Safe Web Browsing Script

We are always browsing online, but it is important to remember the rules, especially when we work remotely to help keep you and your network safe.

Cyber criminals can hide malicious software used to steal your information through links and webpages. Be extra cautious when an application is asking you to enter your username and password, and never enter work login credentials into non-work applications.

To help minimize cyber risks on your mobile device or laptop, follow these best practices for browsing the web securely:

1. Do not click on any links anywhere! The most common places are on websites or emails if you do not recognize it. Be aware of shortened URLs, which are shortened versions of long website links. Examples include bit.ly, tinyurl.com and goo.gl URL shortener. Cyber criminals can use shortened URLs to hide a link to a virus, malware, or phishing scam website.
2. Be aware of anything you download. Installing a malicious application can give cyber criminals a gateway to your device.
3. Only browse work related sites from your work device. You increase the risk to your organization’s network every time you browse sites for personal reasons. For example, never access personal emails on a work device.
4. Regularly check your work devices for system updates. If the update is not automatically applied, make sure to manually do it when you get the notification.

Remember, it is everyone’s responsibility to safeguard the network, system and our information from cyber threats.

Thank you for watching.