Social engineering

- human side of information security
- manipulating people through a variety of strategies
- We are almost vulnerable when we are responding instead of thinking clearly
- understanding The target, how human reals and how stress reactions can be leveraged to meet a goal

authority

Relies on fact that most people will obey someone who Appears to be incharge or knowledgeable regardless of whether or not they actually are

intimidation

Relies on scaring or bullying an individual into taking a desired action

consensus

Is a principle of convincing victims that others have already trusted a threat actor

#Scarcity

Making scenarios where something look more desirable because it may be the last one available

#familiarity

Reply on you liking the individual of even the Organization the individuals claiming to represent

trust

Social engineer use this technique work tO build a connection with target

Urgency

Creating a feeling that the action must be taker quickly due to some reasons

Social engineering techniques

Phishing

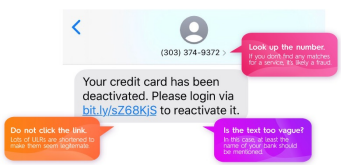
- focused on information, username, password, credit card number and related data
- Done via EMAIL
- Spear phishing - targeting an individual or groups in an organisation
- Whaling - targeting an specific individual(big fish) like CEOs and CFOs
- Defense - awareness, detecting phishing mails

#Vishing

- accomplished via voice or voicemail
- Reply on phone calls to social engineering targets into disclosing personal information
- Relies on a sense of urgency with and imminent threat or issues needs to be solved

Smishing

- via text message
- Attempt to get users to click on a link in a text message



Misinformation and Disinformation

- misinformation is incorrect information, often resulting from getting facts wrong
- Disinformation is incorrect,inaccurate or outright false information that is intentionally provided to serve an individual or organisation's goal

Impersonation

- pretending to be someone
- Using techniques to make target believe the impersonator
- Leads to identity fraud or identity theft

Business Email Compromises (BEC)

- uses legitimate email addresses to conduct scams and other attacks
- Invoice scams, gift cards scams, data theft
- BEC is also called EAC (Email Account Compromise)
- Defence - multi factor authentication, awareness training

PRETEXTING

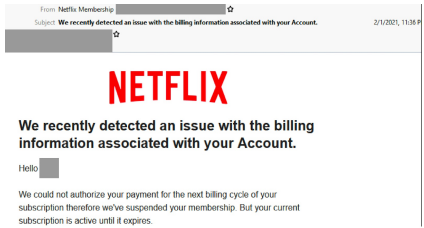
- Using a made up scenario to justify why you are approaching an individual
- Defence - verification call

Watering Hole Attacks

- uses websites that targets frequently visits
- Attackers focuses on either targeting the site or deploying malware through other means such as advertising network

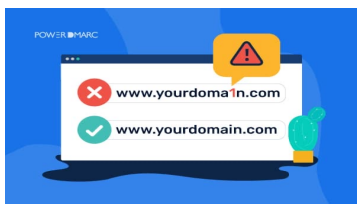
#Brand Impersonation

- Brand impersonation or brand spoofing is a type of phishing attack
- Attack uses emails that are intended to appear to be from a legitimate brand , even using email templates used by the brand itself
- Used in attempts to get users to log into their existing account, particularly for stores and banks

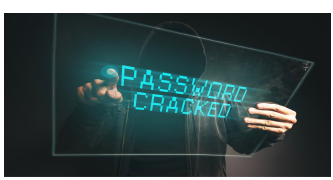


Typosquatting

- uses misspelled and slightly off but similar to the legitimate site URLs
- Rely on the facts that people will mistype URLs and end up on their sites



Password Attacks



Brute-force attacks

- iterate through passwords until they find one that works
- Process that involves trying different variations until it succeeds

Password Spraying Attack

- attempts to use a single password or small set of passwords against many accounts
- Particularly effective if attackers knows victims specific default passwords or set of passwords

Dictionary attacks

- use a list of words for their attempts
- John the Ripper- a open source password cracking tool that have word lists(dictionary) built in