

Comment reconnaître un mail de phishing ou d’hameçonnage ?

Publié le 25/10/2021 Mis à jour le 12/02/2026 12 minutes de lecture

Le **phishing** ou **hameçonnage** est une technique frauduleuse destinée à leurrer un internaute pour l’inciter à communiquer des données personnelles en se faisant passer pour un service connu ou un proche. Si les tentatives d’hameçonnage sont aujourd’hui de mieux en mieux réalisées, **un mail de phishing présente souvent des signes d’alerte** qu’il est possible de déceler : offre alléchante, apparence suspecte, pièce jointe inattendue, adresse d’expédition fantaisiste…

- [Comment repérer un mail de phishing ?](#)
- [Quelles sont les formes les plus courantes de phishing par email ?](#)

dailymotion est désactivé

Autorisez le dépôt de cookies pour accéder à cette fonctionnalité.

Autoriser les contenus dailymotion

Service d’assistance

Victime d’une cybermalveillance ?

Démarrer un diagnostic

Comment repérer un mail de phishing ?

Si les emails de phishing sont conçus pour être quasi-similaires aux mails dont ils ont usurpé l’identité, il est parfois possible de repérer les signaux d’une tentative de phishing. Bien que l’hameçonnage se présente sous diverses formes, on retrouve en effet souvent des indicateurs similaires. En voici une liste non exhaustive.

Si vous repérez un ou plusieurs de ces signaux d’alerte, et au moindre doute, contactez l’expéditeur via un autre canal afin de vérifier qu’il est bien à l’origine du message et qu’il ne s’agit pas d’un mail de phishing et d’une usurpation d’identité.

1. Une notification de la messagerie ou de l’antivirus

Votre messagerie ou votre antivirus peuvent vous signaler la réception d’un mail frauduleux. N’ignorez pas leur avertissement et **assurez-vous régulièrement que votre antivirus est activé et à jour**.

2. Un email d’un service ou d’une société dont vous n’êtes pas client

Les cybercriminels n’ont généralement pas accès aux bases de données d’utilisateurs des entreprises dont ils usurpent l’identité et envoient parfois leur mail de phishing au hasard. **Si vous recevez un email d’un service ou d’une société dont vous n’êtes pas client, méfiez-vous. Attention cependant, un cybercriminel peut également s’en prendre aux vrais clients** d’un service ou d’une société, soit parce que le hasard voudra que dans leur envoi de masse leur message de phishing soit adressé à des clients du service usurpé, soit parce qu’ils ont réussi à récupérer une base d’adresses des clients du service concerné .

3. Mail phishing : un nom d’expéditeur inhabituel

La réception d’un message inattendu d’une adresse email inhabituelle, que vous ne connaissez pas ou qui ne fait pas partie de vos contacts, doit éveiller votre attention, même si celle-ci est d’apparence légitime. Si l’adresse email de l’expéditeur vous paraît suspecte, posez-vous les questions suivantes : connaissez-vous l’expéditeur ? Est-il possible que ce dernier vous adresse un message ? Est-ce que le contenu du message vous est réellement destiné ? Est-ce que le sujet abordé vous parle ? S’il s’agit d’un mail de phishing envoyé à échelle industrielle, il sera en effet très peu personnalisé.

4. Une adresse d’expédition fantaisiste

La plupart des phishing par email utilisent des adresses de messagerie qui ne ressemblent pas à des adresses officielles. **Pour vérifier qu’il s’agit bien d’un message officiel, pensez à vérifier l’adresse email de l’expéditeur**. Si cette dernière ne comporte pas le nom de l’entité, qu’elle présente des fautes d’orthographe ou que le nom vous paraît suspect, n’ouvrez pas le message. Il s’agit sûrement d’un mail frauduleux.

5. Un objet d’email trop alléchant ou alarmiste

L’objet d’un mail de phishing est généralement sommaire et cherche à inciter la victime à ouvrir le message. **Un intitulé aguicheur ou inquiétant** – comme « remboursement » ou « alerte de sécurité » – qui transmet un sentiment d’urgence inhabituel.

6. Une apparence suspecte

De nouveaux phishing sont créés chaque jour et les cybercriminels redoublent de créativité pour mettre au point des stratagèmes innovants. Si les méthodes employées sont donc de plus en plus sophistiquées, **certains phishing par email revêtent néanmoins une apparence douteuse**. Images et logos de mauvaise qualité, flous, déformés, pixelisés ou pris de loin, peuvent être le signe qu’il s’agit de captures d’écran ou d’éléments volés sur des sites officiels. Idem si le message vous semble légitime mais que son apparence ne semble plus d’actualité (logo désuet). **De manière générale, si vous observez des différences entre l’apparence de l’email reçu et celle des mails habituels, méfiez-vous**. Il peut arriver que des bugs surviennent mais ces anomalies doivent vous mettre en alerte : il s’agit peut-être d’un mail de phishing.

