SPAM, SCAMS, AND OTHER FALSEHOODS

Introduction

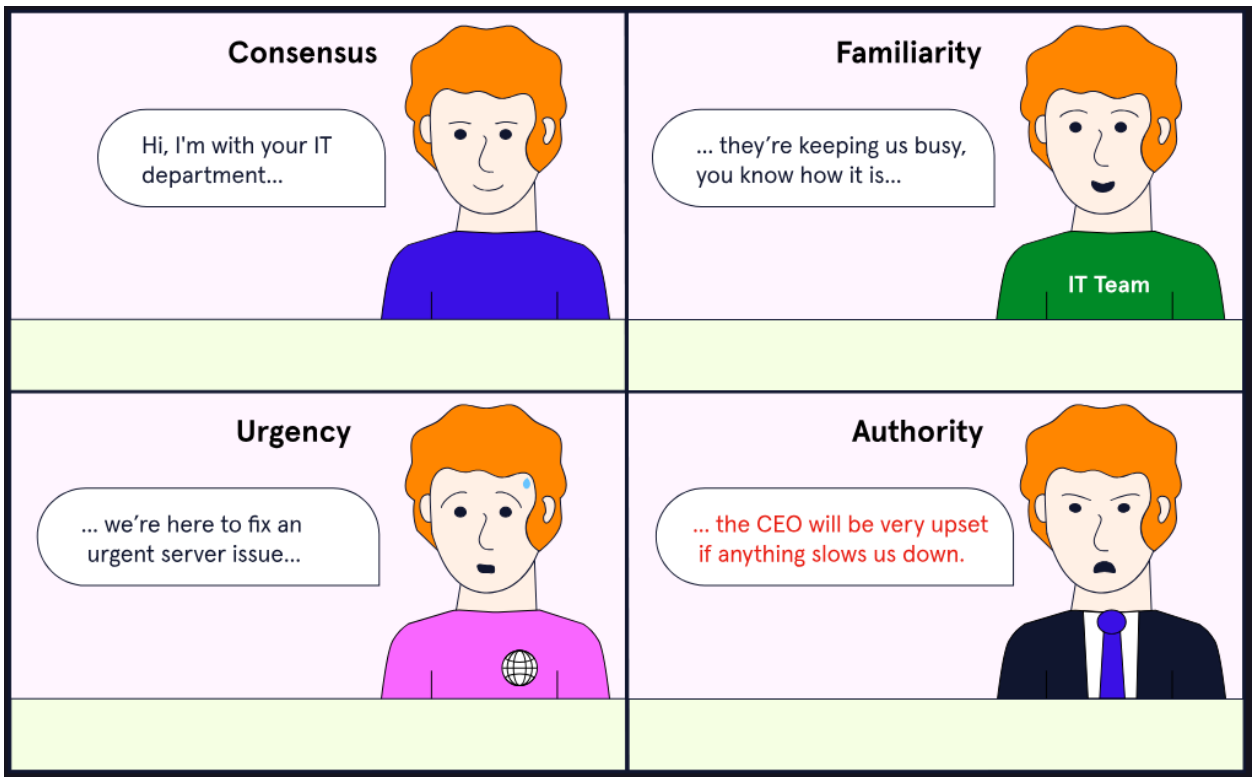
Social engineering tactics usually utilize the following principles:

- **Consensus**: when a social engineer convinces victims that they have already been trusted by others.
- **Familiarity**: when a social engineer uses charisma and likability to get a victim to complete a request.
- **Urgency**: when a social engineer creates a sense of urgency or scarcity to put time pressure on a victim.
- **Authority**: a high-risk strategy in which a social engineer attempts to intimidate a victim or claim authority over them.

While these principles describe the high-level concepts of social engineering, there are many more specific strategies used as well, and we will talk about them in this lesson.

Many of these strategies can be used for both offense and reconnaissance. **Reconnaissance** is the process of interacting with a target in order to gain more information about it.

