



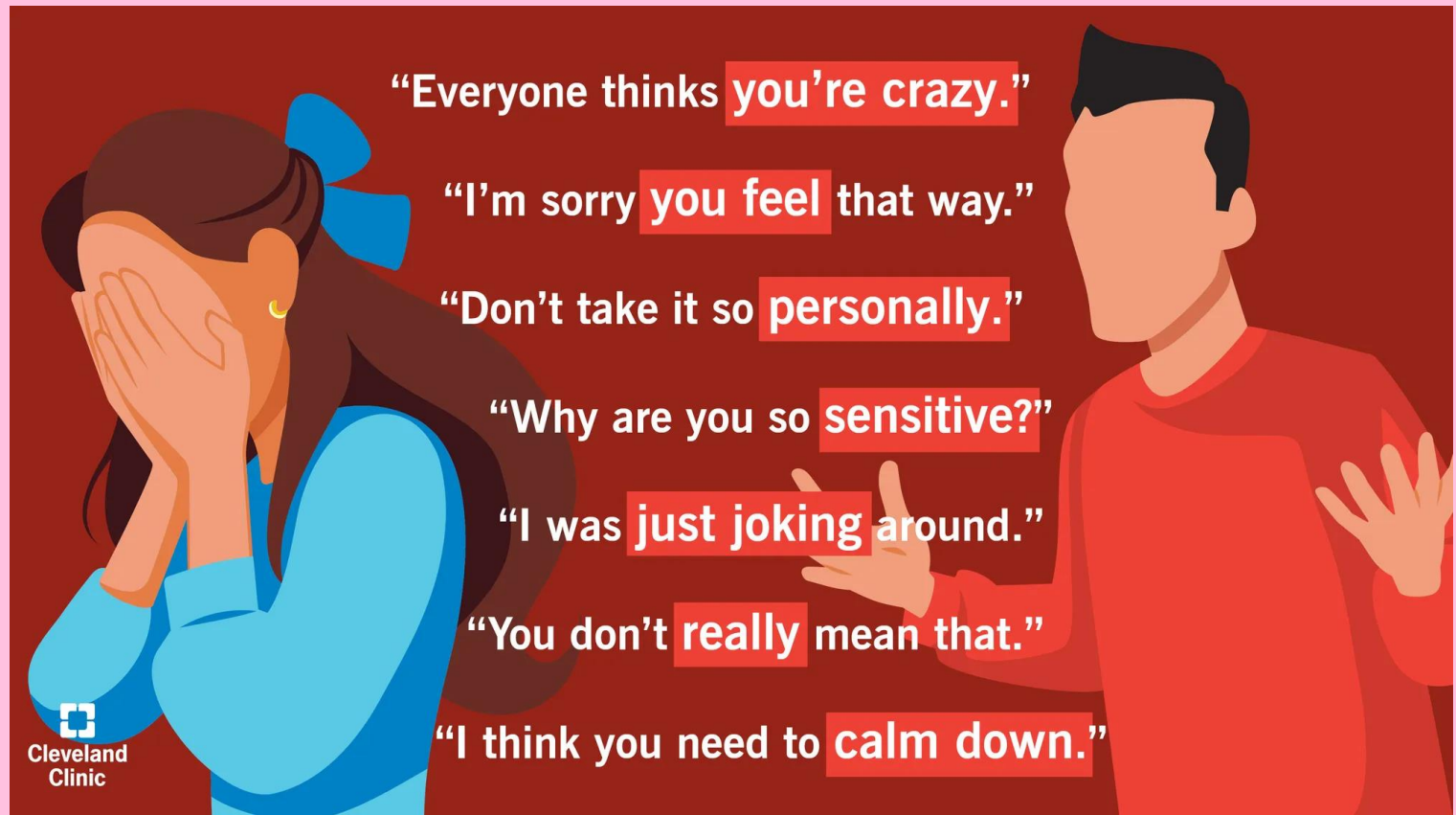
Social Engineering

professional gaslighting



What is Social Engineering?

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.

