Guide de bonne pratique contre le phishing (pour un simple utilisateur)

GUIDE ANSIE

Sommaire

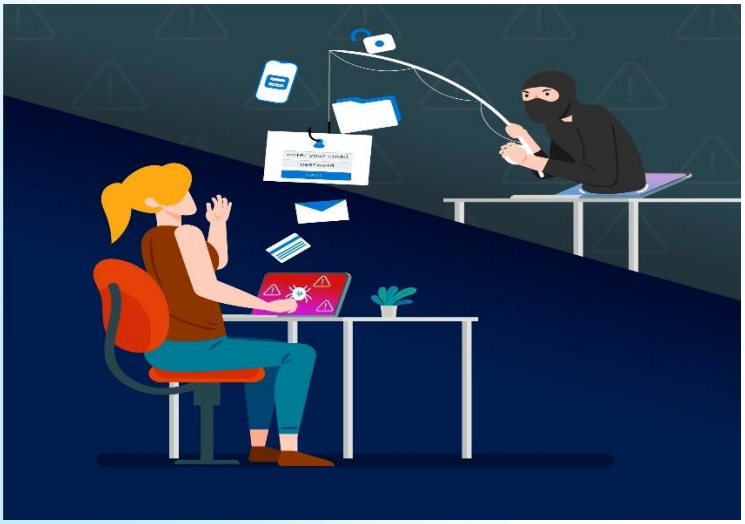
Introduction

L'hameçonnage est une forme de fraude dans laquelle un attaquant se fait passer pour une entité ou une personne de bonne réputation dans un courrier électronique ou d'autres formes de communication. Les attaquants utilisent généralement des e-mails de phishing pour distribuer des liens ou des pièces jointes malveillants qui peuvent exécuter diverses fonctions. Certains extrairont les identifiants de connexion ou les informations de compte des victimes.

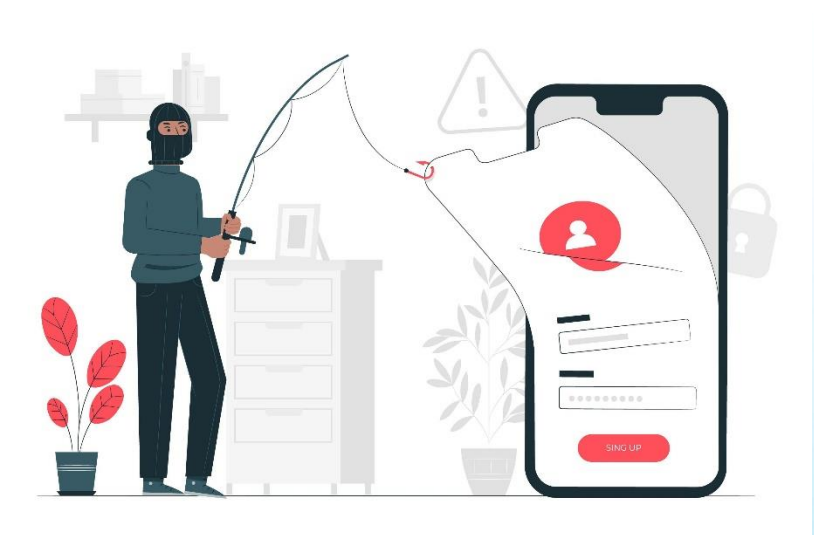
L'hameçonnage trompeur est populaire auprès des cybercriminels, car il est beaucoup plus facile d'amener quelqu'un à cliquer sur un lien malveillant dans un e-mail d'hameçonnage apparemment légitime que de percer les défenses d'un ordinateur. En savoir plus sur le phishing est important pour savoir comment le détecter et le prévenir.

I. Le Phishing c'est quoi ?

C'est une attaque basée sur l'ingénierie sociale (faille humaine) qui consiste à duper la victime par l'intermédiaire d'un courrier électronique. Par le biais d'un formulaire factice, les pirates obtiennent des informations personnelles telles que numéro de compte bancaire, numéro client, code confidentiel, mot de passe. Après avoir récupéré ces informations, les pirates réalisent des transactions financières frauduleuses et revendent parfois ces informations volées.



II. Comment fonctionne le phishing ?



Qu'elles soient menées par e-mail, sur les réseaux sociaux, par SMS ou tout autre vecteur, toutes les attaques de phishing obéissent aux mêmes principes de base.

L'attaquant envoie un argumentaire ciblé visant à persuader la victime de cliquer sur un lien, de télécharger une pièce jointe, d'envoyer les informations requises ou même d'effectuer un paiement.

