Manitoulin
GROUP OF COMPANIES

Que se passe-t-il

lorsque vous cliquez sur un lien d'hameçonnage?

Un élément crucial de la cybersécurité est de ne pas cliquer sur des liens d'hameçonnage ou de télécharger des pièces jointes malveillantes. Que se passe-t-il si vous le faites? Voici quelques conséquences potentielles :

1 Vous devenez une cible de haut profil.

En cliquant sur un lien d'hameçonnage, vous confirmez à l'attaquant que 1) vous êtes une vraie personne, votre courriel est courant, et 2) vous êtes crédule. L'attaquant pourrait utiliser ces renseignements pour construire un profil vous concernant, le vendre à d'autres attaquants, qui vont alors envoyer beaucoup plus de courriels d'hameçonnage menaçants. Vous pourriez également connaître une augmentation importante au niveau des pourriels.

2 Vous avez des renseignements personnels volés.

Dans plusieurs cas, un lien d'hameçonnage vous dirigera vers une page Web qui paraît légitime. La page vous demandera de saisir divers renseignements personnels : votre nom au complet, courriel, nom d'utilisateur, mot de passe et ainsi de suite. Si vous saisissez de tels renseignements, vous transmettez effectivement votre identité à un criminel, qui peut utiliser ces renseignements pour ouvrir des comptes frauduleux en votre nom.

3 Vous perdez le contrôle de vos comptes.

Disons que vous êtes en session dans votre banque bancaire lorsque vous cliquez sur un lien d'hameçonnage. Cela peut permettre à des cybercriminels d'exécuter un exploit connu comme détournement de session. Cela veut dire que les cybercriminels peuvent intercepter les communications entre le site Web de la banque et votre propre ordinateur, et ainsi prendre le contrôle de votre compte. S'ils réussissent, ils auront à présent le même accès que vous. Ils pourront transférer de l'argent, modifier les mots de passe et voler des données personnelles.

4 Vous infectez votre dispositif avec un logiciel malveillant.

Dans des attaques par hameçonnage plus insidieuses, cliquer sur un lien ou télécharger une pièce jointe pourrait entraîner qu'un code malveillant corrompt votre dispositif, vole des données ou, pire encore, infecte votre ordinateur avec un rançongiciel. Les rançongiciels sont particulièrement préoccupants ici, au travail, car ils peuvent chiffrer nos données ou verrouiller nos systèmes jusqu'à ce qu'une rançon soit payée, menant à une perte de revenus et des temps d'arrêt coûteux.

Tous ces scénarios ne sont que des exemples de ce qui pourrait arriver. Peu importe la gravité, il faut éviter à tout prix de se faire piéger par une escroquerie par hameçonnage. N'oubliez pas : les cybercriminels lancent souvent de grandes attaques avec des courriels d'hameçonnage génériques qui activent les avertissements rouges typiques facilement repérables. Mais certaines attaques sont beaucoup plus sophistiquées. Elles peuvent sembler provenir de quelqu'un que vous connaissez, comme un collègue de travail ou un gestionnaire.

Soyez extrêmement prudents lorsque vous manipulez des messages, y compris ceux sur vos appareils mobiles, qui contiennent des liens, des pièces jointes, et des demandes de renseignements ou d'argent. Comme règle : si vous n'êtes pas certain, ne cliquez pas! Signalez immédiatement toute attaque d'hameçonnage.