Computers and Stuff.

Sam Houliston.

Report scams to the ACCC via www.scamwatch.gov.au or by calling 1300 795 995.

How to tell if you've got Malware.

Picture this: you start your computer and wait. And wait. And wait some more. When your desktop finally shows its face, things don't get any better. Your Internet is sluggish, your programs are taking forever to load, and your cursor is dragging 20 seconds behind your mouse. You might have tried to open too many programs at once. Or…You might be infected.

Sometimes a malware infection is as plain as day. Other times it's a silent killer. If you want to know whether or not your machine is sick, you first need to understand the symptoms. So let's take a look at the telltale signs.

You've got ransomware.

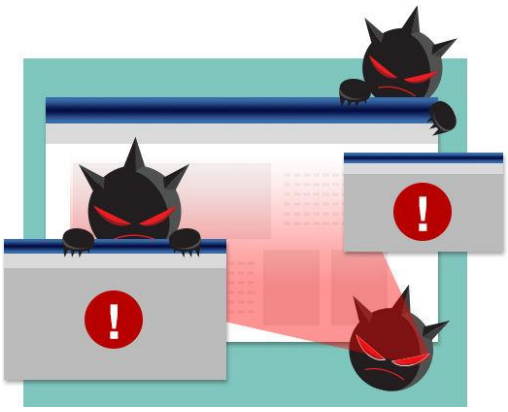
This one's the most obvious. Ransomware authors want to make it perfectly clear that you have a malware infection—that's how they make their money. If you've got ransomware, you'll get a pop-up that tells you your files have been encrypted and there's a deadline to pay a ransom in order to get them back.

Browser redirects.

You click on a link after doing a Google search on "my computer's acting strange." Link opens to a different page. You head back to your search results and try a different link. Same thing happens. Over and over you're redirected to a different site from the one you're trying to reach. That, my friend, is a malware infection.

Different home page.
Say you set your home page to be your favourite sports news site. But for some reason, Yahoo.com keeps coming up. You also notice some new toolbars (rows of selectable icons) below your browser window that you can't get rid of. You could either have a major case of the forgets, or, more likely, you've got an infection.

Bombarded with pop-ups.
A pop-up appears on your computer, you close it, another one opens. Or you're not even online, and you're getting pop-up messages on your system. Some sites admittedly have terrible ad experiences that feel like something nefarious is going on (but really isn't). Most of the time, if your screen is loaded with pop-ups, you're looking at an adware or spyware infection.



Computer running slow.
Lots of things can contribute to a slow computer. You could be running too many programs at once, you may be running out of hard drive space, or there's not enough free memory. If none of those are true for you and your computer is still slow, it's possible you're infected.

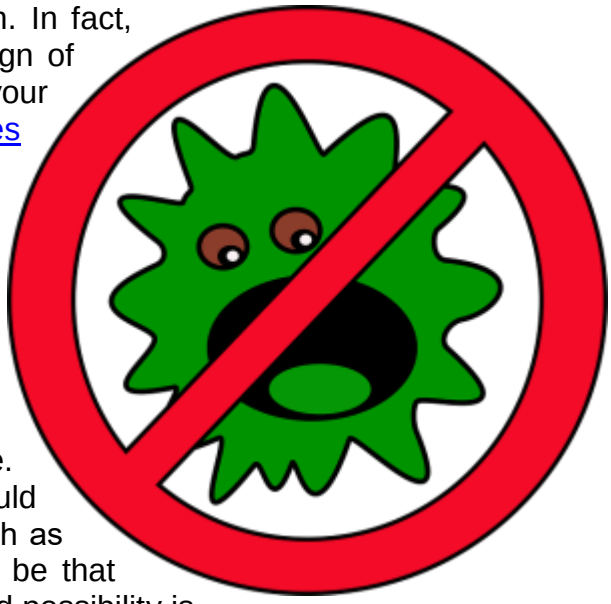
New, unfamiliar icons on desktop.
Maybe your nephew Timmy jumped on without your knowledge and downloaded a photo editing program so he could swap his face with his dog's face and share it on social media. Or perhaps you downloaded a legitimate piece of software and a Potentially Unwanted Program (PUP) hitched a ride. If it's the latter, your computer could be weighed down by PUPs, which Malwarebytes and many other security companies consider malware.