Reconnaissance is very important in social engineering because *having information about a target makes it much easier for a social engineer to manipulate them*. The rise of social media means there is often no shortage of information about a target available online.



Social Engineering with Emails

Sending unsolicited emails, also known as **spam**, is a highly effective social engineering strategy. Most spam emails that show up in our inboxes are obviously fake, and this is deliberate: The scammers who send these emails want *easy victims who won't realize they're being scammed*. Sure, fewer people will open the email, but those who do open it are more likely to be tricked.

The spam used by Social Engineers is often different from these scammers: it's meant to be hard to detect in order to slip through spam filters and appear legitimate. Most of us know not to trust emails from random dating sites we didn't sign up for, but what about emails that *appear* to come from your organization's own IT department? These emails often exploit our **trust**, by appearing to come from legitimate sources, and this can be compounded by a technique known as **prepending**.

Prepending involves altering the subject line, or attaching a message to the email, that says something like "RE:" or "MAILSAFE:PASSED", in order to make it appear that:

- We have already been communicating with the sender, OR
- The email has passed a spam filter.

When done correctly, this can make the unsuspecting victim feel an even greater sense of security.

Hoaxes

Lying to get what you want is a core part of social engineering, and this can come in many forms. Often, it aligns with one or more of the core principles of social engineering. In social engineering, these lies are often called **hoaxes**. One common hoax is to fake security alerts, creating a sense of **urgency** for the victim. These fake alerts often make use of **trust** and **authority** as well, because the alerts appear to come from real sources which instruct the victim to take the required action.

Another type of lie used in social engineering is **pretexting**, which is when a social engineer invents a false pretext, or reason, for why a victim should share information or carry out an action.

If a random person emailed you asking for sensitive information, you would probably ignore them. On other hand, if the person claimed to be the new point of contact for a contractor working with your organization, you might be fooled into revealing information to them.

Social Engineering and URLs

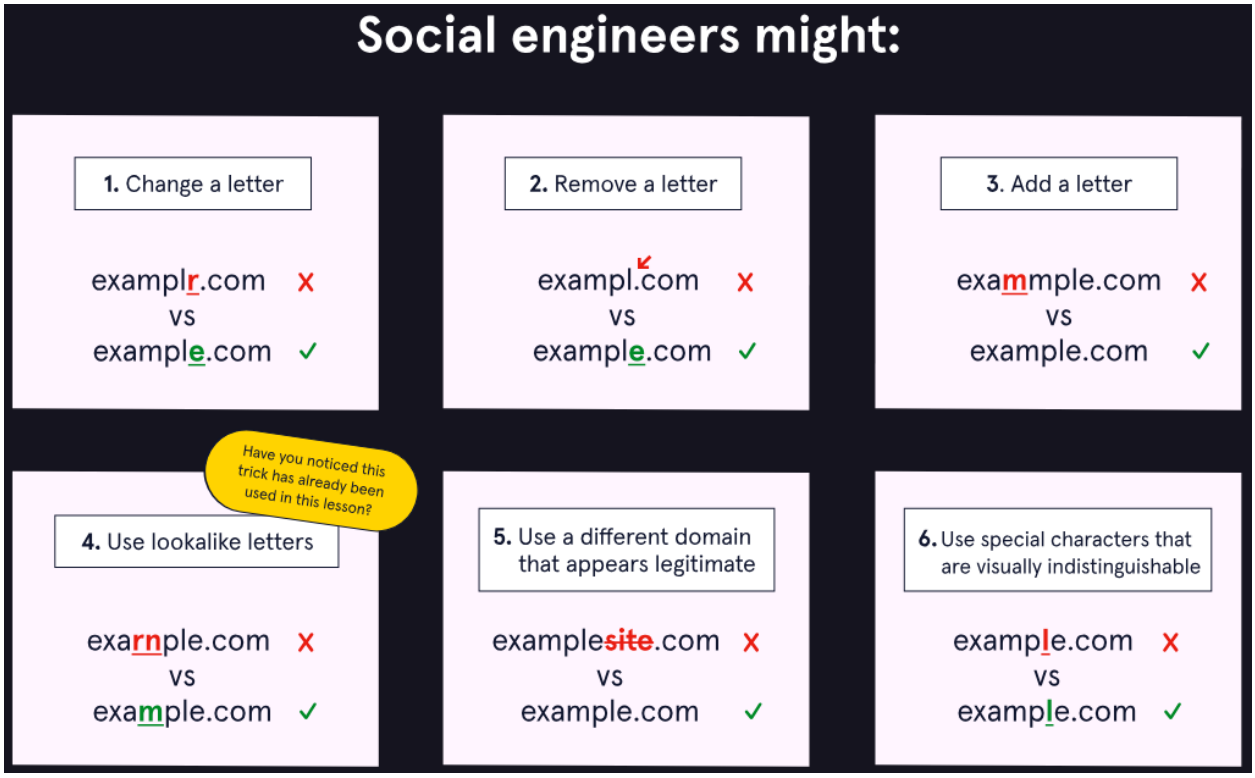
The internet has made it easier than ever to mislead people, and this can occur before a user even connects to a website! Social engineers can trick victims using a simple link to a "trusted" website.

