

# Glossary terms from week 2

## Terms and definitions from Course 1, Week 2

**Adversarial artificial intelligence (AI):** A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently

**Business Email Compromise (BEC):** A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage

**Computer virus:** Malicious code written to interfere with computer operations and cause damage to data and software

**Cryptographic attack:** An attack that affects secure forms of communication between a sender and intended recipient

**Hacker:** Any person who uses computers to gain access to computer systems, networks, or data

**Malware:** Software designed to harm devices or networks

**Password attack:** An attempt to access password secured devices, systems, networks, or data

**Phishing:** The use of digital communications to trick people into revealing sensitive data or deploying malicious software

**Physical attack:** A security incident that affects not only digital but also physical environments where the incident is deployed

**Physical social engineering:** An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location

**Social engineering:** A manipulation technique that exploits human error to gain private information, access, or valuables

**Social media phishing:** A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack

**Spear phishing:** A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

**Supply-chain attack:** An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed

**USB baiting:** An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network

**Virus:** refer to “computer virus”

**Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source

**Watering hole attack:** A type of attack when a threat actor compromises a website frequently visited by a specific group of user

---

Revision #1

Created 2023-06-01 17:02:23 UTC by naruzkurai

Updated 2023-06-03 04:51:01 UTC by naruzkurai