COMMENT ÉVITER LE PHISHING OU LE SMISHING?

écrit par Yannick Lauwers | mai 2, 2023

Dans notre précédente contribution[1], vous avez pu lire que le phishing était un véritable fléau en 2020 et 2021. Cette forme de cambriolage numérique semble encore particulièrement populaire en 2023. Les « hameçonneurs » (phishers) semblent être très ingénieux et conçoivent régulièrement de nouvelles astuces pour escroquer les gens de leur argent ou de leurs données.

Le phishing est une forme de cybercriminalité dans laquelle la victime potentielle est approchée par courrier électronique, par SMS, par les médias sociaux ou par téléphone. L'escroc se fait passer pour quelqu'un d'autre dans le but d'accéder aux données confidentielles des victimes.

Le smishing constitue la variante SMS du phishing. Par exemple, un SMS envoyé peut contenir un lien qui envoie le navigateur du téléphone vers un site web qui installe un logiciel malveillant (malware). En cliquant sur ce lien, les coordonnées bancaires peuvent être extraites pour dépouiller le compte de quelqu'un.

Ces méthodes d'escroquerie sont également devenues de plus en plus difficiles à repérer au fil des ans. Distinguer les faux e-mails des messages dignes de confiance semble être devenu une tâche presque impossible. Néanmoins, nous souhaitons vous donner quelques conseils pour minimiser le risque de phishing ou de smishing.

Vous avez des doutes sur le caractère suspect d'un message? Répondez brièvement à ces questions par vous-même :[2]

– Le message est-il inattendu ?

– Le message est-il formulé de manière urgente ?

– Connaissez-vous l'expéditeur ?

– La question posée vous paraît-elle étrange ?

– Où mène le lien sur lequel vous devez cliquer ? (Conseil : survolez le lien et voyez où il vous envoie. Il est préférable de ne pas ouvrir un lien suspect).

– Est-ce qu'on s'adresse à vous personnellement ?

– Le message contient-il de nombreuses erreurs de langue ?

– Le message est-il dans vos Spam ?

– Quelqu'un essaie-t-il de vous rendre curieux ?

Conclusion

Le phishing ou smishing est un phénomène qui prend de l'ampleur chaque année. Par conséquent, avec la numérisation grandissante de la société, le problème ne semble pas devoir se résoudre à court terme. Le meilleur conseil que nous puissions vous donner en tant que lecteur est donc de toujours être attentif aux messages « étranges » que vous recevez par e-mail ou par SMS. Un message qui est trop beau pour être vrai l'est généralement.

Une transaction particulière que vous avez effectuée vous paraît suspecte ? Contactez Card Stop dès que possible pour faire bloquer votre carte. Vous pouvez le faire au 070 344 344. Sachez que Card Stop n'appellera jamais les gens. Si quelqu'un se fait passer pour un employé de Card Stop au téléphone, il s'agit à 100% d'un escroc.

Si vous recevez un message suspect par e-mail ou par SMS, n'hésitez pas à le transmettre par e-mail à verdacht@safeonweb.be. Ils vérifient les liens et les

pièces jointes de ces messages transférés et sont en mesure de faire bloquer les liens suspects. De cette façon, les internautes moins observateurs qui ont cliqué sur le lien sont également protégés. Agir rapidement réduit les chances que les cybercriminels fassent des victimes. Un homme averti en vaut deux.

Si vous avez encore des questions sur le phishing après avoir lu cet article, n'hésitez pas à nous contacter à l'adresse joost.peeters@studio-legale.be ou au numéro 03 216 70 70.

[1] https://www.studio-legale.be/phishing-het-nieuwe-inbreken-anno-2021/?lang=nl ; https://www.jubel.be/phishing-het-nieuwe-inbreken-anno-2021/

[2] https://www.safeonweb.be/nl/leer-valse-mails-herkennen