Cybersecurity

2.2.4 – Misinformation and Impersonation

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Misinformation/Disinformation

- Refer to the spread of false or misleading information with the intent to deceive, manipulate, or compromise the security of computer systems or users.
- Both can contribute to an insecure cyber environment by creating a lack of trust, confusion among users, and diverting attention from real security issues.

Misinformation

- The dissemination of inaccurate or false information – often *unintentional*.
- Involves spreading incorrect details about a security vulnerability, a software update, or the nature of a particular threat.
- Can lead to confusion and poor decision-making, potentially putting systems at risk.

Disinformation

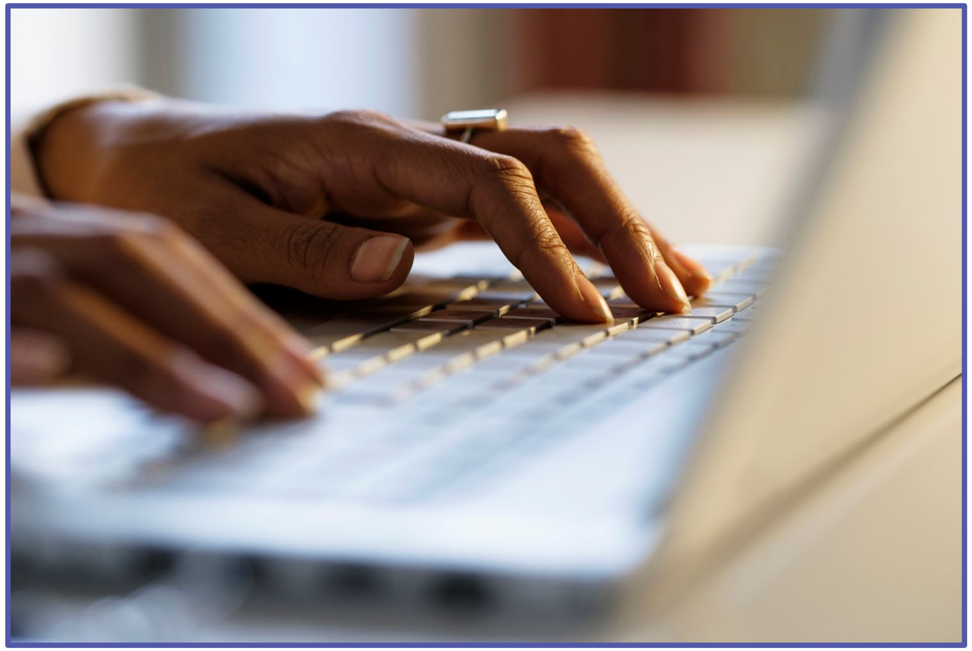
- *Intentionally* spreading false information with the purpose of causing harm, confusion, or manipulating individuals or systems.
- May involve spreading fake security alerts, creating false narratives about cyber threats, or manipulating public perception to divert attention from actual security issues.

Impersonation and Tailgating

- Impersonation uses social engineering to fool someone into unwittingly providing sensitive data to attackers or transferring money to a fraudulent account.
  - Dumpster diving
  - Personalization
- Tailgating, also known as piggybacking, is a social engineering attack where one tries to gain entry to a restricted area without the proper authentication.
  - Can be prevented by implementing security measures such as visitor policies, security questioning, and physical barriers like mantraps.

Business Email Compromise

- Also known as BEC.
- Type of cyberattack where an attacker gains access to or compromises a business email account to conduct fraudulent activities, such as unauthorized fund transfers or invoice fraud.
  - CEO fraud
  - Invoice fraud
  - Employee impersonation



Brand Impersonation

- The act of mimicking or imitating a legitimate brand or company, often with the intent to deceive or defraud individuals.
- Commonly used in phishing attacks.
  - Fake emails
  - Fake websites
  - Social media profiles that mimic reputable brands to trick recipients into divulging sensitive information or spreading malware

Hoaxes

- Deception that can either be humorous or malicious
- Most are not real threats but can be portrayed as real
- Emails, chain letters, urban legends, malware
  - Intent is to mislead and frighten victims hoping to get victims to forward the hoax.

Defense

- Verification is key
- Check credentials
- Call the third party for proof