09.12.2021

Quand Noël rime avec phishing

Il faut toujours redoubler de prudence quand arrivent les fêtes de fin d'année. Les emails d'hameçonnage en particulier sont maintenant devenue une tradition. Cette année, le phénomène est ultérieurement amplifié par l'épidémie de COVID-19 et la numérisation de notre société.

En lançant une attaque de phishing (ou hameçonnage en français), des cybercriminels tentent d'accéder à vos identifiants de connexion, notamment à vos comptes d'e-banking ou de sites marchands. Pour vous protéger ...

- ne cliquez jamais sur un lien reçu par email, SMS ou Messenger, ou que vous auriez obtenu après avoir scanné un code QR, pour vous connecter à un service de banque en ligne.
- ne remplissez jamais de formulaires envoyés par courriel et dans lesquels on vous demande d'indiquer vos identifiants de connexion.
- soyez méfiants à l'égard des pièces jointes de vos courriels et SMS.
- ne révélez au téléphone aucune information confidentielle comme vos mots de passe par exemple.
- tapez toujours manuellement l'adresse de la page d'accueil du site du fournisseur de services ou de la banque dans la barre d'adresse de votre navigateur.
- lorsque la page d'accueil s'affiche, vérifiez la connexion SSL (https:// et symbole du cadenas) et contrôlez l'adresse Internet dans la barre d'adresse du navigateur pour vous assurer que vous êtes bien sur le bon site.
- en cas de doute, contactez toujours directement votre institut financier.