Cybersecurity Badges

Glossary

Bitcoin—an independent digital currency, or cryptocurrency, that is used and distributed electronically.

Black-hat hacker—someone who uses illegal or unethical means to break into computer systems for personal or financial gain.

Cookie—a small data packet that websites can store on your device in order to collect information.

Cyber hygiene—the regular habits that computer users can take to improve their cybersecurity.

Cybersecurity—the protection of digital devices, such as phones or computers, against attacks.

Cyberstalking—the use of the Internet or other digital technology to stalk or harass an individual, group, or organization.

Data vulnerability—a weakness that leaves one's data open to a cyber attack.

Digital footprint—the information that is created as a result of someone's online activity.

Gray-hat hacker—a hacker whose motives and tactics fall somewhere in between black-hat and white-hat hackers. They generally have good intentions and do not plan to steal or exploit the security vulnerabilities they find. However, they may break into systems without the owner's knowledge or permission; and/or they may demand a reward in return for their work.

Identity theft—a type of crime in which someone uses your personal information without your permission.

Log file—a security record of all the security-related events that occur within a given network system. Cybersecurity professionals regularly monitor and analyze these files to look for any abnormalities.

Personally identifiable information (PII)—any information that can be used to identify, contact, or locate an individual, like your name, birthday, address, social security number, and email address or password. You should never share identifiable information with someone you don't know online.

Ransomware—a type of malware that denies you access to your data until you pay a ransom.

Social engineering—a cyber attack strategy that attempts to manipulate or deceive a user so that they give up their personal information.

Social marketing—influencing people to change their behaviors in order to benefit society. This might include campaigns centered on building awareness or support for a cause or asking for individuals to donate or take action.

Steganography—the practice of hiding secret messages in otherwise not-secret mediums.

White-hat hacker—an "ethical hacker" who uses his/her skills in legal ways to protect people and organizations.