Constant crashing.
There are a couple reasons why your applications or system might crash, including potential incompatibility between programs or software and hardware that needs updating. However, some forms of malware, such as rootkits, dig deep into the Windows kernel and latch on, creating instability.

Web browser freezes or is unresponsive.
Slow Internet could be just that—check your WIFI signal or your download speeds with your Internet provider to be sure. But if everything checks out and your browser grinds to a halt, it could be a sign of infection.

Lots of bounced email.
We've all mistakenly typed in the wrong email address and hit "send." But if you're getting a suspiciously high number of bounces, or emails that return to your inbox undelivered, something else is going on. First, your email address could have been hacked and is now being used to spam the crap out of your contacts list. Or malware could be the culprit. How? An infected computer sends out emails using the addresses it found in your computer. If the "To" address doesn't work, the message bounces back to the "From" address, which is often yours.

No sign at all.
Is your computer running like a smooth criminal? No issues whatsoever? You still might be infected. Many forms of malware, including botnets and others designed to steal your data, are nearly impossible to detect unless you run a scan. In fact, whether it's plainly obviously or there's no real sign of malware, you should be regularly scanning your computer with security programs like Malwarebytes Anti-Malware. If malware is detected, follow these simple steps to clean your computer.



Malware is not exclusive to computers either, it can also affect your mobile devices.

Battery life drains quickly.
Oh yes, your cell phone is not immune to malware. If you notice your battery life draining quickly, it could be that you've got some hefty programs open, such as games or music streaming services. It could also be that your battery is on its last leg. Unfortunately, the third possibility is mobile malware.

Unusually large bill.
This one's pretty clear-cut. Pay close attention to your mobile phone bill. Are you being charged for messages you didn't send? Is your data plan getting busted? Are you getting texts from your provider saying you owe money for something you didn't purchase? Mobile malware is to blame. You can protect against mobile threats using anti-malware software designed specifically for smartphones and tablets. For example, Malwarebytes Anti-Malware Mobile

safeguards Android devices from malware, infected applications, and unauthorized surveillance.

How does anti-malware work?

For the better part of 20 years, cyber security remained mostly under the public awareness radar. It was not exactly a topic for discussion at the Griswold family Christmas party.

“Mom in 1995: You're doing what, Timmy? Making antivirus? I thought you did something with computers, not medicine!”

Fighting cyber crime fell squarely on the shoulders of computer scientist heroes - until now!

Now that cyber security is being covered in the news and talked about at the dinner table, people are realizing they need to step up and join in the fight. They're faced with important questions like: what's a virus, what's malware, what's the difference between antivirus and anti-malware programs, and how does any of this work?

So let's start at the beginning. How does anti-malware work? Before we can tell you that, we need to backtrack a little and explain about malware.

What is malware?
Malware is bad software, plain and simple. It's code that was created for the purpose of doing something sinister to your computer. Most of the time, it infiltrates a person's system without their knowledge. There are many different types of malware and here's where it starts to get confusing. Types of malware were typically named not for what they do but how they attack the machine. This is because engineering nerds who were the first to encounter malware were more interested in the method of delivery instead of the end-goal—which is why one category of malware that "tricks" a system in order to invade it is called a Trojan horse and not, say, a data deleter.

Other types of malware include viruses, which infect legitimate files, backdoors, which can open programs and steal data from your computer, and rootkits, which can spy and collect passwords. One of the more dangerous forms of malware, aptly named ransomware, literally holds your files for ransom by encrypting them. If you pay up, you might get the decryption key to regain access to them. If you don't, they're unavailable forever.

Another form of malware that is perhaps a little less mal is called a Potentially Unwanted Program (PUP). "Potentially Unwanted Programs is a euphemism," says Scott Wilson, Technical Product Manager at Malwarebytes. "These are programs you actually agree to install, but the agreement is generally obtained in a sneaky manner, such as having a pre-checked box on one of the many installation pages you need to click through. Many people find these programs to be annoying—interfering with your search behaviour or displaying advertising on your computer are common behaviours—so anti-malware products help you deal with and remove such programs."

