SENSIBILISATION AUX RISQUES NUMÉRIQUES 5

Recommandations de Cybermalveillance.gouv.fr

	L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

Voici quelques mesures préventives pour éviter ce piège.

1. NE COMMUNIQUEZ JAMAIS D'INFORMATIONS SENSIBLES PAR MESSAGERIE OU TELEPHONE

Aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

2. AVANT DE CLIQUER SUR UN LIEN DOUTEUX, POSITIONNEZ LE CURSEUR DE VOTRE SOURIS SUR CE LIEN…

(Sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

3. VERIFIEZ L'ADRESSE DU SITE QUI S'AFFICHE DANS VOTRE NAVIGATEUR

Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper.

Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

4. EN CAS DE DOUTE,

Contactez si possible directement l'organisme concerne pour confirmer le message ou l'appel que vous avez reçu.

5. UTILISEZ DES MOTS DE PASSES DIFFERENTS ET COMPLEXES POUR CHAQUE SITE ET APPLICATION

Afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels.

Vous pouvez également utiliser des coffres forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.

6. SI LE SITE LE PERMET,

Vérifiez la date et heure de dernière connexion à votre compte afin de repérer si des accès illégitimes ont été réalisés.

7. SI LE SITE VOUS LE PERMET,

Activez la double authentification pour sécuriser vos accès.

SI VOUS ÊTES
VICTIME

- Si vous avez malencontreusement communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte,

  FAITES OPPOSITION IMMÉDIATEMENT

  auprès de votre organisme bancaire ou financier et déposez plainte au commissariat de police ou à la gendarmerie la plus proche.

- Si vous avez constaté que des éléments personnels servent à usurper votre identité,

  DÉPOSEZ PLAINTE

  au commissariat de police ou à la gendarmerie la plus proche.

- Si vous êtes victime d'une usurpation de votre adresse de messagerie ou de tout autre compte,

  CHANGEZ IMMÉDIATEMENT VOS MOTS DE PASSE.

- Si vous avez reçu un message douteux sans y répondre,

  SIGNALEZ-LE À SIGNAL SPAM (Signal-spam.fr)

Vous pouvez également

SIGNALER UNE ADRESSE DE SITE D'HAMEÇONNAGE

À PHISHING INITIATIVE (Phishing-initiative.fr)

qui en fera fermer l'accès.