7. Une absence de personnalisation

Généralement, les emails officiels qui vous sont adressés mentionnent votre nom, or l’**hameçonnage « bon marché » consiste à envoyer à échelle industrielle le même mail de phishing de manière dépersonnalisée** à une large base de données d’adresses mail. Si le message ne mentionne pas votre nom ou encore qu’il utilise une formule un peu vague de type « Cher client privilégié », méfiez-vous.

8. Une demande inhabituelle

Connaître l’adresse email de l’expéditeur n’est pas un critère de confiance absolu : le cybercriminel peut avoir usurpé l’adresse de messagerie d’un proche ou d’un service connu. Remarquez-vous une incohérence, sur la forme ou le fond, entre l’email reçu et ceux que l’expéditeur vous envoie d’habitude ? Soyez vigilant aux éléments suspects, notamment si le message contient un lien cliquable, une pièce jointe, ou vous demande des informations.

9. Une demande d’informations confidentielles

En règle générale, les demandes d’informations personnelles – identifiants de connexion, informations bancaires… – ne se font jamais par email. Aucune entité légitime, gouvernementale, professionnelle ou autre n’est en droit de vous demander votre code de carte bancaire ou vos codes d’accès personnels par message. **Ne communiquez rien de confidentiel par écrit**, même s’il s’agit d’un expéditeur qui prétend faire partie de votre entourage.

10. Un message aguicheur ou inquiétant

Un mail de phishing fait souvent part d’une offre, d’un remboursement ou d’un gain inespéré. Vous venez de remporter un lot important alors que vous n’avez pas joué et que vous n’êtes pas client de l’entreprise qui vous a soi-disant envoyé le message ? Il s’agit probablement d’une tentative de phishing. **Un mail frauduleux peut également faire état d’un besoin urgent ou d’une menace imminente qui requiert une action immédiate**, comme la fermeture de votre compte si vous n’agissez pas tout de suite. En pressant leurs victimes, les cybercriminels tentent de les déstabiliser et de les pousser à prendre des décisions erronées.

11. Mail phishing : des fautes de français surprenantes

Soyez vigilant à la qualité du texte de l’email. L’hameçonnage par mail comporte souvent des fautes de frappe, d’orthographe ou de grammaire. Des erreurs de formulation, de mauvaise traduction ou une syntaxe inhabituelle dans des communications officielles doivent également vous alerter. Certains textes de phishing proviennent de l’étranger et sont traduits par des logiciels, ce qui peut expliquer des tournures de phrases inhabituelles et des caractères accentués mal retranscrits. Toutefois, on constate au fil du temps que le niveau de français des tentatives d’hameçonnage s’améliore de plus en plus. Faites donc preuve de vigilance.

12. Une incitation à cliquer sur un lien ou une pièce-jointe

Un mail de phishing cherche généralement à pousser la victime à cliquer sur un lien. Même si le lien semble rediriger vers la page officielle d’un site, il l’amènera sur une page frauduleuse ressemblant beaucoup au site officiel. Avant de cliquer, pensez à vérifier l’adresse des sites web mentionnés. Pour cela, positionnez le curseur de votre souris sur le lien proposé sans cliquer afin d’afficher le lien complet et l’adresse où il mène réellement. S’agit-il bien de l’adresse officielle du site annoncé dans le message ? Si l’adresse n’est pas ressemblante, qu’elle est mal orthographiée, qu’elle ne vous dit rien et que le lien vous paraît douteux, il s’agit peut-être d’une tentative d’hameçonnage. Lisez attentivement les liens avant de cliquer. Parfois, un seul caractère peut changer dans l’adresse du site pour vous tromper. Pour vérifier que l’adresse correspond exactement à la page de connexion officielle, rendez-vous directement sur le site de l’organisme en question en saisissant manuellement son adresse dans votre navigateur.

Un mail de phishing peut également vous inciter à ouvrir ou télécharger une pièce jointe (une image, un fichier audio ou vidéo, un document PDF, une pièce jointe au format HTML...). Évitez ainsi de cliquer sur des pièces jointes que vous n’attendiez pas, envoyées par des expéditeurs inconnus ou douteux. Une fois ouverte, la pièce jointe peut vous rediriger vers un site frauduleux vous réclamant des informations confidentielles, voire installer un virus sur votre ordinateur ou votre téléphone.

