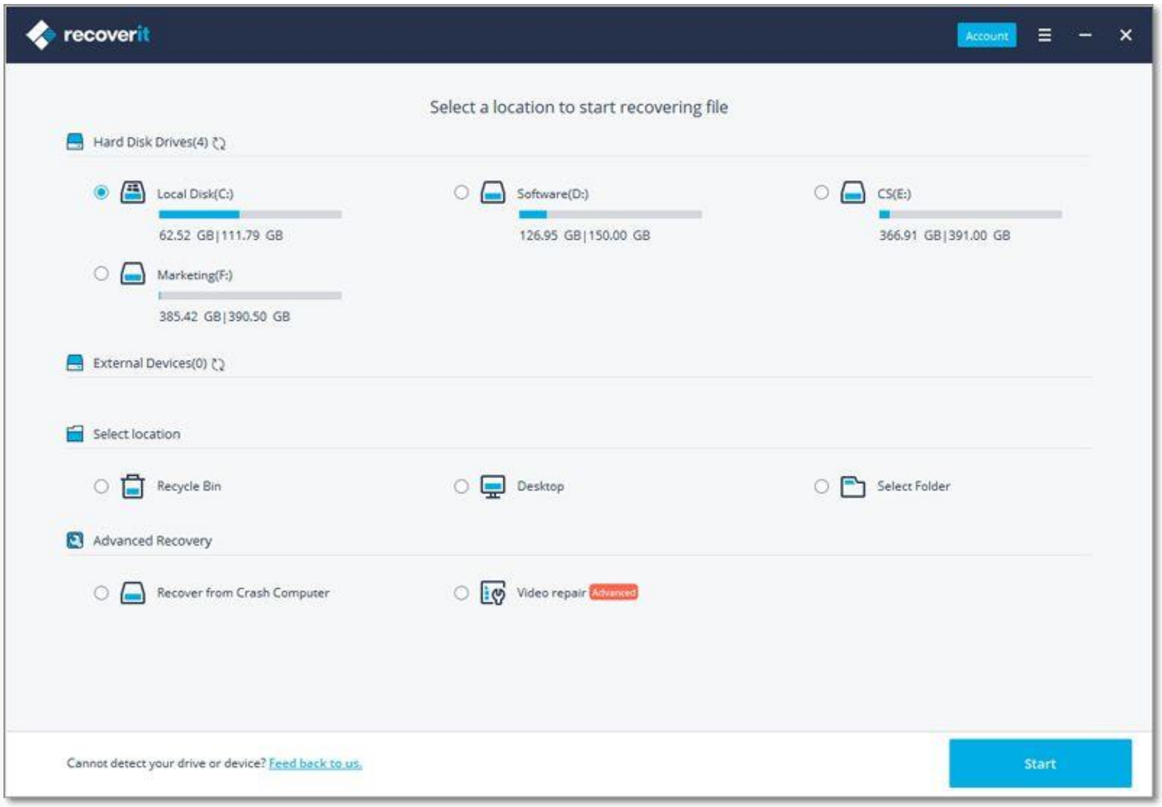
The firmware component or the important system files can be wiped off entirely from your computer. It can also be physically damaged or crashed due to the lack of free space on the disk.

Solution: Create a bootable recovery media using Recoverit

This is what makes Recoverit a complete data recovery solution. Using it, you can even create a bootable media and perform data recovery on a crashed system as well. The application can make a CD, DVD, or a USB drive into a bootable WinPE media.

Step 1: Start crashed system recovery

Firstly, install and launch Recoverit on any working computer and from its home, select the crashed system recovery option. Subsequently, connect the CD/DVD or the USB drive to your system (that you wish to make a bootable media).



Select a location to start recovering file

Hard Disk Drives(4)

● Local Disk(C:) 62.52 GB|111.79 GB
○ Software(D:) 126.95 GB|150.00 GB
○ CS(E:) 366.91 GB|391.00 GB
○ Marketing(F:) 385.42 GB|390.50 GB

External Devices(0)

Select location

○ Recycle Bin ○ Desktop ○ Select Folder

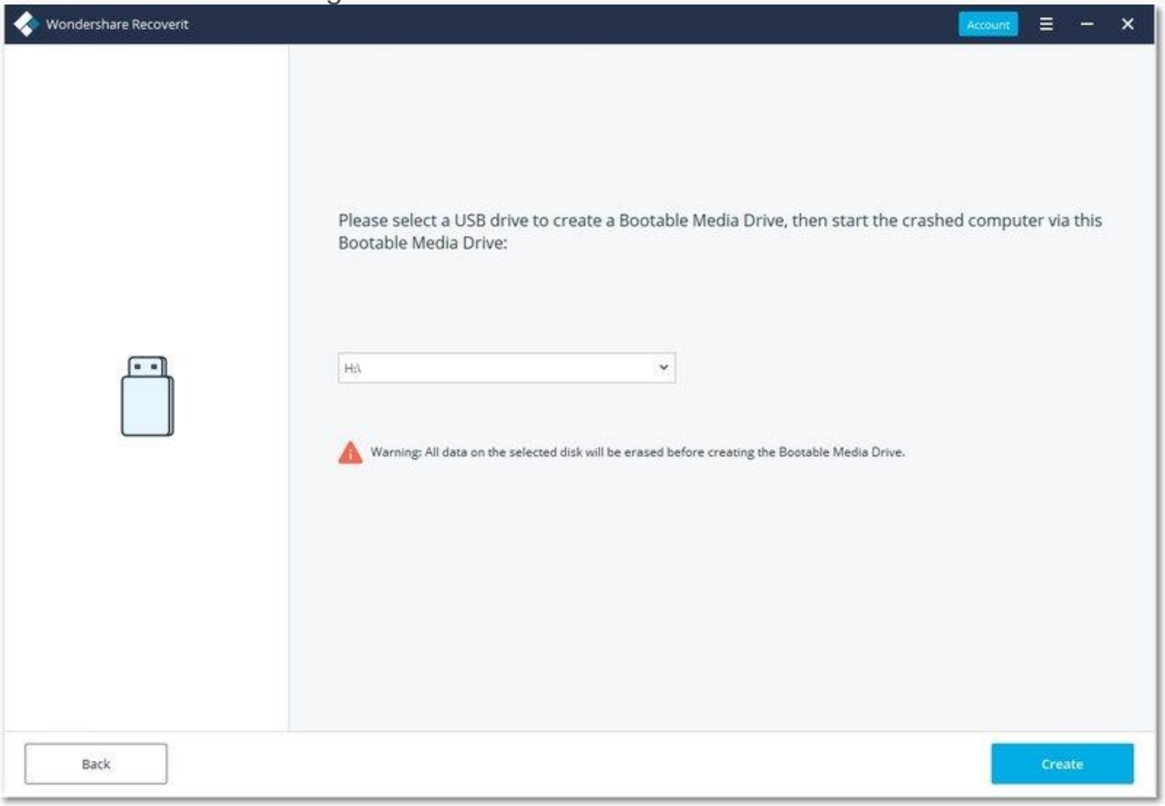
Advanced Recovery

○ Recover from Crash Computer ○ Video repair Advanced

Cannot detect your drive or device? Feed back to us.

Step 2: Create a bootable media

Select the drive you wish to convert to a bootable media from the interface. You need to confirm it as the existing data on the drive would be deleted.

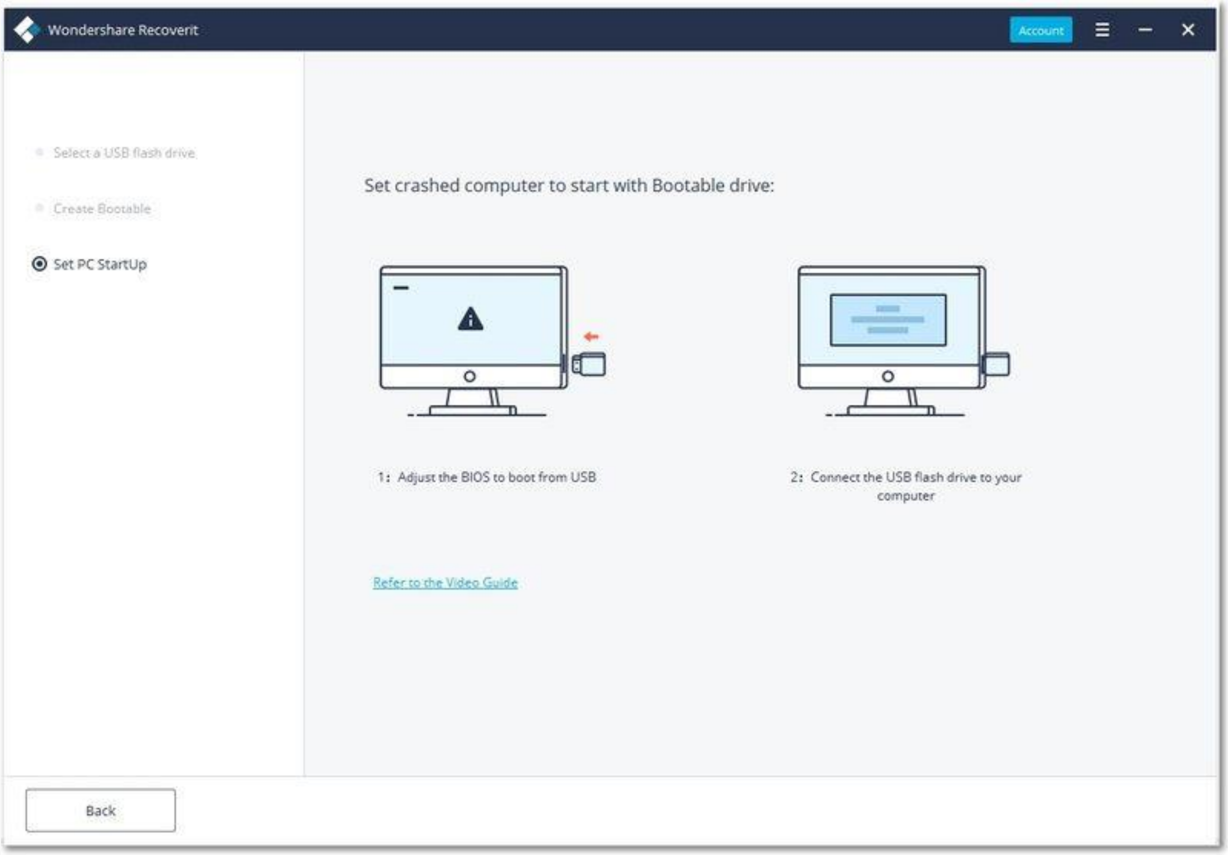


Please select a USB drive to create a Bootable Media Drive, then start the crashed computer via this Bootable Media Drive:

H:\

Warning: All data on the selected disk will be erased before creating the Bootable Media Drive.

Once the process is completed, the application will let you know that the bootable media has been created. You can now unmount it from the system.



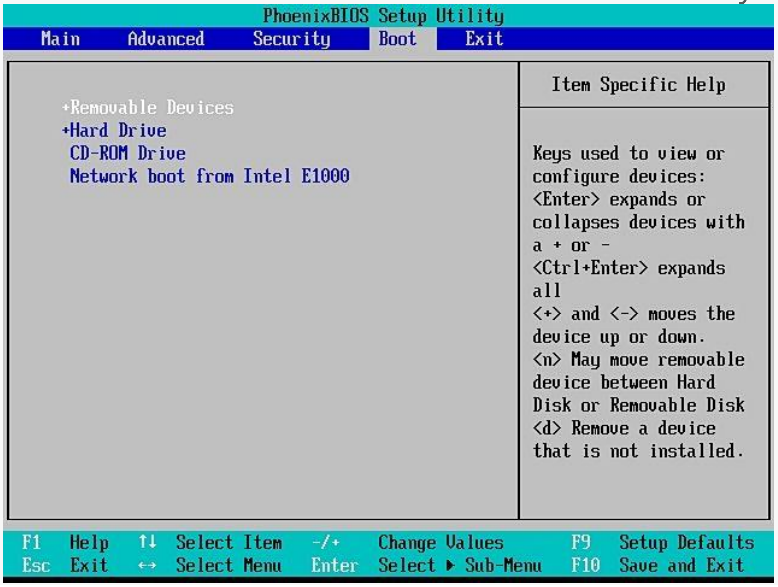
Set crashed computer to start with Bootable drive:

1: Adjust the BIOS to boot from USB

2: Connect the USB flash drive to your computer

Step 3: Boot the crashed system

Turn on the non-booting system and press the BIOS key (F12/F10/DEL) to enter its boot settings. From here, you can change the priority of the booting media (the connected USB drive or CD/DVD). Exit the BIOS settings and boot your system from the connected media to start Recoverit data recovery.



```
                     PhoenixBIOS Setup Utility
  Main     Advanced     Security    Boot    Exit

                                          Item Specific Help

     +Removable Devices
     +Hard Drive                          Keys used to view or
      CD-ROM Drive                        configure devices:
      Network boot from Intel E1000       <Enter> expands or
                                          collapses devices with
                                          a + or -
                                          <Ctrl+Enter> expands
                                          all
                                          <+> and <-> moves the
                                          device up or down.
                                          <n> May move removable
                                          device between Hard
                                          Disk or Removable Disk
                                          <d> Remove a device
                                          that is not installed.

 F1   Help   ↑↓  Select Item   -/+     Change Values       F9    Setup Defaults
 Esc  Exit   ↔   Select Menu   Enter   Select ▸ Sub-Menu   F10   Save and Exit
```

Disk Error 12. Computer Virus & Malware

Computer viruses and malware infect the system and corrupt the system files that are stored on the hard drive. These viruses and malicious software usually enter the system from an outside source, for instance, the internet and an external hard drive. These viruses first tend to attack the hard disk and then spread to other computers that are linked through the same network.

Keeping your computer’s operating system updated is one of the solutions to this problem. Moreover, another possible solution is the installation and frequent updating of an antivirus software program. This antivirus is going to protect your system and your hard drive and make sure that it remains safe from their threat.

Disk Error 13. Manufacturing fault

Hard disks that haven’t been tested beforehand become unresponsive after a few months of use. This problem is encountered usually with new hard disks. The reason for this is more often than not a manufacturing fault which causes the hard disk to fail.
The best way to solve this problem is to be careful when purchasing a new hard disk. It is crucial to test the new hard disk before installing it in your computer system. However, if you have a hard disk with a manufacturing fault and it becomes unresponsive then the only solution available is to replace it.

