Authentication	The process of identifying a user's identity, making sure that they can have access to the system and/or files. This can be accomplished either by a password, retina scan, or fingerprint scan, sometimes even a combination of the above.
Botnet	a network of computers that have been infected with a virus, and now are working continuously in order to create security breaches. These attacks come in the form of Bitcoin mining, sending spam e-mails, and DDoS attacks.
Data Breach	The result of a hacker successfully breaking into a system, gaining control of its network and exposing its data, usually personal data covering items such as credit card numbers, bank account numbers, Social Security numbers, and more.
DDoS	a favourite Black Hat tool. Using multiple hosts and users, hackers bombard a website with a tidal wave of requests to such an extent that it locks up the system and forces it to temporarily shut down.
Domain	A series of computers and associated peripherals (routers, printers, scanners), that are all connected as one entity.
Encryption	Coding used to protect your information from hackers. Think of it like the code cipher used to send a top-secret coded spy message.
Exploit	A means of attack on a computer system, either a series of commands, malicious software, or piece of infected data. Note that in this context, it is a noun, not a verb.
Firewall	Any technology, be it software or hardware, used to keep intruders out.
Hacker, Black Hat	Any hacker who attempts to gain unauthorized access to a system with the intent to cause mischief, damage, or theft. They can be motivated by greed, a political agenda, or simply boredom.
Hacker, White Hat	A hacker who is invited to test out computer systems and servers, looking for vulnerabilities, for the purposes of informing the host of where security needs to be buffed up.
Malware	describes a wide variety of bad software used to infect and/or damage a system. Ransomware, worms, viruses, and trojans are all considered this. It is most often delivered via spam emails.
Phishing	A scam where a hacker poses as a legitimate business or organization (especially credit card companies, banks, charities, Internet providers, other utilities) in order to fool the victim into giving them sensitive personal information or inducing them to click a link or attachment that ends up delivering malware
Ransomware	A form of malware that hijacks your system and encrypts your files, denying you access to them until you send money to unlock everything
Spoofing	when a hacker changes the IP address of an email so that it seems to come from a trusted source.
Spyware	A form of malware used by hackers to have an overview of your computer activities. If a mobile device such as a smartphone is infected, a hacker can read your text messages, redirect your phone calls, and even track down where you are physically located!
Trojan Horse	Yet another form of malware, this one a misleading computer program that looks innocent, but in fact allows the hacker into your system via a back door, allowing them to control your computer.
Virus	Malware which changes, corrupts, or destroys information, and is then passed on to other systems, usually by otherwise benign means (e.g. sending an email).
VPN	a method of connecting a series of computers and devices in a private encrypted network, with each user's IP address being replaced. Users get Internet anonymity, making it difficult for hackers to attack.

Worm	Malware that can reproduce itself for the purposes of spreading itself to other computers in the network. Particularly nasty, they can either be simply a means of slowing down a system by eating up resources, or by committing exploits such as installing back doors or stealing data.
Rootkit	a collection of programs or software tools that allow hackers to remotely access and control a computer or network. Although they do not directly damage users, they have been used for other purposes that are legal, such as remote end-user support. However, the majority of them can open a backdoor on the targeted systems for the introduction of malware, viruses, and ransomware. Typically, it is installed without the victim's knowledge via a stolen password or by taking advantage of system flaws.
BYOD	company policy that permits, encourages, or mandates employees to access enterprise systems and data using their own personal devices, such as laptops, tablets, and smartphones, for work-related activities.
Pen-testing	An approach to security evaluation where manual exploitations and automated techniques are used by attack and security professionals. Only environments with a solid security infrastructure should employ this advanced kind of security evaluation with a mature security infrastructure.
Social Engineering	is a growingly popular way to access restricted resources, instead of breaking in or utilizing technical hacking techniques. This strategy relies on user manipulation and human psychology. An employee might get an email purporting to be from the IT department in order to deceive him into disclosing private information rather than trying to uncover a software weakness in a company system.
Clickjacking	when someone is tricked into clicking on one object on a web page when they want to click on another. In this manner, the attacker is able to use the victim's click against them. It can be used to enable the victim's webcam, install malware, or access one of their online accounts.
Deepfake	A piece of audio or video that has been altered and changed to make it seem authentic or credible. The most perilous aspect of the prevalence of deepfakes is that they can easily convince individuals into believing a particular tale or idea, which may lead to user behaviour that has a greater impact on society at large, such as in the political or financial spheres.
MFA	makes it more difficult for hackers to access your account by requiring you to provide at least two different credentials. It requires a second factor to confirm your identity in addition to your username and password, such as a one-time security code, a fingerprint scan, or a face recognition scan.
PenTest	simulates a cyberattack on your computer system to look for weaknesses that could be exploited. It involves attempting to get into any number of application systems (such as frontend/backend servers, APIs, etc.) in order to find security holes like unsanitized inputs that are vulnerable to code injection attacks.