Security Glossary

DFNDR Lab's glossary of cyber security, mobile threats, and related terms.

Adware
A type of software that shows you extra promotions that you cannot control as you use your device.

Banker Trojan
A type of trojan specifically created to steal confidential information from customers of online banks or other payment platforms.

Carder
People who buy, sell, and trade online credit card data stolen from phishing sites or from data breaches at retail stores.

Cybercrime
Any unlawful or criminal activity that is being done over the internet or by using computing devices, including fraud, blackmail, identity theft, phishing, etc.

Crimeware
Any program designed to fraudulently obtain financial gain to the detriment of affected people.

DoS / Denial of Service
A type of attack that shuts down a device or network and prevents intended users from accessing certain services.

Dropper
An executable file that injects different types of viruses into a device.

Hacker
Someone who accesses a device illegally or without authorization.

Hacking tool
Any program used by a hacker to carry out actions that cause problems for the user of the affected device.

Hijacker
Any program that changes the browser settings to make a homepage or the default search page different from the one set by the user.

Hijacking
A type of attack in which the attacker takes control of communication between two entities and masquerades as one of them.

Hoax
A trick message containing a warning of something, like a virus, that doesn't actually exist.

Keylogger
A type of trojan spyware that is capable of collecting, saving, and even publishing a list of all keystrokes (information that has entered through the keyboard) made by a user.

Link virus
A type of virus that modifies the address where a file is stored, replacing it with the address of the virus instead of the original file.

Malware
MALicious softWARE. All programs that contain malicious code, whether it is a virus, trojan or worm.

Password stealer
Software that collects and saves confidential data, such as user passwords (using keyloggers or others).

Payload
Pieces of code written to perform actions on infected devices beyond simply spreading the worm, such stealing data, deleting files, etc.

Phishing
An attempt to trick you into giving out your personal or financial information, such as user-names, passwords, or credit card numbers.

Ransomware
A type of software which stops you from using your device or encrypts your files, offering to unlock only on the condition that you pay a ransom.

Riskware
Legitimate software that contains loopholes or vulnerabilities that may be exploited by hackers for malicious purposes.

Scam
Any fraud in which a person is tricked into giving money, under false promises of economic gain.

Social Engineering
A tactic used by hackers that appeals to the weaknesses of people, such that the person on the other end of the informational transaction is eventually convinced to perform some task.

Spammer
A person responsible for or the program that sends large numbers of spam emails or mass-mail threats like phishing and malware.

Spyware
Software that collects personal information, such as browsing activity, preferences, and interests, and uses them without adequate consent.

Trojan
Software that claims to perform one activity but actually does another, typically malicious, such as stealing sensitive data or redirecting you to shock sites and other unwanted content.

Virus
A type of malware that inserts itself into a file or executable software and can cause effects such as slowing down the system, destroying or modifying files, and logging keystrokes.

Vulnerability
A flaw or error in a software or IT system that may allow a hacker to take advantage and exploit it for a malicious purpose.

Worm
A stand-alone malware, similar to a virus, that can self-replicate and propagate via networks, without human help, to other device systems.