

Comment reconnaître un email frauduleux



Quelques bons réflexes du quotidien peuvent vous permettre d'éviter les pièges du phishing ou autres fraudes sur Internet. Au cours de votre navigation soyez vigilant et respectez quelques bonnes pratiques de sécurité.

- [Les bons réflexes contre le phishing](#)
- [Solutions de protection contre le phishing](#)
- [Comment agir face au phishing ?](#)
- [Consultez nos exemples d'emails et de sites frauduleux](#)

Les bons réflexes contre le phishing

Vérifiez la provenance des e-mails reçus

Qui vous adresse ce message ? Si le nom de l'expéditeur est inconnu, cela doit vous alerter.

Lorsque vous recevez des emails commerciaux, vérifiez qu'ils contiennent des éléments permettant d'identifier clairement l'expéditeur :

- le logo et nom de la marque
- des mentions légales
- des mentions liées à la CNIL
- un numéro RCS.

Détectez les indices de phishing

- Informations douteuses ou incohérentes
- Langue étrangère
- Fautes d'orthographe
- Message alarmiste et urgent
- Message concernant votre carte bancaire ou la gestion de vos comptes vous demandant de communiquer des informations telles que vos identifiants de connexion, votre numéro de carte bancaire...

Adoptez les réflexes contre le phishing

Dans le corps de l'email, il est important d'éviter de cliquer trop vite sur les liens proposés et de vérifier la cohérence du message qui vous est adressé. Si vous avez un doute, tapez directement l'url dans votre navigateur ou rendez-vous directement sur le site de la marque. Attention également à l'ouverture de pièces jointes dans un e-mail. Ne les ouvrez que si vous connaissez l'expéditeur.

Bon à savoir : Les e-mails Carrefour Banque contiennent des informations pour assurer le respect de vos données personnelles. L'information RCS suivante :

« *CARREFOUR BANQUE, S.A. au capital de 101 346 956,72 euros, dont le siège social est situé au 1, place Copernic - 91051 ÉVRY Cedex. RCS ÉVRY n° 313 811 515.*

n°ORIAS : 07027516 (www.orias.fr). »

est présente sur l'ensemble de nos communications et atteste de l'identité de Carrefour Banque. Ces informations se trouvent en bas des e-mails. Les e-mails Carrefour Banque sont écrits en respectant l'orthographe et la grammaire.

[Consultez nos exemples d'emails et de sites frauduleux](#)

Solutions de protection contre le phishing

La plupart des navigateurs Internet inclus par défaut un système de détection de sites frauduleux. Ce système permet de vérifier la concordance entre l'adresse d'un site Internet et sa localisation officielle et ainsi de déjouer les copies de sites de banques ou de sites marchands. Lorsque vous consultez votre messagerie depuis un navigateur vous avez donc la possibilité d'être protégé par le phishing mais aussi de le signaler.

Comment agir face au phishing ?

Vous pouvez signaler des sites dont le contenu est illégal ou des emails que vous jugez frauduleux sur le portail officiel de signalement des contenus illicites de l'Internet www.internet-signalement.gouv.fr