La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

Stop au phishing

Vue d'ensemble

Les emails et les services de messagerie (tels que Skype, Twitter ou Snapchat) sont l'un des principaux moyens de communication. Nous utilisons non seulement ces technologies quotidiennement pour travailler mais aussi pour rester en contact avec nos amis et notre famille. En conséquence, beaucoup de personnes dans le monde dépendent de ces technologies, devenues l'une des principales méthodes d'attaque utilisées par les cyber-attaquants, une méthode d'attaque appelée phishing (ou hameçonnage). Apprenez ce qu'est le phishing et comment vous pouvez repérer et arrêter ces attaques, que vous soyez au travail ou à la maison.

Qu'est-ce que le phishing

Le phishing est un type d'attaque qui utilise le courrier électronique ou un service de messagerie pour vous tromper dans une action que vous ne devez pas entreprendre, par exemple cliquer sur un lien malveillant, partager votre mot de passe ou encore ouvrir une pièce jointe infectée. Les attaquants travaillent dur pour rendre ces messages convaincants et appuient sur vos déclencheurs émotionnels, tels que l'urgence ou la curiosité. Ces messages peuvent donner l'impression qu'ils proviennent de quelqu'un ou de quelque chose que vous connaissez, comme d'un ami ou d'une entreprise de confiance. Ils peuvent même ajouter les logos de votre banque ou falsifier l'adresse e-mail pour que le message apparaisse plus légitime. Les attaquants envoient ensuite ces messages à des millions de personnes. Ils ne savent pas qui prendra l'appât, tout ce qu'ils savent c'est que plus ils enverront de messages, plus les victimes seront nombreuses.

Protégez-vous

Dans la plupart des cas, l'ouverture et la lecture d'un e-mail ou d'un message sont acceptables. Pour qu'une attaque de phishing fonctionne, les criminels doivent vous inciter à faire quelque chose. Heureusement, il y a des indices vous permettant de déceler qu'un message est une attaque, voici les plus courants:

- Un énorme sentiment d'urgence, exigeant une «action immédiate» avant que quelque chose ne se passe, comme menacer de fermer un compte ou de vous envoyer en prison. L'attaquant veut vous pousser à faire une erreur.
- Vous mettre la pression pour contourner ou ignorer vos politiques ou procédures au travail.
- Un fort sentiment de curiosité ou quelque chose de trop beau pour être vrai (non, vous n'avez pas gagné à la loterie).

- Une formule générique comme « Cher client ». La plupart des entreprises ou des amis qui vous contactent connaissent votre nom.
- Demander des informations hautement sensibles, telles que votre numéro de carte de crédit ou votre mot de passe ou toute autre information que l'expéditeur légitime devrait déjà connaître.
- Le message indique qu'il provient d'une organisation officielle, mais il a une mauvaise grammaire ou orthographe ou utilise une adresse e-mail personnelle telle que @gmail.com.
- Le message provient d'un e-mail officiel (par exemple, votre patron) mais possède une adresse de réponse vers le compte de messagerie personnel de quelqu'un.
- Vous recevez un message de quelqu'un que vous connaissez, mais le ton ou la formulation ne lui ressemble pas. Si vous êtes suspicieux, appelez l'expéditeur pour vérifier qu'il l'a bien envoyé. Il est facile pour un cyber-pirate de créer un message qui semble provenir d'un ami ou d'un collègue.

En fin de compte, le bon sens est votre meilleure défense. Si un e-mail ou un message vous semble étrange, suspect ou trop beau pour être vrai, il peut s'agir d'une attaque de phishing.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Tonia Dudley développe et exécute des programmes de sensibilisation à la sécurité depuis 2011, ce qui inclut l'élaboration d'un programme primé d'entraînement sur le phishing (ou hameçonnage). Vous pouvez la retrouver sur www.linkedin.com/in/toniadudley.

Sources

Ingénierie sociale :	https://www.sans.org/u/Cb1
Aider les autres à se protéger :	https://www.sans.org/u/Cb6
Faire ou ne pas faire par courriel :	https://www.sans.org/u/Cbg
Fraude au Président :	https://www.sans.org/u/Cbl
OUCH ! Traductions et archives :	https://www.sans.org/u/Cbq

Licence