A strategy known as **pharming** refers to when a social engineer redirects victims from a legitimate website to their malicious website instead. This generally involves tampering with DNS information for a computer, a network, or a larger portion of the internet. Pharming can be 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.

Another strategy used to lure unsuspecting victims onto malicious websites is typosquatting. **Typosquatting** is when an attacker will register a domain *very* similar to an existing legitimate website, then wait for people to visit the malicious domain. For example, an attacker might register code**A**cademy.com to trick users who are trying to visit codecademy.com. Victims might visit this malicious domain through a mistake as simple as mistyping or misremembering a URL.

If you're skeptical of this strategy, try finding the differences between these URLs:

- `kerning.com` VS `keming.com`
- `google.com` VS `goggle.com`



Identity Fraud

Identity fraud refers to when an attacker uses a victim's personal information. Many of us have heard of examples of malicious actors pretending to be someone for financial gain. For example, using someone else's credit card or bank account.

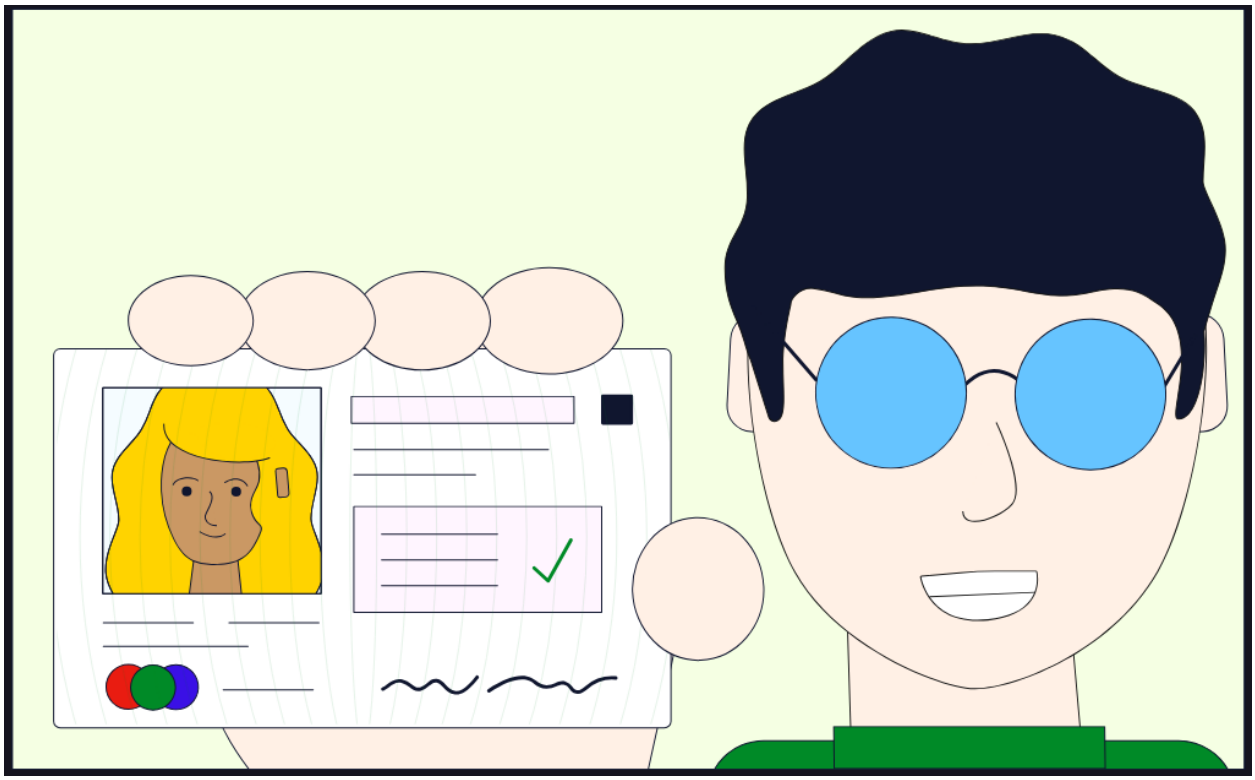
Identity fraud isn't just used for financial gain. It can also be used by social engineers to more convincingly impersonate a victim, either by posing as the victim to mislead others or to gain additional access to the victim's accounts and resources.

