

# Cyber sécurité au quotidien - 9 réflexes clés

---

Avec Internet et la généralisation des smartphones, de nombreuses fraudes ont vu le jour, se renouvelant sans cesse avec toujours plus d'ingéniosité. Face à ces cybers risques, vous, utilisateur, avez un rôle clé en matière de prévention, particulièrement pour protéger l'accès à votre banque à distance et pour vos paiements quel que soit l'équipement que vous utilisez (ordinateur, tablette, smartphone). Ce guide vous propose les réflexes de cyber sécurité à adopter au quotidien.

**A savoir :** si vous êtes victime de cyber malveillance, des conseils pratiques sont disponibles sur [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr) le site national d'assistance et de prévention du risque numérique.

## 1. Je ne réponds pas aux sollicitations

*Sollicité par courriel (phishing) ou sms (smishing), vous pourriez être conduit sur un faux site où vos données, de connexion bancaire ou de paiement, seraient récupérées pour être ensuite utilisées à votre insu.*

**Pour me protéger :**

- **Ne cliquez jamais sur les liens** et ne téléchargez pas les pièces jointes d'un courriel si vous trouvez l'expéditeur douteux.
- **Prenez votre temps** pour faire les vérifications nécessaires, surtout si le message est alarmiste et demande une action urgente (paiement, envoi d'informations personnelles, etc.).
- **Ne donnez pas suite à un SMS** vous incitant à un appel ou une connexion depuis votre téléphone. En cas de doute, transmettez le SMS au 33700 ou sur [www.33700-spam-sms.fr](http://www.33700-spam-sms.fr) pour signaler la tentative d'escroquerie.

**Réagir en cas d'escroquerie :**

- **Informez la banque** ou l'organisme dont semble provenir le message pour leur signaler des tentatives de fraude utilisant leur identité.
- Si vous pensez avoir fourni vos données à un escroc, **signalez-le immédiatement** à l'organisme concerné pour stopper au plus vite toute escroquerie en cours.
- Si vous avez fourni vos codes d'accès de banque à distance, **contactez immédiatement votre banque**, aux coordonnées habituelles, pour lui signaler.
- Si vous avez malencontreusement communiqué des éléments sur vos moyens de paiement, **faites opposition immédiatement**.

- Si vous avez indiqué des mots de passe ou code à un tiers, **changez-les** rapidement.
- **Surveillez vos comptes** pour détecter des opérations frauduleuses et les contester.

## 2. Je protège mes données personnelles

*Sur Internet, sites marchands, sites de rencontre ou réseaux sociaux par exemple, vos données personnelles pourraient être volées. Un escroc pourrait même tenter de vous séduire à seule fin de les récupérer, et ensuite les utiliser en se faisant passer pour vous. L'usurpation d'identité est en forte recrudescence.*

### Pour me protéger :

- Vos données, c'est vous. Soyez aussi vigilant qu'avec vos papiers d'identité ou vos clés.  
**Maîtrisez les données que vous communiquez et à qui.**
- **Sauvegardez régulièrement vos données** sur un support externe (disque dur par exemple).
- **Mettez à jour vos systèmes et anti-virus** sur ordinateur, tablette, mobile et objets connectés...
- **Verrouillez vos appareils** par des mots de passe ou codes.
- **Différenciez vos mots de passe** selon le service utilisé, changez-les régulièrement et choisissez-les avec soin. Evitez les dates de naissance par exemple. Ne les enregistrez pas et ne les notez pas.
- **Disposez d'adresses mél différentes** selon l'usage (professionnel, personnel, achats, etc.).
- Paramétrez avec soin votre compte sur les réseaux sociaux et réservez l'accès aux amis ou relations proches.
- **Effacez votre historique** de navigation **et les cookies**. N'acceptez pas les cookies, sauf de sites sûrs.
- Consultez les politiques de gestion des données personnelles des sites que vous consultez.
- Limitez les autorisations demandées par les applications que vous installez sur votre smartphone à celles qui sont nécessaires.

