Social Engineering Red Flags

Hackers want your organization's crown jewels and they won't stop until they get what they want. The bad guys will use every evil trick, from emails that try to steal your username and password to wearing a uniform and following you into the office. As scary as this sounds, you can protect yourself and your organization – if you know the warning signs.

How They Do It

You are the weakest link in your organization's defenses. The bad guys hack humans using social engineering, which is the act of manipulating you into divulging confidential information or performing actions that aren't in your best interest or in the best interest of your organization. Their goal is to obtain your trust and then use that relationship to trick you into giving them what they want.

What to Watch For

Red flags are signs of danger or a problem. Being aware of these warning signs can help you to protect yourself and your organization from a hacker's attack. Always be suspicious and keep your eyes open. When you encounter a red flag, make sure that you **stop**, **look**, and **think** before you take an action.

Some Common Red Flags

Here are some of the most common red flags you are likely to encounter and examples of what each may look like.

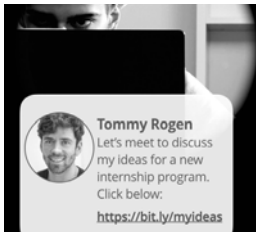
Tailgating: Someone following you or your co-workers inside. They may not have a badge or say their badge isn't working.

Unfamiliar Individuals: Someone hanging or walking around without an escort. They may even look official and be dressed in a uniform.

Shoulder Surfing: Someone standing behind you and watching over your shoulder while you type. They could be in line next to you at the coffee shop, hoping to watch you enter your username and password.

Unlocked Devices: These provide easy access to your personal information and into your organization's network. For example: stepping away from your computer to get something from the printer, even if it's only for a second.

Messy Desks: Important documents, flash drives, and password lists left unsecured. Even in an area you believe is secure, these items can easily "disappear".



Fake Profiles: These look like legitimate social media profiles, often with connections you recognize. They will contact you and attempt to trick you into taking an action that benefits them.

Phishing: Using malicious emails that are disguised as legitimate in order to trick you into providing sensitive information or taking a potentially dangerous action. This could look like an email from your bank asking you to open an attachment to review some "suspicious" charges.

Pretexting: Someone contacting you and lying about who they are to trick you into giving them something they want. You might receive a phone call from IT, saying they need your help to verify that a patch was properly installed.

Sense of Urgency: A time-sensitive request that urgently needs you to take some type of action. This could be a message from your boss that says if you don't wire funds to a client in the next hour, an important account will be lost.

Vishing: It's like phishing, but over the phone (voice phishing = vishing). It could be an official-sounding call or voice message asking you to provide information or take an action.

Smishing: It's like phishing, but through text messages [Short Message Service (SMS) phishing = smishing]. It could be an unexpected text message asking you to verify some information by opening a link.

How to Stay Safe

Don't give up hope and just wait for bad things to happen. Stay alert for all red flags. Be proactive; you can make a difference. Here are some actions that keep yourself and your organization safe.

- If a request seems suspicious, call the person directly to verify it's legitimate.
- Pay attention to your surroundings.
- Be cautious before sharing any personal or organizational information.
- Always lock/secure your devices before walking away from them.
- Don't leave mobile devices unattended.
- Keep your desk clean and lock things up when they're not in use.
- Follow your organization's security policies.
- Always stop, look, and think before you take any action.

Echelon Technologies, LLC | 480-787-5600/877-218-1112 | Info@echelontechs.com | www.echelontechs.com