Social Engineering:

1. **Phishing**- combination of social engineering and spoofing. It persuades or tricks the target into interacting with a malicious resource disguised as a trusted one, traditionally using email as the vector. An example of this occurring in the real world is Facebook and google between 2013 and 2015. A phisher took advantage of both companies using quanta as a vendor and sent fake invoices which they both paid for years.
2. TypoSquatting - threat actor registers a domain name that is like a real one, hoping that users will not notice the difference. These are also referred to as *cousin, lookalike,* or *doppelganger* domains. Example: Canadian teenager Mike Rowe registered a website under the name "MikeRoweSoft." Microsoft handed the teenager a cease and desist.
3. Hoaxes- An email alert or web pop-up will claim to have identified some sort of security problem, such as virus infection, and offer a tool to fix the problem. The tool of course will be some sort of Trojan application. This could be a message saying that your family member is stuck somewhere, and you should pay money so that the sender can get it to them.
4. Shoulder Surfing- a threat actor can learn a password or PIN (or other secure information) by watching the user type it. An example of this would be when you go to put in your pin while using an ATM and someone steals it by looking at your pin.