connect SMART

Protect yourself online

Cyber Security Jargon Buster

https://www.connectsmart.govt.nz/

newzealand.govt.nz

Adversary	In cyber security, an adversary is a malicious entity whose aim is to prevent users from protecting privacy, integrity and data.
Air gap	Air gap or air wall is a network security measure on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks – such as the public Internet.
Antivirus software	Antivirus software, sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software.
Application whitelisting	Application whitelisting is where limitations are placed on a computer or system so that only approved programmes and software libraries can be used. It is designed to protect against unauthorised and malicious programs executing on a computer.
Back-up	Copying and archiving personal data so it may be restored in case of loss.
Backdoor	A backdoor is a way of bypassing normal authentication in a system. Backdoors are often used for securing unauthorized remote access to a computer.
Black hat	A black hat hacker is a type of hacker who violates computer security for little reason beyond maliciousness or personal gain.
Botnet	Botnet is a number of Internet-connected computers communicating with other machines located in a shared network. A collection of infected computers may be remotely controlled to conduct malicious activities such as to send spam.
Brute force cracking	Brute force cracking (or brute force) is a trial and error method to get into a system, where brute force is used through exhaustive effort rather than intellectual strategies.
CERT	CERT was once an acronym for 'computer emergency response team'. Since 1997, CERT has been a registered trademark owned by Carnegie Mellon University and is no longer used as an acronym, but is a system to deal with cyber incidents.
Clickjacking	Clickjacking is a technique used to deceive users into clicking a link which they did not intend to click. This is accomplished by creating a transparent frame above the window the user is viewing and any click the user does performs another action such as agreeing to a prompt. For example, a developer could create a clickjack site that causes the user to agree to give them rights to that person's webcam without them knowing.
Cloud computing	A service model that enables access to a shared pool of computing resources such as data storage, servers, software applications and services.
Compressed file formats	A type of file format which compresses data to consume less storage space and network bandwidth. Examples of compressed file formats include .zip files, .rar files and .jar files.
Cookies	An HTTP cookie (also called web cookie, Internet cookie or browser cookie) is a small piece of data sent from a website and stored in the user's web browser while the user is browsing. Cookies were designed for websites to remember information such as items added in the shopping cart in an online store or to record the user's browsing activity including recording which pages were visited in the past.
CORTEX	CORTEX is a project to counter cyber threats to organisations of national significance – e.g. to operators of critical national infrastructure. It involves GCSB implementing capabilities to protect these organisations against advanced malicious software ('malware'). The capabilities delivered by CORTEX cannot be used for purposes other than cyber security. The detection and disruption of malware by GCSB is governed by warrants and access authorisations approved by the Minister Responsible for GCSB and the Commissioner of Security Warrants.

Critical infrastructure

The physical facilities, supply chains, information technologies and communications networks which if destroyed, degraded or rendered unavailable, damage national security or the social or economic wellbeing of the nation.

CryptoLocker

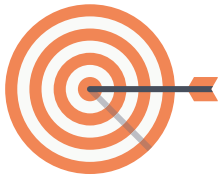
CryptoLocker is a ransomware trojan spread through email attachments. It targets computers running with a Microsoft Windows operating system and encrypts certain file types, which then displays a message offering to decrypt the data if a payment is made by a stated deadline.

Cyber adversary

An individual or organisation (including an agency of a nation state) that conducts cyber espionage, crime or attack.

Cyber attack

A cyber attack includes any deliberate acts through cyber space to manipulate, destruct, deny, degrade or destroy computers or networks, or the information resident in them, including anything from hacking a website or sending spam email.



Cyber espionage

Offensive activity designed to covertly collect information from a user's computer network for intelligence purposes.

Cyber intrusion (hacking, unauthorised access)

Occurs when someone gains access to a computer or device without the owner's permission. Also referred to as unauthorised access or hacking.

Cyber resilience

Cyber resilience involves detection, protection and recovery from cyber incidents. Government agencies and businesses need to have timely, actionable cyber security information and advice and be able to deal with a trusted agency when they have a cyber security incident. Cyber resilience is one of the four goals in New Zealand's Cyber Security Strategy.

