Semaine 3 – Navigation sécurisée sur le Web

Navigation sécurisée sur le Web

Conseils pour rester en sécurité lorsque vous naviguez sur le Web

Nous naviguons toujours en ligne, mais il est important de se souvenir des règles

Surtout lorsque nous travaillons à distance pour vous aider à rester en sécurité et protéger notre réseau.

Les cybercriminels peuvent cacher des logiciels malveillants utilisés pour voler vos informations par des liens et des pages web.

Soyez très prudent lorsqu'une application vous demande de saisir votre nom d'utilisateur et votre mot de passe,

et ne saisissez jamais les identifiants de connexion professionnelle dans les applications non professionnelles

Pour minimiser les risques d'une cyberattaque sur votre appareil mobile ou votre ordinateur portable, suivez ces bonnes pratiques afin de naviguer sur le Web en toute sécurité

Pensez avant de cliquer

Soyez conscient du téléchargement d'applications

Les appareils de travail ne sont pas pour l'utilisation personnelle

Vérifiez régulièrement les mises à jour

1. Ne cliquez sur aucun lien! Les endroits les plus communs sont sur des sites web ou dans des courriels si vous ne le reconnaissez pas

Soyez conscient des URL raccourcies, qui sont des versions réduites de longs liens vers des sites web.

Des exemples de réducteur d'URL incluent bit.ly, tinyurl.com et goo.gl.

Les cybercriminels peuvent utiliser des URL raccourcies pour masquer un lien vers un virus, un logiciel malveillant ou un site web d'hameçonnage frauduleux.

2. Soyez conscient de tout ce que vous téléchargez. L'installation d'une application malveillante peut donner aux cybercriminels une passerelle vers votre appareil

3. Naviguez seulement des sites reliés au travail sur votre appareil de travail. Vous augmentez le risque du réseau de votre organisation chaque fois que vous naviguez sur des sites pour des raisons personnelles.

Par exemple, n'accédez jamais aux courriels personnels sur un appareil de travail.

4. Vérifiez régulièrement les mises à jour système de vos appareils de travail. Si la mise à jour n'est pas appliquée automatiquement, assurez-vous de le faire manuellement lorsque vous recevez la notification.

N'oubliez pas que c’est la responsabilité de chacun de protéger le réseau, le système et nos informations contre les cybermenaces.

Merci d’avoir regardé cette vidéo