

Social Engineering

malicious activities accomplished through human interactions

Phishing -> Type of attack that attempts to trick individual into providing sensitive information

Vishing -> Phishing through voice

Smishing -> Phishing through SMS

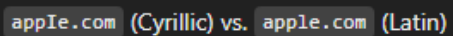
Misinformation -> false/inaccurate information WITHOUT malicious intention

Disinformation -> false/inaccurate information WITH malicious intention

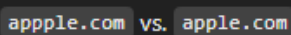
Impersonation -> Spoof an e-mail to pretend to be someone

Pretexting -> Technique where an attacker creates a fabricated scenario or pretext to manipulate individuals

Homograph attacks -> Use similar-looking characters from different writing systems to create deceptive domains

A screenshot of a text editor or terminal window showing the comparison of two domain names: 'appIe.com' followed by '(Cyrillic)' and 'vs. apple.com' followed by '(Latin)'. The text is white on a dark background.

Typosquatting -> Takes advantage of common typos or misspellings in domain names

A screenshot of a text editor or terminal window showing the comparison of two domain names: 'appple.com' followed by 'vs. apple.com'. The text is white on a dark background.

User training:

- Phishing campaign
- Look for links
- Look for the e-mail sender
- Everything urgent