COMMON SOCIAL ENGINEERING TECHNIQUES

Why Social Engineering?

The Human Factor is the weakest link and usually can be hacked easier than machines.

Cyber Attacks are on the rise and are always steps ahead in comparison to the defensive side, and statistics show that the victims are attacked using easy Social Engineering techniques resulting in major security breaches affecting some of the largest businesses in the world.

In 2020:
3.86 Million Dollars was the estimated cost of a data breach according to IBM.
27.7% is the average probability that an organization will experience a data breach.

There are 3 different types of strategies:

Physical Social Engineering Attacks

Various Attacks can take place while being in person such as:

a) Public Wi-Fi: Hackers often take advantage of a man in the middle attacks on users, since all it takes is to launch fake websites fooling users into login while dumping credentials in plain text or sniffing the network and gather information.

b) Unprogrammed visits: Often a business receives visitors impersonated as a different service such as pretending to be an electrician, for an ISP company to gain access to your local network.

c) Mirroring Conversations: Hackers perform reconnaissance and study behavioral information about you, to start a topic that they know is interesting to you and mirror your conversation making a more easy approach, to then ask a favor to use the premises for restrooms - and gain access to your local network.

d) Purposely leave Devices: Hackers would leave USB sticks that needs to be plugged, Phones, Laptops on purpose after they leave. Through it, it could contain malware, that would allow them to connect back to the network and gain access.

f) Trickster employees: Hackers could apply for a computer job in companies, and due to their skill can get the job, in order to infiltrate the business, perform the attacks, and often would quit or even stay inside, leaking information about your company.

Voice Call Social Engineering Attacks

Social Engineering attacks can also be performed during a phone call to extract personal information such as:

a) Hackers create scenarios pretending to be from the support department, saying there is a serious issue with your machine, and require immediate access remotely - forcing you to let them in using panic as a drive to follow their instructions, allowing a hacker access.

b) Hackers create scenarios pretending to be from management, and orders you to give personal info about a suspect, which results in using their fake power, to gain sensitive information about a target.

c) Hackers use vishing techniques by playing pre-recorded messages pretending to be your bank and forcing you to confirm your account information followed by the hash sign - which gives them access to sensitive information.

Online and Digital Social Engineering Attacks

a) Hackers clone known websites and create fake login pages, and combine it with a Phishing Attack mimicking a company by sending a malicious link spoofing an email, to gain sensitive information or install malware.

b) SMS-based attacks, hackers spoof the sender, making you believe it's someone you trust, and forcing you to click on a malicious link - to gain information or access your device.

c) Fake Social Media Business pages also can be created, to make it look exactly like your business, and contact users impersonating your company with a fake account, and distribute malicious files that would give them access.

These are some of the common techniques that are being used by criminal hackers to target companies.

1 in every 99 emails sent is phishing attacks using Social Engineering.

It has to do with manipulating your employees, and attackers understand the way of choosing their prey, rather than thinking that criminal hackers will only target your business directly. The good news is that educating your employees and raising awareness can decrease the probability of a successful social engineering attack.