AKTUALIT&#65533;T

S&#65533;CURIT&#65533;

Dienstag, 5. mai 2026

Vigilance num&#65533;rique : comment &#65533;viter les pi&#65533;ges des mails et sms frauduleux ?

L?hame&#65533;onnage (ou phishing en anglais) est un SMS ou mail frauduleux destin&#65533;s &#65533; tromper la victime pour l?inciter &#65533; communiquer des donn&#65533;es 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 sophistiqu&#65533;e et il est parfois difficile de la rep&#65533;rer. Alors voici 5 points de vigilances pour se prot&#65533;ger d?une tentative de phishing.

Comment rep&#65533;rer et &#65533;viter l?hame&#65533;onnage ?

1- V&#65533;rifier l?exp&#65533;diteur

Une adresse mail inconnue, inhabituelle ou fantaisiste ? Si l?adresse s?&#65533;loigne trop du format d?une adresse officielle, ne comporte pas le nom de l?entit&#65533;, qu?elle pr&#65533;sente des coquilles, ou que le nom vous para&#65533;t suspect, c?est probablement une fausse.

2- S'assurer de la personnalisation du mail

Une m�thode d?hame�onnage consiste � envoyer � grande �chelle le m�me mail d�personnalis� � une large base de donn�es d?adresses mail ou de num�ros de t�l�phone. Si le message ne mentionne pas votre nom ou encore s?il utilise une formule vague comme « Cher client privil�gi� », m�fiez-vous.

3- Analyser le sujet

Si le sujet est inattendu ou que vous remarquez des incoh�rences sur le fond et la forme, entre le mail re�u et vos �changes pr�c�dents avec cet interlocuteur, il peut s?agir d?une usurpation de messagerie. Ne r�pondez pas et signalez le message* si vous le pouvez.

4- M�fiez-vous en cas d?urgence ou de promesse de gain

Si le message contient une offre trop all�chante, une promesse de r�mun�ration ou de remboursement imm�diate ou un ton d?urgence qui incite à agir imm�diatement, n?agissez jamais sous la pression ! Si l?interlocuteur est s�rieux, il vous recontactera.

5- Ne pas cliquer sur des liens ou pi�cesjointes suspects

La plupart du temps, les services professionnels (Ameli, les imp�ts, votre banque) ne vous envoient pas de messages vous invitant à cliquer directement sur un lien. Dans le cas où l?�metteur vous invite à cliquer sur un lien, il est conseill� 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 v�rifier le format de l?adresse et sa vraisemblance. De mani�re g�n�rale, soyez vigilant aux «l�ments suspects, notamment si le message contient un lien cliquable, une pi�ce jointe, ou vous demande des informations. Si un doute subsiste, il est toujours pr�f�rable de ne pas faire l?action demand�e.

Pour vous informer davantage, obtenir une assistance, ou signaler une tentative d?hame�onnage, vous pouvez vous rendre sur le site cybermalveillance.gouv.fr