Published on *University of Colorado* (https://www.cu.edu)

Home > Be Cyber Smart: Learn the Basic Terms

Be Cyber Smart: Learn the Basic Terms [1]

At a time when we are more connected than ever, being “cyber smart” is of the utmost importance. This year has already seen more than a fair share of breaches, including the SolarWinds and Kaseya breaches as well as a high-profile cyberattack on the Colonial Pipeline and other critical infrastructure. Furthermore, as has been underlined by these recent breaches, cyberattacks are becoming more sophisticated.

Being cyber smart is one of the best ways to protect yourself and others from cybercriminals. Learn these terms and increase your cyber smart IQ.

Antivirus Software

A program that monitors a computer or information system to detect or identify major types of malicious code and to prevent or contain malware incidents.

Authentication

The process of verifying the identity or other attributes of a computer user or device. *Are you who you say you are?*

Authorization

A process of determining whether you can have and have been granted access to specified or privileged types of information or systems.

Cloud Computing

A computing service where an organization gives limited access to their computing resources to other organizations and individuals. Resources are often used for storage but may be used for compute power or networking infrastructure. Often referred to as “someone else’s computer” since whenever cloud computing is used, you are using a computer owned by a different organization.

Cyberattack

A large-scale attempt to gain unauthorized access to systems, services, resources, or information. An attempt to compromise a system’s availability and integrity.

Cybercriminal

A person who engages in criminal activity by means of computers or the internet. Also referred to as a hacker or bad actor.

Cybersecurity

Practice of protecting information and communications systems from damage, unauthorized use or modification, and exploitation. Through strategy, policies, processes, and awareness, cybersecurity aims to prevent cybercriminals from accessing, changing, or destroying sensitive information; extorting money from users and organizations; and disrupting normal business processes.

Data Availability

Data that is both appropriately secured and available to authorized users when needed.

Ensuring the availability of information is a key principle of security.

Data Integrity

Data that is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner. Ensuring the integrity of information is a key principle of security.

Domain Name

The name of a website. It is what comes after “@” in an email address, or after “www.” in a web address. Examples include @gmail.com, cu.edu, google.com, youtube.com, and wikipedia.org. See URL for more information.

Encryption

The process of converting data into a form that can be only accessed by authorized people or devices. Typically, access is granted through passwords or decryption keys. Examples include emailing sensitive information or website transmissions that includes financial numbers.

Firewall

A defensive, computer security system that restricts internet traffic going in, out and within a network. The goal is to keep the cybercriminals out.

Information Security Risk

The potential for an adverse impact that stems from the loss of confidentiality, integrity, or availability of information. Security risks are one type of business risk.

Learn more about potential adverse impacts to the university’s mission, function, and reputation. [2]

Internet Protocol (IP) Address

An internet version of a home address for your computer, which is identified when it communicates over a network. It is a unique number that identifies a device on the internet or a local network. It communicates the address of the computer in a way that is easier for computers to use but is hard for humans to remember. (The domain name functions as a link to the IP address.)

Insider Threat

The threat that an employee or contractor using authorized access to compromise the confidentiality, integrity, or availability of sensitive information

Internet of Things (IoT)

A system of internet-connected objects that can collect and transfer data over a wireless network. Examples of IoT include thermostats, cars, lights, and refrigerators.

Learn more: Smart Home Devices Need Smart Security [3].

Malicious Code

Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Often found in email that contains fake and malicious links.

Malware

A general term that describes all forms of malicious software designed to have an adverse impact of a computer or information system. Common forms include viruses and ransomware.

Multifactor Authentication (MFA)

MFA, sometimes referred to as two-factor authentication of 2FA, is an authentication process that verifies you are who you claim to be. You are required to provide two or more pieces of evidence when logging in to account. A typical example: you log into a website that sends a numeric code to your mobile phone, which you then entered to gain access to your account.

