The topic of **cyber security** is sweeping the world by storm with some of the largest and most advanced companies in the world falling victim to cyber-attacks in just the last 5 years. Against that backdrop, highly personal and sensitive information such as social security numbers were recently stolen in the **Equifax hack**, affecting over **145 million people**. Unfortunately, as long as computers exist, we are at risk of having our digital data compromised and manipulated. However, living in the digital age is not all that scary – especially if you know what you're doing. Understanding how your device works is not as hard as it sounds. But, if you could nail long division in the 4th grade, then you can learn cyber basics that will get you pretty far in your own personal security as well as your company's.

We're here to make this learning curve easier by providing a list of the **25 most important cyber security terminology that everyone should know**:

1. Cloud

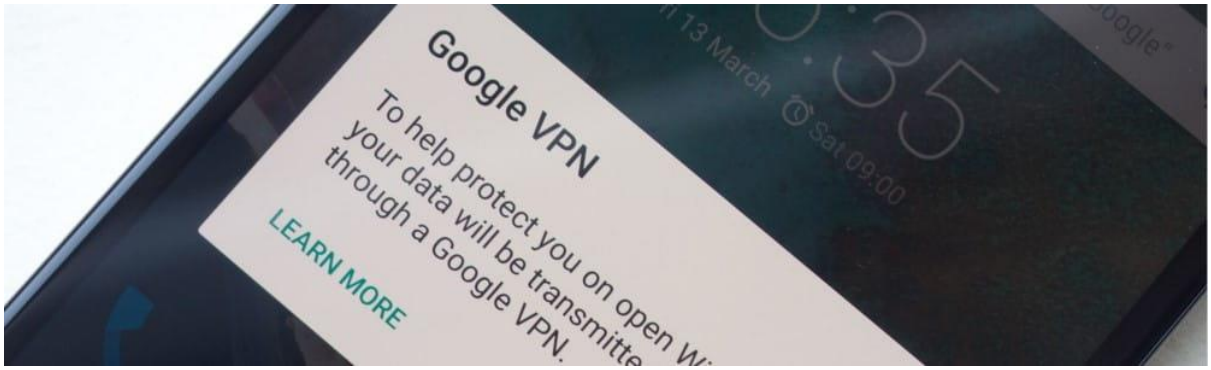
A technology that allows us to access our files and/or services through the internet from anywhere in the world. Technically speaking, it's a collection of computers with large storage capabilities that remotely serve requests.

2. Software

A set of programs that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. For example, Microsoft Office is an application software.

3. Domain

A group of computers, printers and devices that are interconnected and governed as a whole. For example, your computer is usually part of a domain at your workplace.



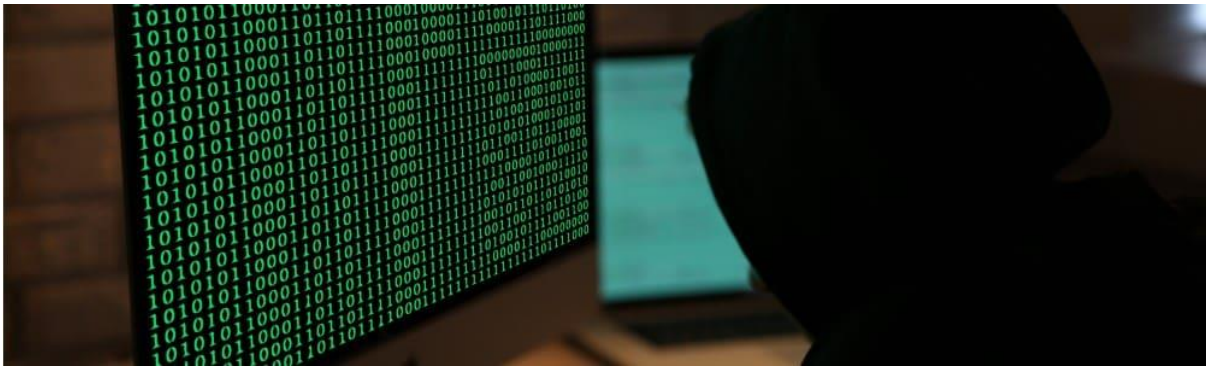
4. Virtual Private Network (VPN)

A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic.

RELATED: Law Firms Are Targets For Hackers, Cybersecurity Experts Say

5. IP Address

An internet version of a home address for your computer, which is identified when it communicates over a network; For example, connecting to the internet (a network of networks).

