AFFISEO

Mémo : reconnaître un faux e-mail en 30 secondes



Guide offert · Reconnaître un faux e-mail d'hameçonnage avant qu'il te coûte cher

DANS CE MÉMO

7	9	1	2
points à garder	cases à cocher	infographie	schémas

POUR ALLER PLUS VITE

FORMATION GRATUITE

Les formations gratuites

9 formations, vidéos et PDF, sans carte bancaire

YOUTUBE

Ma chaîne YouTube

Mes tests et mes coulisses en vidéo

Par Romain Brunel, entrepreneur et AI business builder

L'ESSENTIEL

Les points à garder

1. Les 5 questions avant de cliquer, dans l'ordre
2. Lire le domaine après le @ et dans un lien, de droite à gauche
3. SPF, DKIM, DMARC : ce qu'un « PASS » prouve et ne prouve pas
4. Un mail qui connaît ton IBAN peut être faux
5. Changement de RIB : contre-appel au numéro connu, toujours
6. Les gestes dans l'ordre si tu as cliqué
7. Où signaler : Signal Spam, Phishing Initiative, 33700, PHAROS

MON AVIS

Il faut arrêter d'apprendre aux gens à chercher le cadenas. C'était un bon réflexe il y a longtemps, aujourd'hui il rassure surtout les victimes. Le seul réflexe qui tient, c'est de lire le domaine.

À COCHER

Ta check-list

- [ ] Mettre en favori les sites de ta banque, des impôts, de ta boutique et de ton outil de paiement
- [ ] Vérifier le domaine après le @ de chaque mail qui demande une action
- [ ] Survoler chaque lien avant de cliquer et lire le domaine de droite à gauche
- [ ] Ne jamais ouvrir une pièce jointe imprévue sans confirmation par un autre canal
- [ ] Activer la double authentification sur ta messagerie et ta banque
- [ ] Installer un gestionnaire de mots de passe
- [ ] Fixer une règle : aucun changement de RIB sans contre-appel au numéro connu
- [ ] Créer ton compte Signal Spam et signaler le prochain faux mail
- [ ] Noter quelque part le 0 805 805 817 et le 116 006 en cas de souci

MES NOTES

Reconnaître un faux e-mail

Le mémo à garder sous la main

L'ESSENTIEL EN 1 COUP D'ŒIL

1 L'hameçonnage

Un faux expéditeur de confiance
veut tes codes ou ton argent

2 33 %

des demandes d'aide en 2025
particuliers, +71 % en 1 an

Au moindre doute

je ferme le mail,
j'ouvre le site moi-même

3 5 questions

Attendu ? Domaine après le @ ?
Lien ? Demande ? Pression ?

4 Il sait ton IBAN ?

Ça prouve une fuite,
pas l'expéditeur

5 Tu as cliqué

Banque, mots de passe, preuves, plainte

Signaler : Signal Spam, 33700, Phishing Initiative

Source : Cybermalveillance.gouv.fr, mars 2026

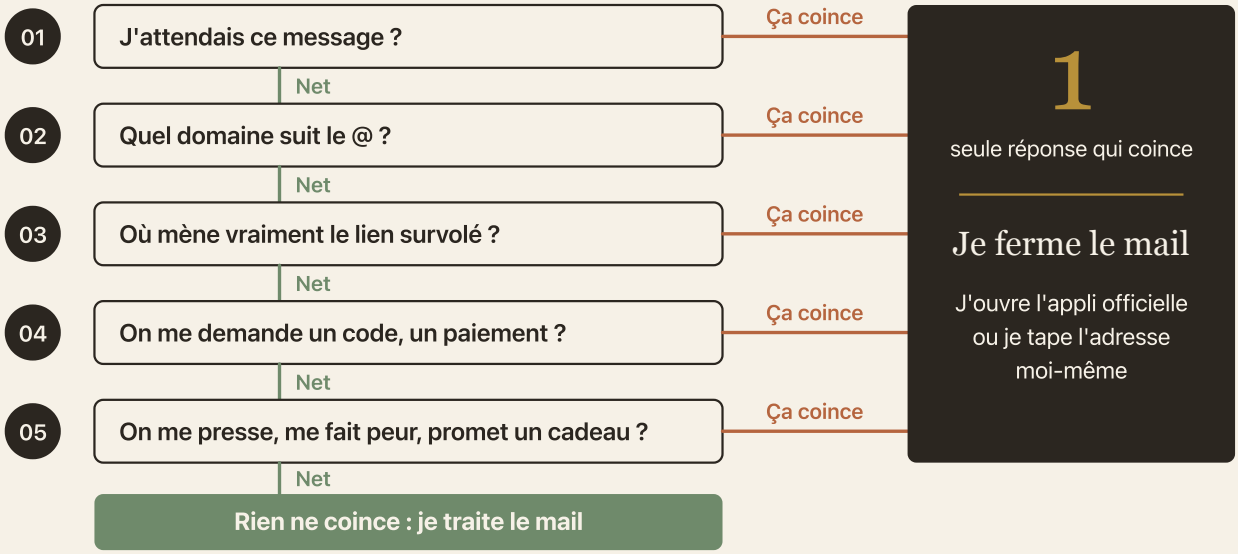
affiseo.fr

EN SCHÉMAS

Pour visualiser

5 questions avant de cliquer

Toujours dans le même ordre : 30 secondes une fois le pli pris



affiseo.fr

Le nom affiché ne prouve rien

Seul le domaine après le @ dit qui envoie vraiment

01 / CE QUE TU VOIS

Le nom affiché

Libre

n'importe qui peut l'écrire

- « Service des impôts »
- « Support Shopify »

02 / CE QU'IL FAUT LIRE

L'adresse complète

Après @

le domaine, lu jusqu'au bout

- Lettre doublée : impots.gouvv.fr
- Mot ajouté : securite-client-banque.com

« PASS » en SPF, DKIM, DMARC : vrai domaine, pas forcément honnête

affiseo.fr

POUR ALLER PLUS LOIN

Et maintenant ?

Ce mémo te donne l'essentiel. Pour passer à l'action pas à pas, je t'ai préparé des formations gratuites, sans carte bancaire.

FORMATION GRATUITE

Les formations gratuites

9 formations, vidéos et PDF, sans carte bancaire

Voir les formations gratuites ›

QUAND TU VEUX ALLER PLUS LOIN

Le HUB AFFISEO

Mes OS IA, les lives mensuels, 500+ élèves

Découvrir le Hub ›

Romain