Online Security: Malware, Spyware and Viruses

Description

Online Security: Malware, Spyware and Viruses

Malware is a term used to describe any type of malicious software such as viruses, spyware and other code deliberately designed to:

1. Stop your computer working properly
2. Delete or corrupt your files
3. Steal information from your computer
4. Allow others to access your computer and your information.

The consequences of an infection on your computer can be serious, and can include loss of access to your files or even identity theft and fraud.

Most Common Types of Malware

Malware Type	Description

Spyware	Spyware tracks your actions on your computer and the internet, collecting passwords, monitoring web activities such as auto-filled forms containing financial or personal data, or even activating webcams or speakers. It may disguise itself as legitimate software, such as Trojan software that downloads and instals spyware without user awareness.
Viruses	Viruses are software or code that infiltrates your computer or applications, replicates itself, and spreads through your internet connection. Once installed, viruses can corrupt your computer or legitimate software, steal and transmit data, or overload your computer's resources until it becomes inoperable.
Ransomware	Ransomware instals itself and locks access to your files, displaying a demand for payment, often in bitcoin, to regain access. While payment may restore access temporarily, the underlying issue must be addressed to prevent recurrence. Payment does not guarantee file recovery, and the ransom amount can be substantial.
Trojans	Trojans appear harmless but are designed to carry out harmful tasks once downloaded and installed. They can deliver viruses, spyware, or other malware types. Trojans may disguise themselves as legitimate software or files to deceive users into installing them, leading to various malicious activities on the affected system.

Note that while scams, phishing, or identity theft aren't themselves malware, the malware can often be assisting with these criminal activities.

For more information on types of malware, visit the following sites:

- cyber.gov.au: What is ransomware?
- cyber.gov.au: What is malware?
- Threats and extortion scams

Frequently Asked Questions

- 1How does malware get on my device?

Your computer can be infected in many ways, including:

- Clicking on legitimate-looking website links that turn out to be false
- Visiting websites that have been infected by malware
- Downloading infected apps and files from the Internet
- Opening infected email attachments
- Social media messages at random with links
- SMS messages with links
- Allowing someone to remotely access your computer

- 2How do I prevent malware getting on my device?

The best way to protect yourself against a malware infection is to install appropriate software on your device.

Anti-malware solutions differ in effectiveness and the range of malware types they cover. Some may only scan for existing viruses; others will detect malware hidden in downloaded files or sitting on the website you've just opened. Some packages will block downloads, or clean software as it's downloaded.

At a minimum, all anti-malware software solutions should be able to scan for viruses and alert you to any potential malware. Some products may also include alerts when you visit a suspicious or dangerous website, and firewall protection.

To select the right solution for your needs, we recommend you do some research on the various products on the market. Some products are available for free, while others cost money – either a one-time cost, or an ongoing subscription. Paid products may provide more tools than free ones, depending on your requirements.

- cyber.gov.au: Anti-virus software
- No more ransom: a website that may help remove ransomware from your computer.

- 3What are built-in malware scanners for Windows?

Current Windows versions have a built-in malware scanner as part of its Windows Security suite Microsoft Defender Antivirus. Defender will search for any files or programs on your computer that can cause harm to it, across email, apps, the cloud and the internet.

Be careful however, as Defender is only updated when Windows is updated. Like any other virus program, if this is not done regularly then it may be unaware of, and unable to detect, newer forms of malware.

We recommend you turn on automatic updates for Windows to keep yourself protected.

- 4What anti-virus software is available?

  The following software listings provide overviews of anti-virus software for both Mac and Windows.

  Note that most of the packages listed have paid subscriptions, but some may have free trials or limited-service versions.

  Generally, if the same software names keep occurring in lists and articles, they are well-known and relatively trustworthy.

  Many of these listings will differentiate between malware, spyware, and virus software. Some packages cover all three terms; some will do just one or two. These may be a little more specific than anti-malware software in general, particularly the free packages.

