**SPAM, SCAMS, AND OTHER FALSEHOODS**

**Introduction**

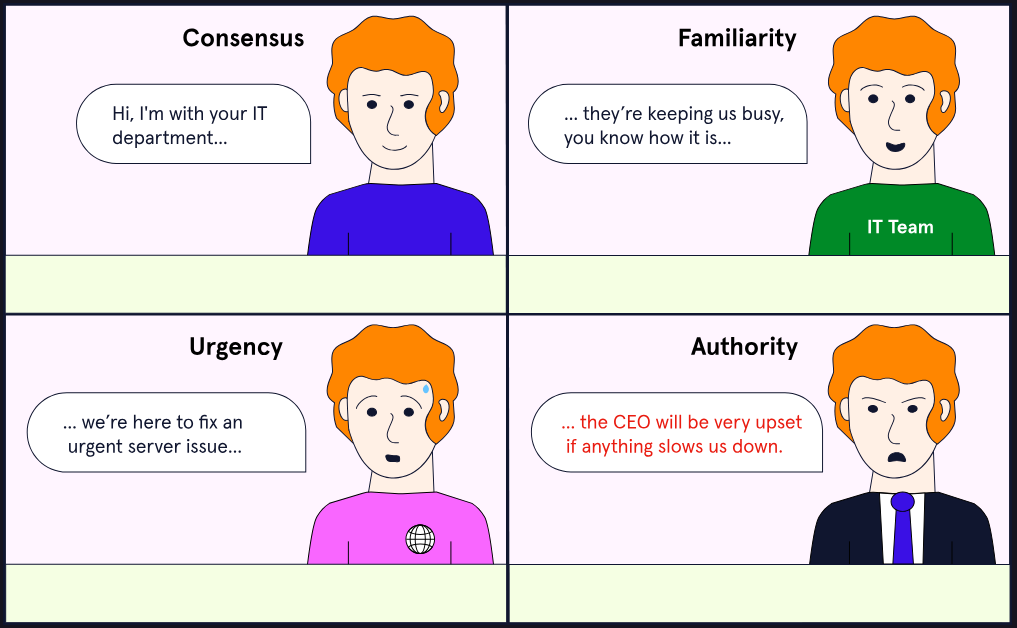
Social engineering tactics usually utilize the following principles:

* **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](https://www.codecademy.com/resources/docs/cybersecurity/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](https://www.codecademy.com/resources/docs/cybersecurity/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.