On an individual scale, this could be something like using stolen personal information to "recover" a bank account or target an organization that the individual works for.

This type of fraud can also happen on a larger scale, such as in the form of **invoice scams**, where an attacker alters details on an invoice to steal money. One form of invoice scam involves using social engineering to pose as

an employee of one organization and sending fraudulent invoices to other companies.

If the attacker is successful, the second company won't notice the issue and will just pay the invoice!

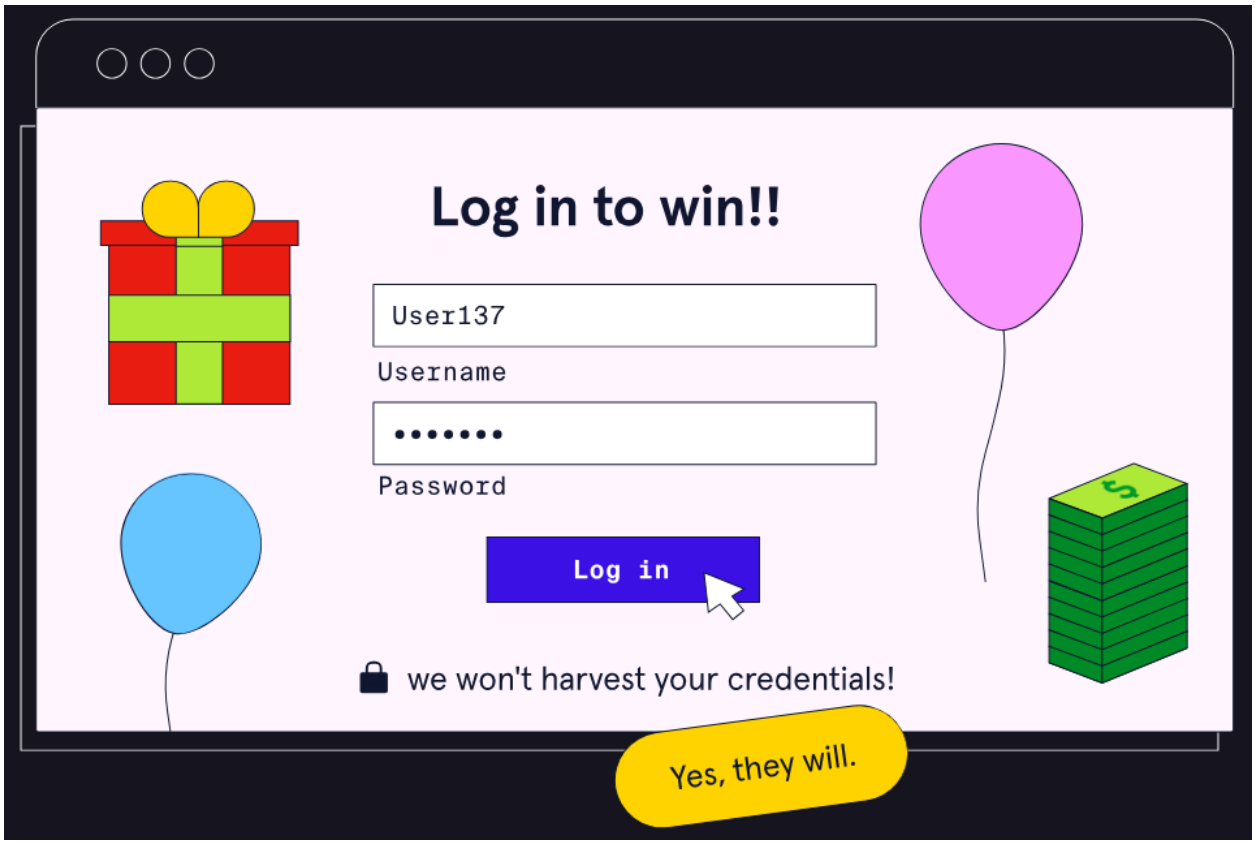


Credential Harvesting

Credential harvesting is when an attacker obtains, or harvests, a victim's credentials. This can be targeted at a specific user, as part of a multi-stage attack, but credentials are often stolen from many users at once, usually for financial gain.

One method of targeted credential harvesting is known as a watering hole attack. A **watering hole attack** is when an attacker compromises a third-party service, software, or website used by a target in order to get access to the target. The third-party service is the "watering hole" that the victims are all using, or "drinking from". This is an example of how poor security on the part of third-party vendors can compromise the security of the organizations that hire them.

One example of a watering hole attack occurred in 2012, when a hacker group targeted websites promoting political activism. The attack involved redirecting victims to a different compromised site, which would attempt to download malware onto the victims' computers.