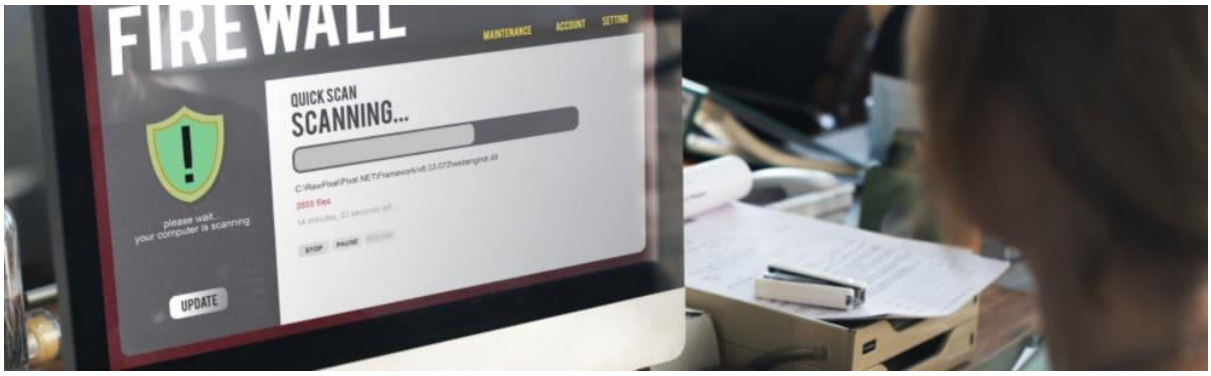


6. Exploit

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.

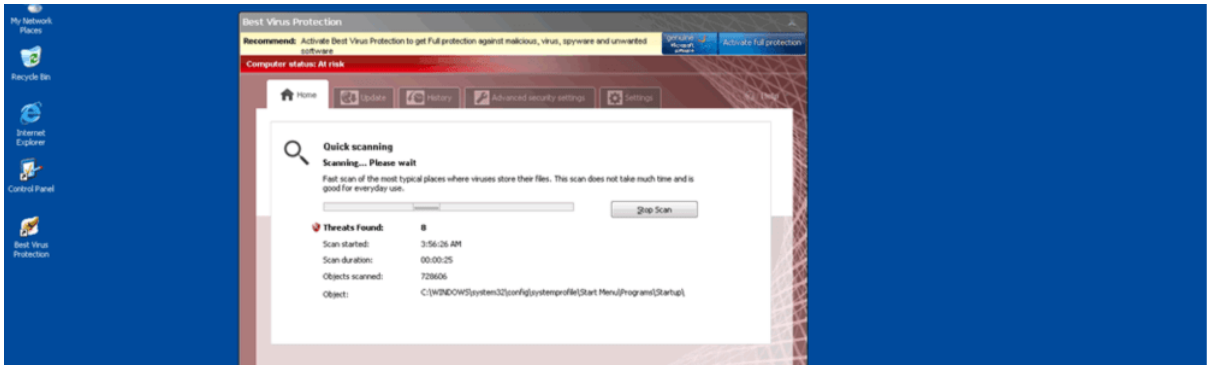


8. Firewall

A defensive technology designed to keep the bad guys out. Firewalls can be hardware or software-based.

9. Malware “the bad guy”

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.



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 like Stuxnet have caused physical damage.

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. For example, WannaCry Ransomware. For more information on Ransomware, check out our free Ransomware Guide.

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.

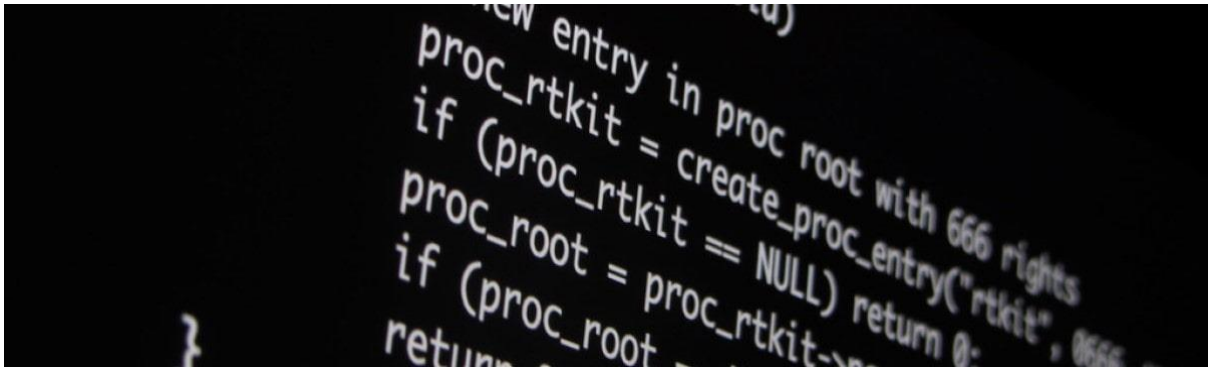
14. Bot/Botnet

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”.

