9 Cybersecurity Terms You Need To Know

Staying ahead of the latest threats is hard. Not understanding the technical jargon makes it harder. This article defines 9 words to know, and shares pro tips to keep you safe and protected.

These days, keeping your devices secure, data private, and online world safe from harm seems like a daunting task. While plenty of reliable solutions exist for **desktop** and **mobile**, knowing where you're vulnerable can be difficult … especially if you're not familiar with the jargon thrown around regarding the latest data breach.

It is imperative to stay ahead of cybercriminals who look to profit by violating your right to freely and safely access the internet. We've identified 9 terms to know, along with our tips to keep you protected.

1. **Botnet.** A botnet (ro**bot** and **net**work) is a network of devices infected by an attacker, and then used together to perform tasks such as carrying out DDoS attacks (see below), mining Bitcoins, and spreading spam emails. Nearly any device connected to the internet, including home routers, can be infected and pulled into a botnet without its owner ever noticing.

2. **Data breach.** A data breach happens when a company's network is attacked and valuable data is stolen—usually customer log-in credentials, credit card details, and social security numbers. The stolen data can then be abused in myriad ways: held for ransom (see Ransomware below), sold on the darknet, and, of course, used to make purchases. Often hackers try to crack email passwords, then test those log-in details on other popular sites, since many people use the same credentials for multiple accounts—a big no-no.

3. **DNS attack.** DNS stands for "domain name server," which uses the name of any common website to redirect traffic to its own IP address. For instance, you'd expect "google.com" to take you to Google's IP address. Using a DNS hijack, however, cybercriminals can translate "google.com" to their own IP address, redirecting you to malicious sites where they can collect your information or have you download malware. In an attempt to get you to click on a link, DNS hijacks can also deliver altered search results.

4. **DDoS attack.** Attackers use DDoS (Distributed Denial of Service) attacks to render a network unavailable. They do this by overwhelming the targeted machine with massive requests from multiple devices. The target suffers a severely clogged bandwidth, and legitimate connections become impossible. These attacks are typically carried out by botnets (see above).

5. **Mobile banking Trojans.** It looks like your trusted banking app, but that's just an overlay. Underneath, a mobile banking Trojan tricks you into entering financial credentials and personal information. It can also gain administrative rights to intercept SMS messages, making it possible to record two-factor authentication codes as well.

6. **Open Wi-Fi.** Encrypted connections protect you. Open Wi-Fi networks are unencrypted, which is why they're risky. Anyone can create a fake hotspot and trick your device into joining it automatically. When you use open Wi-Fi without protection like a VPN (see tips below), anyone on that network can see the sites you visit, your log-in passwords, your financial and personal data, and more. Hackers often name their phony Wi-Fi networks after popular spots (like "Starbucks"), knowing that most devices automatically rejoin hotspots they've used in the past. Hackers can even redirect your unencrypted traffic, sending you to malicious sites.

7. **Phishing.** Used by cybercriminals to trick people into giving up sensitive information, phishing scams pose as emails from an organization or person you know. There is usually a link or attachment included, which it tries to get you to click so that you'll unwittingly allow malware to download to your system. Sometimes phishing scams look indistinguishable from the sites they're imitating, and they attempt to trick you into entering your password info.

8. **Ransomware.** Ransomware is malware that takes hold of your system and encrypts it, sometimes attacking individual files. Trying to access the encrypted files triggers a note that claims you are locked out until you make a payment (more than $600, on average). The messages sometimes appear to be from an official government agency accusing you of committing a cyber-crime, which scares many into paying the ransom. Payment is often demanded in Bitcoins.

9. **Spyware.** Spyware is malware used by hackers to spy on you, so they can access personal information, banking account details, online activity, and anything else they may find valuable. On mobile devices, spyware can know your whereabouts, read your text messages, redirect calls, and much more.

Tips to keep yourself safe and secure