HSB
A Munich Re company

cyber safety

Glossary of Terms

It's a complex world full of risk. Our global cyber team has put together this explainer containing common cyber terms to help you support your clients and colleagues.

Algorithm — Code written to instruct hardware/software assets to follow a specific set of complex instructions.

Anti-Virus (anti-malware) — Any software that works to identify malware and remove it from a given system or network.

Authentication — The process of proving a user is who they say they are by using various tools and systems.

Backing Up (backup) — A way to duplicate an infected or unransomed system in order to restore it at a later date if needed.

Behaviour Monitoring — The process hackers use to keep a record of a victim's behaviour in order to use the gathered information to steal their identity or attack their social media connections.

Blacklist — A list that exists on a server or computer that blocks unwanted connections for specific IP addresses. (See whitelist.)

Bug — An error or mistake in software or hardware that may be exploited by hackers.

Clickjacking — A malicious process in which a victim is tricked into clicking on a URL, button, or other screen object.

Cloud Computing — A process by which computer files and resources are stored and accessed in a location other than the user's phone or computer.

Cracker — The industry term for "hacker." (See hacker.)

Critical Infrastructure — The computer hardware and networks needed for daily operations.

Cryptography — The mathematical security strategies used to protect data and provide security, confidentiality, and authentication.

Cyber Attack — Any attempt to gain access or exploit a computer system or phone.

Cyber Security — The process of protecting digital assets on any kind of network.

Data Breach — A breach occurs when hackers are able to access data that had previously been stored in protected and anonymous ways.

DDoS (distributed denial of service) Attack — An attack that attempts to halt access to any resource by using multiple computers to overload a computer, server, or network.

Digital Certificate — A digital assurance by a third party that a digital property or identity is legitimate.

Digital Forensics — The process of uncovering the history within server logs and other digital records to expose potential unseen vulnerabilities and exploits within a system.

Eavesdropping — The act of listening in on a transaction, communication, data transfer, or conversation.

Encryption Key — The secret number value used by a algorithm to control the encryption and decryption process.

Firewall — A security tool, which may be a hardware or software solution, that is used to filter network traffic.

Hacker — A person who has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations, and altering its abilities and capabilities.

Identity Cloning — A form of identity theft in which the attacker takes on the identity of a victim and then attempts to live and act as the stolen identity.

Identity Fraud — A form of identity theft in which a transaction, typically financial, is performed using the stolen identity of another individual. The fraud is due to the attacker impersonating someone else.

ISP (internet service provider) — The organization that provides connectivity to the internet for individuals or companies.

Key Logger — Software or other eavesdropping measures used to record the keystrokes of a victim as they are typed.

LAN (local area network) — An interconnection of devices (i.e., a network) that is contained within a limited geographic area.

Link Jacking — A potentially unethical practice of redirecting a link to a middleman or aggregator site or location rather than the original site the link seemed to indicate it was directed towards.

Malware (malicious software) — Code written for the purpose of causing harm, disclosing information, or violating security. The following are examples of malware: virus, worm, Trojan horse, logic bomb, backdoor, remote-access Trojan (RAT), rootkit, ransomware, and spyware/adware.

MFA (multi-factor authentication) — A security measure that protects individuals by requiring users to provide two or more authentication factors to access an application, account, or virtual private network (VPN). This adds extra layers of security to combat more sophisticated cyber attacks, since credentials can be stolen, exposed, or sold by third parties.

Pen Testing — Short for penetration testing. This is the act of intentionally attempting to gain access to hardware, software, or physical security measures to test the robustness of a security measure.

Phishing — A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over email, text messages, through social networks, or via smartphone apps.

POS (point of sale) Intrusions — An attack that gains access to the POS (point of sale) devices at a retail outlet, usually aimed at copying legitimate credit card numbers.

Ransomware — A form of malware that holds a victim's data hostage on their computer, typically through robust encryption.

Restore — To bring a system back to an originally clean and safe backed-up state.

Social Engineering — A hack focusing on people rather than technology. Social engineering seeks to use knowledge of one's life and habits to gain trust or exploit vulnerabilities.

Spam — Unsolicited messages or communications received in an email or via text messaging, social networks, or VoIP.

Spear Phishing — A form of social engineering attack that is targeted to victims who have an existing digital relationship with an online entity such as a bank or retail website.

Spoof (spoofing) — The act of falsifying the identity of the source of a communication or interaction. It is possible to spoof IP addresses, MAC addresses, and email addresses.

Spyware — Malware that spies — or monitors online activities — and reports them to a cybercriminal.

Trojan Horse (Trojan) — Malware unknowingly embedded within a benign host file that a user downloads or installs.

Two-Factor Authentication — The means of proving identity using two authentication factors, which is considered stronger than any single-factor authentication. A form of multi-factor authentication.

VPN (virtual private network) — A communication link between systems or networks that is typically encrypted to provide a secure, private, isolated pathway of communications.

Virus — A form of malware that often attaches itself to a file or system as a parasite. When activated, the virus can infect other systems connected to the infected computer.

Vishing — A form of phishing attack taking place over VoIP. In this attack, the cybercriminal uses VoIP systems to be able to call any phone number toll-free.

Vulnerability — Any weakness in an asset or security protection that would allow for a threat to cause harm.

Whitelist — A list of approved resources that a system uses to grant access. The opposite of a blacklist.

Wi-Fi — Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet.

Zero Day/0-Day — A vulnerability in software or hardware that is typically unknown to the vendor and for which no remediation or fix is available. The vendor has zero days to prepare a solution as the vulnerability has already been attacked or exploited.

Protect yourself and your business against cybercrime and cybersecurity risks such as breach of personal information, identity theft and online fraud events, cyberbullying, cyber extortion including ransomware, and cyber attacks to operational systems. Cyber insurance protects businesses and homeowners from hefty legal and operational expenses as they respond to cyber-attacks.

Cyber insurance coverage is vital in today's modern world as we rely heavily on digital information, computer systems, and connected smart homes; and conduct business and personal matters using online platforms, including the exchange of personally sensitive information.

For more information on cyber insurance, please visit HSB.ca/cyber

HSB
A Munich Re company

Leading the charge in cyber protection

Cyber safety for our modern age.