SAFE COMPUTING

Security is needed to protect the confidentiality, integrity, and availability of information. Security protects that data from cyber attacks and hacking. Privacy is the right to control data generated by one's usage of computing innovations and restrict the flow of that data to third parties.

Privacy and security are concerns with any interaction on the internet. Once a company's security or privacy has been compromised, it takes years, if ever, for customers to trust that company again. Target, Ashley Madison, AOL, Yahoo, and Facebook are examples of large companies that have had their data compromised, with some of those companies never recovering consumers' trust.

Personally, identifiable information (PII) is information about an individual that identifies, links, relates, or describes that person. Examples of PII include the following:

- Social security number
- Age
- Race
- Phone numbers
- Medical information
- Financial information
- Biometric data

PII can be analyzed and processed by businesses and shared with other companies. The information collected has enabled companies to gain insight into how to interact with customers better. PII and other information can be used to enhance a user's online experience. PII can also be used to simplify making online purchases.

PII has monetary value. The entire business model for some computing innovations is to sell user information to targeted advertisers. As a result, concerns have been raised over how companies handle the sensitive information of their consumers.

Information placed online can be used in ways that were not intended and that may have a harmful impact. For example, an email message may be forwarded, tweets can be retweeted, and social media posts can be viewed by potential employers.

Once information is online, it is difficult to delete. 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.

Cyber criminals are creative in their methods for stealing PII data. One such data breach was an app developed to use on Facebook that was a personality quiz. The app was designed to take the information from those who volunteered to give access to their data for the quiz. This quiz generated more data when the quiz was shared with friends and family. The data were then sold to the political consulting firm Cambridge Analytica, which used the data for targeted ads during the 2016 presidential election campaign. Facebook was fined $5 billion by the Federal Trade Commission for violating consumers' privacy rights.

Technology enables the collection, use, and exploitation of information about, by, and for individuals, groups, and instructions. For example:

- Search engines can record and maintain a history of searches made by users.
- 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.

A computing innovation generates metadata that can have the effect of reducing the privacy of the user. Metadata can include geolocation, time, date, filename, and so on. This rapid sharing of user data can often have significant impacts beyond the intended purpose or control of the programmer.

For example, user data can be sold to targeted marketing companies. Marketers can use large data sets to target audiences who are likely to buy their products. For example, the author of this text adopted a puppy named Lilygoose. Soon after the adoption, the author received an advertisement for puppy products. This advertisement included the dog's name, breed, and color. (A picture of Lilygoose is provided above for reference.)

The same open standards that fueled the growth of the internet have, at the same time, left users open to malware. Antivirus software and firewalls can help avoid malware. However, some cyber criminals hide malware in antiviral software! Users must always be aware of who they trust.

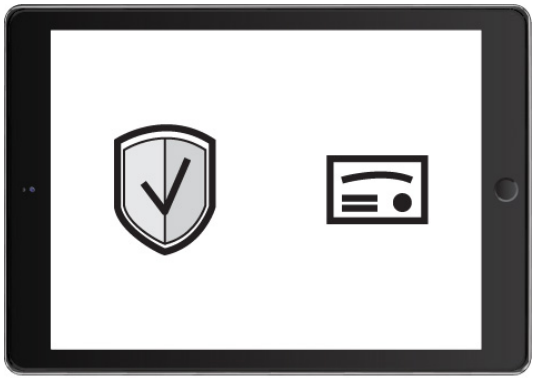
Authentication measures protect devices and information from unauthorized access. Examples of authentication measures include passwords and multifactor authentication. A strong password should be easy to remember but difficult for someone else to guess. A weak password would be something that PII data can predict. Combinations of your birthday and your elementary school would be easy to guess if cyber criminals have your PII data.

Multifactor authentication is a method of computer access control in which a user is granted access only after successfully presenting several pieces of evidence to an authentication mechanism, typically in at least two of the following categories:

- Knowledge—something the user knows
- Possession—something the user has
- Inherence—something the user is

Multifactor 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.

Digital certificate authorities issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.

