CyberTutorial Web.App

Social Engineering

What is Social Engineering?

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in person, and via other interactions.

Why Social Engineering ?

- Easier than technical hacking
- Hard to detect and track

The Mind of a Social Engineer:

- More like actors than hackers.
- Learn to know how people feel by observing their actions.
- Can alter these feelings by changing what they say and do.
- Make the victim want to give them the information they need.

Social engineering attackers have one of two goals:

1. Sabotage: Disrupting or corrupting data to cause harm or inconvenience.
2. Theft: Obtaining valuables like information, access, or money.

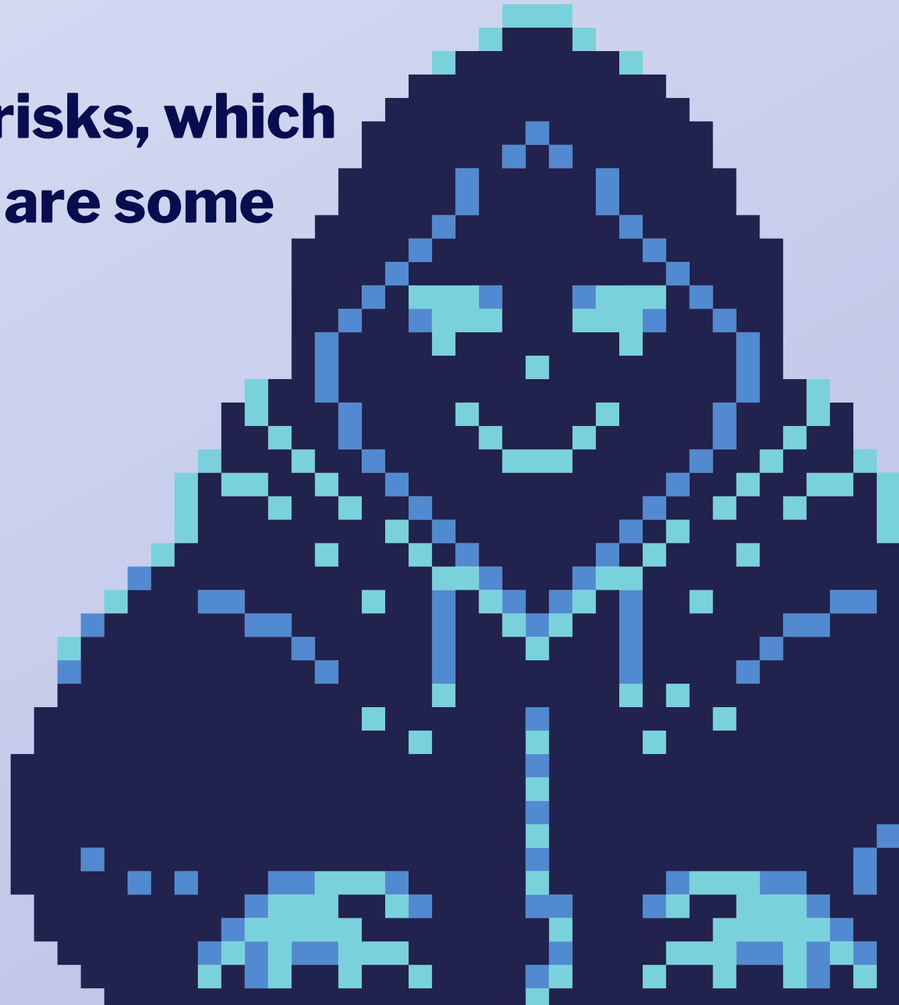
Social Engineering: Potential Impact

- Data leak
- Loss of public trust
- Financial loss
- Loss of new or existing clients
- Increased audit cost

How to Spot Social Engineering Attacks:

Attackers expect you to act before considering the risks, which means you should do the opposite. To help you, here are some questions to ask yourself if you suspect an attack:

- **Did this message come from a legitimate sender?**
- **Did my friend send this message to me?**
- **Does the website I’m on have odd details?**
- **Does this offer sound too good to be true?**
- **Are attachments or links suspicious?**
- **Can this person prove their identity?**



How to Prevent Social Engineering Attacks:

- Use strong passwords (and a password manager)
- Avoid sharing names of your schools, pets, place of birth, or other personal details.
- Be very cautious of building online-only friendships.
- Never let strangers connect to your primary Wi-Fi network.
- Keep all network-connected devices and services secure.
- Don’t ever leave your devices unsecured in public.