•**Account takeover:** An account takeover is when a fraudster uses personal information to obtain products and services. Credit card fraud is the most rampant, but skimming and phishing are also common types of account takeovers.

•**Anti-virus:** Anti-virus software runs continuously in the background of a computer and scans for viruses, worms and malware every time the user accesses a website or downloads anything.

•**Bait and switch:** A bait and switch attack is when a hacker buys advertising space on a webpage and then links the advertisement to a page infected with malware.

•**Black hat hacker:** All hackers are capable of compromising computer systems and creating malware, but black hat hackers use these skills to commit cybercrimes.

•**Blockchain:** A blockchain is a string of time-stamped digital records shared between multiple computers. If the data in one block changes, all subsequent blocks in the blockchain reflect the alteration and become invalid. Blockchains help prevent identity theft and fraud by making it difficult to tamper with the data in a block.

•**Bot:** Short for "robot," a bot is an autonomous program that interacts with computer systems in a way that appears or attempts to appear human. Hackers can use bots to mine for usernames and passwords used to commit identity fraud.

•**Cookie theft:** Cookie theft is when a cybercriminal makes copies of unencrypted session data and then uses that data to impersonate someone else.

•**Credential cracking:** Credential cracking describes the various methods — word lists, guessing and brute-force — cybercriminals use to obtain passwords. Credential cracking threats are why it's important to create varied and complicated passwords for all accounts.

•**Criminal impersonation:** Someone commits criminal impersonation when they assume a fake or false identity, usually for political or financial gain.

•**Cybersquatting:** Also sometimes called domain squatting, cybersquatting is when a domain name is stolen or misspelled to attract users for exploitation or profit.

•**Cryptovirology:** Cryptovirology is the study of how cryptology is used to create dangerous malware.

•**Data breach:** A data breach is when private or confidential information is released to an untrusted environment. Cybercriminals can infiltrate a data source physically or remotely bypass network security to expose passwords, banking and credit data, passport and Social Security numbers, medical records and more.

•**Dark web:** The dark web is the part of the internet that can only be accessed through Tor browser software, which keeps visitors anonymous and untraceable. It's not illegal to be on the dark web, but many illegal transactions occur on the dark web (such as buying credit card or Social Security numbers).

•**Deep web:** The deep web is the part of the internet that's not accessible through standard search engines such as Google or Bing. Password-protected and dynamic pages, encrypted networks and the dark web are all part of the deep web.

•**Encryption:** Encryption is a way to scrambled data using computer algorithms to prevent unauthorized access to data or sensitive information.

•**Firewall:** In computing, a firewall is a software program that blocks unauthorized users from getting in without restricting outward communication.

•**Formjacking:** Formjacking is when a hacker infiltrates an e-commerce checkout page to steal credit card information. Similar to an ATM skimmer for the internet age.

•**Ghosting:** In the context of identity theft, ghosting refers to when someone steals the identity of a dead person.

•**Grey hat hacker:** Grey hat hackers' ethics are somewhere between black and white hat hackers. Grey hat hacking involves illegal cyberactivity, but the hacker often reports vulnerabilities to the system's owner and requests a fee in exchange for the information — if a system's owner does not comply with their request, the grey hat hacker usually exploits the newly discovered cybersecurity vulnerability.

•**Honeypot:** A honeypot is a decoy target used to mitigate cybersecurity risks or get more information about how cybercriminals work.

•**Identity cloning:** Identity cloning is a type of identity theft in which a fraudster assumes someone else's identity and attempts to live under that assumed identity.

•**Identity score:** Similar to a credit score, an identity score is a system that gauges an individual's data for legitimacy.

•**Imposter scam:** Imposter scams involve a fraudster posing as a different person for financial or political gain. Usually, the imposter tricks others into giving them money through email, over the phone or via online dating services.

•**Internet of Things:** The Internet of Things, or IoT, describes the interconnectedness of all devices that access WiFi, including cell phones, cameras, headphones and an increasing number of other objects, including washing machines and thermostats.

•**Keylogger:** A keylogger is a computer program that records a person's keystrokes to obtain confidential data.

•**Malware:** A portmanteau of "malicious" and "software," malware describes any software created with the specific intent to cause disruption or damage. Trojans, bots, spyware, worms and viruses are all types of malware.

