Whittlesey Technology

ASSURANCE | ADVISORY | TAX | TECHNOLOGY

Whittlesey's 2022 Cybersecurity Month Weekly Guides

Here's a set of resources that you can use to help keep your organization secure this month and beyond.

Week 1:

Social Engineering Study Guide

Week 2:

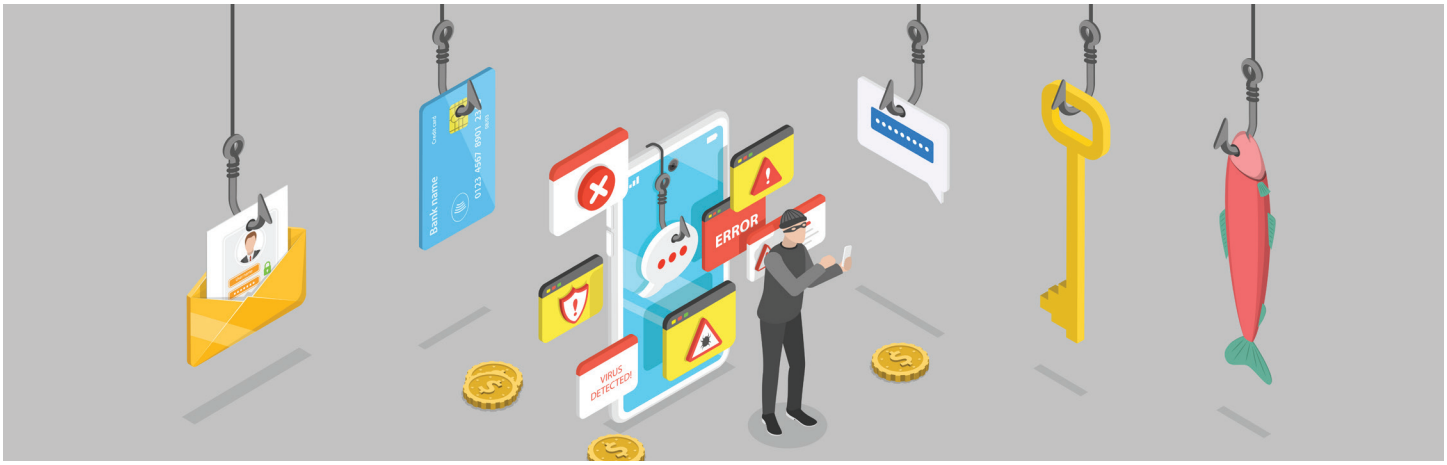
Uncovering and Reviewing Links (URLs)

Week 3:

Protect Your Personal Information

Week 4:

Keeping Your Passwords Squeaky Clean



Security Hints & Tips:

Social Engineering Study Guide

Social engineering is when someone tries to manipulate you into performing an action or sharing confidential information. Unfortunately, cybercriminals use social engineering to access computer systems, gather information, or make money. Most successful social engineering attacks are caused by human error. If you familiarize yourself with common social engineering methods, you may be able to recognize and stay safe from an attempted social engineering attack. In this study guide, you can learn about social engineering and ways you can protect yourself from social engineering attacks.

Social Engineering Tricks

Cybercriminals can use several different methods to trick you with a social engineering attack. Let's go over three common social engineering methods that you may encounter and examples of each method:

Malicious Links: Cybercriminals may use malicious links to trick you into downloading dangerous software or opening an unsafe webpage. They may send you a phishing email, which is an email that may try to convince you to share sensitive information, click an unsafe link, or download a malicious attachment. For example, you could receive an email that contains a link to access shipping information for an order. Because the email seems legitimate, you may be tempted to click the link. Then, the link could download malicious software that allows the cybercriminal to control your computer.

Fake Web Pages: Cybercriminals may create fake web pages to trick you into logging into the page or entering sensitive information. For example, you could receive a phishing email that contains a link to log in to LinkedIn. Because the email seems legitimate, you may be tempted to click the link and enter your login credentials. Once you've entered your login credentials, the cybercriminal can log in to your LinkedIn account, view your personal information, and change your password so that you can't access your account. Social Engineering Tricks

Impersonation: Cybercriminals may impersonate a celebrity or someone you know to trick you into revealing sensitive information, clicking an unsafe link, or downloading a malicious attachment. For example, you could receive a phone call from a cybercriminal posing as your internet provider. The cybercriminal could tell you that your monthly payment is overdue and mention your account number and date of birth. Because the call seems legitimate, you may be tempted to provide your payment information. Keep in mind that impersonation attacks can also occur over email, text message, or social media.

Tips for Staying Safe from Social Engineering

Now that you're more familiar with social engineering tricks, let's go over some tips that you can use to protect yourself from social engineering attacks:

- Before clicking a link, hover your mouse over the link to make sure that the link is secure and matches the website you're looking for.
- Instead of clicking a link or a button in an email to navigate to a website, navigate directly to the website by entering the URL into your address bar.
- Before sharing sensitive information such as your birth date or your payment information, verify that the source you're sharing the information with is legitimate.
- If someone you know messages you to ask about your organization or sends you a link, call or text the person directly to make sure the request is legitimate. If a message seems suspicious, it likely is suspicious.

Whittlesey Technology

ASSURANCE | ADVISORY | TAX | TECHNOLOGY

Security Hints & Tips:

Uncovering and Reviewing Links (URLs)

You probably use URLs every day to access important websites such as your email inboxes, online banking accounts, and social media profiles. Unfortunately, cybercriminals can use URLs to direct you to malicious websites, to steal your personal information, or to initiate downloads of malware onto your devices. It's important to always think before you click so that you can protect yourself and your organization from cyberattacks.

Common URL Scams

Cybercriminals use a variety of methods to trick you into clicking on URLs. A few of the most common URL scams are explained below:

Misleading URLs: If you receive an email with information about a special deal, you may be tempted to click the link in the email to learn more. However, it's important that you stop and think before you click. Cybercriminals often include misleading URLs in phishing emails. These URLs may be disguised as links to legitimate websites, or they may be hidden by a "Click Here" link for a fake offer or promotion.

Shortened URLs: Shortened URLs are URLs that have been shortened to make them easier to view and share. These URLs are often used in marketing campaigns and for certain social media platforms such as LinkedIn. Unfortunately, these links are also convenient for cybercriminals. Cybercriminals can use URL-shortening software to hide full URLs that lead to malicious websites. Then, cybercriminals can send a shortened URL to you in a phishing email, hoping that you'll click the URL since you can't see anything suspicious about the URL itself.

Insecure URLs: When verifying that a website is safe to visit, it's important to look at the first few letters of the website's URL. Many URLs will either begin with HTTP or HTTPS. The difference between these two prefixes is that HTTPS is secure, while HTTP is not secure. Websites that use HTTPS are encrypted, which means the information on these sites is protected against unauthorized users. Websites that use HTTPS are typically more secure than other websites, but it's important that you still take precautions when using HTTPS websites, too.

Tips for Staying Safe

Don't fall for these scams! Follow the tips below to stay safe:

- Hover your mouse over links before you click. When you hover your mouse over a link, you will be able to see the URL that you will be taken to if you click.
- If you receive an email with a link to a special deal or promotion, navigate to the organization's website in your browser instead of clicking the link. By visiting the organization's website directly, you can ensure that the deal or promotion is legitimate.
- Before you click a shortened URL, make sure it's legitimate. You can use an online URL checker to view the full URL.

Whittlesey Technology

ASSURANCE | ADVISORY | TAX | TECHNOLOGY

Security Hints & Tips:

Protect Your Personal Information

For years, we've been warned not to share too much personal information with people we meet online. Now, you can shop online for almost any product, manage your finances with online banking services, and chat with friends and strangers on social media platforms. While you enjoy all the conveniences of modern technology, are you paying attention to all the ways that it can be used against you? Let's take a look at ways that you can protect your personal information.

Guard Your Login Credentials

If cybercriminals steal your login credentials, they can access your accounts and find your personal or professional information. Follow these tips to protect your accounts:

- Don't enter your login credentials unless you are certain that a website or app is secure.
- Use unique passwords for each of your accounts. A password manager can help you keep track of all your passwords, and multi-factor authentication (MFA) can add another layer of security.
- Use passwords and update the security software for all of your devices. In addition to computers and smartphones, there are several other devices that can connect to the internet. If you don't protect these devices, they can be vulnerable to hacking, too.

Be Aware of Data Tracking

When you're online, your activity can be tracked by the websites that you visit and by third parties who collect data through those websites. Data tracking allows websites to remember your preferences, but it also allows third parties to use your information in ways that don't benefit you. Follow these tips when browsing the internet:

- Watch out for unusual cookies. Cookies are small pieces of data that websites share with your web browser. Some cookies are used to analyze how you interact with the website, while others are used for authentication purposes, security measures, or targeted ads. If you don't want third parties to develop a profile about your online and offline activities, look out for cookies that track your location, purchase history, and search history.
- Pay attention to who has access to information about you. If an organization's website is tracking your information and the organization isn't careful about who they sell the collected data to, the organization could put you at risk of cyberattacks. When you create an account or use a service, read the organization's privacy policy to learn what personal data will be collected and who your data will be shared with.
- Choose your own settings for data tracking. Most websites will ask you for permission to track your activity through cookies. You can opt-out of or block most third-party cookies. If you want to only allow certain permissions, you can adjust your web browser's settings.

Avoid Oversharing on Social Media

Social media can be used to update friends and family about your life, but cybercriminals can also use your accounts as an easy source of information. Follow these tips when using social media:

- Guard your personally identifiable information (PII) by limiting what information you share online.
- Check your privacy settings to minimize the information that can be viewed by the public, especially if you use your real name or the same alias across multiple websites. Cybercriminals can scour the internet for any information associated with your name or accounts.
- Watch out for subtle methods of information gathering, such as quizzes that ask for personal details like your mother's maiden name or your date of birth. Over time, cybercriminals could collect enough details to hack your accounts or steal your identity.

Remember that you are an important part of your organization's human firewall. Make sure to use strong passwords, use multiple layers of security, and be aware of what data you share and who you share it with. If your personal information is ever shared in a data breach, make sure to quickly change your passwords and reach out to your IT team for guidance. Stay safe!

Whittlesey Technology

ASSURANCE | ADVISORY | TAX | TECHNOLOGY

Security Hints & Tips:

Keeping Your Passwords Squeaky Clean

Did you know that the average person uses the same three to seven passwords to log in to over 170 online accounts? In addition to being reused, these passwords are often weak and can be easily guessed by cybercriminals. If cybercriminals guess these passwords, they could access the majority of their victim's online accounts. Even worse, the victim may not know that their password has been compromised for several months or years. To keep your passwords squeaky clean and safe from cybercriminals, follow the tips below:

Create Strong Passwords

Creating strong passwords helps prevent cybercriminals from gaining access to your online accounts. Your passwords should be as long, complex, and random as possible. While many websites only require passwords to be eight characters long, we recommend making your password at least 12 characters long. You should also include a combination of lowercase and uppercase letters, numbers, and symbols in your password. To keep your accounts extra safe, you can use password phrases, or passphrases. However, when you create your password or passphrase, make sure that you don't use any personal information that a cybercriminal could guess.

Don't Reuse Passwords

Reusing passwords for your online accounts may be convenient, but it's also risky. If you reuse passwords, you could be at risk of having multiple accounts compromised at once. If a cybercriminal guesses your password, they could access multiple accounts instead of just one account. Cybercriminals can also sell passwords or make them available online. Creating a unique password for each online account reduces the risk if one of your passwords is compromised.

Use a Password Manager

You're probably wondering how you are supposed to remember long, complex passwords for all of your online accounts. The answer is a password manager. You can use password managers to securely store all of your passwords. Instead of having to remember passwords for every online account, you only have to remember one password for your password manager. In addition to storing your passwords, many password managers can also generate passwords for you based on specific criteria.

Use Multi-Factor Authentication

You can also use multi-factor authentication (MFA) to secure your online accounts, if available. MFA requires multiple forms of authentication, such as a password and a code from your smartphone or a USB smart key. By requiring you to use multiple forms of authentication, cybercriminals will have a harder time gaining access to your account, even if your password is compromised.

Nobody wants cybercriminals to guess their passwords. To keep your passwords squeaky clean and safe, remember to create strong passwords, avoid reusing passwords, and use a password manager or MFA, if possible.

Mark R. Torello, CPA, CFE, CISA, CRISC, CITP
Partner-in-Charge, Technology

860.524.4433
mtorello@WAdvising.com

Whittlesey Technology

Headquarters
280 Trumbull Street, 24th Floor
Hartford, CT 06103
860.522.3111

One Hamden Center
2319 Whitney Avenue, Suite 2A
Hamden, CT 06518
203.397.2525

14 Bobala Road, 3rd floor
Holyoke, MA 01040
413.536.3970

WAdvising.com