So what, exactly, is anti-malware software?

Now that you know a little bit about malware, let's discuss the programs that were designed to fight it off. Anti-malware is a piece of software that you knowingly install on your computer with the purpose of protecting your system from malware infiltration and infection. Anti-malware programs are able to do this in three ways: they detect malware on your computer, safely remove it, and clean up any of the damage to the computer that the malware may have caused.

In addition, some premium programs, like Malwarebytes Anti-Malware Premium, have malicious website blocking and real-time protection. In plain English, this means the programs block websites created with the intent of delivering malware as well as those that might be compromised by malware. It also means that the anti-malware runs continuously in the background so that if a piece of malware does try to install on your system, it steps in and shows the bad guys who's boss.

How does anti-malware software do its job?

Many programs scan for malware using a database of known malware definitions (also called signatures). These definitions tell what the malware does and how to recognize it. If the anti-malware program detects a file that matches the definition, it'll flag it as potential malware. This is a good way to remove known threats, but it does require regular updates to make sure the program doesn't miss out on newly developed malware.

Another way anti-malware (AM) detects bad software is a form of analysis called heuristics. An alternative to database scanning, heuristic analysis allows anti-malware programs to detect threats that were not previously discovered. Heuristics identifies malware by behaviours and

characteristics, instead of comparing against a list of known malware. For example, if an application is programmed to remove important system files, the anti-malware software may flag it as malware (since applications should not be doing that). But, heuristic analysis can sometimes result in "false positives," or programs flagged as malware that are actually legitimate.

A third way AM software can find malware is by running a program it suspects to be malicious in a sandbox, which is a protected space on the computer. The program believes it has full access to the computer when, in fact, it is running in an enclosed space while the anti-malware monitors its behaviour. If it demonstrates malicious behaviour, the anti-malware will terminate it. Otherwise, the program is allowed to execute outside the sandbox. However, some forms of malware are smart enough to know when they're running in a sandbox and will stay on their best behaviour…until they're allowed free access to the computer. Sneaky little scoundrels.

Thankfully, anti-malware doesn't just flag malware and be on its way. Once malware has been found on a system, it needs to be removed. Many threats can be deleted by the anti-malware program as soon as they are detected. However, some malware is designed to cause further damage to your computer if it is removed. If your anti-malware suspects this is the case, it will usually quarantine the file in a safe area of your computer's storage. Basically, the anti-malware puts the malware in a timeout. Quarantining a malicious file prevents it from causing harm, and allows you to remove the file manually without damaging your computer.

So there you have it! That's anti-malware in a nutshell. Now that you're armed with this knowledge, you can calm your conspiracy theory uncle down when he worries about the hackers who are going to steal information from his online Christmas orders. The fact that he knows this is a possibility is a step in the right direction. And the fact that you can now educate him is a win in the fight against malware.

10 ways to protect against hackers

Hackers are a scary bunch—whether working as part of a criminal syndicate or an idealist with a political agenda, they've got the knowledge and the power to access your most precious data. If hackers want to target a particular company, for example, they can find vast amounts of information on that company just by searching the web.

They can then use that info to exploit weaknesses in the company's security, which in turn puts the data you've entrusted to that company in jeopardy.

Think of your home computer as a company. What can you do to protect it against hackers? Instead of sitting back and waiting to get infected, why not arm yourself and fight back?

1. Update your OS and other software frequently, if not automatically. This keeps hackers from accessing your computer through vulnerabilities in outdated programs. For extra protection, enable Microsoft product updates so that the Office Suite will be updated at the same time. Consider retiring particularly susceptible software such as Java or Flash.

2 Download up-to-date security programs, including antivirus and anti-malware software, anti-spyware and a firewall (if your OS didn't come pre-packaged with it). To trick even the most villainous hackers, consider investing in anti-exploit technology, such as Malwarebytes Anti-Exploit, so you can stop attacks before they happen.

3. Destroy all traces of your personal info on hardware you plan on selling. Consider using d-ban to erase your hard drive. For those looking to pillage your recycled devices, this makes information much more difficult to recover. If the information you'd like to protect is critical enough, the best tool for the job is a chainsaw.

