COMMENT PROTÉGER VOS DONNÉES CONTRE LES ATTAQUES D'HAMEÇONNAGE PAR COURRIEL

Il existe plusieurs différents types d'hameçonnage, mais l'hameçonnage par courriel demeure le plus commun. Répondre à un message, cliquer sur un lien ou télécharger un fichier suspect peut causer la corruption de données, la fuite d'informations confidentielles et la contamination d'appareils ou de réseaux.

Voici comment éviter d'être victime d'hameçonnage :

1 Inspecter l'adresse courriel de l'expéditeur

L'hameçonnage utilise des adresses courriel falsifiées pour cibler les utilisateurs. Le message peut sembler provenir d'une marque ou d'un site bien connu. Vérifiez si des mots ou des caractères ont été ajoutés ou changés, et s'il y a des fautes d'orthographe dans le nom de domaine.

2 Examiner les formules de politesse et le ton du message

Méfiez-vous des courriels qui utilisent des formules de politesse génériques et un ton urgent. Les courriels d'hameçonnage ciblent plusieurs personnes à la fois et enjoignent le destinataire à prendre des mesures immédiates, habituellement sans ligne d'ouverture personnalisée.

3 Vérifier la présence des coordonnées de l'expéditeur

Ne répondez pas à des courriels qui ne contiennent aucune information sur les coordonnées de l'expéditeur, comme son numéro de téléphone, son adresse courriel ou l'emplacement de son bureau.

4 Ne pas envoyer des informations sensibles par courriel

Ne jamais divulguer des informations confidentielles en réponse à un message électronique, même s'il utilise un ton urgent. Les cybercriminels tirent profit des techniques d'ingénierie sociale pour obtenir des données personnelles, comme des noms, adresses, informations bancaires et plus, qui peuvent servir à des activités frauduleuses.

5 Éviter de cliquer sur des liens non sollicités

Évitez de cliquer sur des liens qui proviennent d'expéditeurs ou d'organisations inconnus. Vous pourriez être redirigé vers un site Web ou démarrer un téléchargement qui peut compromettre vos données ou contaminer votre appareil.

6 Éviter d'ouvrir des pièces jointes suspectes

Évitez d'ouvrir des pièces jointes provenant d'expéditeurs inconnus ou simplement pour satisfaire votre curiosité. Les pièces jointes suspectes peuvent transporter des charges de maliciels et de rançongiciels susceptibles de corrompre vos données et d'endommager votre appareil.

7 Installer un filtre anti-hameçonnage pour votre compte courriel

Assurez-vous d'avoir un filtre anti-hameçonnage compatible au logiciel de courrier électronique installé sur votre ordinateur. Il est également possible d'en installer un dans votre navigateur. Bien qu'il ne permettra pas de bloquer l'entrée de tous les messages d'hameçonnage, il réduira considérablement le nombre de tentatives qui apparaissent dans votre boîte de réception.