FORTRA

Terranova Security®

Qu'est-ce que l'hameçonnage vocal et par texto ?

L'hameçonnage vocal (vishing) et l'hameçonnage par message texte (smishing) sont des cyberattaques qui reposent sur l'envoi de messages textes ou vocaux créé pour manipuler les victimes et voler des informations confidentielles. En général, ces messages utilisent un ton convaincant pour inciter les victimes à répondre ou à prendre une action immédiate.

Exemples de tactiques de smishing et de vishing

01 FAUX LIENS

Dans ce scénario de smishing, l'expéditeur prétend représenter une vraie organisation et joint un lien semblant légitime dans un message texte. L'objectif du message est d'inciter l'utilisateur à cliquer sur le lien et à poser une action comme de mettre à jour des informations de connexion.

02 ATTAQUE DE MALICIEL

Les messages textes de smishing peuvent également inclure un lien vers un fichier exécutable qui installe un maliciel sur l'appareil de la victime. Ce type d'attaque utilise souvent un logiciel de type Cheval de Troie pour enregistrer les mouvements du clavier, ce qui facilite le vol de mots de passe et d'autres données sensibles.

03 HAMEÇONNAGE VOCAL

Les attaques de vishing les plus courantes prennent la forme de faux appels qui semblent provenir des sources suivantes : votre banque qui appelle pour rapporter des activités suspectes, le gouvernement ou le fisc, une équipe de soutien informatique qui prétend vouloir réparer votre ordinateur, ou une organisation qui vous offre un prix ou un rabais important.

04 SCANNAGE DE NUMÉROS DE TÉLÉPHONE (WARDIALING)

Cette technique de vishing utilise un logiciel pour appeler des indicatifs régionaux spécifiques et diffuser un message enregistré qui semble provenir d'une banque, d'une entreprise ou du service régional de police. Lorsqu'une victime répond, le message automatisé lui demande de partager des données sensibles.

05 VOIX SUR IP (VoIP)

La technologie VoIP permet aux cybercriminels de facilement créer de faux numéros qui semblent locaux ou qui utilisent le préfixe 1-800. Certains numéros usurpent même l'identité d'organisations locales, comme des ministères ou des hôpitaux.

Qui peut être la cible de smishing et de vishing ?

Tout type d'entreprise, de gouvernement, d'organisation ou d'individu peut être la cible d'une attaque. Les cybercriminels cherchent des victimes prêtes à croire au bien-fondé des messages urgents de smishing et de vishing tout en utilisant un langage intimidant pour pousser les utilisateurs à prendre action immédiatement.