# SOCIAL ENGINEERING

Understand How to Spot Social Engineering Techniques and What it Takes to Stay Cyber Safe

**Social Engineering,** a form of manipulation that exploits human error for monetary gain or to access private information, is more rampant than ever. Especially around the holiday season, threat actors use a wide range of tactics to victimize individuals as well as groups of people, companies, and entire industries.

Check out our handy ECS infographic below to learn more about some of the most prominent forms of social engineering. Then, brush up on our best practices for staying cyber safe!

## Phishing

An email-based attack that tricks the victim into divulging login credentials by persuading them to interact with a file, link, or image disguised as a fake login page. There are many sub-categories of phishing based on varying tactics, including spear phishing (targeted phishing backed by prior research of the victim), vishing (phishing over a voice communication channel such as a phone), smishing (phishing over text/SMS), and whaling (phishing targeting a high-profile target, such as a company executive).

## Baiting

Using conspicuously-placed physical media (such as a flash drive in a company bathroom, elevator, or parking lot) or enticing ads online, victims are lured into accidentally downloading a malware-infected application or visiting a malicious site.

## Pharming

An attack that first infects the victim's web-browser then subsequently redirects and captures (or farms) the user's searches and browsing activity. This typically occurs when the user browses to an unsafe website.

## Watering Hole

A targeted attack where a malicious actor compromises and modifies a trusted website that is frequented by a specific group of users.

## Scareware/Fraudware

An attack that bombards a victim with false alarms and fictitious threats via unprompted-but-legitimate-looking pop-up banners or spam email. Victims are lured into installing malware or are redirected to a malicious site.


## What to do if you suspect you are a victim:

Report suspected social engineering attempts via your company's standard operating procedures, including notifying your supervisor.

## ECS Best Practices for Staying Cyber Safe

- Never click links, files, or images from someone you don't know.
- Never reply to scams or impersonators.
- Ensure your spam filter is active in email settings or install one.
- Install antivirus software.
- Install a firewall.
- Make sure your antivirus and firewall software remain up to date.
- If you think someone is being impersonated, ask them in a sepvarate message over a known communication channel.
- Be careful about what you share online. A skilled threat actor will have researched you!

## How cybersecurity aware are you?

ECS offers a variety of managed, scalable solutions to suit your unique needs, as well as the expertise to help you minimize risk and ensure cybersecurity compliance.

**Reach out today** if you're ready to better protect your organization.