24.11.2021

Les tentatives d'arnaque par courriel sont de plus en plus sophistiquées

Fautes de français et erreurs de présentation permettaient encore jusqu'à il y a quelques années de déceler les emails frauduleux. Bien que la tâche soit aujourd'hui plus difficile, il est encore possible de discerner le vrai du faux.

En envoyant des réponses ciblées à des emails réellement envoyés, des malfaiteurs tentent d'inciter les salariés des entreprises à ouvrir une pièce jointe et poussent la perfidie jusqu'à faire en sorte que le courriel initial apparaisse comme provenant effectivement de la personne à laquelle est adressée la réponse (source : www.cybercrimepolice.ch (http://www.cybercrimepolice.ch)).

En règle générale, on assiste ces dernières années à une professionnalisation croissante des tentatives d'escroquerie sur Internet. Ainsi, les messages de Phishing (https://www.ebas.ch/fr/le-phishing/) reçus par courriel SMS ou WhatsApp sont souvent très crédibles aujourd'hui, aussi bien d'un point de vue de la présentation que du contenu. Et les malfaiteurs ne reculent devant rien pour piéger les consommateurs les moins informés.

La bonne nouvelle : il est encore possible de repérer pratiquement toutes les tentatives d'arnaque, qu'il s'agisse de courriels ou autres systèmes de messagerie. Pour vous protéger, vous et vos dispositifs, il ne vous reste plus qu'à suivre nos conseils :

- Les messages de phishing contiennent presque tous un lien vers un site piraté ou une pièce jointe infectée par un logiciel malveillant. Il convient donc, dans la mesure du possible, de ne jamais ouvrir les liens contenus dans des courriels, SMS ou autre message court, et de toujours taper manuellement l'adresse Internet du service en question (p. ex. votre banque) dans la barre d'adresse de votre navigateur.
- N'ouvrez pas non plus les pièces jointes que vous n'attendez pas ou si vous doutez de l'authenticité du courriel.
- Limitez l'utilisation de vos informations confidentielles (p. ex. identifiants de connexion pour l'e-banking) au but prévu. Ne communiquez jamais ce genre de données à d'autres personnes, pas même aux employés (ou supposés tels) de votre banque ou de toute autre société connue telle que Microsoft ou Apple.
- D'une manière générale, la méfiance est de mise sur Internet. Si vous remarquez quelques bizarreries dans un message, un site web ou un service, contactez votre banque ou le fournisseur sur un canal sécurisé : par téléphone par exemple, en utilisant le numéro direct de votre conseiller client.

Pour en savoir plus et connaître tous les conseils pour se prémunir contre les tentatives de phishing, consultez notre article Phishing (https://www.ebas.ch/fr/le-phishing/).