sovereign®
INSURANCE

25 Cyber Security Terms

Not Just Your IT Security Team Should Know

If you don't think your company has experienced a cyber attack, then your IT security team is doing a great job. The truth is, it's not a matter of 'if' a company will be attacked, it's 'when'. Cyber security doesn't rest solely on the shoulders of your IT team – it's everyone's responsibility. We've put together a glossary of terms to help all employees brush up on their cyber security terminology. The more you know, the more you can do your part to mitigate cyber risks.

1. Black Hat

Hackers who break into a network to steal information that will be used to harm the owner or the users without consent.

2. Bot/Botnet

A type of software application, or script, that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A collection of these infected/controlled computers is known as a botnet.

3. Business Email Compromise (BEC)

When a hacker uses a corporate email account to impersonate the real owner in order to deceive suppliers, customers, partners, etc. into sending money or sensitive data to the attacker's account.

4. Clickjacking

A hacking attack that tricks victims into clicking on an unintended link or button, usually disguised as a harmless element.

5. Cloud	A technology that allows users to access files and/or services (data storage) through the internet from anywhere in the world.
6. Data Encryption	The process of encoding data to prevent theft by ensuring the data can only be accessed with a key (i.e. decryption key) or password.
7. DDoS	An acronym that stands for distributed denial of service. This cyber attack aims to make a service such as a website unusable by 'flooding' it with malicious traffic or data from mutliple sources (often botnets).
8. Decryption	The conversion of encrypted data into its original form.
9. Deepfake	An image or audio or video clip that has been edited and manipulated to seem real or believable. Cybercriminals can then use this content on information channels (e.g. social media) to deploy cybersecurity attacks.
10. Domain	A group of computers, printers and devices that are interconnected and governed as a whole.
11. Exploit	A malicious application or script that can be used to take advantage of a computer's vulnerability.
12. Firewall	A defensive technology designed to prevent unauthorized access. Firewalls can be hardware or software based.
13. IoT Security	Technology that safeguards connected devices and networks in the internet of things (IoT). IoT systems are susceptible to attacks such as denial of service and social engineering.
14. Incident Response Plan	Procedures to help IT staff detect, respond to, and recover from network security incidents.
15. Insider Threat	A threat to the company's data integrity that is coming from someone within the organization.

16. Malware	An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include viruses, trojans, worms, and ransomware.
17. Patching	A small piece of software that a company issues to fix a security flaw.
18. Penetration Testing	A way to evaluate security using hacker tools, and techniques with the aim of discovering vulnerabilities and evaluating security flaws that an attacker could exploit.
19. Phishing (or Spear Phishing)	A technique where cybercriminals send fake emails, texts or websites that look like legitimate correspondence to manipulate employees into gaining access to corporate systems or information.
20. Ransomware	A form of malware that deliberately prevents you from accessing files on your computer, holding your data hostage.
21. Social Engineering	A form of psychological manipulation that targets the user rather than the computer itself. Cybercriminals deceive people to gain sensitive and private information.
22. Spyware	A type of malware that functions by spying on user activity without their knowledge.
23. Two-Factor Authentication	A security process that asks users to provide two different authentication factors to verify themselves (also called two-step verification or dual-factor authentication).
24. Vendor Email Compromise (VEC)	An attack that aims to take over the email account of a vendor.
25. White Hat	An ethical computer hacker, or cyber security expert, who is employed to test an organization's infrastructure vulnerabilities.

sovereign® INSURANCE

© 2020 The Sovereign General Insurance Company, a member of The Co-operators group of companies. Sovereign® is a registered trademark of The Sovereign General Insurance Company. Not all advertised products may be available in all jurisdictions. For full terms and conditions, including coverage limitations and exclusions, please refer to the policy wording. The Sovereign General Insurance Company is committed to protecting the privacy, confidentiality, accuracy and security of the personal information that we collect, use, retain and disclose in the course of conducting our business. Visit sovereigninsurance.ca or call toll free at 1-800-661-1652 to learn more.