Tech Talk: 6 Cybersecurity Terms You Need To Know

Here are six cybersecurity terms that are important to know to help protect you and your business from attacks.

1) Hacker

Although having nothing to do with coughing, when you discover your computer or digital device has been "hacked," you may just want to choke! Security hackers are computer criminals that, by means of exploiting weaknesses in a computer network or system, can access—and ultimately take over—your computer's data, including sensitive, private information. Some hackers even go as far as to hold your data hostage for a ransom payment. Whatever the motive for the hacker's actions, whether malicious or for their own entertainment, these individuals can destroy your company's entire network.

2) Virus

Unfortunately, chicken soup is not the cure when your digital device catches a virus. These malicious "contagious" software programs can infect a computer by reproducing itself and "spreading" to data files and infecting critical sections of the hard drive. After a virus has infected a computer, it can wreak all sorts of havoc, such as accessing private information, corrupting or even destroying enough data to make your once-powerful computer nothing more than an expensive paperweight. Good network protection is key because after one computer is infected, a virus can spread through the server and infect every computer in an office.

3) Trojan Horse

Like its namesake, this deceiving computer program is used to get into a computer by making the user think they are downloading a standard program update or opening an innocent email attachment. Trojan horses are different from viruses, in that they usually are not designed to "infect" other files, but rather, can be used to contact a "hacker" who can then access everything from bank account information, passwords or personal identity addresses.

4) Malware

Simply put, "malware" is an abbreviation for "malicious software." The term "malware" was coined in 1990, and is used interchangeably with the term "computer virus."

5) Phishing

Unlike the pleasant recreational pastime, this kind of phishing can result in snagging an unknowing user's sensitive data when they take the "bait." These phishing schemes send requests from what appear to be legitimate entities such as banks, online payment processors or popular social websites, to lure unsuspecting individuals to disclose personal information. These schemes can be elaborate, producing fake websites that look almost exactly like the legitimate one.

6) Social Engineering

Many "phishers" have advanced their "baiting" techniques to now include social media. While many of the more popular social media sites, like Facebook and Twitter, attempt to protect their visitors, hackers are very adept at finding loopholes in even the most secure sites.

No one who has a website, utilizes the Internet for any reason, or is part of a connected digital network is immune to cybersecurity threats. To protect yourself and your organization:

- Be aware, be diligent and pay attention to any abnormal or suspicious activity or behavior on your computer
- If you are suspicious of an email request for information, pick up the phone and call the alleged source, to see if it is legitimate
- Have an ongoing defense plan in place to thwart cyber attacks, and update on a regular basis
- Hire an experienced IT support firm to install anti-virus software, perform routine monitoring and updates to ensure you're taking every precaution to "stay one step ahead" of the hackers and the ever-evolving techniques they use to get into your computer, and your life!