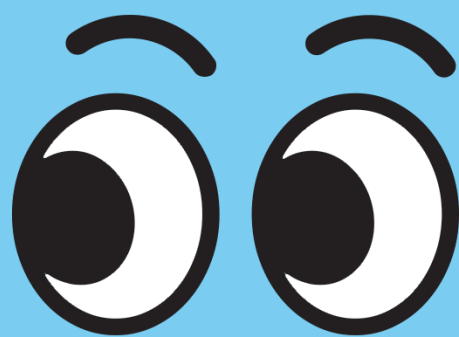


SOCIAL ENGINEERING

What Do You Need to Know?

HOW CAN YOU RECOGNIZE ATTEMPTS?

It is important to know the normal look to something (such as a website, or email template). If you notice that any of those look different, or you don't feel confident about the authenticity of it, most likely it is a social engineering attempt. Knowing the normal is a very helpful thing to do. For example, an email asking you to confirm your recent purchase from Apple is not real.



[Block Pop-Ups on Chrome](#)

POP-UPS

Pop-ups are a normal thing, another window that opens up. However, they can be used negatively. A pop-up with a virus warning asking you to call a number is an example of a social engineering attempt through this manner. Browsers now let you block popups.

HOW CAN YOU REPORT ATTEMPTS OR ATTACKS?

There are many resources you can utilize to report attempts or attacks, through the U.S. government. The CISA manages this.



[Report Phishing Attacks](#)

[Avoid Social Engineering/Phishing Attacks](#)



WHAT CAN YOU DO?

Educating other people about these things is the best thing that can be done. The more that people know what this stuff is, the less likely people will fall victim to them.