Disk Error 14. Heat

Heating is a common problem associated with hard disks. If the system is overused, the fans of the hard disk start moving slowly and the system starts heating up immediately after being booted. Moreover, clicking noises can be heard from the hardware of the system too which is an indication that the hard disk is overheated. The reason for this is the lack of proper ventilation or a faulty CPU fan which overheats the system to the point that the hard disk crashes.

The solution to the heating issue is to ensure that the CPU fan has been installed properly and is providing sufficient cooling to the hard disk. Moreover, you can install an application that keeps you notified about the temperature of your hard disk. If it starts exceeding the maximum limit, shut down the PC for a while and let it cool down before resuming your work.

Part 4: Not Sure of Hard Disk Error? Here Are Some Common Solutions

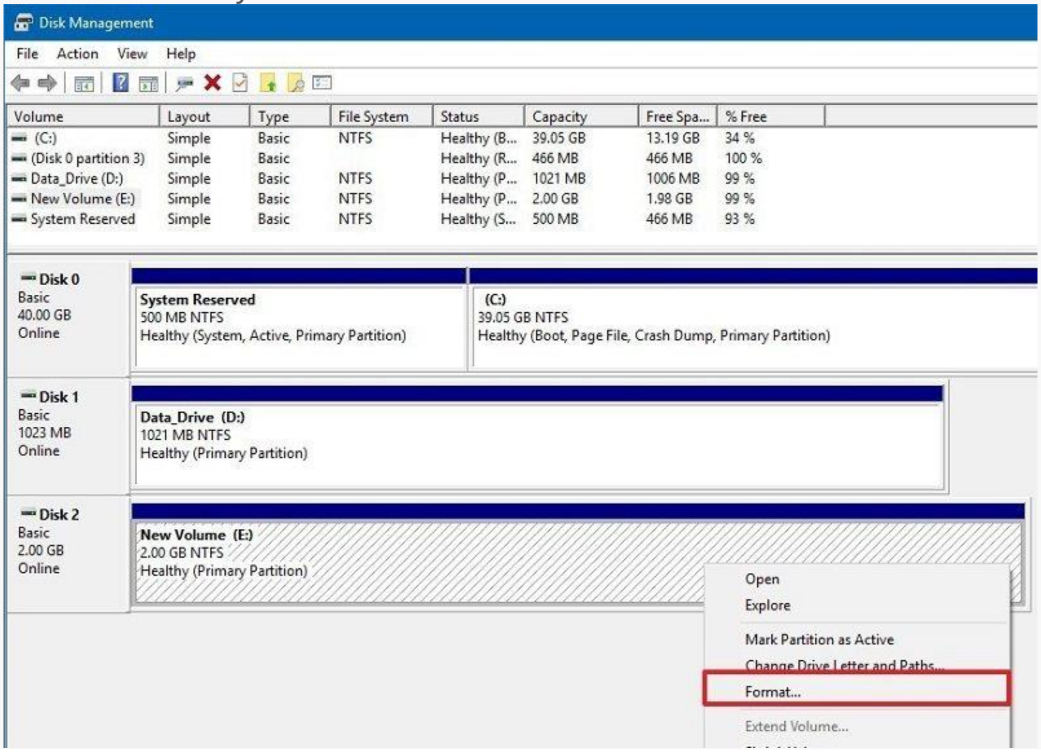
We have already discussed some specific hard drive issues and solutions in the previous section. Though, there are times when users are not able to identify what is wrong with their hard drive in the first place. In this case, you can consider the following troubleshooting hard drive suggestions.

1. Let your system rest

If your hard drive has been overheated, then this would most likely solve the problem. Simply shut down your system and let it rest for a few minutes. Turn it on when the system is not heated and the surrounding area is well ventilated.

2. Format the hard drive

In case if the hard drive issues are caused by malware or a logical error, then you can just format it to fix this. If your hard drive's icon is not getting displayed on My Computer, then launch the Disk Management tool on it. Select the disk space, right-click, and choose to format it. Confirm your choice and wait for a while as the hard disk would be formatted entirely.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	39.05 GB	13.19 GB	34 %
(Disk 0 partition 3)	Simple	Basic		Healthy (R...	466 MB	466 MB	100 %
Data_Drive (D:)	Simple	Basic	NTFS	Healthy (P...	1021 MB	1006 MB	99 %
New Volume (E:)	Simple	Basic	NTFS	Healthy (P...	2.00 GB	1.98 GB	99 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	500 MB	466 MB	93 %

Disk 0
Basic
40.00 GB
Online

System Reserved
500 MB NTFS
Healthy (System, Active, Primary Partition)

(C:)
39.05 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
1023 MB
Online

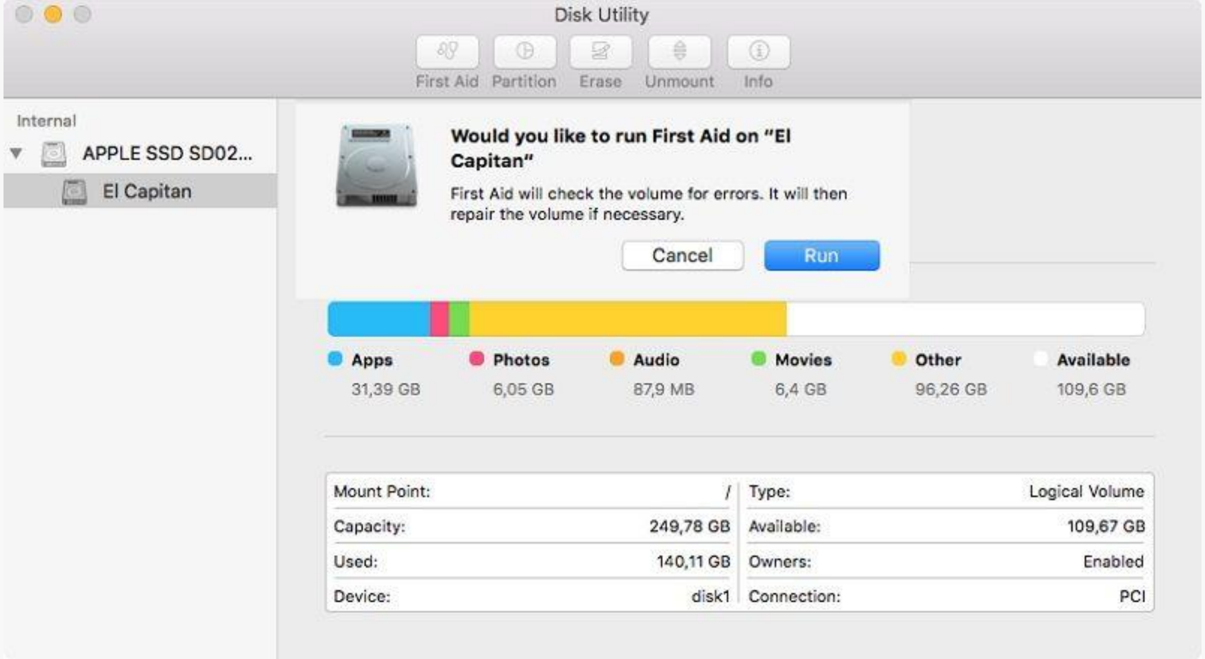
Data_Drive (D:)
1021 MB NTFS
Healthy (Primary Partition)

Disk 2
Basic
2.00 GB
Online

New Volume (E:)
2.00 GB NTFS
Healthy (Primary Partition)

3. Run Disk Repair

If there is a minor hard disk problem, then you can easily fix it by performing an automated repair. To do this, you can take the assistance of the system's native feature or a third-party tool. For instance, Mac's Disk Utility is an excellent option to repair a hard drive malfunction scenario. Just launch Disk Utility, select your drive, and click on the "First Aid" option to repair it.



Would you like to run First Aid on "El Capitan"

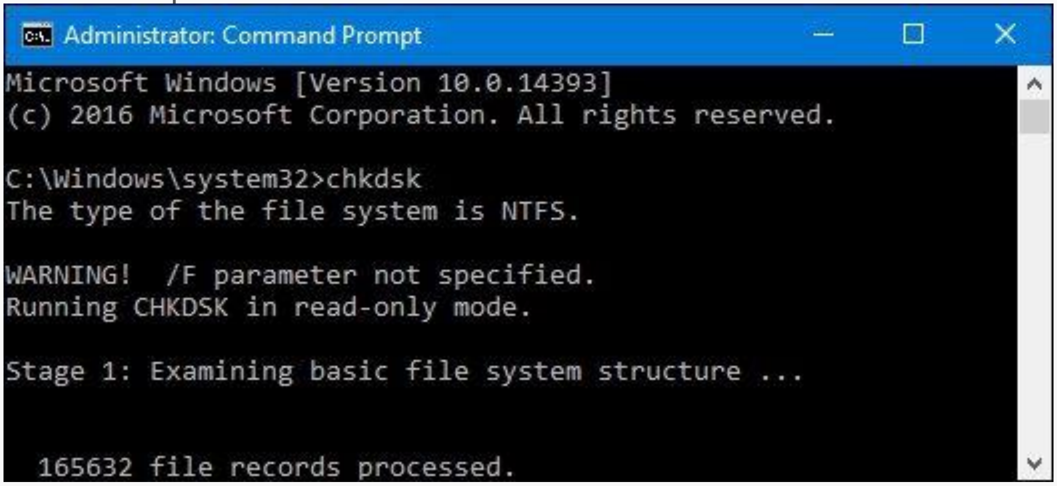
First Aid will check the volume for errors. It will then repair the volume if necessary.

Apps	Photos	Audio	Movies	Other	Available
31,39 GB	6,05 GB	87,9 MB	6,4 GB	96,26 GB	109,6 GB

Mount Point:	/	Type:	Logical Volume
Capacity:	249,78 GB	Available:	109,67 GB
Used:	140,11 GB	Owners:	Enabled
Device:	disk1	Connection:	PCI

4. Use the CHKDSK Command

If you are using a DOS-based operating system, then you can just take the assistance of the Check Disk (CHKDSK) command. To do this, just launch Terminal/Command Prompt on your system and type the command "CHKDSK" followed by the drive name you wish to scan. Your system will carefully scan the respective drive and will get rid of minor drive problems.



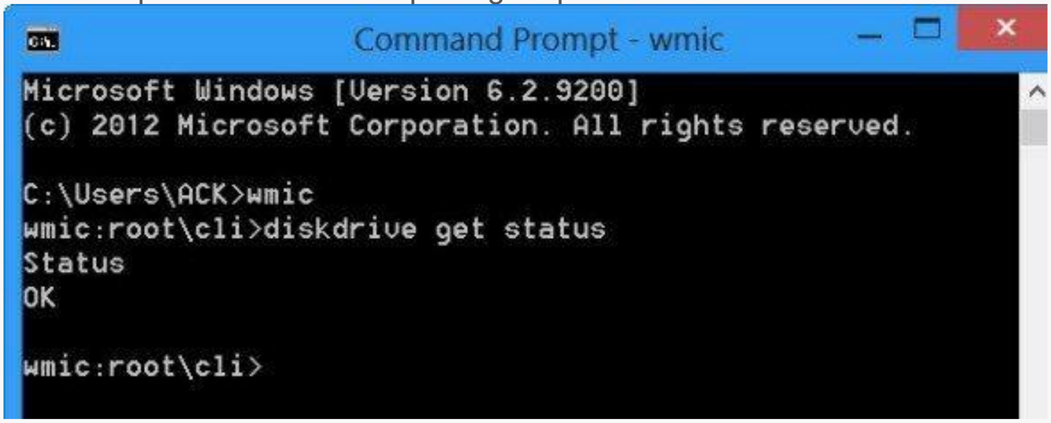
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>chkdsk
The type of the file system is NTFS.

WARNING!  /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...


  165632 file records processed.
```

Part 5: Tips on How to Use a Hard Drive

By now, you must be able to fix all kinds of hard drive problems and related issues. Though, if you do not want to face any unwanted situation like this in the future, then consider the following tips:

1. Check hard disk's health regularly

A lot of users don't know this, but you can check the health of a hard disk on Windows pretty easily. All you need to do is launch Command Prompt and enter the "wmic" command. It stands for Windows Management Instrumentation Command and will check the working of the disk. If the health is critical, then you can take a backup of your data and perform different repairing steps.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\ACK>wmic
wmic:root\cli>diskdrive get status
Status
OK

wmic:root\cli>
```

2. Keep at least 20% storage free

Needless to say, if you will cram your hard drive with too much data, then it can affect its overall functioning. Make sure that you keep at least 20% of the total space free to keep it running smoothly.

3. Avoid unexpected shutdown

Try not to turn your system off while an application or a crucial process is still being running in the background. This can tamper with a system file or process related to its hard disk.

4. Keep your system updated

If you don't want to suffer from any compatibility issue or a malware attack, then make sure that you keep your system updated. It will install all the essential patch files and keep the drivers up to date.

5. Avoid overheating and physical damage

Last, but most importantly, try to avoid any unwanted physical or water damage on your system. Also, make sure that the disk is not exposed to a magnet, which can lead to data loss in it. Keep the system ventilated or place it on a cooling pad to prevent the overheating of the drive.

6. Protect your important data

The following are some tips that you need to remember if you don’t want to lose your precious data.

- Install a good anti-virus program on your computer and regularly update it.
- Always create backups of your data in a separate location.
- Never shut down your computer system while any program is running.
- Don't write and add new data after the loss of hard disk data.
- To retrieve data safely, resort to **Recoverit Data Recovery**.

Common PC Hardware Problems

June 15, 2020 by Molly Owen

In general, PCs are built with all security measures because all of their sensitive components and hardware will be housed inside a casing to protect the components from dust and other harsh elements. However, some common PC hardware problems occur despite the protection. Even though the most complex computer issues at the workplace can often be solved by the business IT support team, there are many other small, but common, problems that occur quite often on a personal computer. It’s very important to identify and recognize such problems. The following are some of the commonly found hardware related problems on your PC.

Blank monitors

A blank monitor is the most common computer problem. Most people who work with computers might have dealt with such a non-working blank monitor at least once. In such cases, first and foremost is to check the supply cord and power systems. Sometimes, the video cable might be loosened. Just push the video cable and place it again, it should help you now.

Mouse Problems

The mouse is used for a variety of purposes, such as playing games or opening files, and moreover, it facilitates easy navigation, thus easy access to your data. The most common problems related to the mouse include failure to move, connection problems, freezing on the screen, or damage to the mouse.

Jumpy Mouse

Jumpy Mouse! Sounds strange right? Actually, a jumpy mouse is just a muted mouse i.e. cannot be scrolled. If you have a track and ball mouse, then simply turn it over and open the ball container, and remove the excess debris and clean the dirt that lines the rollers. For an optical mouse, eliminate the dust that has collected around the optical sensor.