4. Do not use open WIFI; it makes it too easy for hackers to steal your connection and download illegal files. Protect your WIFI with an encrypted password and consider refreshing your equipment every few years. Some routers have vulnerabilities that are never patched. Newer routers allow you to provide guests with segregated wireless access. Plus, they make frequent password changes easier. Speaking of passwords: password protect all of your devices, including your desktop, laptop, phone, smartwatch, tablet, camera, …you get the idea. The ubiquity of mobile devices makes them especially vulnerable. Lock your phone and make the timeout fairly short. Use fingerprint lock for the iPhone and passkey or swipe for Android.

5. It's easy to forget that mobile devices are essentially small computers that just happen to fit in your pocket and can be used as a phone. Your mobile device contains a veritable treasure trove of personal information and, once unlocked, can lead to devastating consequences. Create difficult passwords and change them frequently. In addition, never use the same passwords across multiple services. If that's as painful as a stake to a vampire's heart, use a password manager like LastPass or Roboform.

6. For extra hacker protectant, ask about two-step authentication. Several services have only recently started to offer two-factor authentication, and they require the user to initiate the process. Trust us, the extra friction is worth it. Two-factor authentication makes taking over an account that much more difficult, and on the flip side, much easier to reclaim should the worst happen.

7. Come up with creative answers for your security questions. People can now figure out your mother's maiden name or where you graduated from high school with a simple Google search. Consider answering like a crazy person. If Bank of America asks, "What was the name of your first boyfriend/girlfriend?" reply "your mom." Just don't forget that's how you answered when they ask you again.

8. Practice smart surfing and emailing. Phishing campaigns still exist, but hackers have become much cleverer than that Nigerian prince who needs your money. Hover over links to see the actual email address from which the email was sent. Is it really from the person or company claiming to send them? If you're not sure, pay attention to awkward sentence construction and formatting. If something still seems fishy, do a quick search on the Internet for the subject line. Others may have been scammed and posted about it online.

9. Don't link accounts. If you want to comment on an article and you're prompted to sign in with Twitter or Facebook, do not go behind the door. Convenience always lessens your security posture, linking accounts allows services to acquire a staggering amount of personal information."

10. Keep sensitive data off the cloud. No matter which way you cut it, data stored on the cloud doesn't belong to you, there are very few cloud storage solutions that offer encryption for 'data at rest.' Use the cloud accordingly. If it's important, don't.

Honourable mention:
Alarmist webpages announcing that there are "critical errors" on your computer are lies. Microsoft will never contact you in person to remove threats. These messages come from scammers, and if you allow them to remotely connect to your computer, they could try to steal your information and your money. If that's not a Nightmare on Elm Street, then we don't know what is.

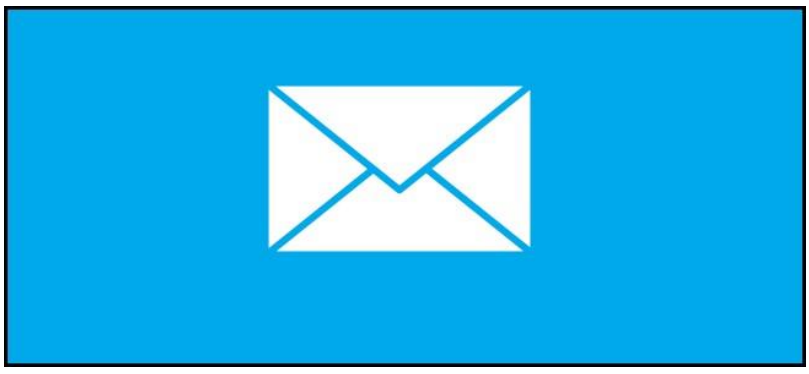
Windows 10 Mail.

Outlook Express was a popular free email program (or application) from Microsoft in the days of Windows XP. But Microsoft discontinued support of Outlook Express. With the advent of Windows Vista, Microsoft brought out a new email application called Windows Mail which was subsequently superseded by a product called Windows Live Mail in 2007. Windows Live Mail also serves as the successor to Outlook Express.

Windows Live Mail can still be downloaded and installed, even on Windows 10. But it looks as if its days are numbered.

