Deception

Social engineering

Its a **non-technical strategy** that **attempts to manipulate individuals** into performing certain actions or divulging confidential information.

Rather than software or hardware vulnerabilities, social engineering **exploits human nature**, taking advantage of people’s willingness to help or preying on their weaknesses, such as greed or vanity.

Pretexting

This attack **occurs when an individual lies to gain access to privileged data**.

(for example attacker pretends to need personal or financial data in order to confirm a persons identity)

Something for something

Quid pro quo attacks **involve a request for personal information in exchange for something**, like a gift.

(for example, a malicious email could ask you to give your sensitive personal details in exchange for a free vacation)

Identity fraud

This is the **use of a person’s stolen identity to obtain goods or services by deception**.

(for example, smo has acquired your data and is attempting to issue a credit card in your name)

Social engineering tactics

Cybercriminals rely on several social engineering tactics to gain access to sensitive info.

Authority

Attackers **prey on the fact that people are more likely to comply when instructed by smo they perceive as an authority figure.**

For example, an executive opens what looks like an official subpoena attachment but is actually an infected PDF.

Intimidation

Cybercriminals will often **bully a victim into taking an action that compromises security**

For example, a secretary receives a call that their boss is about to give an important presentation but the files are corrupt. The criminal on the phone claims it’s the secretary’s fault and pressures the secretary to send across the files immediately or risk dismissal.

Consensus

Often called ‘social proof’, consensus **attacks work because people tend to act in the same way as other people around them, thinking that smo must be right if others are doing so**

For example, cybercriminals may publish a social media post about a ‘business opportunity’ and get dozens of legitimate or illegitimate accounts to comment on its validity underneath, which encourages unsuspecting victims to make a purchase.

Scarcity

A well known marketing tactic, scarcity attacks work because **attackers know that people tend to act when they think there is a limited quantity of smt available.**

For example, someone receives an email about a luxury item being sold for very little money, but it states that there are only a handful available at this price, in an effort to spur the unsuspecting victim into taking action.

Urgency

Similarly, **people also tend to act when they think there is a limited time to do so**

For example, cybercriminals promote a fake time-limited shipping offer to try and prompt victims to take action quickly.

Familiarity

**People are more likely to do what another person asks if they like this person**

Therefore, *attackers will often try to build a rapport with their victim in order to establish a relationship*. In other cases, they may clone the social media profile of a friend of yours, in order to get you to think you are speaking to them.

Trust

Building trust in a relationship with a victim may require more time to establish

For example, a cybercriminal disguised as a security expert calls the unsuspecting victim to offer advice. When helping the victim, the ‘security expert’ discovers a ‘serious error’ that needs immediate attention. The solution provides the cybercriminal with the opportunity to violate the victim’s security.

**Remember that cybercriminals repertory is vast and ever-evolving. Sometimes, they might combine two or more of the above tactics to increase their chances.**

Shoulder surfing and dumpster diving

Shoulder surfing

Simple attack,

That involves **obserbing or literally looking over a target’s shoulder to gain valuable info** such as PINs, access codes, or credit card details

For this they can use binoculars, security cameras…

Dumpster diving

‘one man’s trash is another man’s treasure.’ nowhere is this more true then here

**Process of going through a target’s trash to see what info has been thrown out**.

Impersonation and hoaxes

Impersonation

**It’s the act of tricking smo into doing smt they would not ordinarily do by pretending to be smo else.**

For example, a cybercriminal posing as an IRS employee recently targeted taxpayers, telling the victims that they owed money that had to be paid immediately via wire transfer

Or they can also use impersonation to attack them.

Hoaxes

A hoax **is an act intended to deceive or trick smo** and can cause just as mech disruption as an actual security breach.

For example, a msg that warns of a (non-existent) virus threat on a device and asks the recipient to share this info with everyone they know.

Piggybacking and tailgating

**They occur when a criminal follows an authorized person to gain physical entry into a secure location or a restricted area**. They can do it by:

- **giving the appearance** of being **escorted** into the facility **by an authorized person**.

- **joining and pretending to be part of a large crowd that enters the facility**.

- **targeting an authorized person who is careless about the rules of the facility**.

One way of preventing this is to use two sets of doors. This is sometimes referred to as a mantrap and means individuals enter through an outer door, which must close before they can gain access through an inner door

Other methods of deception

Invoice scam

**Fake invoices** are sent with the **goal of receiving money from a victim** by prompting them to put their credentials into a fake login screen

Watering hole attack

It describes an exploit in which an **attacker observers or guesses what websites an organization uses most often**, and **infects one or more of them with malware**

Typosquatting

This type of attack **relies on common mistakes such as typos made by individuals when inputting a website address into their browser**.

The incorrect URL will bring the individuals to a legitimate-looking website owned by the attacker, whose goal is to gather their personal or financial info.

Prepending

**Attackers can remove the ‘external’ email tag used by organizations** to warn the recipient that an email has originated from an external source.

This tricks individuals into believing that a malicious email was sent from inside their organizations.

Influence campaigns

Often used in cyberwarfare, **influence campaigns are usually very well coordinated and blend various methods** such as fake news, disinformation campaigns and social media posts.

Defending against deception

Organizations need to promote awareness of social engineering tactics and properly educate employees on prevention measures.

- never disclose confidential info or credentials via email, chat… to unknown parties.

- resist the urge to click on enticing emails and web links.

- be wary of uninitiated or automatic downloads.

- establish and educate employees on key security policies.

- do not give in to pressure by unknown individuals.