Social Engineering in the context of IT Security is "any act that influences a person to take actions that or may not be in their best interest."* It is often a confidence trick done to obtain access to systems and confidential data that can be part of a bigger scheme. It is still on the rise and is now the number one cause of breaches.**

Fraudsters are able to trick people by playing on their emotions and getting people to act before they think, something people often do in an emotional state. Examples include:

Desire to please: Pretending to be your boss or other authority figure and telling you to do something that is critical, right away.
Trust: Pretending to be a close friend or relative.
Fear of scarcity: Saying offers are limited and/or will end soon.
Threats to wellbeing: Pretending that access to critical resources such as your bank account or paycheck is about to be cut-off.
Euphoria/Greed/Entitlement: Saying you won something or you are getting a free gift.

Types of Social Engineering attacks include:

Phishing: The most common form of social engineering, phishing uses emails that appear to come from legitimate sources to trick people into providing their information or clicking on malicious links. They frequently employ the tricks that put end users into one of the emotional states that causes them to act without thinking.

Vishing: Uses social engineering over the telephone, sometimes with a rogue interactive voice response (IVR) system to mimic a legitimate institution to persuade you to supply your credentials and other data.

Smishing: Uses SMS text messaging to get you to divulge information or click on a malicious link.

Spear Phishing: Similar to phishing but the attacker customizes the email specifically for an individual to make the phish seem more real. They often target key employees with access to critical and/or confidential data.

Quid Pro Quo: Pretends to be a service provider who keeps calling people until they find someone who actually requested or needs the service.

Baiting: Baiting relies on the greed or curiosity of the victim. For instance, leaving malware infected USB sticks strategically lying around public areas is a common tactic that exploits human's curiosity. Once the infected stick is inserted into a user's computer, the malware is installed. Surrendering login credentials for free online music or movies is another offer that users often cannot resist.

The education and healthcare sectors continue to be plagued by social engineering**. Patients, students, staff, and faculty have all suffered losses from disclosure of personal data and research to unauthorized parties. Knowing what you're up against can help you be more secure. Here are a few things you can do to guard against social engineering attacks:

- **Limit what you share online**. The less you share about yourself, the smaller the target you are for a social engineering attack. Cybercriminals use information you post online to learn how to gain your trust.
- **Answer security questions with information that is not easily discerned**. For example, if a possible security question is “What’s your brother’s name” and you’ve listed him on your Facebook page as your brother (or even got tagged in a pic by him, “Me and my little sis”), you’ve just given away that question to anyone who does a little research. Since websites still insist on using security questions like these, one alternative is to make up answers. You could base them on your best friend’s family, your second-favorite TV show, or another theme that’s easy to remember. (My childhood best friend? Spock. My high school? Enterprise. My first pet? Tribble). You’ll still be able to answer the questions, and it’ll be harder for someone to social engineer or even guess the answers.
- **Protect your credentials.** No legitimate company or organization will ask for your username, password or other personal information via e-mail, phone, or text. The University definitely won't.
- **Beware of attachments.** E-mail attachments are the most common vector for malicious software. When you get a message with an attachment, delete it unless you are expecting it and are absolutely certain it is legitimate. If you’re not sure, call the sender at a number you know is legitimate to check.
- **Confirm identities.** Phishing messages can look official. Cybercriminals steal organization and company identities, including e-mail addresses, logos, and URLs that are similar to the links they're trying to imitate. There's nothing to stop them from impersonating the university, financial institutions, retailers, a wide range of other service providers, or even someone you know.
- **Trust your instincts.** If you get a suspicious message that claims to be from an agency or service provider, use your browser to manually locate the organization online and contact them via the website, e-mail, or telephone number that you looked up – not what was provided in the message.
- **Check the sender.** Check the sender's e-mail address. Any correspondence from an organization should come from an organizational e-mail address.

- **Take your time.** If a message states that you must act immediately or lose access, do not comply.
- **Don't click links in suspicious messages.** If you don't trust the e-mail (or text message or post), don't trust the links in it either. Beware of links that are hidden by URL shorteners or text like "Click Here." They may link to a phishing site or a form designed to steal your username and password.

For other effective cybersecurity habits, check out UC's "Make It a Habit" webpage.

---

*According to "Social engineering (security)" Wikipedia as of July16, 2019

**According to Verizon's 2019 Data Breach Investigations Report