

Les conseils de BNP Paribas pour éviter le phishing

1. Qu'est-ce qu'un phishing ?

Les tentatives de phishing, aussi appelées « hameçonnage » ou « filoutage », consistent à tenter de vous soutirer¹ vos mots de passe² via l'envoi d'emails frauduleux.

Vous recevez un email vous invitant à saisir vos données bancaires ou encore vos identifiants³ et codes d'accès sur un site imitant celui de votre banque, afin de les réutiliser à votre insu⁴.

Une fois ces données saisies, vous pouvez être redirigés vers le véritable site, vous indiquant simplement que votre mot de passe est erroné. Vous pouvez alors ne jamais vous rendre compte que vous étiez auparavant sur un site frauduleux.

2. Comment détecter une tentative de phishing ?

L'émetteur du phishing se fait généralement passer pour un acteur bancaire connu : la plupart des emails frauduleux ont pour expéditeur BNP Paribas, BNPPARIBAS.NET, etc.

L'objet de l'email frauduleux est souvent alarmiste sur la gestion de vos comptes ou votre carte bancaire, pour vous inciter à réagir rapidement.

En voici quelques exemples :

- « Rappel : Votre compte sera limité »
- « Nouvelle sûreté contre l'escroquerie⁵ »
- « Nous avons détecté des transactions inhabituelles sur vos comptes »

La plupart du temps, les tentatives de phishing contiennent un message inquiétant et vous proposent de corriger le problème en remplissant un formulaire sur Internet.

(D'après *Savoir affaires*, Petrini, p. 249)

1. **soutirer** : sottrarre

2. **mots de passe** : password

3. **identifiants** : codici bancari

4. **à votre insu** : a vostra insaputa

5. **escroquerie** : frode