Cybersecurity: Understanding malware

Protect yourself online by understanding common threats.

What is it?

Malware (malicious software) and viruses are the most common type of cyberattacks. They are often delivered through infected emails, texts, or advertisements. Learning how to identify these attacks can help you prevent an infection on your computer, tablet, or cell phone.

Types of malware

These are the most common malware attacks:

- **Viruses** replicate themselves to modify computer programs after they are activated by the user.
- **Worms** are another self-replicating attack that can spread across systems on their own.
- **Botnet** is a network of bots controlled by one person that simulates human activity.
- **Adware** floods your device with unwanted ads.
- **Spyware** secretly observes your device activities and reports it to the attacker.
- **Trojans**, or Trojan horses, give attackers access to your device and personal or financial information.
- **Ransomware** locks you out of your device until a ransom is paid.
- **Keyloggers** track key strokes to collect usernames, passwords, or financial information.
- **Rootkits** give attackers control over a target computer or network, while masking the attack.

Malware can serve more than one purpose. A Trojan, for example, can also include a keylogger.

How can I prevent malware attacks?

Cybersecurity software

You can protect yourself against most kinds of malware by installing high-quality cybersecurity software. See our security software tip sheet for information to help you choose a product that meets your needs.

Phishing scams

Phishing scams are often “spoofed” to look like they’re coming from a trusted source, like a government department, and usually make unusual requests, like asking for payment by gift card.

Often, phishing scams try to create a sense of urgency with time-bound claims. A common example is claiming your account will be lost unless you take immediate action.

Phishing emails and texts can include attachments or links that install malware on your computer. Avoid opening links or attachments unless you are confident you know the sender. If you are unsure whether an email is real, search for the sender’s contact information and call to confirm if they sent the message.

Hover your cursor over the sender’s name to verify the email address. If the name or email domain is different than what is listed in the sender field, you are likely dealing with a phishing email.

You can also hover your cursor over a link to see the destination URL. This will often appear as a small line of text in the lower left-hand side of your internet browser. Do not click any links that point to a different website than what the text suggests or that appear to be alpha-numeric codes.

Here is a low-stakes example: www.alberta.ca.

If you receive a suspected phishing email, delete it without taking the actions suggested. Learn more about common text scams.

Ransomware

Ransomware is a kind of malware that uses encryption to hold your data and information hostage until a ransom is paid. It is downloaded to a device without your consent through malicious links, emails, texts, or websites.

Do not pay the ransom if your device is infected. It does not guarantee that your information will be released or that the ransomware will be removed from the device. Contact a local computer repair service to have it removed.

You can help prevent ransomware by following the same action as you would with a phishing email and by installing high-quality anti-malware software. When in doubt about the legitimacy of an email or text, simply delete it without taking any of the actions requested in the message.

Alberta