

9 Most Common Types of Malware



It was so much simpler when we were growing up...

If you borrowed a floppy disc from a friend and popped it into your computer, you ran the risk of catching a computer virus.

The answer to this risk was simple: Most people installed antivirus software that protected their computers for them. And that was it.

But then two big things came along that changed everything: The internet – and greed.

Back in the day, most computer viruses were written for fun and for the hacker to show off their skills. They were trying to break into computers and access information for the challenge, not the financial reward.

These days, hacking is a profession. And a very lucrative one for some. The internet has made it very easy to access hacking knowledge and powerful automated tools.

There's also organized crime involved in modern-day hacking. The criminals are systematic, thorough, and ruthless with their attacks.

Believe us when we tell you that all businesses are being targeted by hackers all the time. The automated tools make this easy.

Don't ever let anyone lull you into a false sense of well-being about your IT security.

We see cyberattacks on businesses virtually every day. Mostly we see evidence of failed attacks, as the businesses we look after are well prepared and protected.

But occasionally, we speak to business owners or managers we don't (yet) look after, who have been successfully attacked. And the consequences can be devastating, depending on what has happened to them.

Anything that has been designed to steal your data or hurt your computer systems is called malware – for "malicious software."

You can be targeted in a number of different ways. Being aware is the first defensive weapon.

Here's our guide to the nine most common types of malware.



1. Viruses



Malware is much more than viruses, which is why you need a greater spread of defense than just antivirus software.

Viruses can attack by infecting other files, deleting them, or reformatting them and making it very difficult to clean them up. Often, viruses work by replicating themselves or by flooding networks, making it impossible for you to perform simple tasks.

Cleanup can range from difficult to virtually impossible. In many cases, to get things working again, you will need to quarantine or delete the affected files. And possibly even rebuild the computers from scratch.



2. Worms

Worms have been around since the 90s. They work by just one person opening an infected email that will then take down the whole network.

The scary thing about worms is that you don't need to take any action to spread them, unlike a virus. Worms replicate themselves and exploit other software to do their job for them.

You may have heard of the 'iloveyou' worm, which came out 21 years ago. It affected 50 million Windows machines across the world in just ten days. That's how powerful worms can be.

3. Trojans



Trojans – also known as Trojan horses after the Ancient Greek story – have replaced worms as popular hacking tools.

This type of malware takes advantage of its victim's lack of security knowledge. It usually arrives in the form of an email attachment – and these are becoming more and more authentic looking.

Once you open the attachment... bang... it's got you.

Trojans can also be pushed onto devices when you land on an infected website.

This kind of malware is difficult to defend against because it is easy to write and triggered by humans opening malicious files in error.



4. Hybrids

You might associate hybrids with cars that are better for the environment. There's nothing good about a malware hybrid.

Look back at the first three kinds of malware we've talked about and how difficult they are to protect against.

A hybrid is just that – malware with different attributes, such as the disguise of a trojan and the power of a worm.

Now, picture the love child of two of these forms of malware quietly arriving to attack your business.

As you can imagine, it can be very difficult to clean up after a hybrid attack.



5. Ransomware

This might be 5th on our list, but ransomware is the malware most feared by IT professionals.

Ransomware is enormous right now. And businesses like yours are the prime target.

It works by encrypting all your data and holding it hostage. You have no data at all – no customer records, no files, no emails, nothing.

The hackers demand you pay a ransom for them to free your data and give it back to you. This can be thousands of dollars, often asked for in cryptocurrency (such as Bitcoin), which is harder to trace.

Most ransomware is a trojan, meaning it relies on someone accidentally triggering it by opening an attachment or visiting an unsecured website.

Sadly, this type of attack is very difficult to recover from – the financial impact can be huge – and that's without paying the ransom.



Please make sure your files are backed up regularly to avoid loss. You and your team should also be trained to spot the symptoms of an impending attack.

6. Fileless malware



Technically this isn't a different category, but I've included it because it poses a real threat to you and your business.

Around half of all malware attacks are delivered by fileless malware, which is becoming increasingly popular.

Where 'traditional' malware relies on files to spread and infect, this form of malware relies on memory or other

fileless parts of your computer's operating system.

This type of attack is much harder to detect and stop than traditional malware.



7. Adware

You're on a website. There's a pop-up. You click on it. And before you know it, some software is installed on your computer. Or there's a new plug-in to your browser. Or your browser no longer uses your search engine of choice.

Adware is often more annoying than dangerous. But it can slow computers down or make you more vulnerable to other attacks. And anything that's

installed without your express permission is a pest and should be tackled.

8. Malvertising



Don't you love a good word blend?

As you probably guessed, malvertising is malware hidden behind advertising.

Don't confuse this with adware. Malvertising occurs when a cybercriminal pays for an advertisement on a genuine website. When you click on the ad, you're either redirected to a malicious website or malware is installed on your device.

Sometimes, even genuine ads are compromised. Criminals can also use a drive-by download attack that can affect your computer even if you don't click the ad.



9. Spyware

Once again, a very descriptive name. Spyware is used to spy on you.

When installed, spyware can monitor the websites you visit, everything you type (this is known as keylogging), and any other information about you and what you're doing on your device.

It's a good way for someone to find out your login information and passwords.

Spyware is activated when you click on something you shouldn't, such as an attachment, a pop-up, or notification. Or by downloading media from an unreliable source.

Like adware, this is simpler to remove, but by the time you've noticed it, there's the risk you've given away a lot of valuable information.

So, there we have it. The 9 most common types of malware and how they'll affect you and your business.

The impact that many of these forms of malware can have on a business ranges from lost productivity to total bankruptcy.

This guide is a simple summary. We don't want to bore you with facts and figures. But it's safe for you to assume that you don't want to deal with the fallout of a major attack on your business.

Remember what we said right at the start of this guide: **All businesses are being targeted by hackers all the time.**

You need to make sure you're doing everything you can to keep your business safe. This starts with creating a culture of taking your cybersecurity very seriously.

Consult with a trusted IT support partner to find out the best blend of software, training, and procedures to keep your business safe. Contact Yeo & Yeo Computer Consulting today.



[Contact Us Online](#)

Learn more at yeoandyeo-consulting.com

Email: info@yeoandyeo.com

Call 989.797.4075 | 800.607.1446