



Comment survivre à une tentative de phishing

Le phishing — l'hameçonnage — est le point de départ de la majorité des cyberattaques. Un message imite un service que vous connaissez pour vous faire saisir vos identifiants ou ouvrir un fichier. **Ce qui compte, c'est ce que vous faites dans les minutes qui suivent le clic.**



Reconnaître le message

SIX SIGNAUX

- Une **urgence artificielle** : compte bloqué, colis en attente, dernier avertissement.
- Une **adresse d'expéditeur presque juste**, à une lettre ou un domaine près.
- Un **lien qui ne mène pas où il prétend** — survolez-le pour voir l'adresse réelle.
- Une **demande d'informations** qu'un service légitime ne réclame jamais par message.
- Une **pièce jointe inattendue**, surtout un document demandant d'activer les macros.
- Un **ton, une mise en page ou une formulation** légèrement décalés par rapport à l'habitude.



Vous avez cliqué, ou saisi vos informations

URGENCE

- 1 Coupez la connexion.**
Si un fichier s'est téléchargé ou si une installation s'est lancée, analysez ensuite l'appareil avec un antivirus à jour.
- 2 Changez le mot de passe du service concerné.**
Depuis un autre appareil, immédiatement : les identifiants volés sont utilisés dans les minutes qui suivent.
- 3 Changez-le aussi partout où vous l'aviez réutilisé.**
En commençant par votre messagerie.
- 4 Activez l'authentification multifacteur.**
Sur le compte visé, elle bloque l'attaquant même s'il détient déjà le mot de passe.
- 5 Si vous avez communiqué des données bancaires, appelez votre banque.**
Sans attendre, et faites opposition. Signalez l'opération comme frauduleuse.
- 6 Surveillez vos comptes.**
Pendant les semaines suivantes : connexions inhabituelles, messages envoyés, prélèvements inconnus.



Vous n'avez pas cliqué

BON RÉFLEXE

- **Ne répondez pas** — une réponse, même agacée, confirme que l'adresse est active.
- **Signalez le message** via le bouton « signaler comme hameçonnage » de votre messagerie : cela protège les autres destinataires.
- **Prévenez le service imité** s'il propose une adresse de signalement, puis supprimez le message.
- **En cas de doute sur un message légitime**, n'utilisez pas le lien : allez sur le site officiel en tapant l'adresse vous-même, ou appelez le numéro figurant sur vos documents.



À ne pas faire

- ✗ Transférer le message à vos proches « pour les prévenir » : le lien reste actif et circule.
- ✗ Ouvrir la pièce jointe « juste pour voir de quoi il s'agit ».
- ✗ Se dire qu'il est trop tard une fois le mot de passe saisi — le changer immédiatement suffit souvent à devancer l'attaquant.



Pour éviter que cela recommence

PRÉVENTION

- **Ne passez jamais par le lien d'un message** pour vous connecter à un compte : passez par vos favoris ou l'application officielle.
- **L'authentification multifacteur transforme un mot de passe volé en information inutile.**
- **Un gestionnaire de mots de passe ne remplit rien sur un faux site** : s'il ne propose pas vos identifiants, c'est un signal d'alerte.
- **Prenez trente secondes** avant d'agir sur un message urgent : l'urgence est l'outil principal de l'attaquant.

OJCS — Organisation des Jeunes pour un Cyberspace Sécurisé · Guide de survie cyber, fiche 4 sur 6.

Fiche librement reproductible avec mention de la source. Campagne inspirée du *Cyber Survival Guide* de la National Cybersecurity Alliance.