COMMENT PROTÉGER VOS DONNÉES DES ATTAQUES DE MYSTIFICATION

Bien que les fraudeurs utilisent plusieurs tactiques différentes de mystification (spoofing), ils ont tous le même objectif en tête : soutirer des données sensibles et les utiliser pour commettre des actes malveillants. Répondre à un courriel falsifié ou ouvrir un faux site Web peut entraîner la corruption de données, la fuite d'informations confidentielles et la contamination des appareils ou des réseaux.

Voici comment éviter d'être victime de spoofing :

1

S'assurer que le site Web est sécurisé

La plupart des navigateurs indiquent dans leur barre d'adresse si le site est sécurisé ou non. S'il n'y a pas d'icône de cadenas ou de bouclier à gauche de l'URL, ou si l'URL commence avec http plutôt que https, le site Web n'est pas sécurisé et peut être falsifié. Vérifiez l'orthographe de l'URL du site Web ou utilisez un signet.

2

Utiliser un gestionnaire de mot de passe pour les identifiants

Beaucoup de sites Web remplissent automatiquement votre nom et mot de passe, particulièrement si vous avez sauvegardé vos identifiants dans votre navigateur. Pour vous protéger des connexions automatiques, utilisez un gestionnaire de mot de passe pour enregistrer vos identifiants. Si le gestionnaire de mot de passe ne reconnaît pas un site, il ne remplira pas automatiquement vos détails.

3

Examiner le domaine du courriel de l'expéditeur

Méfiez-vous des descriptions d'adresses courriel qui semblent officielles. Il est possible de falsifier le nom d'une adresse courriel. Inspectez l'adresse réelle de l'expéditeur, celle qui contient le symbole « @ ». Les lettres inscrites à gauche et à droite du dernier point de l'adresse courriel représentent le domaine de l'expéditeur.

4

Ne pas cliquer sur des liens suspects

Même si un message semble provenir d'une source légitime, ne cliquez jamais sur des liens suspects. Examinez l'URL de chaque hyperlien avec attention en passant votre souris sur le lien d'appel et en utilisant l'aperçu de texte dans votre fenêtre de navigation ou courriel pour inspecter les éléments de l'adresse du site Web.

5

Ne pas ouvrir les pièces jointes douteuses

Évitez d'ouvrir des pièces jointes provenant d'expéditeurs inconnus ou simplement pour satisfaire votre curiosité, particulièrement si le message vous enjoint de le faire immédiatement. Les pièces jointes suspectes peuvent transporter des charges de maliciels et de rançongiciels susceptibles de corrompre vos données et d'endommager votre appareil.

6

Se méfier de l'identité de l'appelant

Soyez à l'affût des signes indiquant que l'identité de l'appelant a été falsifiée. Les signaux d'alerte les plus courants sont les suivants : un numéro de téléphone qui s'affiche sans parenthèses ou tirets, un numéro très semblable au vôtre (c.-à-d. seulement un ou deux chiffres ont été modifiés) ou si le numéro ou le nom de l'appelant est masqué.

7

Éviter les réseaux Wi-Fi publics non sécurisés

Ne vous connectez jamais à un réseau Wi-Fi public ouvert non sécurisé, même s'il s'agit du seul Wi-Fi disponible. Le fait de fournir votre adresse courriel et d'accepter les termes et conditions du propriétaire d'une connexion Wi-Fi ne signifie pas que vous êtes connecté à un réseau sécurisé.