PC won’t recognize my USB camera

In this case, even when you connect your USB camera, your PC might not be able to recognize it and hence throw errors like “Device not recognized” error. This might be due to the USB connector problems or the software malfunctioning. Before plugging in the camera, turn it on. This action can usually solve your problem.

My smartphone will not synch with my PC

In order to ensure backup of your smartphone, it is important that you regularly sync your phone content with your computer. At times, your PC might fail to sync with your smartphone. It can be due to many reasons. Sometimes it is required that all programs are closed, during syncing or backup.

Keyboard Problems

As we all know the keyboard is a vital part of any computer. It not only allows typing, but it also gives commands as well. However, you might encounter some common potential problems with the keyboard that includes keyboards that will not connect to the computer, stuck keys, broken keyboards, or keyboards where the letters end up jumbled.

Power Cord Problems

Whether it is a laptop or a desktop, power cords are a vital part of any computer. The desktop needs the power cord to work. A laptop can run on batteries for a limited amount of time but then needs the power cord for recharging. The most common problem with the power cord is an improper connection.

Motherboard Problems

The motherboard contains several parts of the computer including the RAM, BIOS system, mass storage, and CPU. The computer motherboard contains several devices, which can create numerous potential problems. Problems with the motherboard range from too little RAM to BIOS problems. Fixing the problems will depend on the specific problem and, in the worst-case scenario, purchasing a new motherboard will fix the problems.

Insufficient Memory

Processor-intensive programs also demand a lot of memory. Random access memory (RAM) aides the central processing unit (CPU) by storing instructions linked to common operations. Without enough RAM, software crashes and slowdowns can occur.

Above mentioned are some of the commonly found PC hardware problems. However, these are minor issues and you can easily find a solution for it. As you can observe most of these issues are related to PC peripherals, for example, Mouse, keyboard, USB camera, etc. Hence, one of the root causes of these issues lies with your devices. Actually some devices need third-party software to be connected to the PC and even for its proper functioning. The software is referred to as Device drivers. Drivers help the operating system to communicate with the hardware and help in the proper functioning of these peripherals. Even your video cards, keyboards, mouse, or any USB device plugged into the computer requires device drivers.

At times, these device drivers become outdated, and hence, PC encounters any of the problems explained above. Most of the time updating your device drivers has resolved all your hardware issues caused by bad device drivers. So, you will have to find out an outdated driver and get the newer version of it and update the driver. In case all the drivers are outdated, then you need to download and update all the drivers in order to fix these PC hardware problems.

This is really a tedious process right. But, this is the only solution to get rid of these issues. One simple solution for this is Remo Driver Discover tool that could scan your PC thoroughly and locate all the outdated drivers. In addition, it even provides a single interface to download and update the device driver in just a few clicks. It is a time-savvy tool; you can make use of it or can do it manually that consumes lots of time. However, the best solution is to always keep updating your drivers to its newer versions and clean the peripherals regularly to avoid dirt that causes jumpy mouse and other problems.

15 Common PC Problems and How to Troubleshoot Them

1. PC Overheating

A **heating PC slows down the whole system and leads to frequent crashes**. Additionally, PC components may also get permanently damaged due to constant exposure to heat.

There are **two main reasons your PC heats up**, i.e. either the cooling system isn't working properly or the PC is heating to the point your cooling system can't handle it anymore. In either case, I have written a comprehensive article on different solutions to handle an overheating PC. Do check it out.

2. Dysfunctional USB Port

If your USB port stops working, it's not necessary that it's broken. Below are some solutions that can fix this issue:

Method 1: Restart the PC

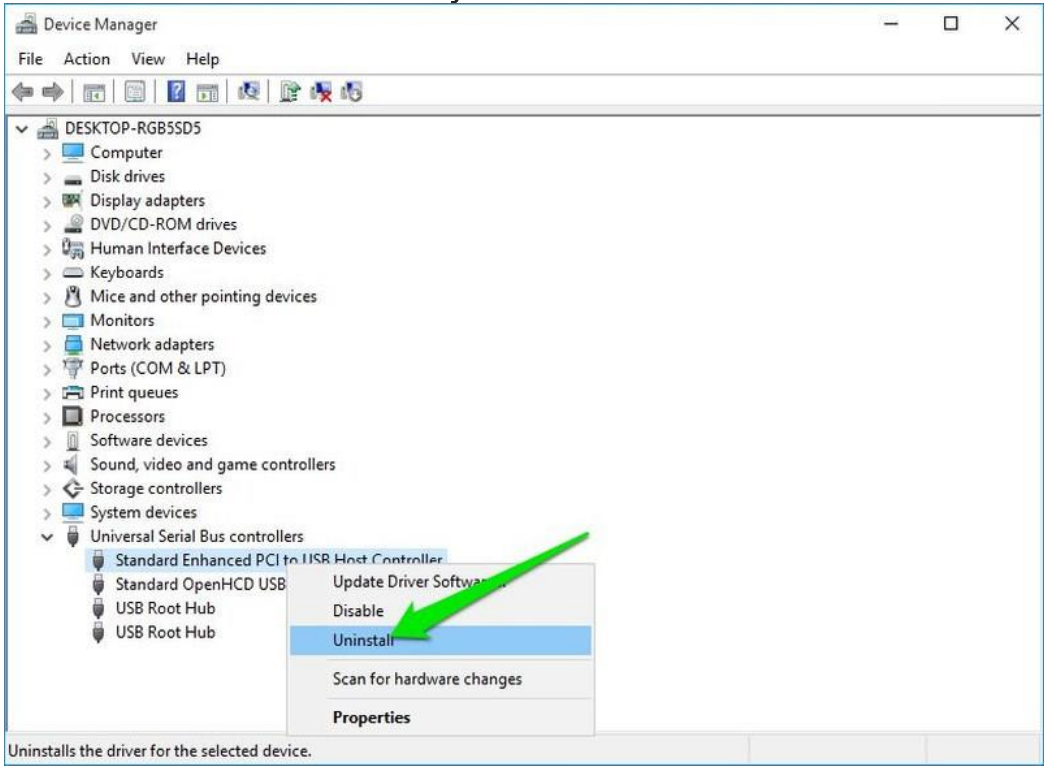
Restarting the PC is the answer to many problems, and it is a common solution to USB port problem as well.

Method 2: Uninstall USB port driver

Uninstalling the driver of the USB port will force Windows to reinstall it when you will restart the PC. This may fix the problem. Here is how to do it:

1. Press `Windows` + `R` keys and enter `devmgmt.msc` in the *Run* dialog to open the **Device Manager**.
2. Here, expand **Universal Serial Bus controllers** option.
3. Now right-click the entry **USB Host Controller** and then click on **Uninstall**.
4. Repeat this for all entries with **USB Host Controller** to uninstall drivers for all the USB ports.

5. Once deleted, restart the PC and **Windows will automatically reinstall the drivers** and fix any driver issues.

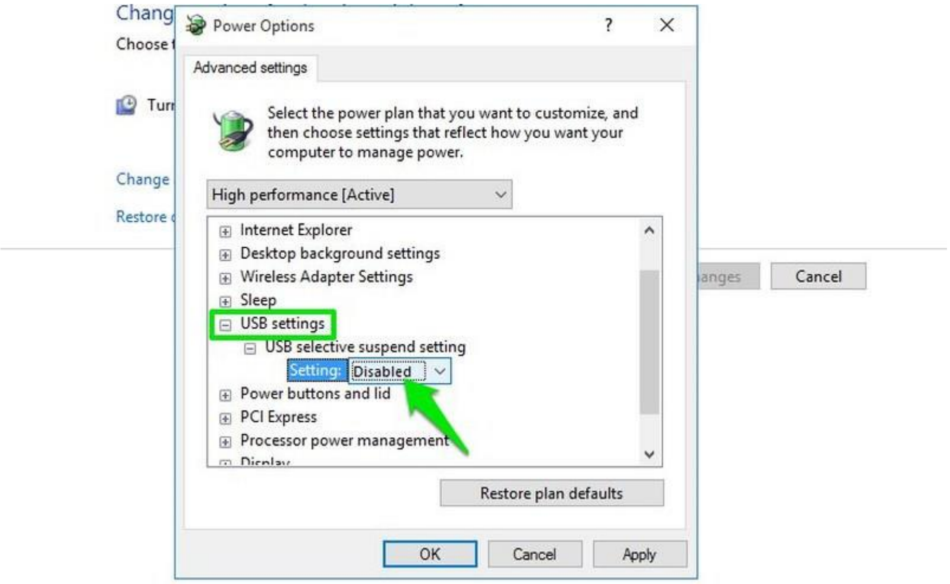


Uninstalls the driver for the selected device.

Method 3: Disable USB selective suspend

USB Selective Suspend is a Windows power saving feature that **suspends unused or idle USB ports to conserve power**. Sometimes it could stop a USB port from working. Here is how to disable it:

1. Press `Windows` + `R` keys and type `powercfg.cpl` in the *Run* dialog to open Windows Power options.
2. Here click on **Change plan settings** next to your current plan and then click on **Change advanced power settings**.
3. Now, expand **USB settings** and disable **USB selective suspend setting**.
4. Restart the PC to see if it fixes the USB port issue.


Power Options

Advanced settings

Select the power plan that you want to customize, and then choose settings that reflect how you want your computer to manage power.

High performance [Active]

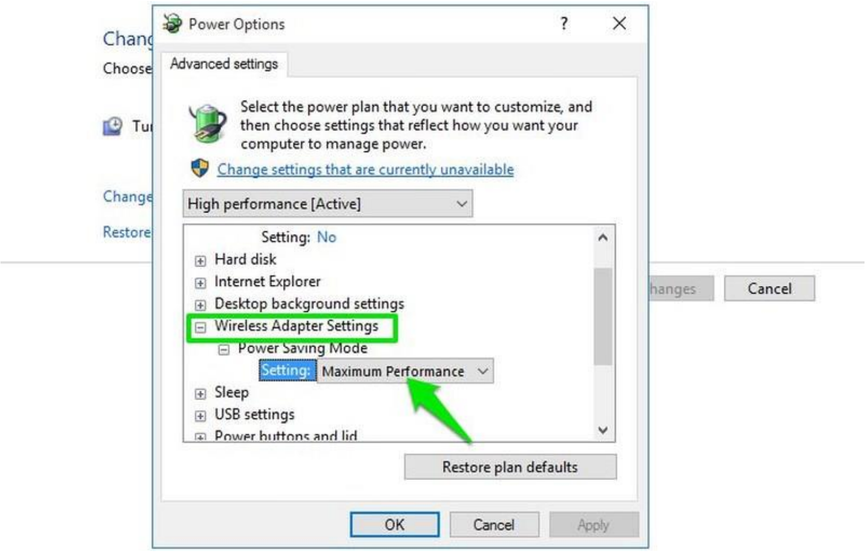
- Internet Explorer
- Desktop background settings
- Wireless Adapter Settings
- Sleep
- USB settings
  - USB selective suspend setting
    - Setting: Disabled
- Power buttons and lid
- PCI Express
- Processor power management
- Display

Note: This option should be kept enabled if you want to save battery power. If it **doesn't fix the USB port issue, then enable it again**.

3. PC keeps disconnecting from WiFi

If your Wi-Fi is working fine but your PC keeps disconnecting from it, then your PC's network card may not be receiving full power. Windows has a **built-in power saver option that gives less power to the network card**. You need to disable this feature:

1. Go to **Advanced settings** in the **Power Options**.
2. Here expand **Wireless Adaptor Settings** and then expand **Power Saving Mode**.
3. Set this to **Maximum Performance**.


Power Options

Advanced settings

Select the power plan that you want to customize, and then choose settings that reflect how you want your computer to manage power.

Change settings that are currently unavailable

High performance [Active]

- Setting: No
- Hard disk
- Internet Explorer
- Desktop background settings
- Wireless Adapter Settings
  - Power Saving Mode
    - Setting: Maximum Performance
- Sleep
- USB settings
- Power buttons and lid

4. PC beeps

The PC **motherboard is smart enough to detect problems** and sounds beeps in different rhythms to tell you. Here is an article on what it actually means when the PC beeps multiple times.

If the PC doesn't start after the beeps, then it's usually difficult to solve the problem yourself. However, I'm going to list down two of the most common problems due to which beeps occur, and thankfully, you can solve them yourself as well.

Problem 1: Out of place RAM

A problem I recently dealt with. If the **RAM inside your PC gets loose or out of place, then your PC will beep 2-3 times** and won't boot at all. The solution is simple, open up the PC (laptop users should let an expert handle this) and **reinsert the RAM**. Here's how:

1. **Take out the RAM completely and clean any dirt inside** the slot using a cotton bud.
2. Now **insert back the RAM** and put enough pressure on both ends to ensure it is fully inside.
3. Afterward, close the clips and **make sure they're properly locked**. Even a slightly loose RAM will be unable to work.

