



Vigilance numérique : comment éviter les pièges des mails et sms frauduleux ?

ACTUALITÉ

SÉCURITÉ

Mardi 5 mai 2020

Vigilance numérique : comment éviter les pièges des mails et sms frauduleux ?

L'hameçonnage (ou phishing en anglais) est un SMS ou mail frauduleux destiné à tromper la victime pour l'inciter à communiquer des données personnelles (mot de passe, date de naissance, adresse) et/ou bancaires en se faisant passer pour un service connu ou proche. Cette arnaque courante devient de plus en plus sophistiquée et il est parfois difficile de la repérer. Alors voici 5 points de vigilance pour se protéger d'une tentative de phishing.



Comment repérer et éviter l'hameçonnage ?

1- Vérifier l'expéditeur

Une adresse mail inconnue, inhabituelle ou fantaisiste ? Si l'adresse s'éloigne trop du format d'une adresse officielle, ne comporte pas le nom de l'entité, qu'elle présente des coquilles, ou que le nom vous paraît suspect, c'est probablement une fausseté.

2- S'assurer de la personnalisation du mail

Une méthode d'hameçonnage consiste à envoyer à grande échelle le même mail d'apparence personnalisée à une large base de données d'adresses mail ou de numéros de téléphone. Si le message ne mentionne pas votre nom ou encore s'il utilise une formule vague comme « Cher client privilégié », méfiez-vous.

3- Analyser le sujet

Si le sujet est inattendu ou que vous remarquez des incohérences sur le fond et la forme, entre le mail reçu et vos échanges précédents avec cet interlocuteur, il peut s'agir d'une usurpation de messagerie. Ne répondez pas et signalez le message* si vous le pouvez.

4- Méfiez-vous en cas d'urgence ou de promesse de gain

Si le message contient une offre trop alléchante, une promesse de rémunération ou de remboursement immédiate ou un ton d'urgence qui incite à agir immédiatement, n'agissez jamais sous la pression ! Si l'interlocuteur est sérieux, il vous recontactera.

5- Ne pas cliquer sur des liens ou pièces jointes suspects

La plupart du temps, les services professionnels (Ameli, les impôts, votre banque) ne vous envoient pas de messages vous invitant à cliquer directement sur un lien. Dans le cas où l'expéditeur vous invite à cliquer sur un lien, il est conseillé de se rendre directement sur le site de l'organisme sans cliquer sur le lien du mail. Vous pourrez alors y entrer vos mots de passe en toute confiance. S'il s'agit d'un compte que vous ne connaissez pas, positionnez votre curseur au-dessus du lien sans cliquer afin de vérifier le format de l'adresse et sa vraisemblance. De manière générale, soyez vigilant aux éléments suspects, notamment si le message contient un lien cliquable, une pièce jointe, ou vous demande des informations. Si un doute subsiste, il est toujours préférable de ne pas faire l'action demandée.

Pour vous informer davantage, obtenir une assistance, ou signaler une tentative d'hameçonnage, vous pouvez vous rendre sur le site cybermalveillance.gouv.fr