FORTRA

Terranova Security®

Comment protéger vos données de l'hameçonnage par texto et de l'hameçonnage vocal

Même les utilisateurs les plus vigilants peuvent être trompés par les messages persuasifs et convaincants d'attaques d'hameçonnage vocal (vishing) et d'hameçonnage par message texte (smishing). En effet, en combinant l'usurpation d'identité avec un langage autoritaire, il peut être difficile de distinguer une activi frauduleuse d'une demande légitime. Voici comment éviter ces types de cybermenaces.

1

LIRE ET ÉCOUTER TOUS LES MESSAGES AVEC ATTENTION

Avant de répondre à tout message texte ou vocal suspect, portez attention au langage utilisé et réfléchissez au message t ansmis. Méfiez- ous des expéditeurs ou des appelants qui utilisent l'intimidation, les menaces et un ton agressif ou urgent. Raccrochez et utilisez les coordonnées officielles pour appeler.

PRENDRE GARDE AUX MESSAGES PROVENANT DE NUMÉROS INCONNUS

Soyez sur vos gardes si un message de smishing ou de vishing provient d'un numéro inconnu ou bloqué. Dans le cas d'une tentative de vishing, renvoyez l'appel sur la messagerie vocale et écoutez attentivement le message qui en résulte avant de faire quoi que ce soit. Ne vous fiez pas au numé o de rappel fourni dans le message.

2

3

REPÉRER L'UTILISATION D'UN LANGAGE MANIPULATEUR

Les cybercriminels qui lancent des campagnes de smishing et de vishing conçoivent souvent leurs messages de façon à profiter des instincts humains de base comme la peur, la convoitise et la confiance. Il est impo tant de faire preuve de jugement et d'analyser chaque message avec attention, à la recherche d'éléments suspects.

DEMANDER DES PRÉCISIONS À L'EXPÉDITEUR

Si un expéditeur tente de vous soutirer de l'information en échange d'un prix ou d'un produit, demandez-lui une preuve vérifiable d son identité et de sa fonction professionnelle. Si l'appelant refuse de vous fournir cela, ou toute autre information pertinente, mettez fin à l échange.

4

5

NE PAS CLIQUER SUR UNE PIÈCE JOINTE OU UN LIEN NON SOLLICITÉ

Comme pour tous les types de cybermenaces, évitez de cliquer sur un lien non sollicité ou d'ouvrir une pièce jointe à un message suspect. Rappelez-vous qu'une organisation ne vous demandera jamais de lui transférer des fonds ou de partager des informations confidentielles par téléphone ou message texte

ÉVITER DE RÉPONDRE AUX DEMANDES D'INFORMATIONS CONFIDENTIELLES

Même si le message de smishing ou de vishing semble provenir d'une banque, d'un hôpital, d'un service de police ou d'un bureau gouvernemental, ne partagez jamais des informations personnelles sans avoir vérifié au p éalable la légitimité de l'expéditeur. Évitez également de donner votre numéro de téléphone via des adresses courriel inconnues.

6