This video should help you properly install the RAM

Problem 2: Recently added hardware

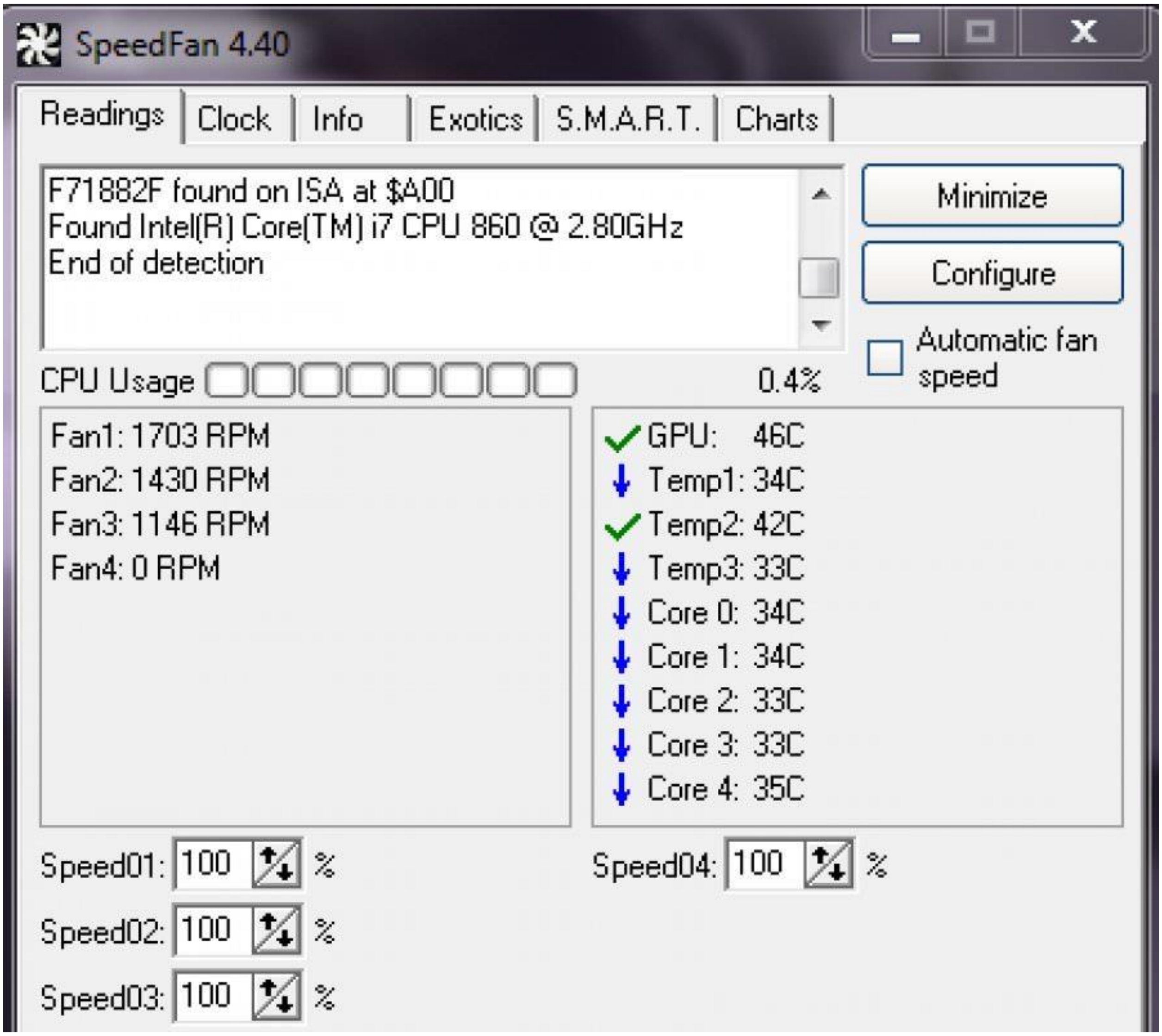
A damaged or **wrongly installed hardware component could lead to beeps**. Take out any newly added hardware components and see if it solves the problem. If the PC works fine afterward, then either **get it installed properly or get it fixed** (or replaced).

5. PC Fans not working

If you notice one or more fans in your PC aren't working, then it could be due to the dirt inside. You will have to open up the PC and **use a compressed air can or a leaf blower** to clean up the fans and other components.

Here's a video to help you with the cleaning process:

If dirt wasn't the problem, then you can also use the SpeedFan app to see what is the problem. The **app will let you control the fans to make them work again**. Although your PC motherboard must support fan control to use this app.



```
F71882F found on ISA at $A00
Found Intel(R) Core(TM) i7 CPU 860 @ 2.80GHz
End of detection
```

□ Automatic fan speed

CPU Usage 0.4%

```
Fan1: 1703 RPM        ✓ GPU:   46C
Fan2: 1430 RPM        ↓ Temp1: 34C
Fan3: 1146 RPM        ✓ Temp2: 42C
Fan4: 0 RPM           ↓ Temp3: 33C
                      ↓ Core 0: 34C
                      ↓ Core 1: 34C
                      ↓ Core 2: 33C
                      ↓ Core 3: 33C
                      ↓ Core 4: 35C
```

Speed01: 100 %   Speed04: 100 %

Speed02: 100 %

Speed03: 100 %

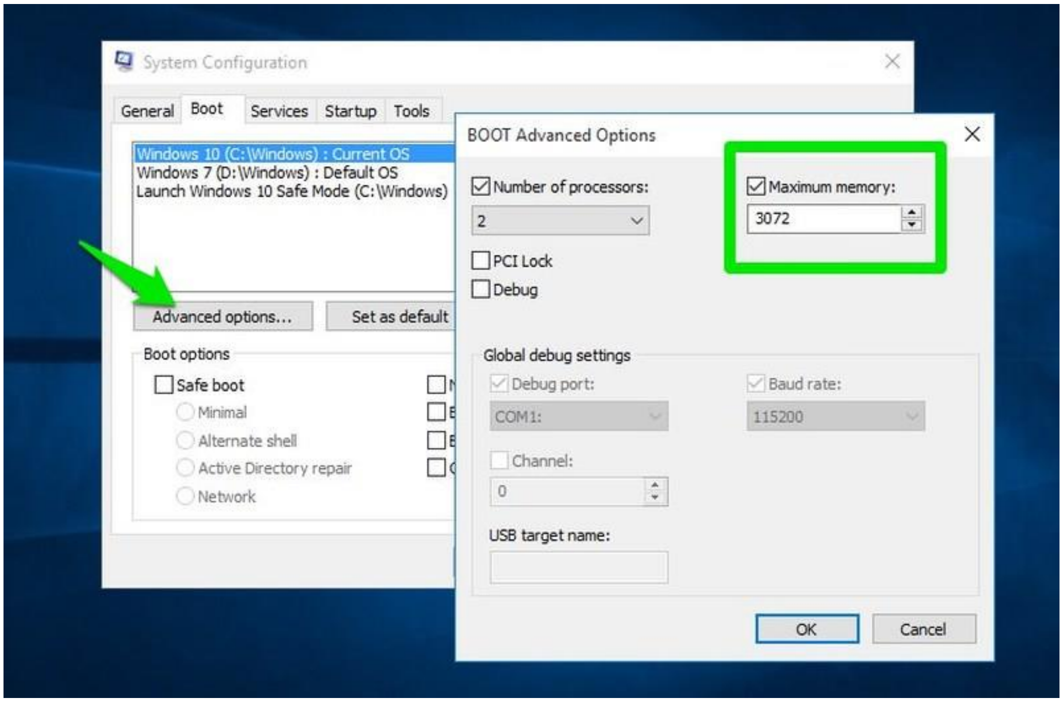
6. PC not using a portion of RAM

Sometimes your PC may not use a portion of RAM. For example, **You may have 4GB of RAM, but your PC only uses 2GB when you check it from the Task Manager**. This is usually a Windows setting issue.

Note: If only a few MBs (200-400MB) of RAM isn't being utilized, then it's probably being used by PC hardware and you can't do anything about it.

The solution to this problem is simple – **Windows must have been configured to only use a portion of the RAM**. Here is how to fix it:

1. Press `Windows` + `R` keys and type `msconfig` in the *Run* dialog to open **System Configurations**.
2. Move to **Boot** tab and click on **Advanced options**.
3. Now check the checkbox next to **Maximum memory** and enter the maximum amount RAM you have installed (in MBs).
4. Click on **OK** and restart the PC to let it take effect.



Windows 10 (C:\Windows) : Current OS
Windows 7 (D:\Windows) : Default OS
Launch Windows 10 Safe Mode (C:\Windows)

☑ Number of processors: 2
☑ Maximum memory: 3072
□ PCI Lock
□ Debug

Global debug settings
☑ Debug port: COM1:
☑ Baud rate: 115200
□ Channel: 0
USB target name:

Good to know: While you are at it, you should also check the checkbox next to **Number of processors** option and ensure your PC is utilizing all the CPU cores as well. Set it to the maximum number if you want to use all of the CPU power.

If this didn't fix the problem, then **there is also a chance one of the RAM isn't installed properly**. Try reinstalling it.

7. Overworking fan

Your PC fan **runs according to how much your PC is heating**. The higher the temperature, the faster the fan will run. In case your PC temperature is fine (you can use HWMonitor to check it), but the fan is running at full speed; then you'll have to manually control it.

You can use the SpeedFan app for this purpose as well. It will **tell you the running speed of all the fans inside your PC** so you can manage their speed. Don't worry about app compatibility, overworking fan problem only happens with motherboards that can control the fans.

8. PC crashes before loading the OS

If your **PC only shows manufacturer logo and then crashes** right before it was supposed to load the operating system, then it's a **problem with RAM or hard disk**. As the OS is unable to load, then either the RAM is corrupted and can't hold the boot loader or the **hard drive is damaged** and can't load data inside it.

If you have multiple RAM slots, then **taking out each one of them one by one and starting the PC** will help find the culprit. In the end, you will have to replace the corrupted RAM or the hard disk, whichever has the issue.

9. PC isn't powering on

If your PC is not powering on at all – not even a single light in it, then it must be a problem with the power source.

Desktop users: If your PC's **extension cord, power outlet, and other connections** are working fine, then the problem may be with the PC's power cable. **Replace the power cable of the monitor with the CPU's** (if you don't have a spare) to see if it turns on. You'll have to get a new power cable if this fixes the problem.

Laptop users: Take out the battery and put it back before starting the laptop. If this doesn't work, then **take out the battery again and connect the charging cable to the laptop**. Start the PC on charger power and see if it works. You will have to replace the battery if it fixes the problem.

Note: You should also remove all types of external devices connected to your PC while trying this. A malfunctioning device might cause this issue.

10. Noisy PC

If you hear a lot of extra noise while using the PC, then most probably it is a plea to clean it up. **Get it cleaned or use a can of compressed air or leaf**

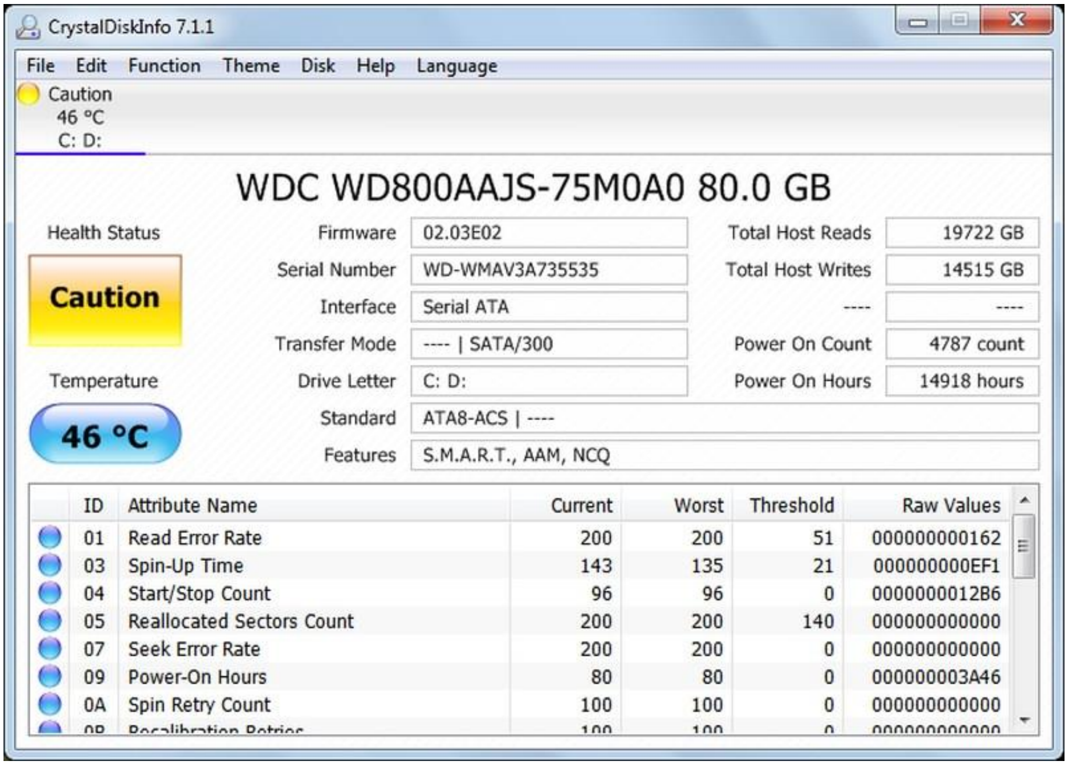
blower to clean it up yourself. If you have overclocked your PC GPU and CPU, then they could be the reason for the noise as well.

Here is a video with simple methods to clean your PC:

There is also a chance that **a disc inside the DVD ROM is making the extra sound**. You can check this article about all the PC components that create noise for more information.

11. Noisy hard drive

If you hear **clicking or grinding sound from the hard drive**, then it might be time to get a new one. Hard drives have a limited lifespan and **loud sounds are the main sign of a near hard drive failure**. You can use CrystalDiskInfo hard drive monitoring tool to check the health of your hard drive. The tool will tell you the current health of the hard drive with signs like "Good", "Caution" or "Bad".



Caution
46 °C
C: D:

WDC WD800AAJS-75M0A0 80.0 GB

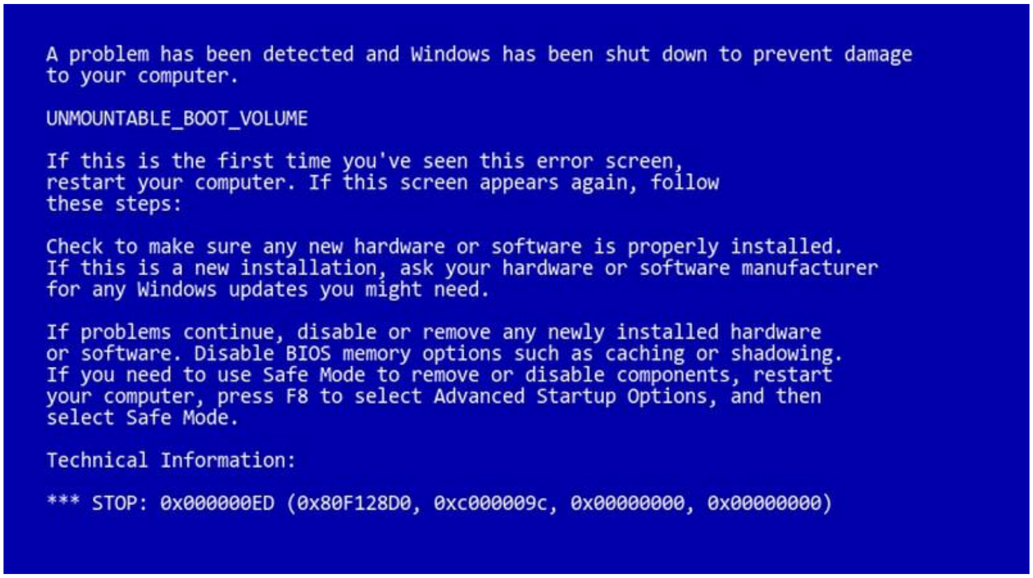
Health Status	Firmware	02.03E02	Total Host Reads	19722 GB
Caution	Serial Number	WD-WMAV3A735535	Total Host Writes	14515 GB
	Interface	Serial ATA	----	----
	Transfer Mode	---- | SATA/300	Power On Count	4787 count
Temperature	Drive Letter	C: D:	Power On Hours	14918 hours
46 °C	Standard	ATA8-ACS | ----		
	Features	S.M.A.R.T., AAM, NCQ		

	ID	Attribute Name	Current	Worst	Threshold	Raw Values
●	01	Read Error Rate	200	200	51	000000000162
●	03	Spin-Up Time	143	135	21	000000000EF1
●	04	Start/Stop Count	96	96	0	0000000012B6
●	05	Reallocated Sectors Count	200	200	140	000000000000
●	07	Seek Error Rate	200	200	0	000000000000
●	09	Power-On Hours	80	80	0	000000003A46
●	0A	Spin Retry Count	100	100	0	000000000000
●	0B	Recalibration Retries	100	100	0	000000000000

You should back up all your data immediately and **try to get another hard disk** before this one fails on you.

