INFORSUD TECHNOLOGIES
Solutions et impulsions pour l'avenir

HAMEÇONNAGE OU PHISHING
Les bonnes pratiques !

HAMEÇONNAGE OU PHISHING

est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe, données bancaires, etc.) en se faisant passer pour un tiers de confiance.
Il peut s'agir d'un faux email, SMS ou appel téléphonique de votre banque, d'un opérateur de téléphonie, d'un fournisseur d'énergie, d'une administration, etc.

MESURES PRÉVENTIVES

1

NE COMMUNIQUEZ JAMAIS D'INFORMATIONS SENSIBLES PAR MESSAGERIE OU TÉLÉPHONE

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

VÉRIFIEZ TOUJOURS UN LIEN EN LE SURVOLANT AVEC LA SOURIS

Avant de cliquer sur un lien, positionnez votre souris sur ce lien (sans cliquer) ce qui affichera l'adresse vers laquelle le lien pointe réellement. Nous vous recommandons d'aller sur le site de l'organisme directement en passant par vos favoris que vous aurez vous-même créés.

2

3

VÉRIFIEZ 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 pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

EN CAS DE DOUTE, CONTACTEZ L'ORGANISME CONCERNÉ PAR LE MESSAGE

Cet appel pourra confirmer le message ou l'appel que vous avez reçu.

4

5

UTILISEZ DES MOTS DE PASSE DIFFÉRENTS POUR CHAQUE SITE OU APPLICATIONS

Il ne vous viendrait jamais à l'idée d'utiliser la même clé pour toutes les serrures, c'est pourquoi il est recommandé d'avoir un mot de passe différent et robuste pour chaque compte.
Vous pouvez également utiliser des coffres-forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.

VÉRIFIEZ SI L'HEURE ET LA DATE SONT COHÉRENTES

Si le site le permet, vérifiez les dates et heures de dernière connexion à votre compte afin de repérer si des accès illégitimes ont été réalisés, hors des heures de travail.

6

7

ACTIVEZ LA DOUBLE AUTHENTIFICATION

Quand cela est possible et que le site ou l'application vous le permet, activez la double authentification pour sécuriser vos accès.

inforsud-technologies.com 0 811 349 609

RÉFÉRENCÉ SUR LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

INFORSUD TECHNOLOGIES

Solutions et impulsions pour l'avenir

HAMEÇONNAGE OU PHISHING

Les bonnes pratiques !

SI VOUS ÊTES VICTIME ?

1

CONTACTEZ DIRECTEMENT L'ORGANISME CONCERNÉ

Dès le moindre doute, contactez directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

FAÎTES OPPOSITION IMMÉDIATEMENT

Si vous avez communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte bancaire, faîtes opposition immédiatement auprès de votre organisme bancaire ou financier.

2

3

CHANGEZ IMMÉDIATEMENT VOTRE MOT DE PASSE

Changez votre mot de passe immédiatement ainsi que sur tous les autres sites ou services sur lesquels vous l'utilisiez.

CONSERVEZ LES PREUVES

En particulier, le message d'hameçonnage reçu.

4

5

SIGNALEZ LE SPAM

Si vous avez reçu un message douteux sans y répondre : cliquez ici pour signaler votre spam.

SIGNALEZ UNE ADRESSE FRAUDULEUSE DE PHISHING

Vous pouvez également signaler une adresse de site d'hameçonnage à phishing initiative qui en fera fermer l'accès : cliquez ici pour signaler l'adresse.

6

7

DÉPOSEZ PLAINTE

En fonction du préjudice subi (débits frauduleux, usurpation d'identité…) déposez plainte au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.

POUR ÊTRE CONSEILLÉ.E

En cas d'hameçonnage, contactez info escroqueries au **0 805 805 817** (numéro gratuit).

inforsud-technologies.com 0 811 349 609

« Cybermalveillance.gouv.fr – Données originales téléchargées sur Cybermalveillance.gouv.fr, publié le 08/04/2021. »

RÉFÉRENCÉ SUR LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR