

What is malware?

Malware is software designed by cybercriminals for malicious purposes and can vary heavily in complexity and purpose. For example, ransomware will encrypt a computer, rendering it unusable unless a fee is paid to the cybercriminals for the decryption key. Other malware is created to be harder to detect but can be just as impactful. For example, infostealer malware is designed to quietly collect sensitive information such as passwords, identity credentials, financial details and photos.

How to avoid installing malware

- ☐ **1. Don't always trust the first result from Google.** When you are reviewing search results, look closely at the domain name for slight variations. Official websites usually have clear and recognisable domains, such as .com, .org, .gov or country-specific domains. For example, for a Microsoft product, the URL should clearly include microsoft.com.
- ☐ **2. Always download software directly from the developer's official website.** If you need an Adobe product, you should only be downloading it from the Adobe website. Use official stores like the Microsoft Store where possible.
- ☐ **3. Use a trusted antivirus.** Look for highly rated brands and verify their performance through independent sources like AV-Comparatives, AV-Test, or PCMag.
- ☐ **4. Don't paste unknown commands into PowerShell/Terminal.** Scammers are creating lures to convince people to paste commands into their devices **which then** downloads malware.
- ☐ **5. Just because it's from a trusted partner, doesn't mean it's trusted.** Cybercriminals are compromising email accounts to send requests to known business partners to install malware. Be wary of any strange requests coming from all email sources.
- ☐ **6. Enable [User Account Control](#) for Windows.** This feature requires administrator credentials to approve new programs that can make changes to the device, giving a second set of eyes for anything your employees may be trying to run.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Potential signs of a malware infection

Malware infection can be difficult to detect without proper training and tools. But there may be signs that your device has been infected. Such as:

- ☐ **Unusual pop-ups:** You experience excessive pop-up ads, even when you're not browsing the internet.
- ☐ **Disabled security software:** Your antivirus or firewall settings are altered or disabled without your knowledge.
- ☐ **Unfamiliar programs:** New or unfamiliar programs appear on your device that you didn't install.
- ☐ **Browser redirects:** Your web browser redirects you to unfamiliar websites or changes your homepage and search engine settings.
- ☐ **Unusual activity on accounts:** You see unauthorised changes in your online accounts, such as sent emails or social media activity you didn't initiate.
- ☐ **Someone is demanding money through an email:** Someone may send you an email claiming to have access to your files or other sensitive information. This email may also contain images of your desktop background, or sensitive information such as your passwords. This may be a sign of an infostealer malware infection.
- ☐ **Your cursor is moving on its own:** Malware may install remote access tools, allowing cybercriminals to remotely interact with your device.

If you notice any of the above, it's essential to run a full antivirus scan and if an infection is found, take steps to remove any detected malware promptly. In some cases, you may not be able to achieve this (for example, in the case of ransomware), so extra guidance has been provided.

Additional guidance: Ransomware

If you are unable to access any of your files and there is a ransom note on your desktop, this is a sign that ransomware has infected your device. You can follow the steps below for malware remediation but also seek the immediate assistance of the ACSC on 1300 CYBER1 (1300 292 371).

Never pay the ransom – the cybercriminal group responsible may be under international sanctions, and sending funds could be breaking Federal law.

For additional information, please see IDCARE's [Ransomware Fact Sheet for Small Businesses](#).

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Remediating Malware on your devices

If you suspect malware has been downloaded to your device, follow the below steps:

- ☐ **1. Disconnect the device from all network connections:** This includes the internet, any local networks you may have setup, and shared folders accessible on your network or intranet.
- ☐ **2. Perform an offline scan of the device:** Check to see that your anti-virus software is running and no unknown files have been excluded and marked as safe. Ensure you perform a full scan of the device.
- ☐ **3. Follow the antivirus instructions:** Most antivirus programs will prompt you with actions when a threat is detected, such as 'Quarantine', 'Remove', or 'Ignore'. In general, choose 'Quarantine' or 'Remove' to isolate or delete the threat.

Additional guidance:

Update the antivirus: Make sure your antivirus software is up to date before and after the scan to ensure it has the latest virus definitions.

Review recent activity: Check recent downloads, email attachments, or websites visited to identify the potential source of the virus. Avoid accessing those files or sites again.

Check for identity documents: Change any stored passwords and replace potentially compromised documents on the affected device. For help with concerns about compromised identity documents, call IDCARE on 1800 595 170.

Consider if an Eligible Data Breach has occurred: If malware has exposed your employees or customers sensitive information, this may cause a data breach. For additional information, please see [IDCARE's Business Data Breach Fact Sheet](#).

Seek out an I.T professional: If the problems persist, seek the assistance of a trusted IT professional.

Additional resources and information

Educating employees about the risks involved with malware, how infections happen, and steps to take if a device is suspected to have been infected by malware is the most effective mitigation. The end user is the first and best line of defence, but mistakes are made every day, so implementing a simple but effective layered approach to security as outlined in this document is the first step to improving the cyber resilience of your business.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

The ACSC also features an [online tool](#) which guides users through most of the steps that appear in this document, albeit in an online manner.

Further education and simulation

If you would like to improve your small business's online security, you may like to take our [Cyber Resilience Health Check](#), which is a five-minute questionnaire to assess your existing cyber-related business practices against current cyber threats. Upon completion of this you have an option to book a free 30-minute session with a Cyber Advisor who can guide you with steps to uplift your cyber resilience.

There are several companies that offer services in relation to malware prevention, with a focus on education and simulated phishing attacks. **KnowBe4** is a leading platform that offers security awareness training and simulated phishing attacks, enabling organisations to assess and enhance their employees' readiness against cyber threats. Another notable service is **Cofense**, which focuses on phishing defence through employee training and phishing simulation tools, helping organisations identify weaknesses and improve overall security posture. Additionally, **PhishLabs** offers a similar suite of services, including simulated phishing campaigns and ongoing education, aimed at fostering a culture of security awareness among employees.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 170 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.