Click Thinking Spotlight

Vocabulary of Information Security

While the subject of Information Security can seem overwhelming, understanding the vocabulary is the first step toward comprehension. Here we take a look at some of the key terms and concepts.

- An asset is anything of value to an organization, such as information, physical or intellectual property—even its employees.
- Examples of assets can include credit card numbers, financial data, personnel records, networks, laptops containing important files and more.
- A threat is an event that, if realized, would bring harm to an organization or its assets.
- Information security threats can include phishing attempts, hacks and ransomware attacks, malware and spyware, theft of physical property—even attempts to shut down a website by flooding it with traffic.
- A threat actor is a broad term for any individual or group that seeks to conduct malicious activities against a business or organization.
- Cybercriminals are hackers and attackers that use techniques like phishing and ransomware to scam or extort victims and organizations.
- Hacktivists are politically or socially motivated individuals that disrupt online traffic and websites to further their agendas.
- State-Sponsored Attackers are entities backed by governments that infiltrate larger organizations to steal sensitive data.
- Insider Threats are individuals within an organization who provide sensitive data to others unwittingly, by being deceived, through negligence or intentionally.
- An attack is a threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.
- Attacks can target organizations and individuals and may be driven by greed, vengeance, ego, a desire to harm or humiliate, a quest for political superiority or other reasons.
- Risk is a concept that acknowledges undesired events, like attacks, can occur that may compromise an organization's information, disrupt operations or damage property.
- A vulnerability is any weakness in a system that can be exploited. A vulnerability can be technical, physical, human or any other point where an organization can be compromised.

For the Vocabulary of Information Security module, see your manager or information security contact.