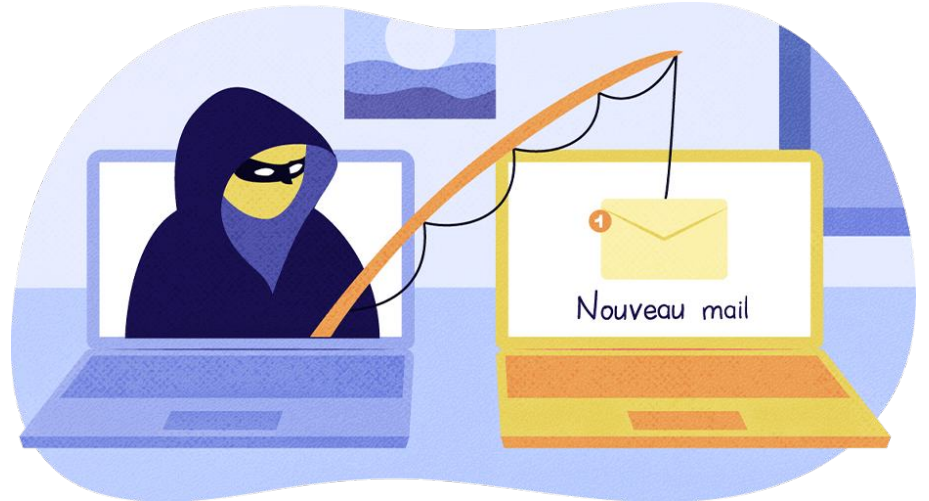


En résumé

Comment se protéger du phishing ?



Qu'est-ce que le phishing ?

- + **Origine** : contraction de "fishing" (pêcher) et "phreaking" (piratage téléphonique).
- + **Objectif** : voler des données personnelles (mots de passe, coordonnées bancaires) pour soutirer de l'argent ou usurper une identité.
- + **Des méthodes variées** : e-mails, SMS, appels téléphoniques ou réseaux sociaux, messages alarmistes incitant à agir rapidement (compte expiré, colis à récupérer, remboursement urgent) ou encore lien vers des pages frauduleuses.

Quelles sont les différentes attaques de phishing ?

- + **Spear Phishing** : ciblage individuel, souvent dans un contexte professionnel, e-mails personnalisés pour augmenter les chances de succès.
- + **Whaling** : vise des dirigeants ou cadres avec accès à des données sensibles.
- + **Clone Phishing** : copie d'un e-mail légitime modifié avec des liens ou pièces jointes malveillants.

Comment éviter de tomber dans le piège ?

- + **Ne jamais communiquer d'informations sensibles** (codes bancaires, mots de passe).
- + **Vérifier l'adresse e-mail de l'expéditeur** et ne pas cliquer sur des liens douteux.
- + Se méfier des **messages trop urgents ou mal rédigés**.
- + **Activer la double authentification** et utiliser des mots de passe uniques.
- + **Installer un antivirus** et mettre à jour ses logiciels de protection.

Que faire en cas d'attaque ?

- + **Si vous avez donné vos identifiants** : Changez immédiatement vos mots de passe.
- + **Si vos coordonnées bancaires ont fuité** : Contactez votre banque pour faire opposition.
- + **Si vous avez un doute** : Signalez l'arnaque sur les plateformes dédiées.

 signal-spam.fr 33700.fr phishing-initiative.fr