Learn more: Back to Basics: What’s multi-factor authentication - and why should I care [4].

Need to Know or Least Privilege

A practice of restricting sensitive information to only those with an authorized need to know the information. Access to the information must be necessary for people to conduct their official duties. This term also includes anyone that the people with the knowledge deemed necessary to share it with.

The goal is to 1) make it difficult for unauthorized access to occur and 2) limit access to the smallest possible number of people.

Learn more: Data Classification [5]

Phishing

A type of electronic scam and deceptive tactics that cybercriminals use to manipulate people into doing what they want with the goal of stealing information and money.

The tactics used, sometimes called “social engineering,” are the foundation of all phishing scams conducted through email and text messages, and mobile phone calls.

Learn more: Phishing Scams FAQs [6].

Ransomware

A type of malicious software (malware) that locks and encrypts your computer or files, and then demands a ransom to remove the malware and restore access. Ransomware is often delivered through a phishing email with an attachment or link that, when clicked, installs the malware.

Learn more: What is Ransomware? [7]

Security Incident or Breach

Any event that, regardless of accidental or malicious cause, results in the any of the following:

- Disclosure of sensitive information to someone unauthorized to access it
- Unauthorized alteration of information
- Loss of information that is legally or contractually bound to protect
- Disrupted information technology service

Learn more: Reporting an Incident [8].

Sensitive Information

Information that must be protected from compromise, such as unauthorized or accidental access, use, modification, destruction, or disclosure. Classifying or labeling the information, such as “highly confidential,” helps determine the minimum security requirements necessary to keep it safe.

Learn more about sensitive information at CU: Data Classification [5].

Social Engineering

Deceptive techniques used to manipulate and deceive people with the goal of gaining sensitive information, such as financial data and passwords. The techniques are designed around how people think and act, such a willingness to help people and delivered through email and text messages, phone calls, and in-person encounters.

Software Vulnerability

A flaw or weakness found in software code that could impact the software's performance and security, allowing cybercriminals to exploit and gain access to systems and information.

Spam

Unsolicited, unwanted email sent to large volumes of recipients.

Spoofing

In cybersecurity, spoofing is a practice used by cybercriminals to electronically disguise themselves as known and trustworthy sources. Examples include a message being sent from a false email address or a malicious website link that appears to be a reputable business.

Spyware

A type of malicious software (malware) that spies on your computer activity without your knowledge. Spyware can also collect account and financial information.

Uniform Resource Locator (URL)

A complete web address used to find a particular web page. The domain name is the name of the website; the URL will lead to any one of the pages within the website. Examples of an URLinclude:

- https://www.cu.edu/security [9]
- https://en.wikipedia.org/wiki/University_of_Colorado [10]
- https://www.youtube.com/feed/trending [11]

Virtual Private Network (VPN)

VPN is an encrypted—secured—connection over the Internet from a computer device to a network, helping to safely transmit sensitive information.

Virus

A computer program that can replicate itself, infect your computer without your permission or knowledge, and then spread to another device or information system.

If you have any questions or recommendations for terms, please contact the awareness team at securityawareness@cu.edu [12].

Groups audience:
Office of Information Security

Source URL: https://www.cu.edu/security/be-cyber-smart-learn-basic-terms

Links
[1] https://www.cu.edu/security/be-cyber-smart-learn-basic-terms
[2] https://www.cu.edu/security/about-adverse-impact
[3] https://www.cu.edu/security/smart-home-devices-need-smart-security
[4] https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care
[5] https://www.cu.edu/security/data-classification
[6] https://www.cu.edu/security/awareness/phishing-scams-faqs
[7] https://www.cu.edu/blog/ois-blog/what-ransomware
[8] https://www.cu.edu/security/reporting-incident
[9] https://www.cu.edu/security
[10] https://en.wikipedia.org/wiki/University_of_Colorado
[11] https://www.youtube.com/feed/trending
[12] mailto:securityawareness@cu.edu