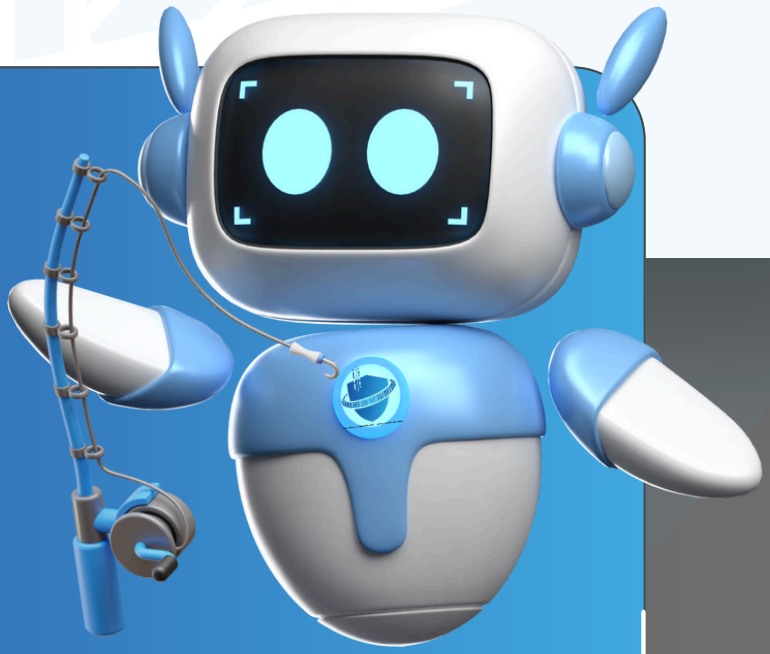
PHISHING ou HAMEÇONNAGE

CENTRE CYBER DU PACIFIQUE

EN BREF

QU'EST-CE QUE C'EST ?

Le phishing (ou hameçonnage en français) est une cyberattaque visant à tromper les utilisateurs pour leur soutirer des informations personnelles sensibles (identifiants, mots de passe, numéros de carte de crédit, etc.). Les attaquants se font passer pour des entités de confiance (banques, entreprises, services en ligne) à travers des emails, des messages ou des sites web falsifiés.



Le phishing est un délit, cela peut être qualifié d'escroquerie (article 313-1 du Code pénal), cela peut impliquer une usurpation d'identité (article 226-4-1 du Code pénal), une fraude informatique (article 323-1 du Code pénal) ou une atteinte à la vie privée et vol de données personnes (articles 226-16 à 226-24 du Code pénal).

QUE FAIRE ?

1. Ne paniquez pas, mais agissez rapidement
2. Changez immédiatement tous vos mots de passe
3. Surveillez vos comptes bancaires
4. Signalez l'email ou le site
5. Analysez votre appareil
6. Informez votre entourage

▶ Voir détail page "Que faire"

COMMENT S'EN PROTEGER ?

- Soyez vigilant face aux emails et messages suspects
- Vérifiez l'URL des sites
- Utilisez un logiciel antivirus et un anti-phishing
- Activez l'authentification à deux facteurs (2FA)
- Méfiez-vous des offres trop alléchantes
- Informez-vous et vos proches

▶ Voir détail page "comment s'en proteger"

PHISHING ou HAMEÇONNAGE

CENTRE CYBER DU PACIFIQUE

QUE FAIRE ?

Le phishing est une menace cyber courante, mais évitable en adoptant de bonnes pratiques. En restant vigilant et en utilisant des outils de sécurité adéquats, vous pouvez réduire considérablement le risque d'être victime d'hameçonnage.
Si vous êtes victime, que vous avez cliqué sur un lien ou donné vos informations, voici les démarches prioritaires à suivre :

1. NE PANIQUEZ PAS
Surtout ne pas paniquer mais agir rapidement et effectuer les tâches suivantes.

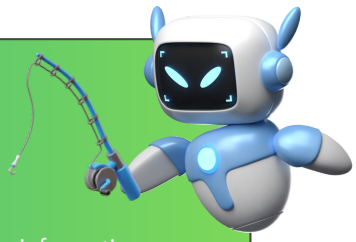
2. CHANGEZ IMMÉDIATEMENT TOUS VOS MOTS DE PASSE
Surtout sur les comptes sensibles (messagerie mail, banque, réseaux sociaux etc.).

3. SURVEILLEZ VOS COMPTES BANCAIRES
Vérifiez s'il y a des transactions suspectes et informez votre banque si nécessaire.

4. SIGNALEZ L'EMAIL OU LE SITE
Le signaler aux autorités compétentes ou à l'entreprise légitime dont le nom a été usurpé.

5. ANALYSEZ VOTRE APPAREIL
Utilisez un logiciel antivirus pour vérifier la présence de logiciels malveillants.

6. INFORMEZ VOTRE ENTOURAGE
Si vous avez partagé des informations compromettantes, prévenez vos contacts qu'ils pourraient aussi recevoir des messages de phishing.



QUEL EST LE PROCÉDÉ D'HAMEÇONNAGE ?

LE PHISHING CONSISTE À :
Envoyer des emails ou messages trompeurs qui semblent provenir de sources légitimes.
Diriger les victimes vers des sites web frauduleux qui imitent des sites légitimes pour voler des informations.
Inciter les victimes à cliquer sur des liens malveillants ou à télécharger des pièces jointes infectées.

LES ATTAQUES DE PHISHING PEUVENT SE MANIFESTER SOUS DIFFÉRENTES FORMES :
Emails d'hameçonnage : demandes frauduleuses d'informations sensibles.
Smishing (via SMS) et Vishing (via appels téléphoniques) : Variation du phishing utilisant d'autres canaux.
Sites web falsifiés : Copie de sites officiels pour voler des données.

PHISHING ou HAMEÇONNAGE

CENTRE CYBER DU PACIFIQUE

COMMENT S'EN PROTÉGER ?

Voici des mesures pour prévenir les attaques de phishing :

Soyez vigilant face aux emails et messages suspects :

- Vérifiez l'expéditeur (adresse email) et méfiez-vous des fautes d'orthographe ou des demandes très urgentes.
- Ne cliquez jamais sur des liens ou pièces jointes non sollicitées, surtout si le message demande des informations sensibles.

Vérifiez l'URL des sites :

Avant de saisir vos informations personnelles, assurez-vous que le site web est légitime. Vérifiez que l'URL commence par "https://" et que le nom de domaine est correct.

Utilisez un logiciel antivirus et un anti-phishing :

Un bon logiciel de sécurité peut détecter et bloquer les tentatives de phishing et protéger vos appareils.

Activez l'authentification à deux facteurs (2FA) :

Pour vos comptes importants (banque, email, réseaux sociaux), ajoutez une couche de sécurité supplémentaire en activant la 2FA.

Méfiez-vous des offres trop alléchantes :

Les attaques de phishing exploitent souvent des promesses trop belles pour être vraies, comme des gains de loterie ou des réductions incroyables.

Informez-vous et vos proches :

Plus vous êtes conscient des risques du phishing, plus vous pourrez reconnaître et éviter ces tentatives. Formez également votre entourage pour les protéger.