Avoiding Social Engineering Attacks

Social Engineering: Phishing

Phishing is a type of social engineering attack in which a threat actor, posing as a trustworthy source, attempts to trick a victim into doing something, either through email, webpages or even by phone.

How To Spot Phishing

How can a user spot phishing attacks? Look out for:

- Suspicious domains and email addresses
- Punctuation errors
- Typos
- Unusual scenarios
- Suspicious attachments or links
- Incorrect formatting

If something seems wrong, assume it is! Don’t be afraid to double-check and verify.

Phishing Uses

Phishing is a social engineering tactic that can be used for many things, such as stealing credentials or getting malware onto a system.

Specialized Types of Phishing

Some specialized types of phishing include:

- **Vishing**: “Voice” phishing uses spam calls
- **Smishing**: “SMS” phishing uses text messages
- **Spear Phishing**: A phishing strategy that targets specific victims
- **Whaling**: A phishing strategy that targets high-profile victims

What Is Reconnaissance?

In Cybersecurity, **reconnaissance** refers to when an attacker interacts with a victim's system in order to gain more information about a victim or their system. Sometimes reconnaissance refers to when pen-testers are trying to gain more information about a system. While pen-testers have good intentions and are often employed by the company they're performing reconnaissance on, they may act like attackers during this process.

Social Engineering: Spam

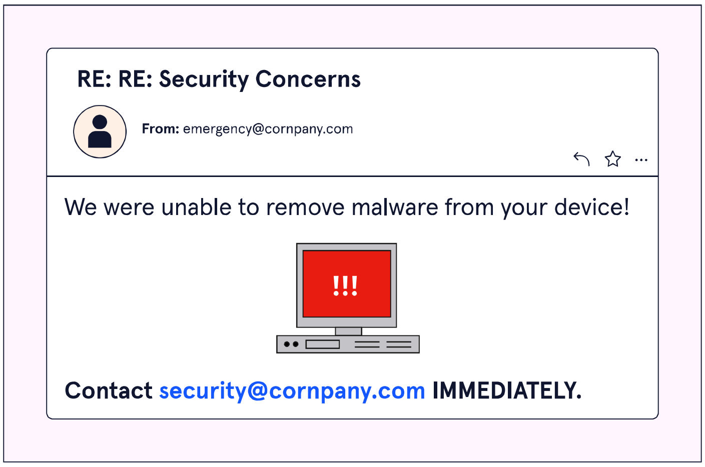
During their social engineering attempts, attackers can often use **spam**, also known as unsolicited email, to target victims.

Social Engineering: Hoaxes

During their social engineering attempts, attackers can often use **hoaxes**, usually in the form of false security alerts, to target victims.

Prepending

In Cybersecurity, prepending refers to when an attacker prepends, or attaches, a trustworthy value like "RE:" or "MAILSAFE: PASSED" to a message in order to make the message appear more trustworthy.
Values like that are usually automatically added by a user's email client. This can make a user think their email client trusts the message and is safe to open.



RE: RE: Security Concerns

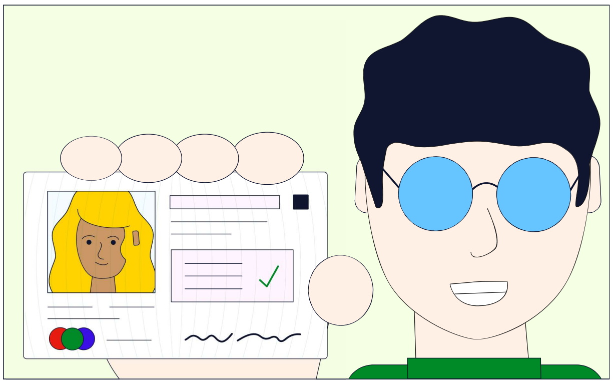
From: emergency@cornpany.com

We were unable to remove malware from your device!

Contact security@cornpany.com IMMEDIATELY.

Identity Fraud

In Cybersecurity, **identity fraud** refers to when an attacker uses a victim's personal information, typically to impersonate the victim.



Cybersecurity: Pretexting

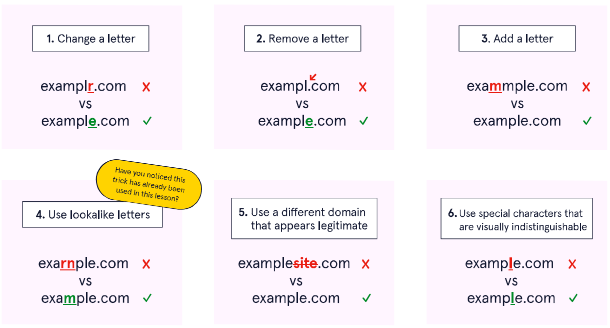
In Cybersecurity, **pretexting** refers to when an attacker tricks a victim by giving a false pretext, or reason, for why the victim should share information with the attacker.

Cybersecurity: Pharming

In Cybersecurity, **pharming** refers to when an attacker redirects victims from a legitimate website to their malicious version. This is often done by making the name resolution process point to a different IP address. A popular use of this is to harvest banking credentials from unsuspecting victims.

Cybersecurity: Typosquatting

In Cybersecurity, **typosquatting** refers to when an attacker deliberately registers a website domain with a name that is extremely close to that of a legitimate website.
Attackers do this with the expectation that a user might accidentally interact with their website or content instead of that of the legitimate website.
The image shows some examples of how attackers might use “typos” to trick victims.



Cybersecurity: Credential Harvesting

In Cybersecurity, **credential harvesting** refers to when an attacker attempts to harvest, or learn, a victim's credentials.
Often, the attacker may just want to gain a large database of credentials rather than exploiting the user directly.

Cybersecurity: Watering Hole Attacks

In Cybersecurity, a **watering hole attack** is when an attacker hacks a third-party service or software that a group of victims uses in order to gain access to a victim or the victim's company's services.
The third-party service is the "watering hole" that the group of victims are using, or "drinking" from.

Influence Campaigns & Social Media

Influence campaigns created by threat actors might use social media to push their narrative and affect public opinion. Bots and armies of posters (sometimes utilizing hacked accounts) may post messages that repeat or reinforce the hoaxes or false narrative pushed by influence campaigns.

Cybersecurity: Influence Campaigns

In Cybersecurity, an **influence campaign** refers to a large-scale campaign launched by a threat actor, or group of threat actors, with a lot of power (like a hacktivist group, nation-state actor, or terrorist group) that seeks to shift public opinion.
It can be assumed that this shift is generally in *bad faith* or might seek to push a *false narrative*.

Influence Campaigns & Hybrid Warfare

In Cybersecurity, hostile Influence campaigns can be utilized as a part of **hybrid warfare**.
Hybrid warfare is a type of warfare that uses conventional and unconventional means. To fit into the category of hybrid warfare, a campaign might use tactics like espionage, hacking, and spreading disinformation or fake news.