Le cas du spear phishing ou attaque par hameçonnage ciblé

Le spear phishing est une forme d’hameçonnage sur-mesure qui fait appel à des techniques d’usurpation d’identité et d’ingénierie sociale avancées afin que l’objet et le contenu de l’email soit en totale cohérence avec l’activité exercée par la victime. Ce type de mail de phishing très sophistiqué usurpe l’identité d’une personne morale ou physique connue du destinataire dans le but de le leurrer et l’inciter à ouvrir une pièce jointe frauduleuse ou cliquer sur un lien malveillant. Via cette opération, le cybercriminel peut infiltrer l’appareil de la victime et même par rebond le système d’information de son organisation.

Quelles sont les formes les plus courantes de phishing par email ?

De nouveaux phishing sont créés chaque jour et les techniques employées par les cybercriminels sont de plus en plus innovantes. Il n’est donc pas possible de réaliser une liste exhaustive de toutes les formes d’arnaques par hameçonnage existantes. Cependant on peut recenser les formes de phishing par email les plus courantes et les identités les plus susceptibles d’être usurpées.

1. Exemples de mails qui doivent vous alerter

La plupart des phishing par email peuvent être classés dans plusieurs catégories. Voici les exemples que vous êtes le plus susceptible de rencontrer en cas de mail frauduleux :

- **Demande de mise à jour ou de confirmation de données personnelles** – identifiants, mots de passe, coordonnées bancaires… – par un prétendu organisme public ou commercial de confiance, sous peine de sanction.
- **Défaut de paiement ou problème de facturation** : un faux mail vous informe qu’un bien ne peut être expédié en raison d’un problème de facturation ou que vous devez régler un impayé.
- **Demande d’informations inattendue** pour un remboursement, une annulation de commande, une livraison, etc.
- **Demande d’informations contre l’envoi d’un cadeau** ou pour participer à un jeu-concours avec un gain attrayant, ou encore pour récupérer le gain d’une loterie.
- **Demande de règlement** pour éviter la fermeture d’un accès, la perte d’un nom de domaine ou une prétendue mise en conformité RGPD.
- **Appel aux dons frauduleux**.
- **Appel à l’aide** : le cybercriminel se fait passer pour un proche, expliquant qu’il se trouve dans une situation désastreuse qui requiert votre aide financière.
- **Les chaînes d’emails** type porte-bonheur, pyramide financière, appel à solidarité ou alerte virale, peuvent dissimuler une tentative de phishing.

2. Exemples d’identités susceptibles d’être empruntées

L’usurpation d’identité étant la base de l’hameçonnage, les cybercriminels n’hésitent pas à se faire passer pour des organismes connus de tous lorsqu’ils adressent un mail frauduleux.

- Les administrations comme le Trésor public (les impôts), la Sécurité sociale (ameli), la Caisse d’assistance familiale (Caf), etc.

Exemple d’un message frauduleux aux couleurs de l’Assurance Maladie.

- [Les banques](#)

À propos des cookies sur www.cybermalveillance.gouv.fr

Nous utilisons des cookies pour vous offrir une expérience utilisateur de qualité, mesurer l’audience, intégrer des contenus multimédias et provenant de réseaux sociaux. Le dépôt de ces cookies est soumis à l’obtention de votre consentement préalable, à l’exception de certains cookies nécessaires au fonctionnement du site et du cookie de mesure d’audience MATOMO exempté de consentement.

Vous pouvez paramétrer votre choix finalité par finalité, en cliquant sur **«paramétrer les cookies»**. Ces choix sont modifiables à tout moment : [Cliquez ici pour modifier vos préférences](#).

Vous pouvez choisir de ne pas autoriser le cookie MATOMO en installant un cookie d’exclusion : [Cliquez ici pour installer le cookie d’exclusion](#).

Le GIP ACYMA est responsable de traitement des cookies, sauf pour les cookies tiers. Le traitement est basé sur l’intérêt légitime du GIP ACYMA. Pour plus d’informations sur les cookies, voir notre [politique de confidentialité](#).

[Paramétrer les cookies](#)

[Tout Refuser](#)

[Tout accepter](#)

en ligne (Cloud)

- Les sociétés de livraison
- Les systèmes de paiement en ligne

Pour aller plus loin

Comment se protéger du phishing ? Que faire si on est victime d'hameçonnage ? Comment signaler un phishing par email ? Quelles infractions peuvent être retenues contre les auteurs d'un mail de phishing ? Retrouvez l'ensemble de nos conseils dans notre [article dédié](#). Retrouvez également les principales formes de phishing existantes dans notre [dossier thématique](#).