Cyber security incident

An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it. A compromise is an incident where the security of a system or its information was harmed.

Cybercrime

Cybercrime is part of a continuum of activity that ranges from cyber safety challenges to threats to national security. Cybercrime can encompass criminal activity, from cyberbullying to state-sponsored theft of intellectual property.

Cybercrime includes:

Pure cybercrime: A crime that can only be committed through the use of ICT or the Internet and where the computer or network is the target of the offence. This is regardless of what the criminal goal is – whether political or financial gain, espionage or any other reason. Examples of cybercrime include producing malicious software, network intrusions, denial or service attacks and phishing.

Cyber-enabled crime: A criminal act that could be committed without ICT or the Internet, but is assisted in scale by the use of technology. This includes a vast amount of serious and organised crime, such as cyber-enabled fraud or the distribution of child exploitation material. However, cybercrime is a subset of general crime, and the boundaries will not always be hard and fast.

Dark web

Dark web is the World Wide Web which exists using public internet but requires specific software, configuration or authorisation to access. Dark web websites hide the IP addresses of the servers that run them. The dark web is a small part of the deep web, which is not indexed by search engines. The Dark Web is used for black market drug sales and child pornography, as well as peer-to-peer networks and file sharing sites.

Deep web

The deep web, invisible web or hidden web are parts of the World Wide Web whose contents are not indexed by search engines. This includes a range of commonly used websites like webmail and online banking, as well as websites behind a paywall.

Denial of Service (DoS or DDOS)	Denial of Service stops software from operating the way it is intended to – like denying access to a website. This is an attempt by a cyber adversary to prevent legitimate access to online services (typically a website), by consuming the amount of available bandwidth or the processing capacity of the computer hosting the online service. DoS can also occur unintentionally through misconfiguration or a sudden and unexpected surge in legitimate usage. When multiple computers are used to conduct these activities, such as through the use of a botnet, it is referred to as Distributed Denial of Service (DDoS).
Drive-by download	Occurs when a user visits a malicious website or a legitimate website that has been compromised. After the visit, the user's system is infiltrated by malicious software designed to automatically run on the user's computer typically without requiring any additional user interaction (permissions).
Encryption	Encryption is the process of encoding digital messages so only authorized parties with a decryption key can read it.
Exploit	A piece of software, collection of data, or sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behaviour to occur on computer software, hardware, or something electronic (usually computerised).
Firewall	A firewall is a network security system that monitors incoming and outgoing traffic based on security rules – establishing a barrier between a trusted internal network and an outside network.
Form-grabbing	A more advanced type of keylogging (see below) where the data is captured from browser forms, before data is sent over the Internet to a secure server. This method is able to acquire data regardless of input method (i.e. through the use of virtual keyboard, auto-fill or copy and paste).
Hacktivism	Malicious cyber activity conducted by issue-motivated groups or individuals for the purpose of promoting a particular cause or targeting a particular person or organisation associated with an issue or cause.
http/https	HTTP stands for Hypertext Transfer Protocol. It is the foundation of data communication for the World Wide Web. HTTPS with an added S means the connection is over SSL (Secure Socket Layer). It is used by web servers to transfer and display content securely.
Internet of Things (IoT)	Internet of Things is the concept of everyday objects having network connectivity, enabling them to share and exchange data.
Issue-motivated group	A coalition of communities or individuals, often loosely formed, that is primarily drawn around a common interest.
Keylogger	Software on a system that records what a user types on their keyboard or what they click with their mouse.
Malware, malicious software	Malicious software is designed to facilitate unauthorised access to a system, or cause damage or disruption to a system. Malware is often downloaded to a user's computer or system by visiting a malicious site, or clicking an unsafe link.
Malvertising	A drive-by download primarily affecting legitimate websites, where the malicious software is delivered to the user via an advertisement.
Network Access Control	Network Access Control is an approach to cyber security which controls who and where users and devices can access a network and what they can do while on it.

