# CyberSecurity Glossary of Terms

## Virus

The defining characteristic of viruses is that they are

self-replicating computer programs which install themselves without user consent.

## Trojan

A Trojan is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

## Worm

A computer worm is a standalone malware program that replicates itself in order to spread to other computers.

## Spyware

Is software that aims to gather information about a person or organization without their knowledge or consent or that asserts control over a computer without the consumer's knowledge.

## Rootkits

A rootkit is a collection of malicious software designed to enable access to a computer that would not otherwise be allowed, while at the same time masking its existence or the existence of other software. Removal can be complicated or practically impossible.

## Keylogging

Is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

## Adware

Is any software package that automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The term is sometimes used to refer to software that displays unwanted advertisements known as malware.

## Bots

An Internet bot, also known as web robot, is a software application that runs automated tasks (scripts) over the Internet. The largest use of bots is in web spidering, in which an automated script fetches, analyzes and files information from web servers at many times the speed of a human.

## Backdoors

A backdoor is a method, often secret, of bypassing normal authentication in a software product or computer system. Backdoors are often used for securing unauthorized remote access to a computer or network.

## BYOD

Bring your own device

## Ransomware

A type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction.

## PUP – Potentially Unwanted Program

Unwanted software bundling is bundled software which computer users are fooled into installing along with a wanted program. This software can display intrusive advertising, or track a user's Internet usage to sell information to advertisers and inject its own advertising into the web .

## Cookies

A cookie is a small script placed on the hard drive of  your computer by the server of a website that you visit. The cookie is placed there for the purpose of recognizing your specific browser / computer combination, were you to return to the same site. A cookie itself cannot harm the computer, as it does not and cannot hold code.

3rd party cookies can potentially contribute to malware propagation. Turn off 3rd party cookies in your browser.

## Hosted ads

are an increasingly prevalent source of malware. All it takes is one click on an infected advertising banner to give a hacker full access to your computer.

## DNS Redirection

Say a user meant to enter "AmericanBank.com", but instead accidentally spelled AnericanBank.com. Cyber-criminals register these misspelled URL's. Treat every entry into an address bar with caution. Measure twice, cut once.

## Wi-Fi Vulnerabilities

Users should never access their bank accounts or any websites containing their personal information over open Wi-Fi networks. Scammers scan through these networks and pick up the log-in credentials.

## Like-jacking

Occurs when criminals post fake Facebook "like" buttons to webpages. Users who click the button don't "like" the page, but instead download malware.

## Link-jacking

This is a practice used to redirect from trusted websites to malware infected websites that hide drive-by downloads or other types of infections.