CYBER OCTOBER

Week 3: Safe Web Habits

For most people, a majority of their computer usage is spent surfing the web. You pop open your favorite web browser and check out your social media, video games, news, and more. It is important to be aware of how to secure yourself as you explore the World Wide Web so your valuable information is not compromised. This week we will be shedding light on the dark mysteries of the web.

Password Security

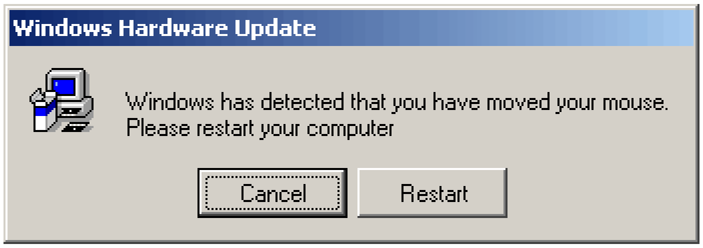
- Do not reuse passwords between multiple sites or applications:
  - Example: If you share the same password between a forum and your e-mail account, if that forum is compromised then they can gain access to your e-mail and from there the rest of your online accounts!
- Password complexity is key! Remember to keep your passwords long and strong:
  - Don't make passwords simple enough that they would be easy to guess. Use a mix of:
    - Lowercase characters
    - Uppercase characters
    - Special + Numeric characters (!@#123)
    - At least 12-15 characters.

Password Managers

Password Managers are a utility that manages all of the passwords for every credential-required application or website you access. It will create a unique and secure password for each website and store it in a database so you do not have to remember it each time. You only need to remember one master password for the database as opposed to the hundreds for each accessed application or site.

Pop-Up Blockers

- Not only can pop-ups be annoying, they can also contain malicious code that can infect your computer with a virus.
- Most browsers come with popup blockers built into them but not all are enabled by default. Ensure you navigate your browsers Settings and check under the "Privacy" or "Security" tab, depending on the browser, to enable your pop-up blocker.



Windows Hardware Update

Windows has detected that you have moved your mouse.
Please restart your computer

E-mail Security

- Be vigilant for suspicious e-mails! Spam e-mails or even mail from people you may know may contain security risks such as phishing links, malicious attachments, or false information.
- Warning Signs of a Malicious E-mail:
    - Notification of password reset or account information change when you did not request it.
    - Spelling/grammar issues or incorrect/discolored company logos. Adversaries will attempt to disguise their e-mail to make it appear as if it is from a legitimate source.
    - A URL link that does not match the known website.
        - Example: www.**w**Google.com instead of www.Google.com

HTTP(s) Protocols

- Hyper Text Transfer Protocol Secure (HTTP) is "the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted…"[1]
- Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP. This secure protocol ensures your data is encrypted, or protected, while accessing that web page.
- The following indicators show examples for Google Chrome, other browsers may use similar indicators or symbols:

  🔒 Secure | https: This indicator found to the left of the URL address bar shows that the website you are on utilizes HTTPS.

  ⓘ www. : This indicator shows the website is not running on HTTPS. This does not mean the website is dangerous, it just shows your information submitted will not be encrypted.

  ⚠ Not secure | ~~https:~~ This indicator shows the website is not secure or utilizes elements that may pose risk to your computer. Submitted sensitive credentials have an increased risk of being compromised on a website like this.

- Sensitive information such as: user credentials, banking information, or personally identifiable information (PII) information runs the risk of being compromised if you submit them on anything besides a HTTPS website.

[1] **https://www.webopedia.com/TERM/H/HTTP.html**