Your Role

Internet Security and You

Picture this . . .

Your organization has thousands of employees in offices located in seven countries, as well as remote workers across the globe.

All it took was one HR manager—using public Wi-Fi during a business trip—to click on a link that exposed the name, driver's license number, date of birth, and bank account number of every employee hired within the past decade.

Now the company will spend millions to remedy this manager's error—and individual employees will spend months, sometimes even years, battling personal identity theft. What if this had been YOU?

Social engineering is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or in the best interest of your organization.

Hacking Humans

The bad guys have discovered an easier way to get what they want – YOU! It's much easier to gain access to your organization's network by simply tricking you into letting them in.

Social engineers are constantly searching for ways to target you and your organization. A favorite method they use is social engineering, which is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or in the best interest of your organization.

Information about you and your organization can be found across the internet. Some of it, like compromised passwords and client databases, comes from data usually obtained illegally by hackers. However, the abundance of information a social engineer can use comes from things you and your organization freely share on social media.

No matter the source of the information, all of it can be used by a social engineer. With just a few quick clicks, a hacker can build a comprehensive profile that puts you and your organization at risk. They will attack using email, software, social media, phone, and text.

Before you post something, think about it from the perspective of a social engineer. Will this information be useful in conning you or your co-worker? All it takes is one mistake and they have their way in. Always think before you share!

Let's take a look at some threats and your role in staying safe.

Security Threats and Your Role in Staying Safe

The bad guys are constantly looking for ways to get past the weakest link.
Empower yourself and keep your organization safe from a variety of social engineering threats.

Phishing

Phishing occurs when the bad guys impersonate legitimate emails using bulk email. Their goal is to trick you into taking some sort of action, such as clicking a link, opening an attachment, or providing information such as account credentials.

The vast majority of successful hacks occur when someone falls for a phishing attack! That means you need to treat every email you receive as a threat, especially if it asks you to take an action.

Smishing/Vishing

Smishing (stands for "Short Message Service (SMS) phishing" which is text-based phishing) and **vishing** (voice-based/phone-based phishing) are two additional ways that social engineers attempt to trick you into taking some action or giving them the information they want.

If a text message or phone call wants you to take an action that is out of the ordinary or seems suspicious, stop! Before doing what is asked, verify the request by calling them back using a publicly known number.

Pretexting

Pretexting involves the creation of a fabricated scenario. For example, the bad guy says they are from IT and work with Sam, who is someone you know—in order to gain your trust and get information (like your username and password) from you under false pretenses.

These types of attacks are on the rise—so it's important to be vigilant and never give information over the phone, in person, or online unless you have confirmed the identity of the person who is asking.

Disinformation

Disinformation is false information created and distributed with the specific intention of manipulating you. Social media is typically used for a disinformation campaign because of how quickly it can spread. You and your organization can suffer significant financial or reputation damage as a result of a successful campaign.

One of the best ways to fight the spread of disinformation is to verify information's truthfulness. Stop and fact-check before acting upon or sharing information.

Fake Profiles

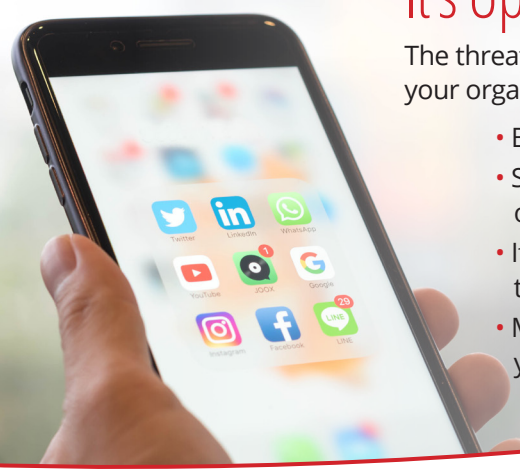
Fake profiles are very convincing profiles created by criminals using real or fake information and connections. They are designed to trick you into clicking a link or taking some kind of action.

Take a close look before acting on any requests that you receive. Some common indicators of a fake profile include model-quality or celebrity look-alike profile photos, an incomplete or generic profile, poor spelling/grammar, or a suspicious work history.

Malware

Malware is short for "malicious software," an umbrella term for all the software out there that is being used by cybercriminals to spy on you and steal your information.

Keeping your apps and security software up to date is an important first step in protecting yourself from malware. However, simply doing that isn't enough. Stop, look, and think before installing anything to your system or mobile device.



It's Up to You

The threats around you are real. How would you feel if you were the one that compromised your organization's network? Keeping the organization safe starts with you.

- Be careful with what you post and share online.
- Stay aware of what is already out there, like compromised passwords and organizational information.
- If something seems suspicious, it is always better to verify that it's legitimate.
- Make sure you stop, look, and think before you take any sort of action!

KnowBe4
Human error. Conquered.