RELATED: 10 Most Important Cyber Security Tips for Your Users

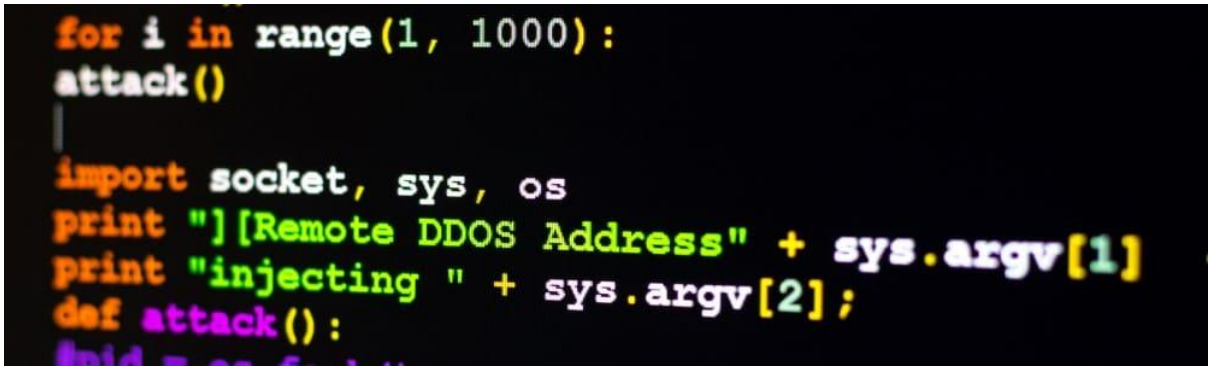
15. Spyware

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.



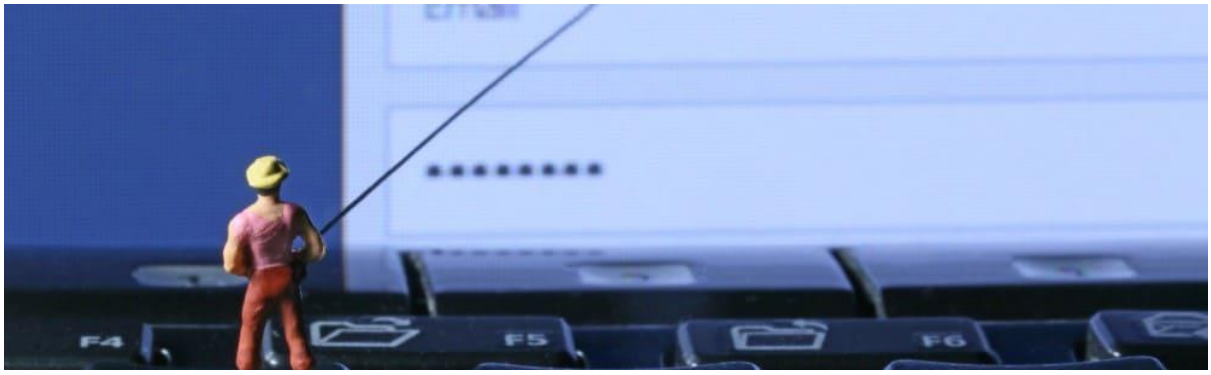
16. Rootkit

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 used by hackers 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. So, 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.

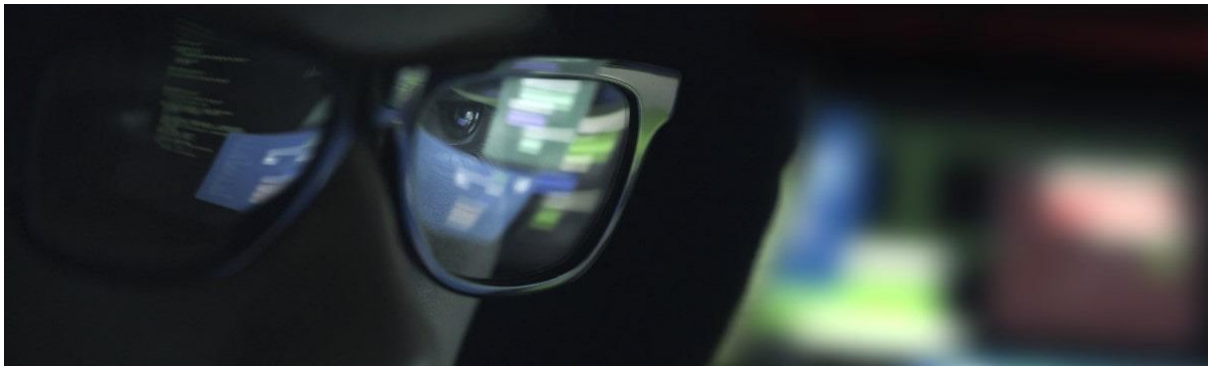
RELATED: Cybersecurity Job Market to Suffer Severe Workforce Shortage

23. Clickjacking

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

24. Deepfake

An audio or video clip that has been edited and manipulated to seem real or believable. The most dangerous consequence of the popularity of deepfakes is that they can easily convince people into believing a certain story or theory that may result in user-behavior with a bigger impact as in political or financial.



25. 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.