12. Blue Screen of Death

The dreaded Blue Screen of Death (BSOD) can occur **due to both software and hardware problems**, but usually, it’s a hardware problem. Whatever the cause, BSOD requires immediate attention as it’s a **sign of a big problem**.



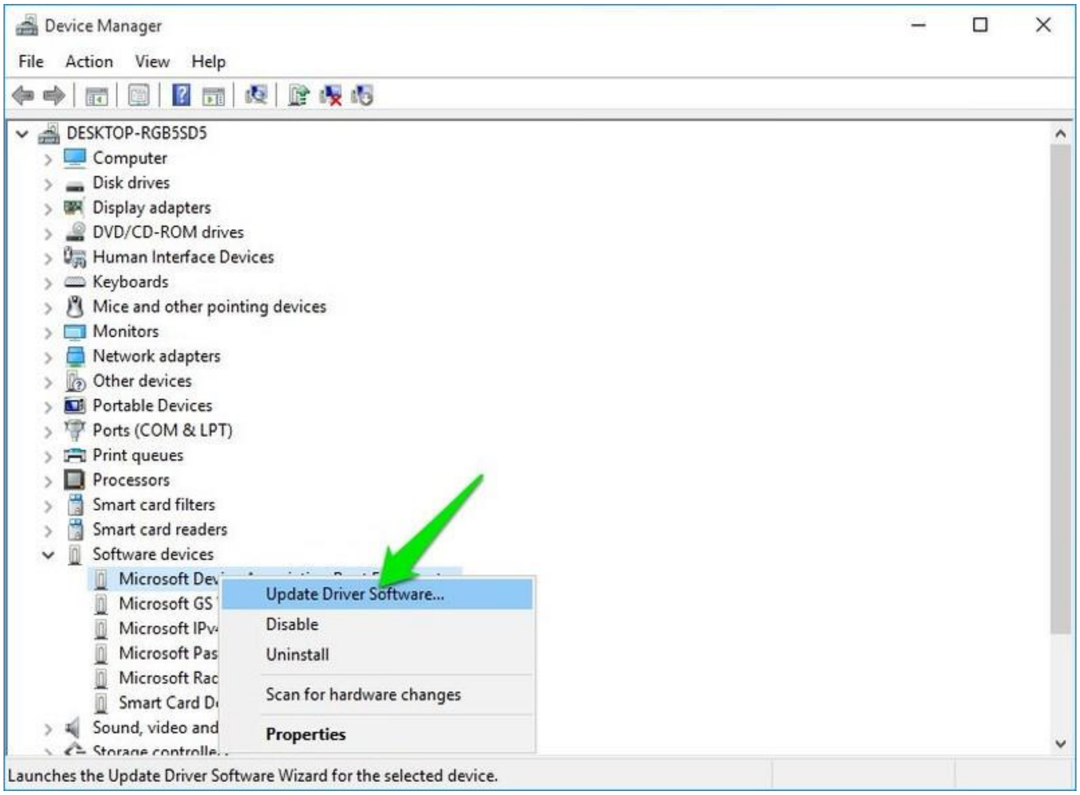
```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

UNMOUNTABLE_BOOT_VOLUME

If this is the first time you've seen this error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical Information:

*** STOP: 0x000000ED (0x80F128D0, 0xc000009c, 0x00000000, 0x00000000)
```

BlueScreenView is a great Nirsoft utility that will show important information if you have recently suffered a Blue Screen of Death. You should be able to identify and solve the problem using this information. Below are some common reasons for BSOD and their solutions.

1. Corrupted drivers

A corrupt driver may be the cause of BSOD. To find that out, use the following steps:

1. Open **Device Manager** by typing **devmgmt.msc** in the *Run*.
2. Here expand each menu and look for a yellow triangle icon next to each driver.
3. If you find any, right-click on it and select **Update Driver Software** to update its driver.



Launches the Update Driver Software Wizard for the selected device.

You can also use a third-party app like IObit Driver Booster to automatically find and fix driver problems.

2. Too much pressure on the RAM

If you **open too many programs that RAM can't handle**, then it may freeze the system and show BSOD. For that, you should either stop opening too many programs or upgrade the RAM.

3. Faulty hard disk

BSOD is also a **sign of a dying hard disk**, use the instructions in problem #11 above to identify hard disk problems.

4. Heating PC

Heating PC also leads to BSOD if **too much pressure is put on the components**. Use the instruction in problem #1 to solve it.

13. Blank monitor

If your monitor isn’t showing anything, then this could be a **problem with the monitor itself or the graphics card**. You should connect the monitor to another PC to see whether the problem is with the PC or the monitor.

If the **monitor isn’t powering on at all**, then replace the power cable with a working one and see if it helps. Here is a good article on [how to fix a monitor that isn’t showing anything]().

14. Monitor goes black after few seconds

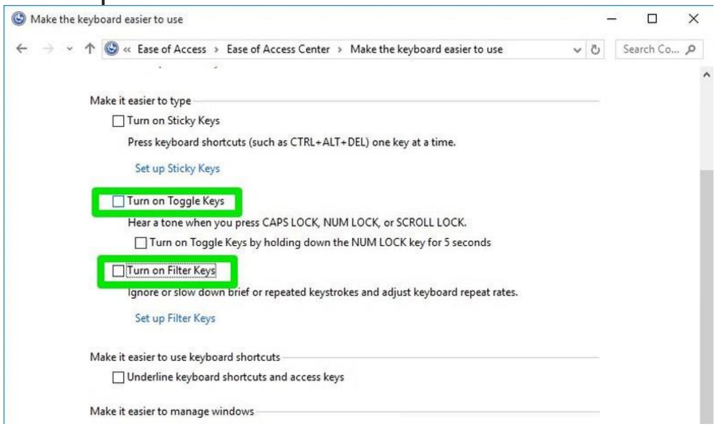
If the monitor goes black after few seconds of display, then it could be a problem with the **color quality or screen adjustment**. Press the auto-adjust button on your monitor to see if it fixes it. If not, then you will have to **change display color from 32bit to 16 bit**.

You can **connect the PC to another monitor to adjust colors from your graphics card settings**. Pressing the auto-adjust may show the display for few seconds. You can use this to your advantage and adjust the color while pressing auto-adjust.

15. Keyboard issues

If your keyboard is **making noise and won’t type repeated words properly**, then there is no problem with the keyboard. You must have enabled toggle keys and filter keys in Windows settings that cause such a problem. To disable them:

1. Open the **Control Panel** and click on **Ease of Access**.
2. Here click on **Change how your keyboard works** button.
3. Now uncheck the checkbox next to **Toggle keys** and **Filter Keys** to solve this problem.


Make the keyboard easier to use
« Ease of Access › Ease of Access Center › Make the keyboard easier to use
Search Co...

Make it easier to type

□ Turn on Sticky Keys

Press keyboard shortcuts (such as CTRL+ALT+DEL) one key at a time.

Set up Sticky Keys

□ Turn on Toggle Keys

Hear a tone when you press CAPS LOCK, NUM LOCK, or SCROLL LOCK.

□ Turn on Toggle Keys by holding down the NUM LOCK key for 5 seconds

□ Turn on Filter Keys

Ignore or slow down brief or repeated keystrokes and adjust keyboard repeat rates.

Set up Filter Keys

Make it easier to use keyboard shortcuts

□ Underline keyboard shortcuts and access keys

Make it easier to manage windows

How to Fix Mouse Left-click Malfunction in Windows

How to Fix Mouse Left-click Malfunction in Windows

Left-click of your mouse is the most used function that helps open files and programs and confirm commands...Read more

Rounding up

Many of the above **hardware problems can be easily fixed by tweaking the settings or using a software**. However, some of them will definitely require you to pay a visit to the computer repair shop.

It’s good to at least know what is wrong with your PC so **you can take the measures accordingly**. Do let us know in the comments if you faced any PC hardware problem before and how you solved it.

1. PRINTER WON’T TURN ON

Try turning on the printer.
We’re not trying to be coy, as this does happen from time to time. People overlook a power button or the plug lying far away from an electric socket.
As team member David DiEugenio explained to us recently:
“I had a customer who complained that the wireless printer we sold them was junk and wouldn’t work. When we got there, we had to explain while the printer did print wirelessly, it still needed to be plugged into the wall with a wire to power on.”
Also, try other power sources if the printer doesn’t boot up.

2. PAPER JAMS

What would a week be without paper jams? Close to heavenly, probably.
There are many reasons for paper jams (and best practices on how to avoid them). For this issue, please watch one of our Printer Self-Help videos:

Here is a short take from the video you can leverage to avoid printer jams:

- Be sure to square off the stack of paper before inserting it in the tray
- Double-check that pages are properly lined up
- Check to ensure the guides are flush with the paper

- Don’t over-fill the tray

3. SLOW PRINTER SPEED

Sometimes it seems a sloth on a hamster wheel has replaced your printer’s insides.
There could be many reasons, beyond a kidnapped hamster – like the need to update software or you’re printing wirelessly too far away from a router. But for a quick hack, you can speed that sloth up by printing in draft mode. Draft mode will also save on ink or toner, even if document quality isn’t as vibrant (no problem for every day, casual documents).

4. DOCUMENTS PRINTING WITH STREAKS

Okay, this hack has to do with copiers or scanners. These imaging devices can be just as frustrating as printers.
Let’s get back to our Self-Help Videos for a fast solution to remove vertical streaks on your documents:

5. PRINTER DOCUMENTS BLOTCHED AND FADED

If your printed documents are starting to look like a 90s website, then it’s highly likely the issue is with your printer cartridges. These printer products are expensive, so best not to replace them at once. First, see if cartridges might have dried up.
In our article How To Properly Care For Your Printer Cartridge, we provide a fix for dried up printer cartridges:
“We suggest, first, obtaining two pieces of paper towels, one damp and one wet. Take out your ink cartridge and blot it onto the damp paper towel a few times – with the print head side down. After blotting the print head, hold the cartridge against a dry paper towel for about 30 seconds to a minute. This action should dissipate the dried ink clogging the head. Repeat this process if you’d like, and then slide the cartridge back into your printer and run a test print.
It should be noted that using paper towels only works with integrated cartridge heads, and not with the type that utilizes cartridges that pop into a print head built into the printer.

Regardless, don't forget that many printers today have a clean cycle or can warn you if the issue goes beyond a congested print head. And it's always sensible to open your printer and check inside for any jammed or broken parts."

Give it a shot, and know the article provides other hacks and processes to maintaining printer cartridges.

6. PRINTER NOT CONNECTING TO WI-FI

We mentioned the printer distance to a router as a potential problem with printing. Other issues are possible. We also mentioned David DiEugenio and telling a customer to connect their printer. Here is David in another of our videos, addressing Wi-Fi connectivity problems:

7. WI-FI PRINTING TAKING TOO LONG

If you're connected to the Wi-Fi, and it feels like you're in the days of AOL dial-up, check that your router is adequate, i.e., able to support at least 802.11n and offer the 5GHz band as well as 2.4 GHz. Ensuring firmware up to date is crucial. Not as crucial but helpful is adding a wireless extender or a repeater to increase performance.

8. NEED TO SECURE YOUR PRINTER

Printer security is a major concern today for business management and leadership.

What many don't know is that printer security can be halfway won in the physical world. Forty-four percent of network-connected printers in offices are not secured against unauthorized access, a partial reason why 90 percent of businesses have experienced a security breach in the last year caused by hard copy documents.

What do you do then?

We advise downloading our popular eBook: 5 Hard Copy Data Security Risks In Every Office

It's free and will even make it very hard for that sloth to sneak into your printer…

9. CAN’T PRINT FROM A MOBILE DEVICE

Mobile printing is becoming popular. That, of course, means a slue of new issues. Instead of being bogged down by the complexity of Wi-Fi to a mobile device, go for the app (or just check out the info graphic at the bottom dealing with getting started with wireless printing).
Most Wi-Fi printers support AirPrint, which allows iOS users to print to them (given that both the iPhone or iPad and printer are on the same Wi-Fi network). Nearly all major printer brands have released apps so that iPhone, iPad, and Android users can print from their devices. Some third-party apps let you print to a wider range of printers. Many manufacturers and third-party apps offer a broader choice of print options than AirPrint. Many can initiate scans too.

10. NEED TO PRINT GREENER

Maybe you’re recycling; maybe you’re purchasing environmentally friendly cartridges or paper. But how do you know if you’re making a difference? That might seem as mysterious as to why the sloth got into your printer or copier.
We got you covered. Download our simple but effective Green Office Printing Scorecard.
If you find you need to increase your green footprint regarding printing, read our article *Top 10 Eco-Friendly Printing Practices For Your Office* or download our free eBook, The Green Office Printing Guide.

We hope this list hacks your way into a better printing experience. If you need complimentary advice, please contact us as we’re in the neighborhood.
As a bonus and as mentioned, check out our infographic, *How to Get Started with Wireless Printing:*

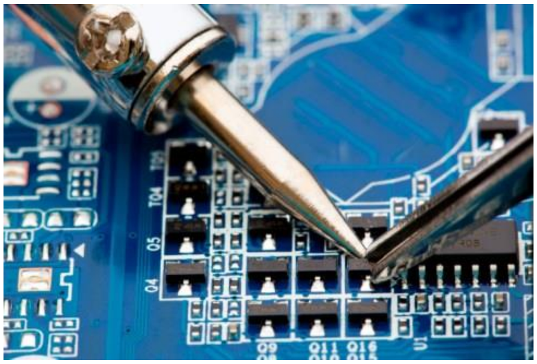
Motherboard Troubleshooting

Common symptoms of motherboard issues are similar to CPU problems: The system does not display anything; an error code appears; one or more beeps occur; the system locks; the system reboots; a Windows BSOD (blue screen of death) appears; or one or more of the ports, expansion slots, or memory modules fails.