  - Tech Radar: The best antivirus software 2024
  - PC Mag Australia: The Best Free Antivirus Protection for 2024
  - Lifewire: The 11 Best Free Antivirus Software of 2024 (Windows only)
  - PC Mag Australia: The Best Malware Removal and Protection Software for 2024
  - Macworld: Best antivirus for Mac: Get the best protection from viruses and malware
  - Lifewire: The 6 Best Free Malware Removal Tools of 2024
  - Techradar: Best malware removal software 2024: free and paid anti-malware tools and services
- 5What are virus scanners?

  On-demand virus scanners only check for viruses when you run them. They will not proactively prevent you from malware, but may be useful to do a quick check of your computer before you download and install a preventative package.

  - Lifewire: 18 Best Free On-Demand Virus Scanners
- 6How do I remove malware from my device?

  Sometimes, despite taking precautions, infections do occur. Some of the signs include:

  - Web browser freezing or becoming unresponsive.

- You get redirected to web pages other than the ones you are trying to visit.
- You see a lot of pop-up messages.
- Your computer runs slower than usual.
- New icons appear on your desktop that you don't recognise.
- Your computer crashes completely (you may see the Windows error screen or a blank screen on an Apple Mac)

If this happens, try the following steps:

1. Remove external drives and devices from your device. Restart in Safe Mode (see our troubleshooting page for your specific device for assistance).
2. Run a scan on your anti-virus software and follow instructions to remove any malware.
3. Restart your computer (see our troubleshooting page for your specific device for assistance).
4. Update your operating system, browser and applications as necessary (if not current).
5. Reset all of your passwords.

The following is a list of software that may help in removing an existing malware attack/infection. Some may not help in preventing an infection in the first place – you may need to install separate software for that.

- Tech Radar: Best malware removal software 2024: free and paid anti-malware tools and services
- Lifewire: The 6 Best Free Malware Removal Tools of 2024

The following list is specifically for removing spyware – software designed to 'spy' on what you do on your computer.

- Lifewire: 11 Best Free Spyware Removal Tools

- 7Additional Protection Tips
  - Ensure anti-malware programs remain updated.
  - Protect your Wi-Fi with a complex password that has numbers, letters and characters (such as ! @ $ % etc). Avoid using property names, family names, pet names, birthdates or key aspects of your life as part of the password.
  - Avoid using free public wifi if possible – these can infect your device.
  - Regularly backup your entire device, as well as important files – both to a local hard drive and a cloud-based service, if possible. This particularly helps with ransomware, as you can simply re-install an earlier, clean version of your files.
  - Be cautious in opening emails from people or companies you don't know. (Even un-expected emails from friends, as they may have been compromised).
  - Don't allow anyone to remotely access your computer.

- 8Additional Information and Resources

  The Australian Cyber Security Centre provides a wide range of resources and further information, specifically tailored to individuals, families, and business users.

