

# Comment détecter e-mail malveillant

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



**Comment détecter e-mail malveillant**

Via votre messagerie ou votre boîte mail, certaines personnes malintentionnées tentent de mettre la main sur vos données personnelles en utilisant des techniques d'hameçonnage (phishing) ou d'escroquerie de type fraude 419 (scam) ! Ces techniques d'attaque évoluent constamment. Les conseils suivants vous aideront à déterminer si un message est légitime ou non.

## Comment repérer une arnaque reçue dans votre messagerie ou votre boîte mail ?

### • Est-ce que le message/courriel vous est réellement destiné ?

1. Généralement, les messages malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés.

2. Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un courriel malveillant.

• **Attention aux expéditeurs inconnus** : soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.

• **Soyez attentif au niveau de langage du courriel** : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration ...).

• **Vérifiez les liens dans le courriel** : avant de cliquer sur les éventuels liens, laissez votre souris dessus\*. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.\* *A noter : cette manipulation est impossible à effectuer depuis un écran de smartphone.*

• **Méfiez vous des demandes étranges** : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.

• **L'adresse de messagerie source n'est pas un critère fiable** : une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami – par exemple pour récupérer l'accès à son compte – contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !

## Comment réagir ?

Si vous avez un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime :

- N'ouvrez surtout pas les pièces jointes et ne répondez pas;
- Si l'escroquerie que vous souhaitez signaler vous est parvenue par un spam (pourriel), rendez-vous sur [www.signal-spam.fr](http://www.signal-spam.fr);
- Supprimez le message puis videz la corbeille;
- S'il s'agit de votre compte de messagerie professionnel : transférez-le au service informatique et au responsable de la sécurité des systèmes d'information de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

## Comment s'en prémunir ?

• Utilisez un logiciel de filtre anti-pourriel ou activez l'option d'avertissement contre le filoutage présent sur la plupart des navigateurs.

• Installez un anti-virus et mettez-le à jour.

• Désactivez le volet de prévisualisation des messages.

• Lisez vos messages en mode de texte brut.

## Si vous êtes victime d'une escroquerie en ligne ?

Signalez les escroqueries auprès du site [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr), la plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements. Pour s'informer sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : contacter Info Escroqueries au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile) – Du lundi au vendredi de 9h à 18h

Rendez-vous sur [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr), la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Que vous soyez un particulier, une entreprise ou une administration, retrouvez :

- des conseils / vidéos pour sensibiliser votre entourage professionnel ou personnel,
- des services de proximité en cas de dommages causés par une attaque informatique.

...[lire la suite]

---

Réagissez à cet article

---

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)

Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !  
Commandez sur Fnac.fr

---

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la

Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

[https://youtu.be/usg12zkRD9I?list=UUoHqj\\_HKcbzRuvIPdu3FktA](https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA)

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr

---



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur [Fnac.fr](https://www.fnac.fr)

Source : *Phishing : détecter un message malveillant* | CNIL