LOSS PREVENTION

Quick Review of Data Security

SAFE INTERNET BROWSING

RECOGNIZING SUSPICIOUS LINKS AND WEBSITES

It's important to remember:

- Links are not always blue underlined text. They can be photos or other content, particularly clickbait. Clickbait is outrageous or sensational headlines or photos that entice users to click on them.
- Links can 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.

AVOIDING SUSPICIOUS LINKS OR WEBSITES

- 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 click on them.
- 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 e-mail 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.

(Over)

LOSS PREVENTION

Quick Review of Data Security

SAFE INTERNET BROWSING

RECOGNIZING SUSPICIOUS LINKS AND WEBSITES

It's important to remember:

- Links are not always blue underlined text. They can be photos or other content, particularly clickbait. Clickbait is outrageous or sensational headlines or photos that entice users to click on them.
- Links can 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.

AVOIDING SUSPICIOUS LINKS OR WEBSITES

- 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 click on them.
- 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 e-mail 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.

(Over)

SECURE WEBSITES

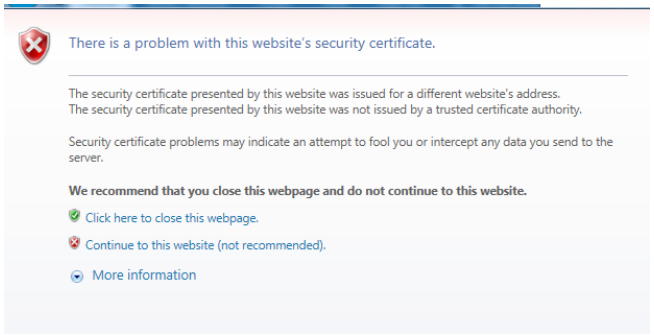
Whenever you enter private, sensitive or valuable information into a website or online form, such as when purchasing items or entering passwords, the website should be secure.

To help identify a secure website, remember the following best practices:

- Look for the presence of a padlock icon and an “https:” prefix to the Web address. These indicate that the site is encrypted and the encryption is current and functioning.

  - A site is not secure if its prefix is merely “http:.”
  - 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.



SECURE WEBSITES

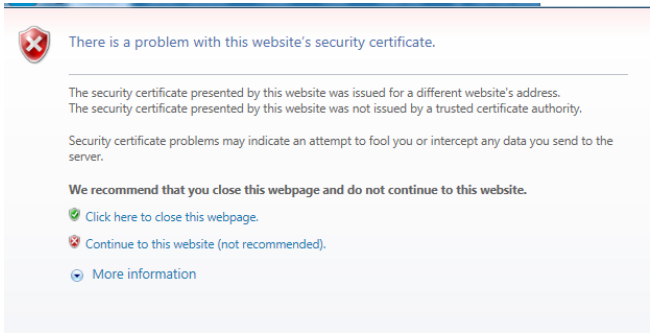
Whenever you enter private, sensitive or valuable information into a website or online form, such as when purchasing items or entering passwords, the website should be secure.

To help identify a secure website, remember the following best practices:

- Look for the presence of a padlock icon and an “https:” prefix to the Web address. These indicate that the site is encrypted and the encryption is current and functioning.

  - A site is not secure if its prefix is merely “http:.”
  - 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.



This document is intended for general purposes only and should not be construed as legal or coverage advice on any specific matter.