Employee Awareness and Training: Social Engineering

- Train employees on possible social engineering techniques and how to combat them

Area of Risk	Attack Technique	Train Employee or Help Desk on:
Phone	Impersonation	Not providing any confidential information
Dumpsters	Dumpster Diving	Not throwing sensitive documents in the thrash Shredding document before throwing out Erasing magnetic data before throwing out
Email	Phishing or Malicious Attachments	Differentiating between legitimate emails and a targeted phishing email Not downloading malicious attachments

Employee Training and Awareness: Data Classification

- Organization should train employees on how to tell if information is considered confidential or not

Area of Risk	Attack Technique	Train Employee or Help Desk on
office	Stealing sensitive information	How to classify and mark document-based classification levels and keep sensitive document in a secure place

Typical Information classification levels:

- Top Secret (TS)
- Secret
- Confidential
- Restricted
- Official
- Unclassified
- Clearance
- Compartmented information

- Security labels are used to mark the security-level requirements for information assets and controls access to it
- Organizations use security labels to manage access clearance to their information assets

Notes:

Separation of Duties (SoD) and Principle of Least Privileges (POLP)

Separation of Duties (SoD)

- **Conflicting responsibilities** create unwanted risks such as security breaches, information theft, and circumvention of security controls
- A successful security breach sometimes requires the collusion of two or more parties. In such cases, separation of duties woks well to reduce the likelihood of crime
- Regulations such as **GDPR** insist on paying attention to the roles and duties of your security team

Principle of Least Privileges (POLP)

- Believes in providing employees with the **minimum necessary** access they need , no more, no less
- Helps the organization protect against from malicious behavior, and achieve better system stability and system security

Information Security Controls

Notes: