



## Cyber Security Term Glossary

**Admin:** The system administrator account, usually reserved for IT to do maintenance and install new programs.

**Anti-Malware:** A piece of software that tries to prevent and remove unwanted malicious software programs from your computer by looking for patterns in created files, running programs, or network activity.

**Anti-Virus:** A piece of software that tries to prevent and remove viruses from your computer by looking for patterns in created files, running programs, or network activity.

**Automatic Updates:** Software updates that occur on their own to patch security issues. Usually initiated by your computer system without your explicit approval.

**Cloud:** A platform for storing and accessing your data and/or programs via the internet.

**Connected Vehicle:** A motorized vehicle with computational abilities such as being able to offer directions, interact with cell phones and MP3 players, and provide real-time tracking data.

**Cyber Security:** The practice of keeping unauthorized users out of your systems and away from your data.

**Data Loss Prevention (DLP):** A strategy deployed to ensure sensitive data is not lost, misused, or accessed by unauthorized users.

**Encrypt, Encryption:** Protecting sensitive information by encoding the file with a password or a key so only authorized parties who have it can view the information.

**Firewall:** A device that controls and restricts the internet access of your local network.

**Hosted:** When a platform, software or website resides in the cloud.

**HTTPS (Hyper Text Transfer Protocol Secure):** A method by which computers establish a secure connection to a remote website to transfer data, such as web pages and other media.

**Intellectual Property (IP):** a work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, trademark, etc.



**Multifactor Authentication:** Adds additional layers of security when signing in to an account with a password. There are multiple ways to use multifactor with one of the most common being a text message. After you enter in your password, the login account will send a text message to your phone with a onetime, expiring code to complete the login. Other methods include: Card Swipes, USB Dongles, Email Message, and Biometrics like fingerprints.

**Mobile Payment Software:** A mobile app which allows a user to accept payment on the go, usually through an attachable card reader. Common software includes Square Reader, PayPal Here and Clover Go.

**Physical Security:** The practice of keeping people away from your physical equipment, such as work stations, servers, mobile devices and other sensitive areas.

**Remote:** A method by which technical support or other works are conducted over the internet.

**Router:** A device that directs traffic from one network (usually the internet) to another (such as your home or office).

**Spreadsheet:** A document in which data is organized into rows and columns. Usually used for accounting, and in products such as Microsoft Excel and Apple Numbers.

**Thumb Drive:** A device that plugs into your computer and/or mobile device that allows the transfer of files. Other names being USB drive, flash drive, jump drives.

**Two-Factor Authentication:** A security measure that uses your phone number, email address, and/or app to send you a temporary password after you login to your account.

**URL (Uniform Resource Locator):** A line of text that starts with a protocol and contains either a domain name or an IP address that refers to a specific service on the internet. Examples: <http://example.com>, <https://example.com>, <ftp://example.com>, <smb://example.com>.

**Virtual Private Network (VPN):** Technology that employs encryption of data between a device and network

**WEP (Wired Equivalent Privacy):** A less secure wireless security algorithm used to secure wireless access points. WEP is considered insecure, but is still commonly used today.

**WPA, WPA2 (Wi-Fi Protected Access):** A more secure wireless security algorithm used to secure wireless access points. WPA and WPA2 are both considered secure.

