



Username

Password

☒ Remember me ☐ Forgot password

Login

COMMENT BIEN LIRE LE NOM D'UN SITE INTERNET ?



- Cherchez la 1^{re} barre oblique « seule » dans l'adresse, après le HTTPS.
<https://www.nomdusite.com/texte/texte/...>
- Retournez de 2 points en arrière dans l'adresse. Ce qui se trouve entre le premier de ces deux points et la barre oblique est le véritable nom du site sur lequel vous serez redirigé si vous cliquez sur le lien.
<https://www.nomdusite.com/texte/texte/...>

EXEMPLES :

- <https://www.digitalwallonia.be/fr/> : digitalwallonia.be est le nom du site web vers lequel vous êtes dirigé.
- <https://digitalwallonia.financement.be/fr/> : vous serez redirigé vers un site appelé « financement.be », et non pas vers digitalwallonia.be.

OÙ TROUVER L'ADRESSE DU SITE INTERNET ?

- Pour un SMS, lisez simplement le nom de domaine² contenu dans le message.
- Pour un e-mail, le lien peut être dissimulé derrière un bouton. Passez simplement votre souris sur le bouton sans cliquer et vous verrez apparaître l'adresse du site. Si vous lisez l'e-mail sur un téléphone portable, vous pouvez appuyer sur le lien pendant quelques secondes sans le lâcher, et l'adresse du site s'affichera directement sur votre écran.
- Si vous recevez un message contenant un QR Code ou un lien court (exemple : lien commençant par « bit.ly ») et que vous doutez de son origine, il est préférable de le supprimer immédiatement, sans cliquer sur le lien.

PHISHING : COMMENT RECONNAÎTRE LES MESSAGES FRAUDULEUX ?

Le phishing (ou hameçonnage) se cache derrière des e-mails, des SMS et des sites web frauduleux, visant à tromper les utilisateurs pour leur soutirer des informations confidentielles. Cyberwal by Digital Wallonia, le programme wallon de la cybersécurité, vous propose des conseils pratiques pour reconnaître les messages de phishing.

COMMENT DÉTECTER UN MESSAGE DE PHISHING ?

Trois techniques sont à **combiner** :

1. LES FAUTES D'ORTHOGRAPHE OU DE SYNTAXE¹

Jusqu'il y a peu, les messages de phishing étaient truffés de fautes, ce qui les rendait facilement reconnaissables. Aujourd'hui, ce n'est plus toujours le cas. L'orthographe reste donc seulement un indice et non un critère unique.

2. L'IDENTITÉ DE L'EXPÉDITEUR

Il convient de vérifier si l'adresse e-mail correspond bien au nom de la personne ou de l'entreprise qu'elle prétend représenter. Attention toutefois : dans certains cas, les fraudeurs sont désormais capables d'envoyer des e-mails en utilisant l'adresse e-mail de la véritable personne.

3. LE LIEN DU SITE VERS LEQUEL VOUS ÊTES REDIRIGÉ

À titre d'exemple, si vous recevez un message prétendant provenir de votre opérateur téléphonique, vous informant que votre facture n'a pas été payée et vous demandant de cliquer sur un lien, vous devez vérifier si le nom du site correspond bien à celui de votre opérateur téléphonique. Cette 3^e technique nécessite de **savoir lire le nom d'un site internet** (👁️) et de savoir comment lire cette adresse **sans cliquer sur le lien suspect**.

FAITES APPEL AUX AUTORITÉS COMPÉTENTES

Si, malgré ces conseils, vous avez été victime de phishing, vous pouvez signaler l'incident sur la plateforme belge SafeOnWeb, mise en place par le Centre pour la Cybersécurité belge : <https://safeonweb.be/fr>

Vous pouvez également transférer directement vos mails de phishing à l'adresse suspect@safeonweb.be

Plus d'infos sur le programme wallon de cybersécurité : www.digitalwallonia.be/cyberwal



¹ Syntaxe : règles d'organisation des mots d'une phrase pour qu'elle soit claire, correcte et cohérente
² Nom de domaine : partie centrale de l'adresse (après « www » ou « https » et avant l'extension « be », « com »...)