filename:comptia-secplussy0601-1-1-social_engineering_techniques
Showname: Security+ \(SY0-601\)
Topic: Threats, Attacks and Vulnerabilities
Episode: Social Engineering

Compare and contrast different types of social engineering techniques

Description: In this episode, we discuss the methods used by bad actors to deceptively manipulate individuals into divulging confidential information through social engineering. We will compare and contrast different types of social engineering techniques like phishing, whaling, spam, spear phishing and more.

---

* Principles of Security
* Vulnerability
* Threat
* Attack
* Social Engineering
    + Phishing \(Authority, Trust, Urgency\)
        - Vishing
        - Smishing
        - Spear phishing
        - Whaling
    + Spam
    + Spam over Internet messaging (SPIM)
    + Pharming
        - Redirection to a bogus site
        - DNS poisoning
        - Malware
    + Watering hole attack
        - Usually starts with reconnaissance
        - Determine what website a target group frequent
        - Inject malicious code into the website
        - Targets get infected as they visit the website
    + Credential harvesting
        - Scraping usernames and password from a website clone \(Familiarity\)
    + Typo squatting
        - URL Hijacking
* Physical Techniques
    + Dumpster diving

    + Shoulder surfing
    + Tailgating
    + Pretexting
        - Creating a fabricated scenario
* Outliers
    + Invoice scams
    + Hoax
    + Prepending
* Most social engineering
    + Impersonation (Urgency)
        - All social engineering
    + Identity fraud
        - All social engineering
    + Eliciting information
        - All social Engineering

[Prepending]:https://www.zdnet.com/article/why-you-need-multi-factor-authentication-now-gmail-phishing-scheme-prepends-url-with-working-script/
[URL]:https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Data_URIs