

Phishing : les bons réflexes pour ne pas vous faire avoir

Un faux message ressemble à un vrai. Quatre réflexes simples suffisent à vous protéger.

RECONNAÎTRE



01

Vérifiez l'expéditeur

Un seul caractère change, et c'est un piège. Survolez un lien sans cliquer : son vrai nom s'affiche.

 micr0s0ft.com microsoft.com

02

Méfiez-vous de l'urgence

« Compte bloqué sous 24 h », « action immédiate »... Les escrocs jouent sur la peur pour vous faire cliquer.

Prenez 2 minutes pour vérifier.



03

Téléphone et QR code

Faux « support it » au téléphone, faux site derrière un QR code : même danger qu'un mail.

 Je raccroche et je rappelle le numéro officiel Je ne scanne pas et je vais sur le site officiel

04

Mot de passe : jamais sur un lien

Même si le message semble venir d'un collègue, ça peut être un vrai piège. Le faux site peut ressembler au site officiel

Ouvrez vous-même le site officiel

RÉAGIR

Un doute ?

- 1 Ne cliquez sur rien
- 2 Ne répondez pas
- 3 Demandez à la DSI

Déjà cliqué ?

Ça arrive à tout le monde. Prévenez la DSI tout de suite et dites ce que vous avez fait : lien, pièce jointe, mot de passe saisi. Plus on agit vite, moins il y a de dégâts.

TRANSMETTRE



Signalez-le à la DSI



Prévenez vos collègues



Partagez ce guide