

Reconnaître un e-mail de phishing

Les 5 signes qui trahissent un message frauduleux — et la règle des 60 secondes.

LES 5 SIGNES

1

L'adresse réelle ne correspond pas

Regardez l'adresse complète de l'expéditeur, pas le nom affiché : paypal.com n'est pas paypal.com.

2

Urgence artificielle

« Sous 24 h », « action immédiate » : la pression est elle-même le signal d'alarme.

3

Le lien ne mène pas où il affiche

Survolez sans cliquer : la vraie destination s'affiche en bas de l'écran. Appui long sur mobile.

4

Pièce jointe inattendue

Principal vecteur des rançongiciels. Confirmez par un autre canal avant d'ouvrir — et sauvegardez vos fichiers.

5

Demande d'informations sensibles

Aucun organisme légitime ne demande mot de passe ou numéro de carte par e-mail.

La règle des 60 secondes

1. Fermez l'e-mail — sans répondre, sans cliquer.
2. Ouvrez un nouvel onglet et allez vous-même sur le site officiel.
3. Vérifiez si le problème existe vraiment. Presque toujours : non.

L'urgence est leur arme. Le temps est la vôtre.

Signaler et réagir

E-mails frauduleux : transférez-les à Signal Spam (signal-spam.fr) · SMS : au 33700.

Pièce jointe ouverte par erreur : analyse antivirus + changez vos mots de passe.

Assistance officielle et gratuite : cybermalveillance.gouv.fr