### Réagir en cas d'escroquerie :

- Vous pouvez **contacter la CNIL** (Commission nationale de l'informatique et des libertés) pour faire valoir vos droits : accès, rectification, etc.
- **Portez plainte** auprès de la police ou de la gendarmerie et signalez une usurpation d'identité.
- Demandez, au site concerné, à récupérer / effacer vos données, et opposez-vous à leur utilisation...
- Si un pirate vous menace de diffuser des photos/vidéos compromettantes de vous si vous refusez de payer une rançon (**chantage à la webcam**), ne répondez pas et **ne payez pas la rançon** réclamée.

### 3. Je me connecte à des sites sûrs pour mes achats en ligne

*De faux sites sont créés et ressemblent à s’y méprendre à de grands sites marchands connus.*

*L’objectif est d’y récupérer des données de connexion à des comptes clients ou encore des données de paiement.*

**Pour me protéger :**

- **Tapez toujours vous-même l’adresse du site** et vérifiez les signes de sécurité (« https », « s » pour secure) devant l’adresse du site, ou cadenas fermé, ou icône d’une clé dans le navigateur).
- **Ne répondez jamais à un courriel douteux** utilisant les coordonnées ou l’identité (logo, visuel...) d’un site marchand.
- **Vérifiez que l’adresse du site est correcte** surtout si vous trouvez que sa page d’accueil ou ses modalités de fonctionnement vous semblent un peu différentes de d’habitude. Différez vos achats en cas de doute.
- Pour un 1<sup>er</sup> achat, **vérifiez les informations du marchand** (nom, adresse, service clients), les garanties de livraison, les modalités de paiement, de retour et de contact, les conditions générales de vente, les avis des internautes...
- Evitez de procéder à des paiements si le site n’a pas mis en place une authentification renforcée type 3 D Secure ou autre, ou s’il est hébergé en dehors de la communauté européenne.
- **N’enregistrez pas vos données** clients et de paiements sur le site.
- Ne divulguez à personne vos identifiants et votre mot de passe de portefeuille électronique.

**Réagir en cas d’escroquerie :**

- En cas de communication des données de votre carte bancaire à un faux commerçant, contactez immédiatement votre interlocuteur bancaire pour lui signaler et faites opposition sur votre carte.
- En cas de fraude avérée, **faites opposition à votre carte** bancaire puis **déposez plainte** auprès de la gendarmerie ou de la police et contestez l’opération auprès de votre banque.
- **Signalez la fraude** à la carte bancaire dont vous avez été victime sur [Perceval](https://www.perceval.fr) accessible depuis [www.service-public.fr](https://www.service-public.fr) (plateforme électronique de signalements d’achats frauduleux en ligne par carte bancaire) pour faciliter le travail des enquêteurs.
- **Vérifiez régulièrement votre compte bancaire** pour déceler toute opération suspecte. Pour une opération que vous considérez ne pas avoir faite, vous avez, à compter du débit en compte, un délai de :
  - 13 mois pour un paiement dans l’Espace Economique Européen (EEE),
  - 70 jours, pour un paiement hors de l’EEE ; ce délai pouvant être prolongé contractuellement à 120 jours.

### 4. Je suis vigilant quand je me connecte à ma banque

*De faux sites sont créés et ressemblent à s’y méprendre à des sites bancaires connus dont ils utilisent l’identité visuelle afin de récupérer des données de connexion à des comptes bancaires ou encore des données de paiement.*

**Pour me protéger :**

- Tapez toujours **vous-même l'adresse** du site bancaire.
- Vérifiez que l'adresse du site est correcte surtout si vous trouvez que sa page d'accueil ou ses modalités de fonctionnement vous semblent un peu différentes. Si besoin, vérifiez-la avec votre conseiller habituel.
- **Consultez les messages de sécurité** de votre banque dans sa rubrique dédiée sur son site Internet.
- **N'enregistrez jamais vos identifiants** bancaires de connexion sur le site ni sur l'application, y compris sur votre smartphone.