Microsoft have recently announced that Outlook.com and Hotmail.com accounts will be upgraded to use new synchronisation technologies after the end of June 2016 but Windows Live Mail will not be upgraded to support these new synchronisation technologies. So, you might have noticed problems getting Windows Live Mail to work with a Gmail account (although it can be made to work by changing Gmail settings - see below) but soon you will also notice problems with Outlook.com and Hotmail.com email addresses, and these problems are probably unresolvable.

So what to do? If you want to continue using free email software from Microsoft the best solution is probably to forget the comfortable old email interface and move boldly into the future. Sorry about that. As THIS link to a PC Mag article advises, "New default apps are part and parcel of major new Windows releases. Long gone is Outlook Express, and the new Windows 10 Mail client is here to fill its role, now with touch-screen support and a new minimalist, flat design."



Don't be frightened by the talk of touch-screen support if you want to use a non-touch screen and a mouse, the new Windows 10 Mail client works fine in that environment too, but it does require learning a new way of doing things, which will be easier to learn if you have used smartphone email. Conversely, if you don't have a smartphone, getting used to the new Windows 10 Mail client will make it easier to get used to smartphone mail in the future.

I'm trying to put a positive spin on this, we'll never live in 2007 again. Not just for mail in Windows, but in general, persevere learning new ways to do things, the past will never return, you can do all sorts of things with the mail built-in to Win 10, even if it isn't obvious at first.

Windows 8 and 8.1 have a built-in email client similar to Win10's, but it's not the same. If you plan to upgrade from Win 8.1 to Win10 soon (probably a good move) do that upgrade before switching to the new email application, since otherwise you might find you loose your contacts, depending on how you have them set up. When upgrading from Win 8.1 to Win 10 it's a good idea to back up everything first. Back up your contacts any way you can, even if it's just by printing them so you don't loose the info.

However, one aspect that a lot of people don't like is the "Sent From Windows Mail" signature that is automatically added to the bottom of the new Win 10 Mail. Of course, you can remove this, here's how:

Open Windows Mail, click on Settings, then Accounts then open the Email Account. You will see that by default the signature is enabled and set to "Sent from Windows Mail", if you wish to disable signatures altogether, you can simply toggle the switch.

Alternatively, you can leave the signature enabled and just change it to something a little more useful.

Always borrow money from pessimists--they don't expect it back.

Fast Startup.

This feature was first introduced to PC users with Windows 8. It was designed to make computers start up much faster and to keep pace with Apple machines. This is how it works.

When you switch off your PC, Windows 8 does a partial hibernate that saves only the kernel session and your device drivers (the system information) to the hibernate file (hiberfil.sys) on your hard disk instead of closing it as it did on all Windows versions prior to Windows 8.

When you start your PC again, Windows uses that saved system information to resume your system instead of having to do a cold boot to fully restart it. Using this technique gives a

significant advantage for boot times, since reading the hiberfile in and reinitializing drivers is much faster (30-70%) on most systems. If you have a motherboard with UEFI, (Unified Extensible Firmware Interface) then fast startup will be even faster.

Gmail and Outlook.

If you've recently set up a Gmail email account or you've bought a new PC computer and you want to use Outlook to handle all your emails, you could have problems configuring Outlook. You enter all the details into Outlook correctly and your Gmail account still won't work - why??

Google considers Outlook to be a non-secure App and blocks your mail from operating in order to keep your account safe. You could also find that Google has blocked Gmail from working with Thunderbird and on the Mail App on your iPhone or iPad with iOS 6 or below. What you'll usually find is an error message telling you you have entered an incorrect Password.

If you're using Windows 7 or later, you can configure the Mail App that comes with those versions of Windows to handle your Gmail account as Microsoft has built Mail with the necessary security standards. But - as you've just bought the latest version of Office you want to use Outlook as it is a magic program and has lots of uses other than just handling emails.

Well, there is a way.

You have to drill down into your Gmail account (go to Gmail.com - enter your login and password) then allow access for less secure apps. There are a few steps involved here, and the video below will show you how to do it.

https://www.youtube.com/embed/v7SHQ3NVdWs?rel=0&amp

You can bet that Microsoft are working on Office and will soon have a patch that will allow you to use Gmail without having to use the less secure method.

This page left blank.