OUCH! Juillet 2022

Les attaques par hameçonnage deviennent de plus en plus travaillées

Les attaques par hameçonnage sont devenues la méthode la plus fréquente pour cibler les personnes au travail et chez eux. Généralement, les attaques par hameçonnage se déguisent sous la forme d'e-mails envoyés par les cyber-attaquants pour vous inciter à faire quelque chose que vous ne devriez pas faire comme ouvrir la pièce jointe d'un e-mail infecté, cliquer sur un lien malveillant ou partager votre mot de passe. Même si ces e-mails existent toujours, beaucoup de cyber-attaquants créent maintenant des e-mails plus personnalisés et plus difficiles à détecter. Ils utilisent des méthodes avancées telles que vous contacter par SMS, via les réseaux sociaux, et même des appels téléphoniques pour vous piéger. Voici leurs dernières astuces et comment vous pouvez les réperer.

Les cyber-attaquants font leurs recherches

Les e-mails d'hameçonnage sont plus faciles à détecter car il s'agit de messages génériques envoyés à des millions de gens. Les cyber-attaquants ne visent personne en particulier ; ils savent juste que plus ils envoient d'e-mails, plus ils ont de chance de piéger des gens. Ces attaques commencent souvent par « Cher Client », elles sont truffées de fautes et la proposition est trop belle pour être vrai, comme des princes nigériens qui vous offrent des millions d'euros.

Les attaques d'aujourd'hui sont bien plus sophistiquées. Ils font maintenant des recherches sur leurs victimes pour créer des attaques plus ciblées. Au lieu d'envoyer un e-mail d'hameçonnage à cinq millions de personnes, ou de faire croire qu'il s'agit d'e-mails génériques envoyés par des entreprises, ils peuvent l'envoyer à cinq personnes seulement et adapter l'attaque pour qu'elle semble provenir d'une personne que nous connaissons. Les cyber-attaquants font cela :

- en faisant des recherches sur nos profils LinkedIn, sur ce que nous publions sur les réseaux sociaux ou en utilisant des informations accessibles au public ou trouvées sur le Dark Web.
- en créant des messages artisanaux qui semblent provenir de la direction, de collègues ou de vendeurs que vous connaissez et avec lesquels vous travaillez.
- en apprenant quelles sont vos passions et en vous envoyant un message en prétendant être quelqu'un qui partage un intérêt commun.
- en déterminant que vous avez assisté récemment à une conférence ou que vous venez de rentrer d'un voyage et en envoyant un e-mail faisant référence à votre voyage.

Les cyberattaquants utilisent activement d'autres méthodes pour envoyer les mêmes messages, par exemple en vous envoyant des SMS ou même en vous appelant directement par téléphone.

Comment détecter ces attaques d'hameçonnage plus avancées

Comme les cyberattaquants prennent leur temps et recherchent leurs victimes, il peut être plus difficile de repérer ces attaques**.** La bonne nouvelle est que vous pouvez encore les repérer si vous savez ce que vous cherchez. Posez-vous les questions suivantes avant de donner suite à un message suspect :

1. Le message crée-t-il un sentiment d'urgence accru ? Subissez-vous des pressions pour contourner les politiques de sécurité de votre organisation ? Le criminel veut vous pousser à faire une erreur. Plus vous avez une impression d'urgence, plus vous avez de chance que ce soit une arnaque.
2. L'e-mail ou le message a-t-il un sens ? Le PDG de votre entreprise vous enverrait-il un SMS urgent pour demander de l'aide ? Votre superviseur a-t-il vraiment besoin que vous vous précipitiez pour acheter des cartes cadeaux ? Pourquoi votre banque ou votre société de carte de crédit vous demanderait-elle des informations personnelles qu'elle devrait déjà avoir sur vous ? Si le message semble étrange ou déplacé, il peut s'agir d'une attaque.
3. Vous recevez un e-mail lié au travail de la part d'un collègue de confiance ou peut-être de votre superviseur, mais le courriel utilise une adresse personnelle telle que @gmail.com.
4. Vous avez reçu un e-mail ou un message de quelqu'un que vous connaissez, mais la formulation, le ton de la voix ou la signature du message sont erronés et inhabituels.

Si un message semble étrange ou suspect, il peut s'agir d'une attaque. Si vous voulez confirmer qu'un e-mail ou un message est légitime, vous pouvez appeler la personne ou l'organisation qui vous envoie le message en utilisant un numéro de téléphone fiable.

Vous êtes de loin la meilleure défense. Faites preuve de bon sens.

Rédacteur Invité

Phil Hoffman est un consultant en informatique semi-retraité qui a 40 ans d'expérience et se concentre sur l'infrastructure et la sécurité. Il est un collaborateur et rédacteur de longue date de OUCH ! et se passionne pour la technologie, le vélo et la photographie.

Ressources

Ingénierie sociale: https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering
Top trois des arnaques: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Hameçonnage par message: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Arnaques et escroqueries vocales: https://www.sans.org/newsletters/ouch/vishing/
Renseignement de sources ouvertes: https://www.sans.org/security-awareness-training/resources/search-yourself-online

Traduit pour la communauté par : Juliette Busson