SOCIAL ENGINEERING

SOCIAL ENGINEERING

TERMS

- **Spam:** unsolicited emails.
- **Prepending:** attaching a message to an email saying something like "RE:" or "MAILSAFE:PASSED" to make it appear that the email is safe and legitimate.
- **Hoaxes:** fake information, like false security alerts.
- **Pretexting:** when an attacker tricks a victim by giving a false pretext, or reason, for why the victim should share information with the attacker.
- **Pharming:** when an attacker redirects victims from a legitimate website to their malicious version.
- **Typosquatting:** when an attacker deliberately registers a website domain with a name that is close to that of a legitimate website.
- **Identity Fraud:** is when an attacker uses a victim's personal information.
- **Credential Harvesting:** when an attacker is attempting to harvest or learn, a victim's credentials.
- **Watering Hole Attack:** when an attacker hacks the third-party service or software a group of victims uses to gain access to a victim or the victims' company.
- **Tailgating:** when an attacker follows someone through a secure door before the door can close.
- **Dumpster Diving:** when an attacker goes through a victim's trash to obtain sensitive information.
- **Shoulder Surfing:** when an attacker looks over someone's shoulder as they type their password.