Motherboard problems and power problems are probably the most difficult issues to troubleshoot. Because various components are located on the motherboard, many things can cause errors. **POST** (power-on self-test) is one of the most beneficial aids for troubleshooting a motherboard. The meaning of any codes that appear on the screen should be researched. If multiple POST error codes appear, you should troubleshoot them in the order they are presented. The following list helps with motherboard troubleshooting:

- Is the motherboard receiving power? Check the power supply to see if the fan is turning. If the CPU or motherboard has a fan, see if it is turning. Check voltages going from the power supply to the motherboard. See Chapter 5 for directions.
- Check the BIOS/UEFI settings (covered in Chapter 4) for accuracy.
- Check for overheating. Power down the computer and allow the computer to cool. Power on the computer with the cover off.
- Check the motherboard for **distended capacitors**. These are small components that might appear to be bulging. If sighted, replace the motherboard as soon as possible.
- Reseat the CPU, adapters, and memory chips.
- Remove unnecessary adapters and devices and boot the computer.
- Plug the computer into a different power outlet and circuit, if possible.
- Check to determine whether the motherboard is shorting out on the frame.
- Check the CMOS battery (see Chapter 5 for how to take voltage readings).
- With a motherboard that has diagnostic LEDs, check the output for any error code. Refer to the motherboard documentation or online documentation for the problem and possible solution.

Motherboard Failure: Diagnosis And Solutions:



Repair of electronic components.

If your computer suddenly (or not so suddenly) stops working, it’s possible the issue is the motherboard. Unfortunately, they’re also one of the most problematic computer components to repair or replace. Not only is the motherboard usually one of the pricier components on the machine, if you have to replace it you often have to replace the CPU and the memory as well – an expense that can mean a whole new computer would actually be a cheaper alternative.

However, before you dig out the credit cards, there are some things to check because that seemingly dead board may, in fact, be okay. In this article, I’ll show you how to diagnose motherboard problems and some alternatives to replacing a broken board.

What Is a Motherboard?

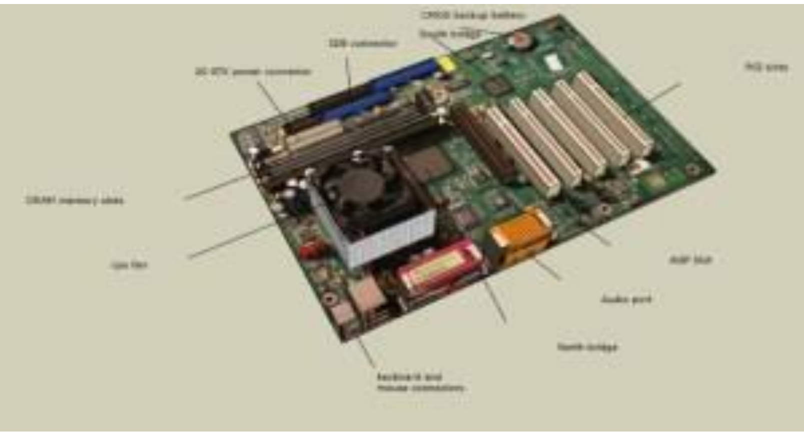
For people who didn’t grow up building computers and who haven’t learned the architecture of these ubiquitous machines, let’s have a brief tutorial about the components of a personal computer and where the motherboard fits into the scheme. Conceptually as well as physically, computers have three basic kinds of components: the processor, the storage (memory and permanent storage as well), and the input/output (I/O) system.

The processor is your CPU, probably a microchip from AMD or Intel, along with your GPU if you have one. The storage is your RAM and your hard drive(s) – where you put your information. Finally, the input/output system is all the elements that let you interact with the computer – the video card and monitor, the keyboard, the mouse, and so on.

So where does the motherboard fit into this system? Well, the motherboard isn’t conceptually important, but it’s physically crucial. It’s the circuit board (really a set of circuit boards put all together) on which all these other components are placed. The CPU plugs into the motherboard, where it communicates via a channel called a “bus” with the hard drive, the memory, the keyboard, and all the rest.

The memory is generally placed directly on the motherboard; the hard drive is probably in its own area, but it connects to a hard drive controller which is located, you guessed it, on the motherboard. The keyboard and the USB slots are wired right into the motherboard. The video card plugs into the motherboard, usually with its own bus.

It’s called a “motherboard” because, like a mothership, it’s the base on which your whole computer operates. No motherboard, no PC.



There are so many wires in there.

Early Warning Signs

If your computer starts to develop issues there are some early warning signs that a part is going bad (most of the time). Here are some things to look out for with your motherboard:

1. Motherboard doesn't recognize/show peripherals.
2. Peripherals will stop working for a few seconds or more.
3. Slow boot-ups could indicate that your motherboard is going bad, though it could be other components as well (more on this below).
4. Computer won't recognize flash drives, or monitor sometimes shows strange lines (particularly relevant if you have onboard video on your motherboard).
5. Motherboard doesn't POST (Power On Self Test).
6. Burning smell or burn marks anywhere on the motherboard itself.
7. Bulging or leaking capacitors

Signs of Failure

Motherboards are historically the most difficult pieces of hardware to diagnose because, in most cases, you have to rule out every other piece of hardware that is connected to it. There aren't usually any real signs of failure, other than your computer suddenly turning into an expensive doorstop.

A hard drive might give you signs of failure, such as blue screens or lost files, but a motherboard will just suddenly stop working. That being said, here are some things you can try first to ensure the problem is with your motherboard instead of another hardware component.

Diagnosing the Problem

There are some easy troubleshooting steps you can take to determine if your motherboard is going bad. Below we break the troubleshooting procedure into two categories: 1) What to check if the computer still passes the POST and boots (or attempts to boot), and 2) what to check if the computer no longer passes the POST or does not even turn on.

Computer Passes POST and Boots OS

If your computer still turns on and even boots into the operating system, you should rule out other hardware components first to make sure these aren't causing the symptoms listed above.

Hard drive(s): Are files taking a long time to transfer? Are you seeing errors or blue screens? Has boot-time increased significantly? Do you hear any clicking or loud whining noises? If the answer to any of these questions is yes, your hard drive may be going bad. It will be worthwhile to run the diagnostic utilities in Windows and/or from the drive's manufacturer. Also, see our companion article on Hard Drive Failure: Warnings and Solutions.

Video: Does the display seem garbled or do you see artifacts on the screen that you did not see before? Do graphics-intensive tasks cause blue screens or instability? If so, your video card may be going bad and will warrant further testing. Also, see our guide on video card failure symptoms for further troubleshooting.

Memory (RAM): Even though it doesn't have any moving parts, there is a chance that your memory could be failing and causing your system to error or become unstable. In this case, a running a diagnostic tool such as Memtest86 or Memtest86+ is recommended for further troubleshooting.

Processor (CPU): Although somewhat rare, CPU failure could be a cause of system instability. If you have an Intel processor, downloading and running the Intel Processor

Diagnostic Tool may uncover issues with the processor itself. For AMD processors, try the AMD system monitor tool.

Power Supply (PSU): A failing or insufficient power supply (or one that is operating out of spec) can quickly cause a system to become unstable and also potentially cause damage to the other computer system components. Ensure you have the proper power supply for your system and double-check the supply's voltages to make sure they are operating in line with their rated output (the voltages can easily be monitored in the BIOS or in software utilities supplied by motherboard manufacturers). If you are still unsure, please also read through our article on power supply troubleshooting.

Motherboard BIOS Updates: Many system instabilities can be fixed by a motherboard BIOS update (especially on newer hardware). Please consult the support site of your motherboard's manufacturer for more details.

Finally, also a brief word on system cooling: In many instances, errors are experienced due to improper cooling or even cooling failure in a computer system. If any of the system's components are operating out of spec due to overheating, system instability can result.

A visual inspection of the system is suggested to make sure that all components are seated properly and being cooled sufficiently (i.e. case and component fans are operating normally). Temps can also be monitored for anomalies inside the operating system using a wide variety of tools – we suggest a few free ones you can use in our article on PC temperature monitoring.

Computer Does Not POST or Turn On

Miniature technicians working on a computer circuit board or motherboard. Tech support concept.

If your computer doesn't pass the POST test or even turn on, hardware failure is almost certain. But the motherboard might still be functional. We want to make certain it's not some other culprit.

The first to thing to do is perform a brief visual inspection on the system itself. Are all components seated properly? If the system turns on, are all the fans spinning? If the motherboard has a visual LED indicator, what color is it (usually green means everything is OK)? If there is any doubt, try re-seating components as necessary and try starting the system again.

Some modern motherboards will even have LEDs for individual components. For instance, if there's a problem with your RAM or CPU, you should be able to find an LED near that specific component, indicating if there's a problem or not (again, green usually means everything is OK).

The second thing to do is confirm whether the motherboard produces error (or beep) codes when trying to start the system up with key components missing (e.g. CPU, RAM, video). This assumes, of course, that the system still turns on.

For example, if you remove the RAM and start the computer, does it respond with error beeps? Do note that some modern motherboards no longer support beep codes (please consult the manual of your motherboard to make sure yours does).   For more details on different motherboard beep (error) codes and what they mean, please consult these resources here.

In some cases it's actually the power supply that's bad. Power supplies can appear to still be functioning, as the power supply fan may still run, as well as the CPU fan and any lights that you might have on your computer. But just because these parts activate, it doesn't mean the power supply is supplying enough juice to the motherboard or other parts of the computer.

The silver CMOS battery inside a motherboard.

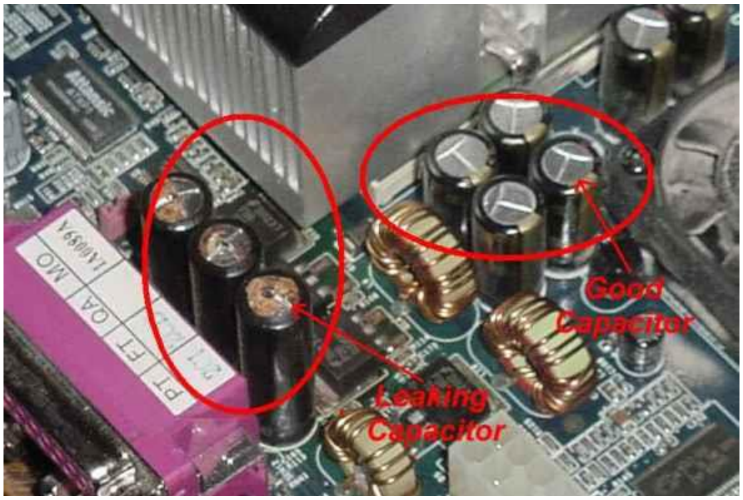
Finally, there are two more quick tests you can perform. The first and quickest is to reset the board's CMOS by removing the battery. The second is to test the components outside the PC case. We have a great step-by-step guide over on the PCMech Forums that will take you through these steps to determine if you have a short or faulty component.

It's Dead – Now What?

Unfortunately, if going through the diagnostic procedures above did not help, it may be time for a new motherboard. There's no real way to tell how your motherboard died. Electronic parts experience wear and tear like anything else.

All parts do eventually die; it's a normal thing, though sometimes motherboards can die from being shorted out by a low-quality power supply. Again, this is something you can determine by putting a new and hopefully higher quality power supply in your machine and seeing if it runs or not.

If you know your motherboard is dead, as an alternate route, you could try and repair your motherboard, but it's no easy task. You would need a solid understanding of electrical components, such as capacitors, for instance. You'd need to not only understand the risk of electrical shock, but also that it's difficult to check if a capacitor is dead on modern motherboards. However, if you want to give it a go, Tom's Hardware has put together an excellent and well-researched guide on replacing capacitors.



The difference between a good capacitor and a capacitor that needs replacing.

For most people, though, they're much better off buying a new motherboard. In this case, it's best to look for an exact replacement. If it's too old, you might want to consider looking into a newer motherboard for your system as long as your components will work with it. On the other hand, it might be worth looking into building an all-new PC if you can afford it.

It’s worth heading on over to the PCMech forums and consulting some of our experts on what board is best to buy for your system. Alternatively, you could get some good advice on building a new PC, if that’s the route you decide to take!

Data Recovery

Another tech support concept of miniature technicians working on recovering data in a hard drive.

As far as data recovery goes with a dead motherboard, you’ve truly lucked out. If it was a dead hard drive, chances are, you’d have to send your hard drive to a data recovery service who would then charge you hundreds or even *thousands* of dollars to recover your data. And that’s *if* your data was even recoverable.

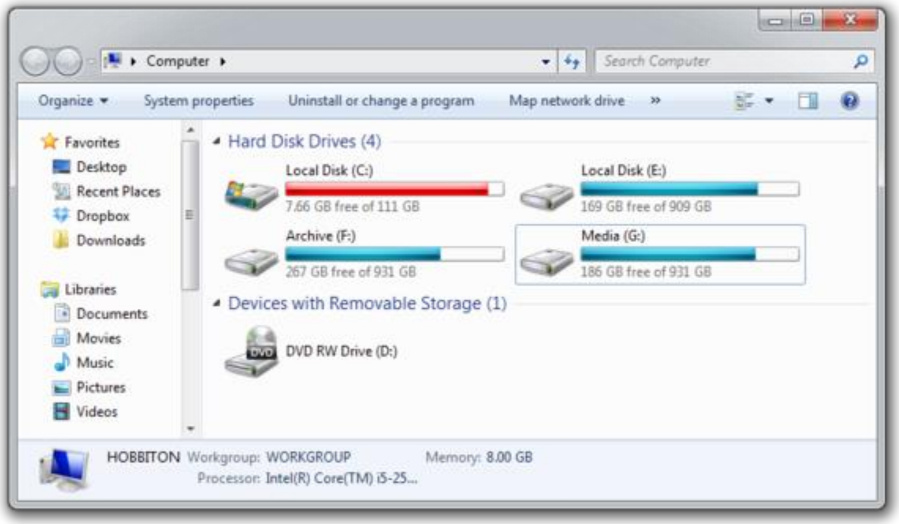
Recovering your data is as simple as getting a new motherboard and putting the computer back together. However, with your old hard drive plugged in, you’ll need to select it as the boot device in the BIOS settings first. After that, all of your data should still be there on bootup.

Alternatively, all you need is an adapter that turns your hard drive into an external hard drive. At that point, you can just plug it into another computer and all of your data should be available.

My computer is too slow

The first step to fixing a slow computer is to verify that your machine is the actual source of the problem. Videos that seem to buffer forever, and websites that take ages to load, may not be your computer’s fault. Geek Squad agent Derek Meister claims that many people mistakenly identify a slow system as the problem when “it’s actually not the computer, [but] their broadband connection.” See “Downloads are taking forever” below for instructions on how to use Speedtest.net to diagnose a slow connection.

If the problem is your PC, check whether you have plenty of free space on the hard drive holding your operating system. Windows needs room to create files while your system is running. If your hard drive is maxed out, performance suffers. Now is the perfect time to clear some space.



Hard Disk Drives (4)

Local Disk (C:) 7.66 GB free of 111 GB

Local Disk (E:) 169 GB free of 909 GB

Archive (F:) 267 GB free of 931 GB

Media (G:) 186 GB free of 931 GB

Devices with Removable Storage (1)

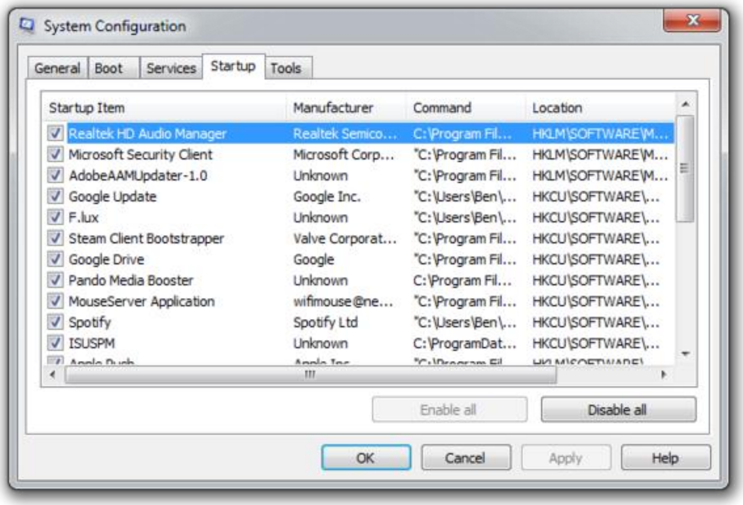
DVD RW Drive (D:)

HOBBITON Workgroup: WORKGROUP Memory: 8.00 GB
Processor: Intel(R) Core(TM) i5-25...

If your computer's operating system resides on an overstuffed C: drive, clearing out some space could boost OS performance.

Microsoft's System Configuration tool is your next-best bet for tackling slow performance. Many applications launch automatically when your machine boots up, which can stretch out boot time—especially on older, slower PCs. Make a habit of trimming the startup items. Open the tool by pressing Windows-R, typing `msconfig`, and pressing the Enter key.

Checking the Startup Item and Manufacturer columns is the best way to figure out which potential performance-killers you can safely disable. Avoid messing with any of the services and programs that have Microsoft Corporation listed as the manufacturer. Items such as AdobeAAMUpdater, Google Update, Pando Media Booster, Spotify, and Steam Client Bootstrapper are all fair game. Regardless, err on the side of caution: If you're not sure what the program or service does, don't disable it.



Startup Item	Manufacturer	Command	Location
☑ Realtek HD Audio Manager	Realtek Semico...	C:\Program Fil...	HKLM\SOFTWARE\M...
☑ Microsoft Security Client	Microsoft Corp...	"C:\Program Fil...	HKLM\SOFTWARE\M...
☑ AdobeAAMUpdater-1.0	Unknown	"C:\Program Fil...	HKLM\SOFTWARE\M...
☑ Google Update	Google Inc.	"C:\Users\Ben\...	HKCU\SOFTWARE\...
☑ F.lux	Unknown	"C:\Users\Ben\...	HKCU\SOFTWARE\...
☑ Steam Client Bootstrapper	Valve Corporat...	"C:\Program Fil...	HKCU\SOFTWARE\...
☑ Google Drive	Google	"C:\Program Fil...	HKCU\SOFTWARE\...
☑ Pando Media Booster	Unknown	C:\Program Fil...	HKCU\SOFTWARE\...
☑ MouseServer Application	wifimouse@ne...	"C:\Program Fil...	HKCU\SOFTWARE\...
☑ Spotify	Spotify Ltd	"C:\Users\Ben\...	HKCU\SOFTWARE\...
☑ ISUSPM	Unknown	C:\ProgramDat...	HKCU\SOFTWARE\...
☑ Apple Push	Apple Inc.	"C:\Program Fil...	HKLM\SOFTWARE\

Windows’ System Configuration Tool lets you disable programs and services that automatically start when you boot your computer.

Once you’ve made all your changes, click *OK* and restart the computer. It should boot up quicker and feel noticeably faster.

Downloads are taking forever

Speedtest.net is your best friend when you’re having connectivity problems. Run a speed test to see what your download and upload speeds are—ideally they should be at least 50 percent of your Internet service provider’s advertised speeds, with a ping under 100 milliseconds.

If the speeds seem solid, make sure that you aren’t inadvertently downloading or uploading anything. Many torrent downloading programs run in the background and minimize into the system tray instead of the taskbar.

A good speed test should give you an accurate assessment of your ping, download speed, and upload speed.

Check your network hardware. Updates for network cards aren’t all that common, but if your card’s manufacturer offers a newer driver, download it. Resetting your router and modem can help with connection problems, too. Most routers and modems have reset buttons, but pulling the power cable for a second or two can do the same thing. Don’t cut the power for much longer, or the hardware may reset itself to factory defaults.

Still having problems? Call your ISP, which can tell you whether the problem is on your end. As a last-ditch measure, the ISP could reset the master connection to your home.

My machine keeps restarting

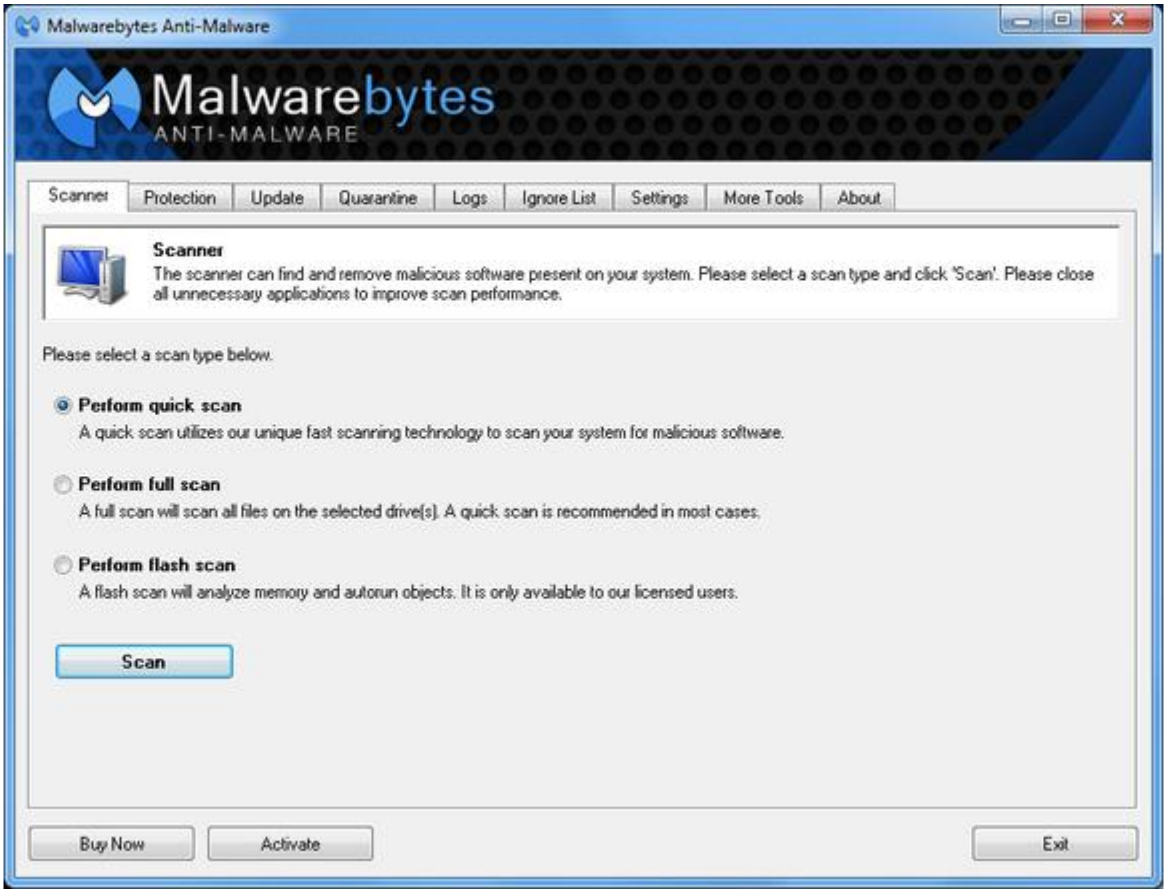
Hardware problems are hard to diagnose and solve. First, confirm that you aren’t just getting the latest wave of Windows updates, which can automatically restart your computer during installation. Then work on updating all of your critical system drivers. Your graphics card, motherboard, and network card drivers are crucial.

“Sometimes it can be viruses, sometimes it can be adware, sometimes it can be overheating, and sometimes it can be something as simple as making sure your video card is updated,” Geek Squad’s Meister says.

Is your computer making weird noises? If you’re lucky all you’ll need to do is give the machine a thorough cleaning. Modern computers have safeguards that shut down the system if a component is overheating, which can be the cause of frequent restarts when you’re running resource-intensive programs or video games.

Pop-up ads are appearing on my desktop

If you’re not running your Web browser and are still getting pop-up ads on your desktop, you’ve most likely installed adware—a program that displays unwanted ads. Although benevolent adware exists, most of the time adware is up to no good. Getting rid of it isn’t easy. “There’s a ton of little system-utility tools out there that promise to clean up everything, with names like PC Speed-up, PC Speed Pro, PC Speedifier,” Geek Squad’s Meister says. “A lot of times those programs are not going to do much. Some programs will work, others are snake oil.”



Scanner

The scanner can find and remove malicious software present on your system. Please select a scan type and click 'Scan'. Please close all unnecessary applications to improve scan performance.

Please select a scan type below.

● **Perform quick scan**
A quick scan utilizes our unique fast scanning technology to scan your system for malicious software.

○ **Perform full scan**
A full scan will scan all files on the selected drive(s). A quick scan is recommended in most cases.

○ **Perform flash scan**
A flash scan will analyze memory and autorun objects. It is only available to our licensed users.

Avoid downloading programs that offer to speed up your PC or clean up your registry. Instead, use a trustworthy adware scanner like the free version of Malwarebytes’ Anti-Malware tool.

Running a full scan with credible antivirus software is your first step. If that program doesn’t find and remove the adware, turn to Malwarebytes Anti-Malware Free, a great utility for removing all types of malware. Just make sure to disable your standard antivirus software before running it.

“Multiple antivirus programs working at the same time will often result in problems,” Falcon Northwest’s Petrie says. “You only want one active, real-time antivirus scanner installed, but it doesn’t hurt to run an additional ‘on demand’ virus or malware scanner.”

Searching online for the name of the advertised product can sometimes yield solutions from fellow victims. If all else fails, there’s always the nuclear option: a complete system reinstall. It might take a long time, but it’s the only surefire way to remove adware or spyware. Remember to back up all your personal files.

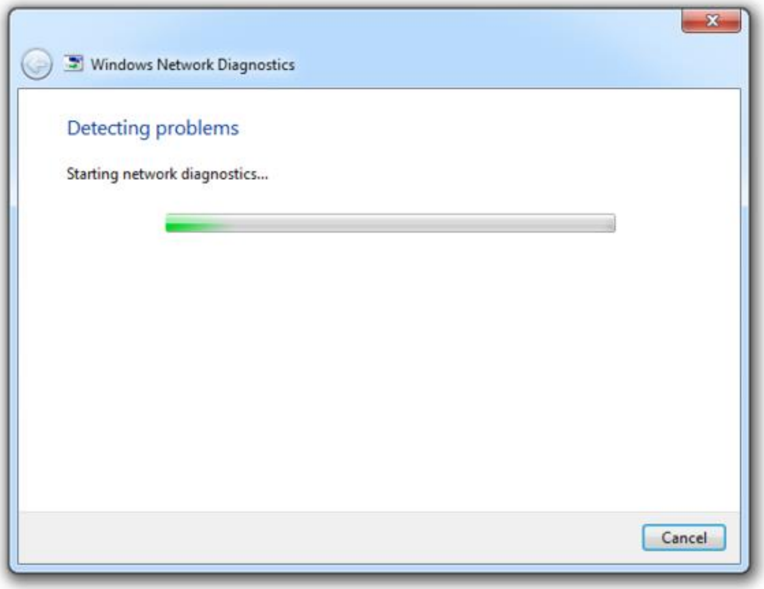
Google doesn’t look right

Browser hijackers are a particularly nasty breed of malware. Such programs take over your Web browser and can stealthily redirect your Google searches and other queries to fake pages meant to steal your personal information or to further infect your system.

Running a real-time antivirus utility is the best way to stay safe. If your browser has already been hijacked, uninstall the browser and use your antivirus program in conjunction with Malwarebytes to remove the intruder.

My Wi-Fi keeps disconnecting

Spotty wireless connections can be a puzzler. Is it your computer? Your router? Your ISP? Try a few things before calling your Internet service provider.

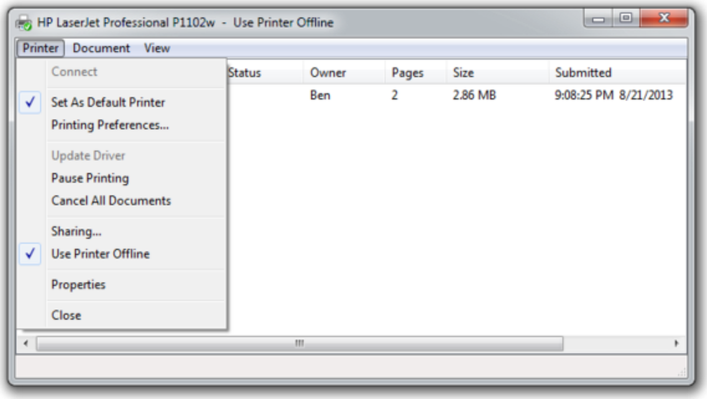


Detecting problems

Starting network diagnostics...

Windows Network Diagnostics may not always solve your problem, but it will usually point you in the right direction.

