**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.

