Déjouer les arnaques par SMS ou par mail

FRANÇOISE LAMBERT

Mails vous invitant à donner vos coordonnées bancaires pour vérifier votre compte, SMS d'une provenance inconnue vous enjoignant, pour un motif prétendument important, à rappeler un numéro, surtaxé évidemment : les arnaques liées aux nouvelles technologies de communication se développent. Comment éviter de tomber dans le panneau...

Vous recevez un mail d'une société ou d'un organisme que vous connaissez vous proposant de mettre à jour vos données personnelles, notamment bancaires, éventuellement en vue d'un prétendu remboursement : sachez que les centres des impôts, les banques et les organismes sociaux n'envoient jamais ce type de messages. Il s'agit sûrement d'une tentative de phishing ou hameçonnage. Il est alors hautement recommandé de ne pas y répondre et de ne pas ouvrir les pièces jointes, les liens ou les images contenus dans le message.

Signaler les mails frauduleux à un service spécialisé

Vous pouvez aussi aider à l'action des pouvoirs publics et des acteurs de l'Internet contre les « spammeurs » en signalant ces messages sur le site

www.signal-spam.fr.

Si vous pensez avoir été victime d'une tentative d'escroquerie, vous pouvez faire un signalement sur la plate-forme Pharos, accessible sur le site

www.internet-signalement.gouv.fr

Votre signalement sera traité par un service de police judiciaire spécialisé et pourra, après vérification, donner lieu à une enquête.

En cas de réception d'un SMS ou d'un spam vocal abusif sur votre **téléphone portable**, vous pouvez le transférer au **numéro 33 700**. Cet envoi est gratuit pour les clients des opérateurs **Bouygues, Orange et SFR**. Chez les autres opérateurs il pourra coûter le prix d'un SMS. Les SMS ou appels vocaux abusifs vont bien souvent vous inciter à rappeler un numéro, surtaxé, en vous annonçant un colis en attente voire… en vous raccrochant au nez. Ne vous fiez pas à l'indication d'un numéro d'appel classique commençant par 01, 02, etc., car vous pourrez être basculé vers un numéro surtaxé.

Pour se prémunir des mails et SMS frauduleux, il convient d'être vigilant, de ne jamais réagir dans l'urgence et de faire preuve de bon sens.

Repères : Qu'est-ce que le phishing ?

Le phishing ou hameçonnage est une technique utilisée par des personnes malveillantes qui se font passer pour un organisme familier (banque, administration, Sécurité sociale) afin de soutirer, par des e-mails frauduleux, des renseignements personnels, comme les mots de passe de comptes bancaires ou les numéros de cartes de crédit.