•**Passive attacks:** Any network attack where the system is monitored or scanned for vulnerabilities is considered "passive attack" because the targeted data isn't modified or damaged.

•**Pharming:** Sometimes called "phishing without a lure," pharming is a type of scam where malicious code is installed onto a device or server to misdirect users onto illegitimate websites.

•**Phishing:** Phishing is a popular type of internet scam in which fraudsters send emails claiming to be from a reputable company to trick individuals into revealing personal information. Phishing attacks decreased from 1 in 2,995 emails in 2017 to 1 in 3,207 emails in 2018.

•**Physical identity theft:** Unlike wireless identity theft, physical identity theft requires an identity thief to be in close proximity to their target. Examples of physical identity theft include stealing a wallet or computer, dumpster diving and postal mail theft.

•**Proxy server:** A proxy server establishes a substitute IP (Internet Protocol) address identity. When you connect online, your computer's IP address is transmitted to websites and establishes your location and may give other identifying details. Proxy servers allow users to connect to the internet anonymously and bypass blocked or restricted websites.

•**PowerShell:** An automated task framework by Microsoft, PowerShell can be embedded in applications to automate batch processing and systems management tools.

•**Ransomware:** Ransomware is a type of malware that threatens to expose or block an individual's or business' data unless a ransom is paid.

•**SIM swap scam:** Sometimes called a port-out scam or SIM splitting, a SIM swap scam is a complex type cell phone fraud that exploits two-factor authentication to access data stored on someone's cell phone. Put simply, if a fraudster has your phone number, they can call your phone company and ask to have the number transferred to "your" new phone. The fraudster then has access to all of your accounts that use two-factor authentication.

•**Skimming:** Skimming is a type of credit card fraud in which the victim's account numbers are copied and transferred to a counterfeit card.

•**Smishing:** Similar to phishing, smishing (or SMS phishing) is when someone attempts to mine sensitive information under a fake identity through text messages.

•**Sockpuppet:** Sockpuppetting is when a person assumes a false identity on the internet for the purpose of deception.

•**Spoofing:** A spoofing attack is when an illegitimate website falsifies data to appear as a trustworthy website to visitors.

•**Spyware:** Spyware is any software designed to gather data from an individual or enterprise. The four primary types of spyware are adware, Trojan horses, tracking cookies and system monitors.

•**Synthetic identity theft:** Synthetic identity theft is when a criminal combines stolen and fake information to create a new, fraudulent identity.

•**System monitor:** Much like it sounds, a system monitor is an application that surveils computer activity. System monitors usually run unnoticed and can record passwords, chats and emails, websites visited and other sensitive or identifying data.

•**Tracking cookie:** Websites use tracking cookies to gather and share data from their visitors. Unlike malware, tracking cookies won't damage computer systems, but they can create privacy concerns.

•**Trojan horse:** Like its classical namesake, a Trojan horse is a type of malware disguised to appear like safe software. Cybercriminals use Trojans to access sensitive data and gain access to private systems.

•**Waterhole attack:** A waterhole attack occurs when a hacker targets a specific group or community. The hacker infects an individual within the targeted group with malware in an attempt to infect the entire group.

•**Wireless identity theft:** Also sometimes called contactless identity theft or RFID identity theft, wireless identity theft is committed by wireless mechanics. Examples of wireless identity theft include phishing and spoofing.

•**Whaling:** Whaling is a phishing attack that targets high-level employees within a company to steal confidential information or sensitive data.

•**White hat hacker:** Unlike a black hat hacker, a white hat hacker uses their ability to break computer networks or bypass security protocols for good rather than evil. White hat hackers are often employed by governments or companies to perform vulnerability assessments.

•**Worm:** A worm is a type of malware that self-replicates and spreads from computer to computer.

•**Virus:** Similar to worms, viruses make copies of themselves. The main difference between viruses and worms is that viruses require a host program to spread.

•**Vishing:** Like phishing or smishing, vishing is when an identity thief attempts to gain sensitive information over the phone.

•**Zero-day exploit:** A zero-day exploit is when cybercriminals target a software the same day weakness in that software is discovered and before a patch can be released to fix the vulnerability.