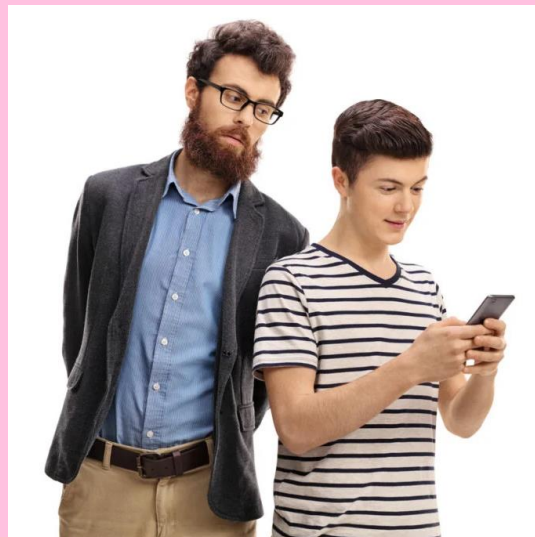


Types of Social Engineering Attacks

- Online and Phone



- Human Interaction



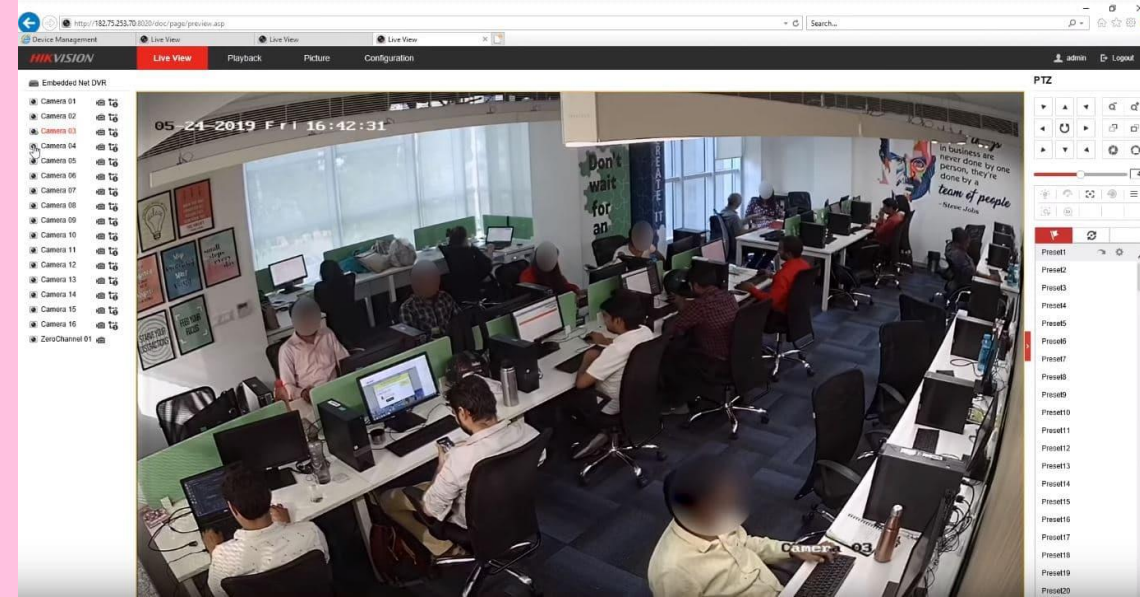
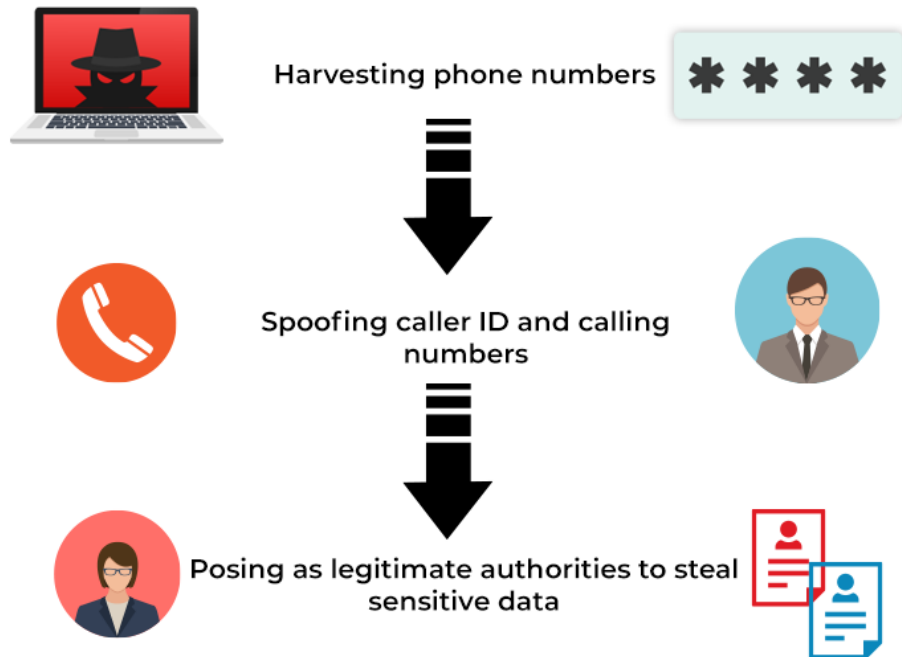
- Passive Attacks



ONLINE AND PHONE

- Phishing scams
- Smishing (fake SMS/text messages)
- Vishing (phone calls/ voice messages)




VISHING ATTACK MECHANISM



EMAIL SPOOFING



The email header is changed so that the message appears to have come from a friend or a legitimate company.

