AMA
Learning

Cybersecurity & Computing Innovations: Notes

In this lesson:

- Online Security
- Legal & Ethical Concerns
- Computing Innovations

Online Security:

- **Personal identifiable information** (PII) is information about an individual that identifies links, relates, or describes them.
- Examples of PII include:
    - Social Security Number
    - Age
    - Race
    - Phone numbers
    - Medical information
    - Financial information
    - Biometric data (fingerprint and retinal scans)
- Search engines can record and maintain a history of search made by users.
    - Search engines can use search history to suggest websites or for targeted marketing.
- Websites can record and maintain a history of individuals who have viewed their pages.
    - Devices, websites, and networks can collect information about a user's location.
- Technology enables the collection, use, and exploitation of information about by and for individuals, groups and institutions.
- Personal data such as geolocation, cookies, and browsing history, can be aggregated to create knowledge about an individual.
- **Personal identifiable information** and other information placed online can be used to enhance a user's experiences.
- **Personal identifiable information** stored online can be used to simplify making online purchases.
- Commercial and government curation (collection) of information may be exploited if privacy and other protections are ignored.
- Information placed online can be used in ways that were not intended and that may have a harmful effect.
    - For example, an email message may be forwarded, tweets can be retweeted, and social media posts can be viewed by potential employers.
- **Personal identifiable information** can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.
- Once information is placed online, it is difficult to delete.
- Programs can collect your information and record where you have been, how you got there and how long you were at a given location.
- Computing resources can be misused. It is important to protect users.

- All real world systems have errors or design flaws that can be exploited to compromise them. Regular software updates help fix errors that could compromise a computer system.
- Users can control the permissions programs have for collecting and user information. Users should review the permission settings of programs to protect their privacy.
- **Authentication** measures protect devices and information from unauthorized access.
    - Examples of authentication measures include strong passwords and multi factor authentication.
    - A strong **password** is something that is easy for a user to remember but would be difficult for someone else to guess based on knowledge of that user.
- **Multifactor authentication** is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism, typically in a least two of the following categories:
    - **knowledge** (something they know like a password)
    - **possession** (something they have like a phone)
    - **inference** (something they are like a fingerprint).
    - Multi Factor authentication requires at least two steps to unlock protected information; each step adds a new layer of security that must be broken to gain unauthorized access.
- **Encryption** is the process of encoding data to prevent unauthorized access
- **Decryption** is the process of decoding data.
- Two common encryption approaches are:
    - **Symmetric key encryption** involves one key for both encryption and decryption.
    - **Public key encryption** pairs a public key for encryption with a private key of decryption.
        - The sender does not need the receiver's private key to encrypt a message, but the receiver's private key is required to decrypt the message.
- **Certificate authoritie**s issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.
- Computer viruses and malware **scanning software** can help protect a computing system against infection.
- A computer **virus** is a malicious program that can copy itself and gain access to a computer in an unauthorized way.
    - Computer viruses often attach themselves to legitimate programs and start running independently on a computer.
- **Malware** is software intended to damage a computing system or to take partial control over its operation.
    - Untrustworthy (often free) downloads from freeware or shareware sites can contain malware.

- **Phishing** is a technique that attempts to trick a user into providing information. That personal information can then be used to access personal information.
    - That information can be used to access sensitive online resources, such as bank accounts and emails.
    - Unsolicited emails, attachments, links, and forms in email can be used to compromise the security of a computing system.

  - These can come from unknown senders ro from known senders whose security has been compromised.
- A **malicious** link can be disguised on a web page or in an email message.
- **Keylogging** is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.
- Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a rogue access point.
  - A **rogue access point** is a wireless access point that gives unauthorized access to secure networks.

<u>Legal and Ethical Concerns</u>

- Material created on a computer is the intellectual property of the creator or an organization.
- Ease of access and distribution of digitized information raised intellectual property concerns regarding ownership, values, and use.
- Measures should be taken to safeguard intellectual property.
- The use of material created by someone else without permission and presented as one's own is plagiarism and may have legal consequences.
- The use of material created by someone other than use should always be cited.
- Creative commons, open source, and open access have enabled broad access to digital information. As with any technology, using computing to harm individuals or groups raises legal concerns. Computing can play a role in social and political issues, which in turn raised legal and ethical concerns.
- Some example of legal ways to use materials created by someone else include:
  - **Creative Commons** - a public copyright license that enables the free distribution of an otherwise copyrighted work. This is used when the content curator wants to give others the right to share, use, and build upon the work they have created.
  - **Open source** - programs that are made freely available and may be redistributed and modified.
  - **Open access** - online research output free of any and all restrictions on access and free of many restrictions on use such as copyright or license restrictions.

<u>Computing Innovations</u>

- The effect of a computing innovation can be both beneficial and harmful
- Not every effect of a computing innovation is anticipated in advance.
- A single effect can be viewed as both beneficial and harmful by different people, or even by the same person.
- Computing innovations have often had unintended beneficial effects leading to advances in other fields.
- A computing innovation can have an impact beyond its intended purpose.
- Advances in computing have generated and increased creativity in other fields, such as medicine, engineering, communications, and the arts.
- Computing innovations can be used in ways that their creators had not originally intended:

- The World Wide Web was originally intended only for rapid and easy exchange of information within the scientific community.
- Targeted advertising is used to help businesses, but it can be misused at both individual and aggregate levels.
- Machine learning and data mining have enabled innovation in medicine, business, and science, but information discovered in this way has also been used to discriminate against groups of individuals.
- Information posted to social media services can be used by others.
    - Combining information posted on social media and other sources can be used to deduce private information about you.