The ABCs of Cybersecurity

ADWARE

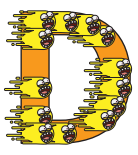
Noticing a lot more ads than usual? You may have downloaded "free" software with embedded advertisements. Adware often collects data without your permission, so keep your antivirus/anti-malware up to date.

BACKUP

Backups may be your best friend! If your device becomes compromised or you experience data loss, you will be thankful for these copies of files and programs.

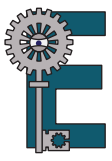
COOKIE

The word "cookie" usually conjures up images of dessert treats, but browser cookies aren't always sweet! Cookies refer to the data servers send to a web browser to keep track of visits. While they can be helpful, they can also be used to disguise malware or track your online activity.



DENIAL OF SERVICE (DOS) ATTACK

This just sounds scary, and it is. To shut down a machine or network, these attacks flood the target with traffic or information to trigger a crash.



ENCRYPTION

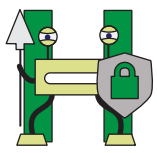
Let's skip the 0s and 1s and just say encryption is the process of converting data (called "plaintext") into a code (called "ciphertext") to prevent unauthorized access.

FIREWALL

The first line of defense, a firewall is a security system that prevents hackers, viruses and malware from intruding into a network. Always check to make sure your home's firewall is turned on.

GATEWAY

A gateway joins two networks so the devices on them can communicate with each other. Without gateways, you wouldn't be able to access the internet.

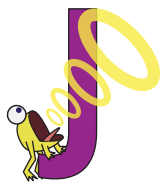


HTTPS

In the address bar of your browser, the portion before the colon is usually http or https. The "s" stands for secure and means communication between your computer and the site should be safe.

IP SPOOFING

Sometimes crimes may be hiding in plain site! IP spoofing or IP address forgery is a technique hackers use to impersonate a trusted source.



JAMMING

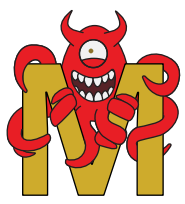
The deliberate blocking of or interference with authorized wireless communications, including cellphone signals.

KEYLOGGER

A program that records (logs) keys struck on a keyboard. Some antivirus software offers protection; see if your current provider does.

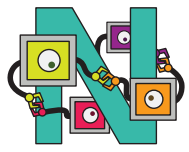
LOGIC BOMB

A piece of code that triggers a malicious program. These can execute viruses and worms at a certain date, such as April Fools' Day.



MALWARE

Shorthand for malicious software, malware comes in many shapes and forms to disrupt computer operations, gather sensitive information, or gain access to files.



NETWORK

Two or more connected computers that share resources. Firewalls, anti-malware, and antivirus software help protect *your* local area network.

OUTSIDER THREAT

Most cyber threats come from outside the network, such as nation-sponsored attackers, hacktivists and other cyber criminals.

PHISHING

These emails appear to be from reputable companies to trick users into revealing personal info — such as credit card numbers — at a bogus website.

QUARANTINE

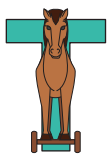
The process of storing files containing malware in isolation for future disinfection or examination.

RANSOMWARE

Malware that encrypts a victim's hard drive and holds the data "hostage" until a ransom is paid. Unfortunately, paying the ransom doesn't guarantee the return of your data.

SOCIAL ENGINEERING

The practice of manipulating or deceiving individuals into divulging personal or confidential information. Phishing and other scams are types of social engineering.



TROJAN HORSE

A type of malware disguised as something else, such as useful software. Sometimes you should look a gift horse in the mouth!

UNIFORM RESOURCE LOCATOR (URL)

We couldn't surf the web without URLs, the addresses that identify each unique file on the World Wide Web.

VISHING

The telephone equivalent of phishing. Scammers call their victims in an attempt to make them release private info used for identity theft.

WORM

These creepy crawlers are malicious programs that can run independently and are designed to infect other computers while remaining active on infected machines.

XML ENCRYPTION

A type of encryption used with Web Services Security (WSS) that helps protect you from cross-site scripting attacks.

YOTTABYTE

The single largest recognized value used with data storage, one yottabyte is equal to one septillion bytes, or 1E+24 for you math nerds.

ZOMBIE MACHINES

A compromised computer that is connected to the internet. Mindless on their own, they can help bring on the computer apocalypse.

Division of
Information Technology