L'omniprésence des réseaux sociaux offre aux hameçonneurs l'accès à un nombre croissant d'informations personnelles de leurs cibles. Armés de toutes ces données, ils peuvent adapter leurs attaques aux besoins, aux désirs et aux situations de leurs cibles, ce qui rend leurs propositions bien plus alléchantes. Dans ces cas de figure, les réseaux sociaux alimentent une ingénierie sociale plus puissante.

Le phishing profite du manque d'attention des utilisateurs et repose sur quatre principes :

- ✓ Usurper l'identité d'une organisation de confiance pour collecter les données personnelles des clients de cette organisation,
- ✓ Demander, sous un faux prétexte, de fournir des informations personnelles,
- ✓ Rediriger la victime vers un site Internet pirate mais identique au site Internet officiel de l'organisation usurpée pour que la victime saisisse les informations demandées,
- ✓ Exploiter les données collectées pour usurper une identité dans le but d'obtenir des avantages et services (argent, biens, papiers d'identité et documents administratifs).

III. Les types de phishing

1. Le spear phishing.

Le spear phishing cible un groupe ou un type spécifique de personnes, par exemple l'administrateur système d'une entreprise. L'email ci-dessous est un exemple d'email de spear phishing. Notez l'attention portée au secteur dans lequel travaille le destinataire, le lien de téléchargement sur lequel l'assaillant demande à la victime de cliquer, et la réponse immédiate exigée.

2. Le whaling

Le whaling est un type de phishing encore plus ciblé qui s'attaque généralement aux PDG, directeurs financiers ou autres directeurs de l'industrie ou d'une entreprise en particulier. Un email de whaling peut stipuler que l'entreprise du destinataire est poursuivie en justice et qu'il doit cliquer sur le lien afin d'obtenir plus d'informations.

Le lien vous conduit à une page où il vous est demandé de saisir des données essentielles sur l'entreprise, telles que le numéro d'identification fiscale et le numéro de compte bancaire.

3. Le smishing/vishing

Le smishing est une attaque qui utilise la messagerie texte ou SMS pour mener l'attaque. Une technique de smishing courante consiste à envoyer un message à

un téléphone portable via un SMS contenant un lien cliquable ou un numéro de téléphone à rappeler.

Un exemple fréquent d'attaque de smishing est un SMS qui semble provenir de votre banque. Il vous indique que votre compte a été compromis et que vous devez réagir immédiatement.

L'assaillant vous demande de vérifier votre numéro de compte bancaire, votre numéro de sécurité sociale, etc. Une fois que l'attaquant reçoit les informations, il peut contrôler votre compte bancaire.

Le but du vishing est le même que les autres types d'attaques de phishing. Cette attaque a lieu via un appel vocal. D'où le « v » à la place du « ph » dans son nom.

IV. Actions proposées contre le Phishing.

- ✓ Former le personnel à reconnaître les courriels falsifiés et frauduleux, ainsi qu'à rester vigilant. Lancer de fausses campagnes d'hameçonnage pour tester l'infrastructure de l'organisation, de même que la réactivité du personnel.
- ✓ Dans l'idéal, utiliser des communications électroniques sécurisées par signatures numériques ou chiffrement pour les opérations financières critiques ou lors d'échanges d'informations sensibles.
- ✓ Éviter de cliquer sur des liens aléatoires, en particulier des liens courts rencontrés dans les médias sociaux.
- ✓ Ne pas cliquer sur des liens ou télécharger des pièces jointes si vous n'êtes pas absolument sûr de la source du courriel.
- ✓ Éviter le partage excessif de renseignements personnels sur les médias sociaux, par ex. la durée de votre absence au bureau ou à domicile, vos informations de vol, etc., car les auteurs de menace les utilisent activement pour recueillir des informations sur leurs cibles.
- ✓ Activer l'authentification à deux facteurs dès que possible pour empêcher les piratages de comptes
- ✓ Au moment de transférer de l'argent sur un compte, revérifier les informations de la banque bénéficiaire par le biais d'un autre moyen. Il ne faut pas faire confiance aux courriels non chiffrés et non signés, surtout dans des cas d'utilisation sensibles comme celui-ci

Conclusion

Il peut être difficile de repérer une tentative d'hameçonnage. Les cybercriminels sont devenus des experts et utilisent des techniques sophistiquées pour obtenir vos renseignements personnels et financiers. Mais la meilleure façon de vous protéger est d'apprendre à reconnaître une tentative d'hameçonnage. Lors de la navigation sur internet, il est judicieux pour l'internaute d'observer certaines mesures comportementales afin de ne pas tomber dans un piège potentiel.