Passwords	Passwords are a string of characters to authenticate a user and gain access. Connect Smart recommends you use complex passwords by including a range of upper and lower case letters, numbers and punctuation; and use different passwords for everything.
Phishing	Phishing is the practice of sending an email pretending to be from a reputable company in order to induce individuals to reply with personal information, such as passwords and credit card numbers.
Phygital	A term newly coined to describe physical experiences blended with real experiences.
Ransomware	Extortion through the use of malware that typically locks a computer's content. Attackers generally require victims to pay a ransom to regain access. It can also be accompanied by a threat that the computer has been locked as a result of illegal or questionable conduct by the victim.
Removable media	Storage media that can be easily removed from a system and is designed for removal, for example USB flash drives or optical media.
Rootkit	A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would it otherwise be allowed – an unauthorized user – while also hiding its existence or the existence of other software.
Sandboxes	A sandbox is a security measure that separates running programmes, sometimes used to trial untested code or untested programmes.
Social engineering	Manipulating a person into performing actions or divulging sensitive information by tricking them to a belief that a request for information (or similar) is legitimate. Cyber adversaries use a wide variety of tools such as email and social media to conduct social engineering against target personnel. This is a growing are of cyber attack.
Software	Software is the encoded information or instructions for a computer. Ensure your software is up to date as it contains "patches" or fixes for the latest known threats.
Sophisticated capability	An adversary with a full range of access, expertise and operational reach. Sophisticated state-sponsored adversaries fully integrate cyber, information operations programs and traditional signals and human intelligence collection capabilities.
Spam	Spam is junk mail specifically sent through electronic messaging systems, and includes a range of unsolicited messages such as advertising or phishing emails.
Spear phishing	Spear phishing are socially-engineered emails, to specific people, often containing a hyperlink or an attachment which when clicked on or opened attempts to download malicious code. The email is crafted to look like an email from a legitimate sender.
Spyware	Spyware is software that aims to gather information about a person or organisation without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the user's knowledge.
SQL injection	A vulnerability allowing a hacker to execute malicious SQL queries (see below) that are passed to a database in a network, allowing them to have greater access to data within that database.
SQL queries	Structured Query Language (SQL) is a standard data retrieval query in computer code.
State-sponsored	An activity initiated and/or conducted by or for a government body.
Tor (anonymity network)	Tor is free software for enabling anonymous communication. It is derived from the acronym from the original software project "The Onion Router". Using Tor makes it more difficult to trace internet activity back to the user.

Tradecraft	The combination of tools, techniques and procedures used by specific cyber adversaries to conduct their activities. These tools, techniques and procedures can be distinct and may be identified and attributed to these adversaries.
Trojan	A Trojan horse or Trojan is any malicious computer program which is used to hack users by disguising its true contents. The term is derived from the Ancient Greek story of the wooden horse that was used to invade the city of Troy. For example – a user may download an app, believing they are downloading legitimate programme, when it is housing a virus.
Two-factor authentication	Two-factor authentication is a method of confirming identity using a combination of two factors – i.e. a password and text to mobile phone.
Virus	A virus is a type of malware which replicates itself and infects other programs.
Vulnerability	In the context of information security, vulnerability is a weakness in system security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.
Watering-hole techniques	Compromise and placement of malware by cyber adversaries on a legitimate website frequented by their intended targets in an attempt to compromise the computers of visitors to the website.
Weaponized documents	Weaponized documents are often sent as email attachments and are encrypted to allow backdoor access points to user computers in order to steal information.
Website defacement	An unauthorised change to the content of a website.
Whaling	Whaling is a larger scale version of "phishing" where the email is targeted specifically at senior executives and high profile targets within businesses.
Wifi	Wifi is technology that allows electronic devices to connect to a wireless LAN (WLAN) network. Wifi can be open or password protected.
Worm	A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.
Zero-day malware	Zero-day malware (also known as a zero-day virus next-generation malware) is a previously unknown computer virus or other malware for which specific antivirus software signatures are not yet available. It is called zero-day because the software's author has zero days in which to plan and advise any mitigation against its exploitation (e.g. issuing patches)