Cybercrime Prevention Flyer

CPF 00006-2021-CID361-9H 1 April 2021

Cyber Terminology 101

With the 2020 global pandemic forcing many to telework, there is now no doubt that we are in a digital age. Smart phones, smart cars, smart homes, and even smart watches — computers are a part of our daily lives. But how much do you know about the cyber realm? You have likely heard quite a few cyber terms before but how familiar with them are you? If asked, could you define them? Well now you can simply refer to this flyer as your quick reference guide for basic cyber terms.

Commonly Used Terms

Antivirus Software: uses virus definitions to determine whether a file contains a virus and must be updated regularly to protect systems and networks against new attack signatures.

Attack: an intrusion against an information system (computer) resulting in the degradation, denial, or destruction of the information or information system (computer).

Bot/Botnet: a software application or tool that performs tasks on command, allowing an attacker to take control remotely of an affected computer—a collection of infected computers is a botnet.

Cache: contains copies of web pages saved by the browser that was used to view them. These files are used to increase the speed of web browsing and are sometimes called temporary internet files.

Cloud: a collection of computers with large storage capabilities that remotely serve requests, allowing you to access files and services through the internet from anywhere in the world.

Cookie: an information packet sent from a website to a web browser that records a user's activity on that website. The information packet is stored on the user's computer and used to provide more personalized services for each subsequent visit to the website.

Domain Name: a text-based translation of the numerical IP address assigned to an internet resource. Most networks and

Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"Do What Has To Be Done"

Cybercrime Prevention Flyer

websites have text-based domain names that people can remember, such as www.army.mil. Domain names are also referred to as internet addresses.

Exploit: a malicious application/tool used to take advantage of a system's vulnerability(ies).

Hacker: an unauthorized user who attempts to or gains access to an information system, the act of which is known as hacking.

Hardware: the physical components of a computer.

Firewall: an access control device (can be software or hardware) that performs specific security activities such as detecting failed attempts at access.

Information System: a complementary network of hardware and software that are used to collect, process, create, store, and disseminate data.

Internet Service Provider (ISP): a company that offers access to the internet.

Intrusion: the unauthorized act of bypassing the security mechanisms of an information system. Unauthorized access to a computer.

Internet Protocol (IP) Address: a unique identifier for each machine or device on a network for the purpose of routing data. An example of an IP address is 131.107.10.7.

Malware: malicious software that attacks a computer. Malware has three categories: viruses; Trojans; and worms. Malware is commonly used to commit fraud and intrusions.

Network: two or more devices that are connected (via wires or wirelessly) and communicate with each other.

Network Intrusion: the compromise of one or more devices on a network or networks, and at least partial access to the resources within.

Social Engineering: a technique used to manipulate and deceive a person in order to gain sensitive and private information or access. Social engineering makes use of previously attained information usually garnered from social media.

Software: a set of programs that can be installed and used to tell a computer to perform a task.

Cybercrime Prevention Flyer

Spam: unsolicited advertising or other information sent out via email or other messaging services.

Trojan Horse: a computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system.

Unauthorized Access: gaining access to any computer resource without permission.

URL: short for Uniform Resource Locator, is a standardized address used to make website connections. Also known as a web address, an example URL is https://www.cid.army.mil.

Virtual Private Network (VPN): a tool that creates a private network connection across a public network connection, providing privacy, anonymity, and security while on the internet.

Virus: a computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a device.

Vulnerability: a weakness in an information system, system security procedures, or internal controls that could be exploited to gain unauthorized access.

Web Browser: also simply browser, is an application which allows users to browse/access the internet. Commonly used browsers include Internet Explorer, Google Chrome, Safari, Opera, and Mozilla Firefox.

Wireless Hotspot: used to refer to a location or device which allows individuals to connect to the internet wirelessly. Cellphones can be used as mobile hotspots, sharing its cellular data connection with another device wirelessly.

Worm: a self-replicating, self-spreading, self-contained program that uses networking tools to spread itself. Or more simply, a worm is a computer program that replicates itself across network connections to other systems.

Worms vs. Viruses: viruses cannot be executed (carried out) unless the infected file is opened while worms are immediately executable. Viruses will not spread to other computers on a network unless a user sends the virus to another computer and a user on that second computer opens the infected file. However, worms send themselves to other computers and sometimes run exploits against other computers, infecting them automatically.

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF