Click Wisely

A MINI TRAINING SESSION FOR LOSS PREVENTION

Quick Take on Data Security

Safe Internet Browsing

TRAINING OVERVIEW AND OBJECTIVES

Overview: Covers recognizing and avoiding suspicious links and websites, and methods to identify secure websites.

Purpose: Trains staff to recognize suspicious links and websites to avoid costly malware and potential data breaches.

Preparation:
- Read and become familiar with this Quick Take. *Change it as needed to reflect procedures and circumstances of your department.*
- Review current IT practices and procedures, and make changes as needed to this Quick Take.

Handouts: Quick Review of Data Security: Safe Internet Browsing

Safe Internet Browsing

Browsing is how people use and interact with the internet. The open access to information from around the world is great, but it also creates many avenues that open our local system to compromise. Several methods can be used to gain unauthorized access to secure systems, but one of the most popular and successful is to direct users to click on links or websites that are not legitimate.

IT professionals work to protect our systems, but it takes all of us doing our part to keep our systems and data secure. Please pay attention.

Recognize Suspicious Links and Websites

To avoid malicious online content, such as viruses, ransomware and spyware, you first have to recognize the attack. Most suspicious links arrive through email as what's called "phishing" attacks. But others commonly arrive disguised as advertisements in pop-ups or on websites.

Pop-ups are webpages that open a new browser window and interrupt browsing. Pop-ups are regularly used for advertising but could also contain links that download viruses or direct you to malicious content.

It's important to remember:
- Links are not always blue underlined text. They can be photos or other items. Particularly items such as clickbait. Clickbait refers to outrageous or sensational headlines or photos that entice users to click on them.
- Links can also be hidden in photos of buttons, such as the close button, which can be particularly common on advertisements or other items that flash across the screen.

Avoid Suspicious Links and Websites

To help prevent accidentally infecting computers or other electronic devices with malicious content, it is important to remember the following best practices:

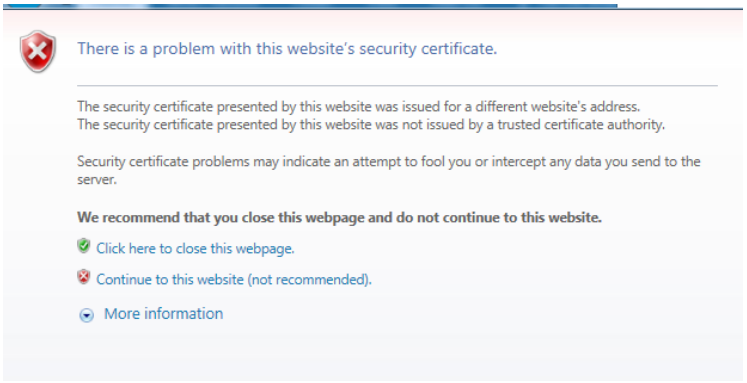
MCIT
This document is intended for general purposes only and should not be construed as legal or coverage advice on any specific matter.
Developed and provided by Minnesota Counties Intergovernmental Trust.

- Maintain a healthy skepticism: If anything sounds too good or too bad to be true it is probably clickbait. Do not click on these links or attachments.
- Avoid clickbait, pop-ups and advertisements: These items try to distract you and entice you to click on them. Although they are not always viruses or malicious content, they are one of the main delivery routes for malware.
- Look for poor spelling and grammar: Many virus and malicious content attacks come from other countries whose residents may have poor English skills. This can be a clue as to whether an email or website is legitimate.
- Review links: Hovering a mouse cursor over a link can reveal the link address either next to the cursor or along the bottom of the screen. Review the link to determine if it seems legitimate. Occasionally links may direct you to sites with names or domains that are similar to trusted sites but with a small variation, such as ".net" instead of ".com." Other sites may be misspelled that with a casual look, you may not notice, such as spelling "Google" with three O's or some other element. These fake sites would then install viruses or capture sensitive information.

Secure Websites

Whenever you enter private, sensitive or valuable information into a website or online form, such as when purchasing items or entering passwords, the website should be secure. To help identify a secure website remember the following:

- Look for the presence of a padlock icon and an "https://" prefix to the website address. These indicate that the site is encrypted and the encryption is current and functioning.
  - If a site's prefix is merely "http://" (does not include the "s" before the colon), it is not secure.
  - Every internet browser is different, and the padlock may be displayed in different locations.
- Stop and consult with IT before proceeding to a site where the user encounters a warning with the site's security certificate.



DISCUSSION QUESTIONS

- What else can we do to ensure that we are safely browsing the internet?
- If we encounter any concerns, to whom should we talk?

Safe Internet Browsing
Session Planning and Review

Trainer	Training Date
Department(s)	

TRAINING GOALS

Employees understand what safe browsing is.

- Employees can recognize unsafe links and websites.
- Employees can avoid unsafe links and websites.

RESOURCES

- "Security Tip: Understanding Web Site Certificates," United States Computer Emergency Readiness Team, Department of Homeland Security, US-CERT.gov
- "Tips—Safe Browsing," United States Computer Emergency Readiness Team, Department of Homeland Security, US-CERT.gov
- "Guidelines on Securing Public Web Servers (NIST special publication 800-44 Version 2)," National Institute of Standards and Technology, NIST.gov

REVIEW

Did the training meet the stated goals?

[add comments here]

How can the training be improved?

[add comments here]

TRAINER COMMENTS

[add comments here]

Attendance Record

Training Session Safe Internet Browsing

Trainer Training Date

Participant Name (printed)	Participant Signature