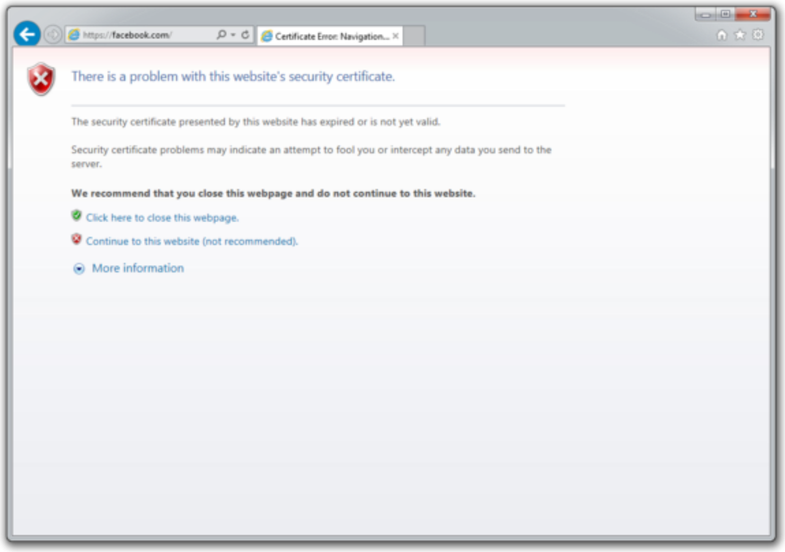
Confirm that your computer is within range of your wireless router. Weak signals mean weak connections. Next, make sure your PC’s wireless card has the latest drivers. Try letting Windows troubleshoot for you by right-clicking the Wi-Fi icon in the taskbar and selecting *Troubleshoot problems*.



Status	Owner	Pages	Size	Submitted
	Ben	2	2.86 MB	9:08:25 PM 8/21/2013

I keep seeing ‘There is a problem with this website’s security certificate’

Sometimes the biggest problems have the easiest fixes. According to support technicians, the lion’s share of issues are due to an incorrect system clock.



There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

The problem is probably with your computer.

Website security certificates sync up with your computer’s clock. Old computers in particular run the risk of having a dead CMOS battery—the watch battery in your computer that keeps its system clock ticking. Click the clock in the system tray and select *Change date and time settings* to correct any issues.

My printer won’t print

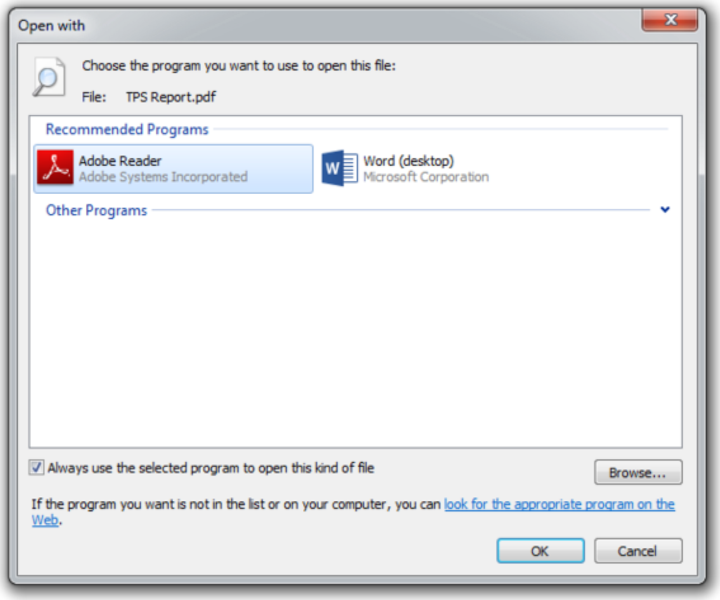
Let’s assume that your printer’s drivers are up-to-date, and that it has enough paper and ink or toner to print. Try turning the printer off and on. Unplug the printer and plug it back in. Check your printer’s print queue by looking for the printer icon in the system tray and double-clicking it. The print queue shows you the status of each job as well as the general status of your printer.

The print queue is your best bet for troubleshooting printer problems—just make sure that ‘Use Printer Offline’ isn’t selected.

Ensure that ‘Use Printer Offline’ isn’t checked. Sometimes, printing while your printer is turned off can cause Windows to set your printer to work offline, and that can stall jobs sent later.

I can’t open email attachments

If you have ever encountered an attachment that you couldn’t open, it was probably because you didn’t have the software necessary to view the file.



Choose the program you want to use to open this file:

File: TPS Report.pdf

☑ Always use the selected program to open this kind of file

If the program you want is not in the list or on your computer, you can look for the appropriate program on the Web.

If you don’t have Adobe Reader or another PDF-compatible program, you won’t be able to open that TPS report.

The usual suspect is the .pdf file, for which you can download a free PDF reader. If your problem involves a different file format, a quick search on the attachment’s file extension (the three letters after the period in the filename) should tell you what type of program you need. If the attachment lacks a file extension (which might happen if it was renamed), adding it back should set things right.

Hardware Troubleshooting Techniques

Troubleshooting Network Cards

Cabling is one of the biggest problems encountered in a network installation. Is it connected? Are all the connections good? Is the cable type correct? Has there been any termination, and if so, has it been done correctly? The most efficient way to test network cable is to use a line tester to check its functionality.

With UTP cabling, simply unplug the cable from the adapter card and plug it into the tester. If coaxial cable is used, you must unplug both ends of the cable from the network, install a terminating resistor at one end of the cable, and plug the other end into the tester. The tester performs the tests required to analyze the cable and connection.

Most network adapter cards come from the manufacturer with an OEM disk or CD-ROM of drivers and diagnostic utilities for that particular card. You can run these diagnostic utilities to verify that the LAN hardware is functioning properly.

However, it might be easier to run the Windows PING utility from the command prompt and attempt to connect to the network. In a LAN environment, you need to know the IP address or the name of a remote computer in the network to which you can direct the PING.
Both PING and TRACERT can be used to identify the IP address of a known network address.

Working on Portable Systems

One of the biggest problems for portable computers is heat buildup inside the case. Because conventional power supplies (and their fans) are not included in portable units, separate fans must be designed in portables to carry the heat out of the unit. The closeness of the portable's components and the small amount of free air space inside their cases also adds to heat-related design problems.

The internal PC boards of the portable computer are designed to fit around the nuances of the portable case and its components, rather than to match a standard design with standard spacing and connections. Therefore, interchangeability of parts with other machines or makers goes by the wayside. The only source of most portable computer parts, with the exception of PC Cards and disk drive units, is the original manufacturer. Even the battery case might be proprietary. If the battery dies, you must hope that the original maker has a supply of that particular model.

Although adding RAM and options to desktop and tower units is a relatively easy and straightforward process, the same tasks in notebook computers can be difficult. In some notebooks, you must disassemble the two halves of the case and remove the keyboard to add RAM modules to the system. In other portables, the hinged display unit must be removed to disassemble the unit. Inside the notebook, you might find several of the components are hidden behind other units. Figure 3.14 demonstrates a relatively simple disassembly process for a notebook unit.

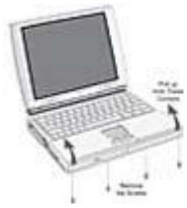


Figure 3.14 Disassembling a notebook computer.

In this example, a panel in front of the keyboard can be removed to gain access to the notebook's internal user-serviceable components. Four screws along the front edge of the unit's lower body must be removed. Afterward, the LCD panel is opened and the front panel of the notebook's chassis is pulled up and away to expose a portion of the unit's interior.

Troubleshooting PCMCIA Problems

One of the mainstays of portable computer products is the credit card-like *PCMCIA cards*, also known as *PC Cards*. The process for troubleshooting PC Cards is nearly identical to troubleshooting other I/O adapter cards.

PCMCIA cards can be plugged into the system at any time and the system should recognize them. In most cases, Windows 9x, Windows Me, Windows 2000, and Windows XP have a copy of the necessary driver software for the PCMCIA adapter being installed and will install it automatically when it detects the adapter. Most Windows operating system versions display messages telling you that they are installing the drivers required. However, Windows 2000 and Windows XP just install the drivers without a notice.

In cases in which the operating system does not have the necessary driver software, it prompts you for a path to the location where the driver can be loaded, when it detects the adapter. PCMCIA manufacturers typically supply drivers for various operating systems on a floppy disk or a CD that comes with the adapter.

To verify that the PC Card device is working, access Device Manager. If there is a problem with the PC Card device, it appears in Device Manager. If the PCMCIA adapter's icon shows an exclamation mark on a yellow background, the card is not functioning properly. Turn the system off and reinsert the device in a different PCMCIA slot. If the same problem appears, three possible sources of problems exist—the card might be faulty, the PC Card controller in the PC might be faulty, or the operating system might not support the device in question.
If the Windows Device Manager displays the PCMCIA socket but no name for the card, the card insertion has been recognized but the socket could not read the device's configuration information from the card. This indicates a problem with the PCMCIA socket installation. To correct this problem, remove the PCMCIA socket listing from Device Manager, reboot the computer, and allow the Windows PnP process to detect the socket and install the appropriate driver for it. If the names of the PCMCIA cards do not appear after the restart, the reinstallation process was not successful. Therefore, the PCMCIA socket you are using is not supported by the operating system version.

If the names of other PCMCIA cards do appear in the Device Manager, but the card in question does not, it is likely that the card has been damaged. To test the PC Card device, insert a different PC Card device of any type in the slot. If the other card works, it is very likely that the card in question has been damaged.

Troubleshooting Portable Unique Storage
As with other PCMCIA devices, PC Card hard drives are self-contained. Plug them into the PCMCIA slot and the system should detect them (they are hot-swappable). If the system does not detect the card/hard drive, use the troubleshooting steps described for other PCMCIA devices.

Troubleshooting Batteries

If you turn your portable computer on and nothing happens, the first things to check out include the power supply and the battery. If the power supply is plugged in, the computer should start up when the On/Off switch is engaged. However, if the computer is running on battery power and the system does not start up, the battery could be bad or need to be charged.

Verify that the battery doesn't need a recharge by trying to start the system with the AC power adapter plugged in. Check the power indicator in the system display panel. If it is on, power is being supplied to the portable. If the indicator is not on, verify that the power cord is securely connected to a live power source. Check all the power connections to ensure that the AC adapter jack is securely connected to the AC adapter port.

If the portable still doesn't start up, you must troubleshoot the system board. If the system runs from the AC adapter, the battery needs to be recharged or replaced.

Although a dead system is a classic battery/power-supply problem, you might encounter several other battery-related problems with portable computers. These include problems that present the following types of symptoms:

- You receive warning messages about the battery not charging.
- The computer experiences intermittent system shut downs when operating with only the battery.
- The computer does not recognize its network connection when operating with only the battery.
- The computer and input devices are slow when operating with only the battery.
- The computer loses the time and date information when operating on battery power.

A loose or improperly installed battery can cause these problems. They can also appear when the battery is toward the end of its charge/recharge cycle. Check the installation and attempt to recharge the battery using the portable computer's AC adapter.

The actual life of a laptop computer battery varies from just under one hour to over two hours in each sitting. If you are experiencing battery life cycles that are significantly shorter than this (for example, 10 to 15 minutes), you might have a problem referred to as *battery memory*.

Battery memory is a condition that occurs with some types of batteries in which the battery becomes internally conditioned to run for less time than its designed capacity (for example, if you routinely operate the computer using the battery for an hour and then plug it back in to an AC source, the battery can become conditioned to only run for that amount of time).

To correct battery memory problems, you must fully discharge the battery and then recharge it. To accomplish this, complete the following steps:

1. Turn the portable's Power Management feature off by accessing the Power Management icon in the Windows Control Panel.

2. Restart the computer and access the CMOS setup utility during bootup.

3. Disable the power management functions in the CMOS settings.

4. Start the portable computer using only the battery and allow it to run until it completely discharges the battery and quits.

5. Recharge the battery for at least 12 hours.

6. Repeat this process several times watching for consistently increasing operating times.

Troubleshooting Docking Stations/Port Replicators

Most docking stations offer an internal power supply that can operate the portable and its peripheral attachments: an external parallel port for printers, a serial port for serial devices (mice and modems), USB ports, external VGA/DVI video and full size keyboard connections, and audio connections for external speakers.

In addition, the docking station can host several types of external storage devices, including full-sized FDD/HDD/CD-ROM/DVD drives. Docking stations might also include one or two PCI slots that allow full-sized desktop adapter cards (SCSI or specialized video or LAN card) to be added to the system when it is docked. They might also provide multiple PCMCIA slots that add to the existing PC Card capabilities of the portable it is supporting.

For the most part, these connections are simply physical extensions of the ports provided by the portable. Therefore, if the port works on the portable and doesn't work when connection is made through the docking station, generally something is wrong with the docking station/port replicator. However, many portable computers employ special keystroke combinations (Fn + some other key) to activate external devices, such as a video display monitors or full-size keyboards.

For example, some portables detect that the external video display has been attached. Others use an Fn key combination to switch the display to the external monitor only, and then use another Fn key combination to send the display to both the LCD panel and the external display (that is, internal, external, or both).

If a peripheral device is not working, one of the first steps to take is to refer to the portable's documentation to ensure that the external device has been activated.

For audio problems, verify that the speakers are connected to the correct RCA mini jacks (not the Line IN or Microphone jacks). Check the documentation to ensure the sound output has not been muted using an Fn key combination.

On Windows operating systems, the hardware profile information for the portable computer can be configured differently for docked and undocked situations. When the computer is docked and turned on, its configuration is reset and the *Eject PC* option appears on the Start menu. However, when the computer is not docked, the Eject PC option is automatically removed from the Start menu.

The Windows 2000 and Windows XP Professional operating systems use hardware profiles to determine which drivers to load when the system hardware changes (docked or undocked). It uses the *Docked Profile* to load drivers when the portable computer is docked and the Undocked Profile when the computer starts up without the docking station. These hardware profiles are created by the Windows XP operating system when the computer is docked and undocked if the system is PnP compliant.

If a portable is not PnP compliant, you must manually configure the profile by enabling and disabling various devices present when docked and undocked.

The first check is to verify the power cord connection and docking power supply. Next verify that the portable has been properly inserted in the docking station or port replicator.

If a single docking station connection does not work, bypass the docking station/replicator and try to operate the peripheral directly with the portable unit. Check the power supply for both the docking station and the peripheral device and verify that both are turned on. Reboot the portable while it is attached to the docking station. Then check any signal cables between the docking station and the peripheral.

If the PS/2 mouse connection does not work, verify that it has not been installed in the PS/2 keyboard connector by mistake. Verify that the mouse port is enabled in the CMOS setup utility. Likewise, if you are using a USB or serial mouse, verify that the port is enabled in CMOS and that it is connected to the correct port.

Check the serial port's configuration settings to verify that a proper device driver has been installed for the mouse.

If the portable's touch pad works but the external mouse does not, check the computer's documentation for an Fn key combination requirement for the mouse.