MODULE PRACTICE

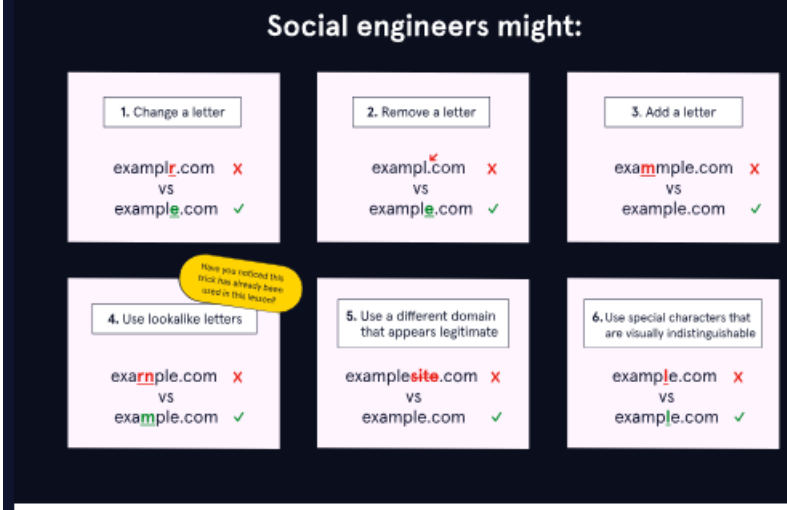
Cybersecurity: Pretexting

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.

Social Engineering: Spam

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

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.

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.

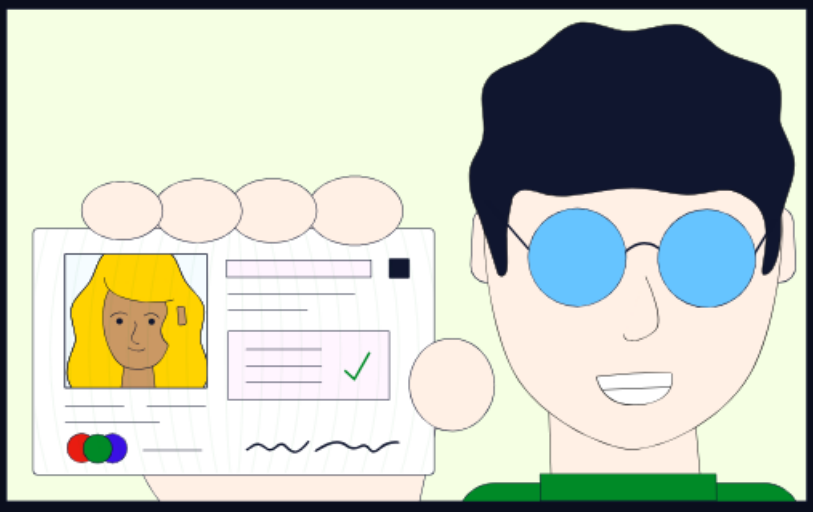
The third-party service is the "watering hole" that the group of victims are using, or "drinking" from.

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.

Identity Fraud



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

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: Hoaxes

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