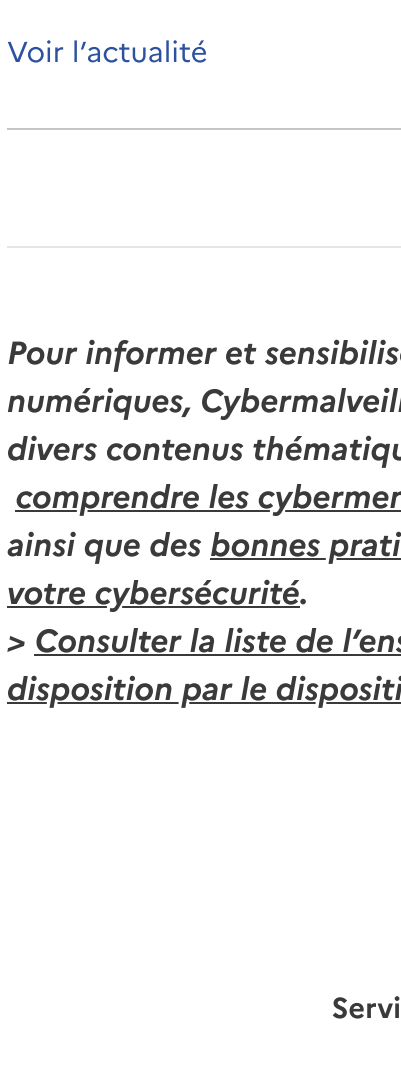


L'hameçonnage ou phishing

Apprenez à repérer et vous prémunir de l'hameçonnage grâce à notre fiche réflexe consacrée au sujet.

Publié le 26/06/2023
PDF 163 Ko

[TÉLÉCHARGER](#) [LIRE](#)



L'hameçonnage ou phishing en fiche mémo

Apprenez à repérer et vous prémunir de l'hameçonnage grâce à notre fiche mémo consacrée

au sujet.

Publié le 02/01/2026
PDF 569 Ko

[TÉLÉCHARGER](#) [LIRE](#)

A LIRE AUSSI



?

Comment signaler un mail de phishing ou d'hameçonnage

[Voir l'actualité](#)

Pour informer et sensibiliser les publics sur les menaces numériques, [Cybermalveillance.gouv.fr](#) met à disposition divers contenus thématiques : des supports variés pour [comprendre les cybermenaces et savoir comment y réagir](#), ainsi que des [bonnes pratiques à adopter pour assurer votre cybersécurité](#).

> [Consulter la liste de l'ensemble des ressources mises à disposition par le dispositif.](#)

Service d'assistance

Victime d'une cybermalveillance ?

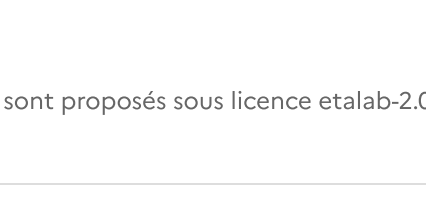
Démarrer un diagnostic

Le contenu proposé vous a-t-il été utile ?

Oui

Non

Partager cet article



Abonnez-vous à la lettre d'information

Abonnement * Tous publics Professionnels

En renseignant votre adresse électronique, vous acceptez de recevoir nos actualités par courriel. Vous pouvez vous désinscrire à tout moment à l'aide des liens de désinscription ou en nous contactant.

Suivez-nous sur les réseaux sociaux

RÉPUBLIQUE FRANÇAISE

Cybermalveillance.gouv.fr
Assistance et prévention en cybersécurité

[GOUVERNEMENT.FR](#) [ELYSEE.FR](#) [SERVICE PUBLIC](#) [LEGIFRANCE](#) [FRANCE.FR](#)

[DATA.GOUV.FR](#)

[Mentions légales](#) | [Politique de confidentialité](#) | [Accessibilité](#) | [Politique des cookies](#) | [Gestion des cookies](#) | [Plan du site](#)

Sauf mention explicite de propriété intellectuelle détenue par des tiers, les contenus de ce site sont proposés sous licence etalab-2.0

À propos des cookies sur [www.cybermalveillance.gouv.fr](#)

Nous utilisons des cookies pour vous offrir une expérience utilisateur de qualité, mesurer l'audience, intégrer des contenus multimédias et provenant de réseaux sociaux. Le dépôt de ces cookies est soumis à l'obtention de votre consentement préalable, à l'exception de certains cookies nécessaires au fonctionnement du site et du cookie de mesure d'audience MATOMO exempté de consentement.

Vous pouvez paramétrer votre choix finalité par finalité, en cliquant sur **«paramétrer les cookies»**. Ces choix sont modifiables à tout moment : [Cliquez ICI pour modifier vos préférences](#).

Vous pouvez choisir de ne pas autoriser le cookie MATOMO en installant un cookie d'exclusion : [Cliquez ICI pour installer le cookie d'exclusion](#).

Le GIP ACYMA est responsable de traitement des cookies, sauf pour les cookies tiers. Le traitement est basé sur l'intérêt légitime du GIP ACYMA. Pour plus d'informations sur les cookies, voir notre [politique de confidentialité](#).