-  Spoofed email from a friend, containing an infected link.
-  Spoofed email from the CEO, requiring sensitive company data.
-  Spoofed email from a vendor, asking for banking credentials.

Email and Phone Number Spoofing

Spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they know or trust.

In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value.



Human Interaction

Attacker might pose as an employee or contractor, perhaps even wearing a uniform or flashing a fake ID, to infiltrate a targeted business. (nobody questions a high vis jacket + ladder combo).



Approaching an employee claiming to have left their identification badge back at their desk or following behind another employee to gain access into the building.



Automatically runs programs once plugged into device



Rubber Ducky :3

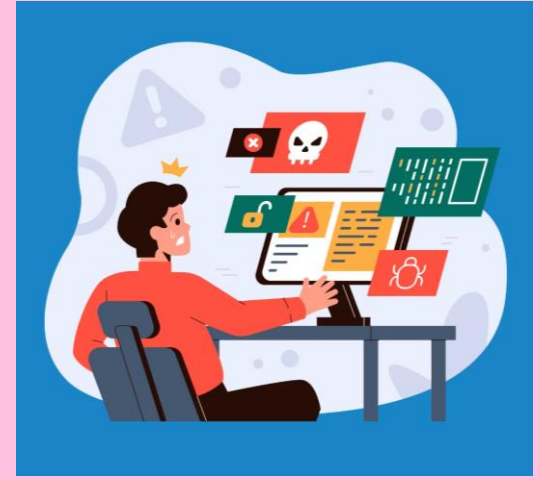
Targeted → Attacker strategically leaves USBs around office building which prompts people to plug them in.

Non-Targeted

Attackers scatter USB drives in public places where the foot traffic is high. They rely on the power of human curiosity and the age-old allure of “free stuff” to get people to pick up and plug in the device.



Malware Infection



KEYLOGGING

Hardware Destruction



PASSIVE ATTACKS

Observing:

- Watch you enter a PIN at an ATM
- See your credit card number at a coffee shop
- Memorize usernames, passwords, and other sensitive information to gain access later

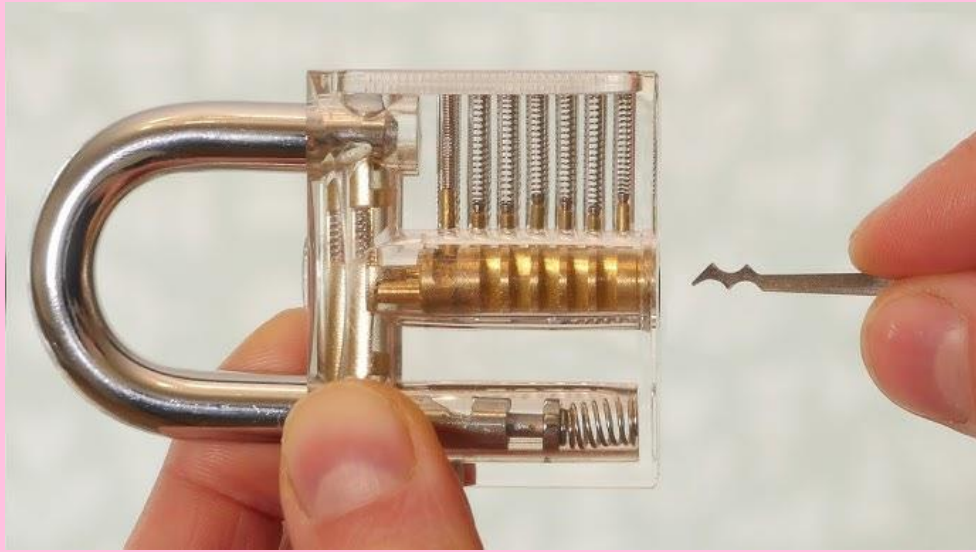
A criminal can learn a lot just by perusing the dumpsters behind your workplace:

- Telephone directories, confidential documents, printed emails, and more sensitive information.
- Discarded computers or mobile devices can be used to retrieve sensitive information.



“shoulder surfing”





LOCKPICKING

Manipulating a lock's components without the original key to gain access.

In cybersecurity, this skill is applied legally and ethically to assess the physical security of facilities during penetration testing or red teaming activities.



**For those who haven't fingered a girl yet, it's
basically this but re-textured**



**This meme has been approved by TEAMWARWICKHATE
#FUCKWARWICK**