Physical Social Engineering Strategies

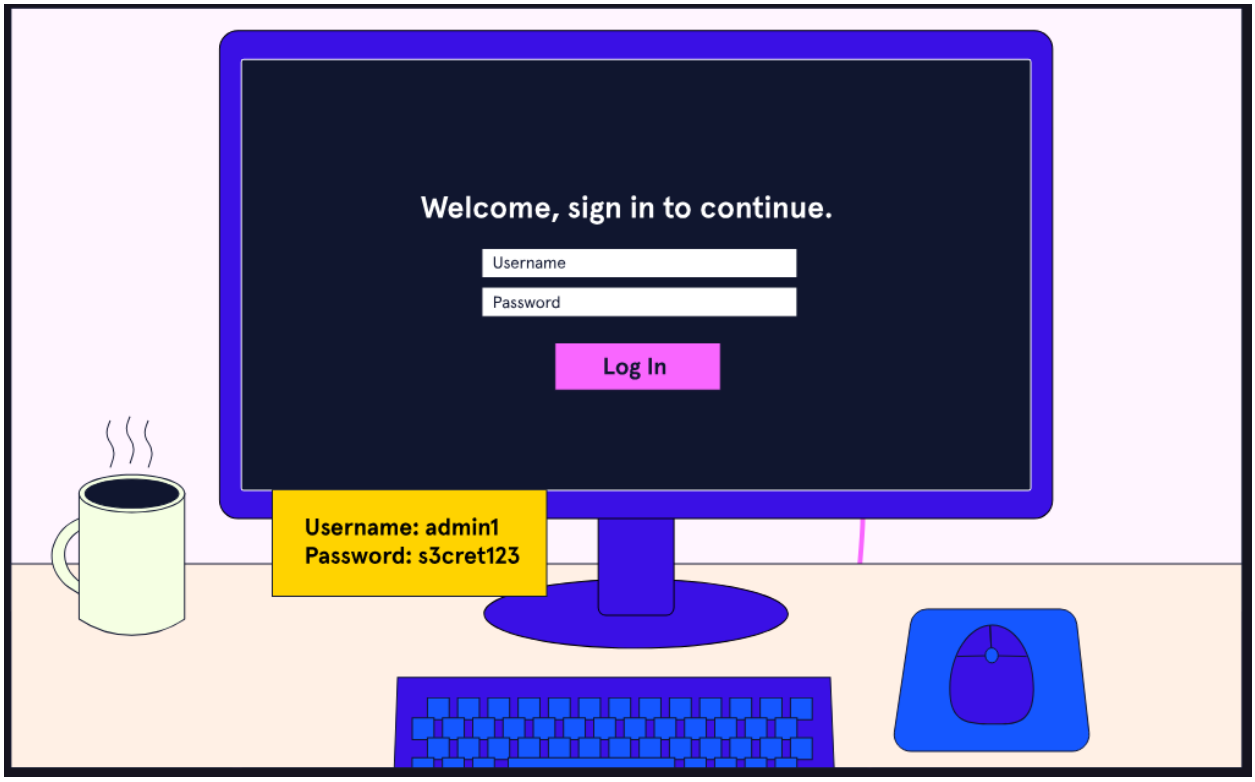
Having physical access to a target opens a world of new possibilities for an attacker, and sometimes *obtaining physical access* can be easier than breaking in using technology. These strategies are centered around bypassing physical security or obtaining credentials in-person rather than through a computer.

Tailgating refers to the act of following someone through a secure door before that door can close. ("What? That counts as a cybersecurity attack?" you ask? Yes, it can be that simple.)

Dumpster diving is, exactly as it sounds, the process of going through trash to obtain sensitive information. While this might sound ridiculous, it's more common than you might think. Organizations often improperly dispose of sensitive documents in a way that leaves them readable by social engineers.

Lots of information can be obtained this way, from passwords on sticky notes to information on employees to tax invoices. Make sure to shred your important papers!

Shoulder surfing refers to the act of looking over someone's shoulder as they type their password. While this does take some practice on the part of the social engineer, it is a very effective way of obtaining credentials... as long as they're able to do it without getting caught!



Review

There are lots of strategies that social engineers can use to exploit victims, all utilizing the principles of consensus, familiarity, urgency, and authority. We learned about the following strategies:

- **Spam**: unsolicited emails.
- **Prepending**: attaching a message to an email saying something like "RE:" or "MAILSAFE:PASSED" to make it appear that the email is safe and legitimate.
- **Hoaxes**: fake information, like false security alerts.
- **Pretexting**: when an attacker tricks a victim by giving a false pretext, or reason, for why the victim should share information with the attacker.

- **Pharming**: when an attacker redirects victims from a legitimate website to their malicious version.
- **Typosquatting**: when an attacker deliberately registers a website domain with a name that is close to that of a legitimate website.
- **Identity Fraud:** when an attacker uses a victim's personal information.
- **Credential Harvesting**: when an attacker is attempting to harvest, or learn, a victim's credentials.
- **Watering Hole Attack**: when an attacker hacks the third-party service or software a group of victims uses in order to gain access to a victim or the victims' company.
- **Tailgating**: when an attacker follows someone through a secure door before the door can close.
- **Dumpster Diving**: when an attacker goes through a victim's trash to obtain sensitive information.
- **Shoulder Surfing**: when an attacker looks over someone's shoulder as they type their password.

Be careful and be aware! Just because a person, site, email, or other source seems trustworthy doesn't mean they are.