INSURANCE BOARD
Partners in Protection

Cyber Security:
Two Dozen Terms to Know

1. **Cloud:** A technology that allows access to files and/or services through the internet from anywhere in the world.
2. **Software:** A set of programs that tell a computer to perform a task compiled into a package that users can install and use.
3. **Domain:** A group of computers, printers and devices that are interconnected and governed as a whole.
4. **Virtual Private Network (VPN):** A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic.
5. **IP Address:** An internet "home address" for your device which is identified when it communicates over a network.
6. **Exploit:** A malicious application or script that can be used to take advantage of a computer's vulnerability.
7. **Breach:** The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.
8. **Firewall:** A defensive technology designed to keep "the bad guys" out. Firewalls can be hardware or software-based.
9. **Malware:** An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer: viruses, trojans, worms and ransomware.
10. **Virus:** A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others. However, in more recent years, viruses have caused physical damage as well.
11. **Ransomware:** A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.
12. **Trojan horse:** A piece of malware that often allows a hacker to gain remote access to a computer through a "back door".
13. **Worm:** A piece of malware that can replicate itself in order to spread the infection to other connected computers.
14. **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 computers is known as a "botnet" and is controlled by the hacker or "bot-herder".
15. **Spyware:** A type of malware that functions by spying on user activity without their knowledge. The capabilities include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more.
16. **Rootkit:** Another kind of malware that allows cybercriminals to remotely control your computer. Rootkits are especially damaging because they are hard to detect, making it likely that this type of malware could live on your computer for a long time.
17. **DDoS:** An acronym that stands for Distributed Denial of Service – a form of cyber attack. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).
18. **Phishing or Spear Phishing:** A technique to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.
19. **Encryption:** The process of encoding data to prevent theft by ensuring the data can only be accessed with a key.
20. **BYOD (Bring Your Own Device):** Refers to a company security policy that allows for employees' personal devices to be used in business. A BYOD policy sets limitations and restrictions on whether or not a personal phone or laptop can be connected over the corporate network.
21. **Pen-testing:** Short for "penetration testing," this practice is a means of evaluating security using hacker tools and techniques with the aim of discovering vulnerabilities and evaluating security flaws.
22. **Social Engineering:** A technique used to manipulate and deceive people to gain sensitive and private information. Scams based on social engineering are built around how people think and act. Once a hacker understands what motivates a person's actions, they can usually retrieve exactly what they're looking for – like financial data and passwords.
23. **Clickjacking:** A hacking attack that tricks victims into clicking on an unintended link or button, usually disguised as a harmless element.
24. **White Hat / Black Hat:** When speaking in cyber security terms, the differences in hacker "hats" refers to the intention of the hacker. For example:
    - **White hat:** Breaches the network to gain sensitive information with the owner's consent – making it completely legal. This method is usually employed to test infrastructure vulnerabilities.
    - **Black hat:** Hackers that break into the network to steal information that will be used to harm the owner or the users without consent. It's entirely illegal.