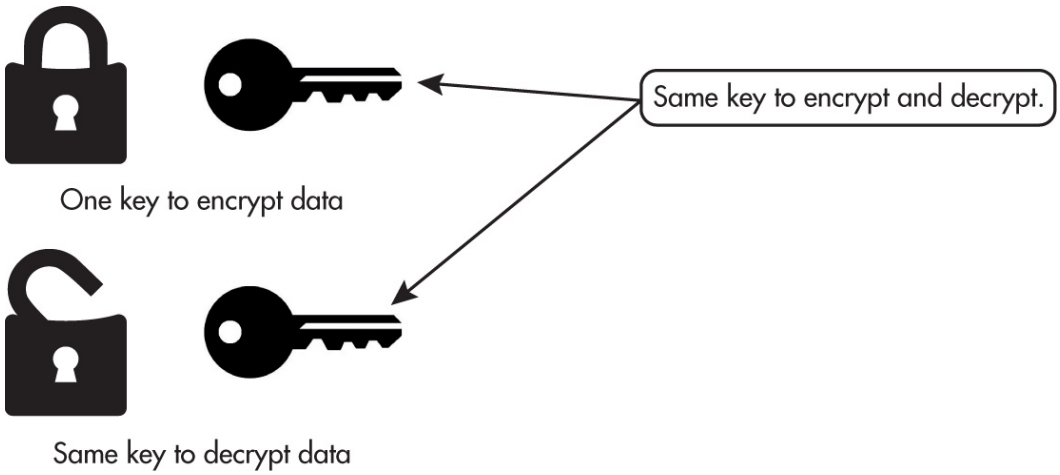


Digital Certificate

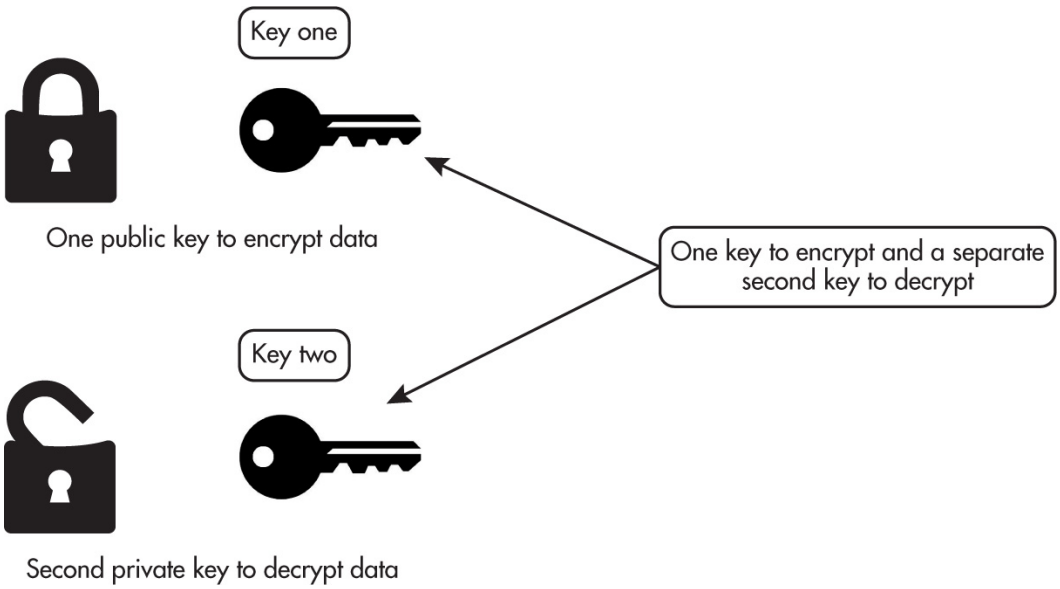
Encryption

To increase security, encryption is used. Encryption uses cryptographic algorithms to encrypt data. Encryption is the process of encoding data to prevent unauthorized access. Decryption is the process of decoding the data.

Symmetric key encryption uses the same key for both encryption and decryption. The one key is a shared secret and relies on both sides keeping their key secret.



Public key encryption (also called asymmetric encryption) uses two keys—one private and one public. Anyone with the public key can encrypt data, and the public key is public. To decrypt, a second key, which is private, is needed.



Phishing

Unauthorized access can be gained to computers in several ways. One method is phishing. Phishing is a technique that directs users to unrelated sites that trick the user into giving personal data. Phishing is a technique used by cyber criminals posing as a legitimate institution to lure individuals into providing sensitive data, such as PII, banking and credit card details, and passwords. This personal information can then be used to access sensitive online resources, such as bank accounts and emails.

Scammers often update their tactics, so phishing attacks can be hard to identify. A common phishing scam involves a malicious link that is disguised on a webpage or in an email message, directing the user to a site that the user identifies as a trusted site. However, the site is not the trusted site but, instead, is a site designed to just look like the trusted site. The spoofed site prompts users to download freeware or shareware that contain malware.

Keylogging

Keylogging is another method involving unauthorized access to a computer. Keylogging is the use of a program to record every keystroke made by the computer user in order to gain fraudulent access to passwords and other confidential information. Keylogging monitors and records every password and credit card number the user types and then sends this information to cyber

criminals who make use of this sensitive data. Some keyloggers are hardware. The physical hardware is installed between the keyboard and the computer. Security software cannot detect hardware keyloggers.

Rogue Access Point

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.