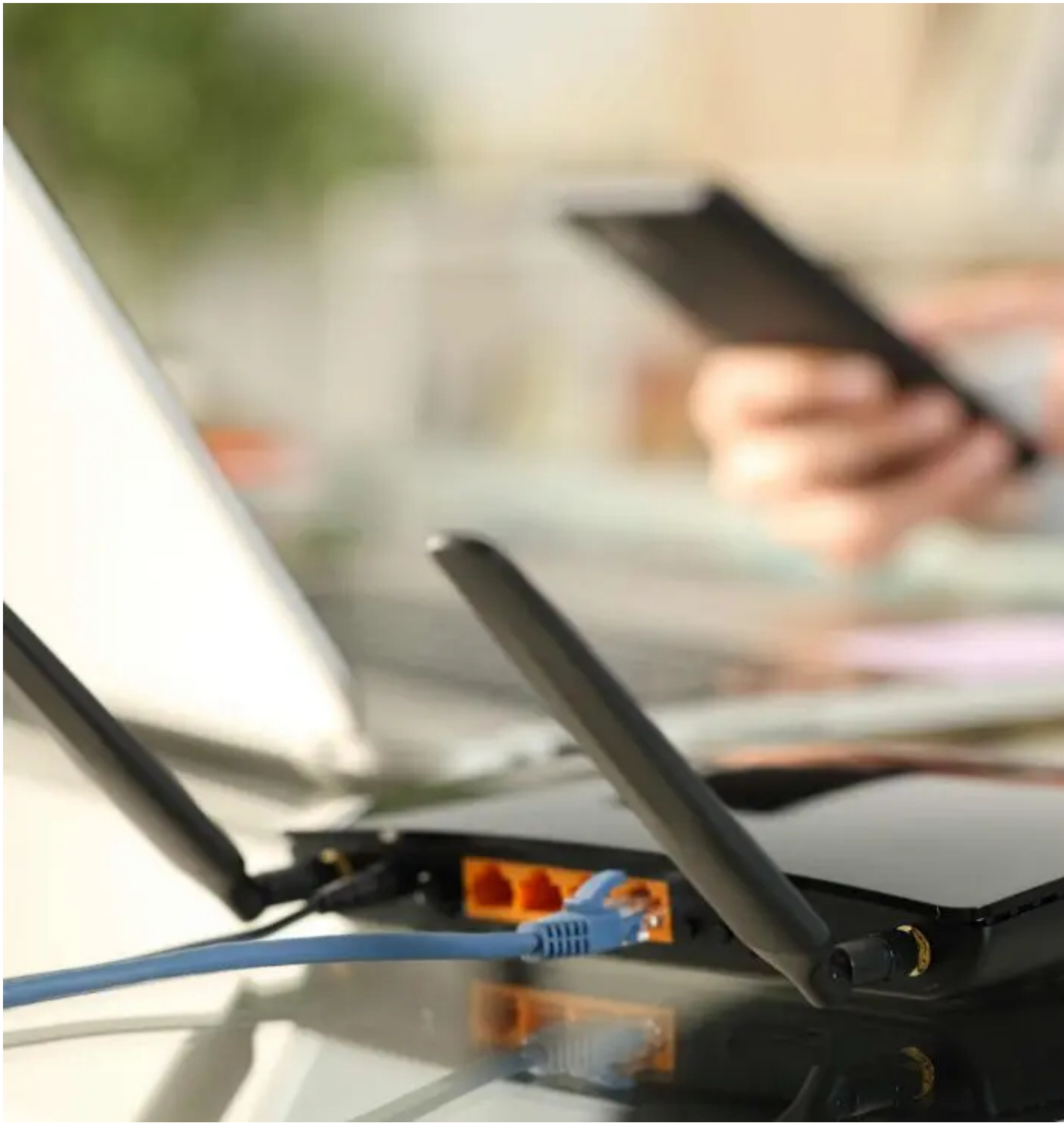
  The ACCC through Scamwatch has information about the various types of scams that can then allow breaches to your computer security.

  If you feel your computer security has been breached, turn off your computer, devices, and internet services and get in touch with an IT technician for support.

- ## Need someone to help install some equipment or want to find a technician or supplier?

  We've got you covered. Head to our directory page where you can find a list of installers, suppliers & technicians around rural and remote Australia.

  Take me there



- ## Explore more of our resources

-
  -

News
November 4, 2024
Telstra 3G shutdown is now complete

- News
  October 25, 2024
  Phones using the 3G network to call triple zero will be disconnected on 28 October 2024

- News
  October 25, 2024
  NBN Co accelerating higher speed tiers in September 2025

- Guides
  October 17, 2024
  Connectivity definitions

- Back to resources

-

Didn’t find the answers you were after?

Chat to us on our hotline with one of our team members and let’s get the conversation

started. If we don’t answer, we’ll get back to you in no time at all.

1300 081 029

Category

1. Tech Tips

Date
31/07/2025
Date Created
12/03/2024