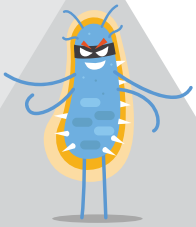
CreativeContent AUSTRALIA

Malware

Malware, or 'malicious' software, is any file or program that causes harm to a computer user and their devices - from stealing personal data, to hijacking computer functions and monitoring user activities without detection. The types of malware include ransomware, spyware, adware, Trojans and worms.

Adware is software that displays advertisements on internet sites, redirecting traffic to their own sites and collecting marketing data on users. Adware is the principal means of launching other malware and poses a threat to a user's personal details as their data can be hacked or sold. Adware is usually installed without consent of the user and can slow a computer's performance.

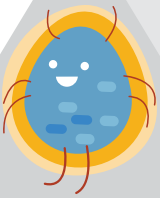


Ransomware can lock a computer and encrypt files so they become inaccessible until a ransom is paid. It spreads through email attachments, infected programs, infected pop-up ads and compromised websites. In many cases, even after paying the ransom, the user's device is not restored.

Spyware is malware that spies on user activity and transmits information to third parties. It can monitor activity, collect keystrokes and gather personal data like email addresses, passwords and credit card details. Spyware can embed itself into critical components of computer operating systems, exploiting memory storage with its monitoring and data collection processes. Installed through email attachments, it can ruin computer performance and destroy information.

Trojan (or Trojan Horse) is often disguised as legitimate software, tricking users into downloading and installing it. Once activated, Trojans enable backdoor access for third parties to steal banking details, financial data, passwords, logins or personal identity. They can install other malware, modify files, anonymise internet activity, disconnect networks and monitor user activity by secretly enabling in-built cameras and external video devices.

A **Bug** is an error, flaw, failure or fault in a computer program or system that causes it to produce an incorrect result or undesired outcome. These flaws usually result from human error, and typically exist in the source code, its design or in components of the operating system. Bugs may only slightly affect a computer's function and can go for a long time without being noticed, or can cause the system to crash and freeze. The most sinister are 'security bugs', which allow attackers to bypass user authentication, obtain unauthorised privileges or steal personal data.



A **Bot** is self-propagating malware designed to infect a system, performing specific operations that connect back to a command and control centre. Bots can be used in botnets – a network of computers infected with malware – and controlled by third parties without the user's knowledge. Criminal gangs use botnets to steal information such as passwords and bank details, commit fraud, spy on webcams and extort users.

A **Rootkit** is designed to provide continued privileged access to a computer, concealing its existence and actions from the user and system processes. This backdoor access can allow hackers to alter files, steal personal information, modify system configurations, install other malware and control the computer as part of a botnet.

A **Virus** is designed to spread from host to host, continually reproducing. It attaches itself to programs and documents, which when opened, activate the code and infect the system. Once a computer is infected, viruses can not only steal passwords and data, corrupt files and spam email contacts, but can also harm host computers and other networks.

A **Worm** is a self-replicating program that penetrates an operating system, spreading malicious code and consuming bandwidth without human activation and user recognition. It can multiply so many times that it takes up entire memory storage systems or hard disk space, causing the computer to run slowly and crash. They often go unnoticed, using networks to send copies of the original malicious code to other computers. Sometimes worms have 'payload' abilities and code designed to steal personal information and data, delete files and modify systems from the computer without detection.