girl scouts Cadette

Cybersecurity Badges

Glossary

Brute-force attack—when an attacker tries many different passwords in hopes of guessing correctly.

Computer network—a group of computers – or other digital devices – connected together in some way.

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

Dictionary attack—when an attacker uses an existing list of words as potential passwords.

Digital footprint—information that exists about a person as a result of their online activity.

Encryption—the process of encoding a message or data so that people need a secret key or password to read it.

Malware—software that aims to cause damage to your computer or network.

Man-in-the-Middle—a type of cyber attack in which a hacker intercepts a message between two entities in order to spy on them or steal their information.

Metadata—data that describes or defines another piece of data.

Nodes—as packets of data travel through a computer network, they stop at many different "nodes" along the way.

Packets—when you send a message, or submit information, through the Internet, your message is broken up into smaller packets of data.

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

Phishing—a type of cyber attack in which a hacker sends an email that contains bad links, harmful attachments, or requests for money.

SMSing—a type of cyber attack in which a hacker sends a text message in order to try and steal your personal information.

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

Spoofing—a type of cyber attack in which a hacker pretends to be someone you know, or an organization you trust, in order to gain access to your information.

Spyware—software that secretly collects information about you.

Two-factor authentication—an extra layer of cyber security that requires two different types of validation (e.g. username/password AND a unique code sent to your phone) before allowing access.