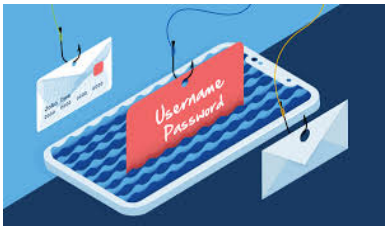
What is Social Engineering?

BANK OF THE WEST
BNP PARIBAS

Social engineering (aka “human hacking) is the art of manipulating people so they give up confidential information. Criminals use social engineering because it is easier to exploit human nature than it is to hack software. 98% of cyber-attacks rely on social engineering and 91% of successful data breaches are a result of phishing emails.



In-Person Social Engineering

- “The Cable Guy” – Pretending to be a service tech to gain access to your business or home
- Six Degrees of Separation – Learning about your social practices and using relationships to gain trust
- Device Leave Behind – Leaving a device in a careless of haphazard location tempting users to plug-in or open
- Open Access – Using or requesting to use your computer and they are left unmonitored
- Neuro-Linguistic Programming – Mirroring your body language, voice, and vocabulary to build a connection on a subconscious level

Phone Social Engineering

- Panic – Calling pretending to be support and providing a frantic scenario that compromises your safety (resetting your password or allowing remote access)
- Anger – Calling pretending to be in a position of authority and using anger to intimidate
- Donations – Calling pretending they are someone from a known organization you might be interested in
- Vishing – Calling with a pre-recorded message pretending to be your bank and asking you to call a number to confirm your account and transactions
- Smishing – Sending a text message requesting personal or financial information

Digital Social Engineering

- Phishing – Sending an email with a domain that looks trustworthy and addresses it from a known contact from that domain; often contains an attachment or link that contains malware
- Social Media Phishing – Building a social media page that mimics a trusted brand
- Typosquatting – Using common typos for brand URLs and mimicking the brand to gain trust

How to Protect Yourself Against Social Engineering

- Be wary of any message that seems suspicious
- Check that the sender name matches the sending email address and website links match the email
- Double check communication that stresses urgency or creates confusion
- DO NOT open emails in the spam folder or emails whose recipients you do not know
- DO NOT open attachments or click links in emails of unknown origin
- Perform backups of your home computer on a scheduled basis to an external hard drive
    - Disconnect the external hard drive after the backup is complete
- Read news articles on current cyber trends and topics; subscribe to the Threat Intelligence Group Open Source email for daily news articles