**Réagir en cas d'escroquerie :**

- **Signalez un site** ou un courrier d'escroquerie sur [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr) et [www.signal-spam.fr](http://www.signal-spam.fr), et avertissez votre banque.
- **Vérifiez régulièrement votre compte bancaire** pour déceler toute opération suspecte.
- Pour une opération que vous considérez ne pas avoir faite, vous avez, à compter du débit en compte, un délai de :
  - 13 mois pour un paiement dans l'Espace Economique Européen (EEE),
  - 70 jours, pour un paiement hors de l'EEE ; ce délai pouvant être prolongé contractuellement à 120 jours.

## 5. Je ne donne pas suite à une proposition de remboursement / une offre trop exceptionnelle

*Le plus souvent, un message vous annonce un remboursement d'un organisme public (ex : Caisses d'Allocations Familiales CAF, sécurité sociale, impôts, etc.) ou une offre irrésistible (ex : un smartphone à 1 € alors que tous les sites le proposent à 700 euros).*

**Pour me protéger :**

- Si c'est trop beau pour être vrai, alors c'est sûrement faux. **Ne donnez pas suite.**
- **Méfiez-vous des offres d'abonnement** cachées qui implique des prélèvements ultérieurs réguliers et plus importants.
- **Assurez-vous de la véracité de l'information** en contactant la personne (ou organisme) au numéro de téléphone (ou adresse) que vous utilisez habituellement et non celui du message qui est probablement faux.

**Réagir en cas d'escroquerie :**

- Ne diffusez surtout pas les messages pour éviter de répandre la fraude.
- **Signalez les messages et sites suspects** via la plateforme PHAROS (plateforme d'harmonisation, de recoupement et d'orientation des signalements) [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr) ou encore [www.signal-spam.fr](http://www.signal-spam.fr). Ils seront traités par des policiers et des

gendarmes rattachés à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (police judiciaire).

- **Signalez rapidement toute anomalie sur votre compte** bancaire et si une opération ne vous concerne pas, prévenez immédiatement votre banque.

## 6. Je suis vigilant face à une offre de placement trop rentable et soi-disant « sans risque »

*Le plus souvent, un message ou un site vous annonce un investissement très rentable et sans risque (ex : diamants, crypto-monnaies, Forex, options binaires, etc.). Promesses de gains irréalistes, faux investissements dans de nouveaux secteurs, faux conseillers financiers, fausse autorité publique ... ou encore placements atypiques, investissements réservés à des privilégiés, les fraudes sont très variées et vos chances de récupérer votre argent très limitées voire inexistantes, les escrocs étant le plus souvent à l'étranger.*

### Pour me protéger :

- Si c'est trop beau pour être vrai, alors c'est sûrement faux. **Ne donnez pas suite.**
- Vérifiez l'agrément de l'intermédiaire sur [Orias](#) et celui de l'entreprise sur [Regafi](#), et pour toute question contactez [l'AMF](#).
- Tapez-vous-même l'adresse du site et vérifiez qu'il est sécurisé (« https », cadenas, etc.).
- Méfiez-vous d'un conseiller trop insistant qui refuse d'indiquer pour quelle société il travaille, qui ne vous pose pas de questions sur votre épargne, ne recherche pas à déterminer votre profil d'investisseur ou pire vous incite à mentir sur votre situation.
- Ne donnez pas suite à un « professionnel de la finance », faux cabinet d'avocats ou encore une personne soi-disant mandatée par une autorité qui vous proposerait de récupérer votre argent perdu sur les sites de trading.
- **Posez des questions sur le placement et exigez une documentation écrite.**
- **Ne versez pas de sommes d'argent, ne donnez pas votre numéro de carte bancaire et ne signez aucun document.**

### Réagir en cas d'escroquerie :

- Ne diffusez surtout pas les messages pour éviter de répandre la fraude. **Contactez l'AMF** ([www.amf-france.org](http://www.amf-france.org)) pour lui signaler toute tentative de fraude.
- **Signalez-les messages et sites suspects via** la plateforme **PHAROS** (plateforme d'harmonisation, de recoupement et d'orientation des signalements) [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr) ou encore [www.signal-spam.fr](http://www.signal-spam.fr). Ils seront traités par des policiers et des gendarmes rattachés à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (police judiciaire).
- Avec une plateforme illégale d'investissement, votre seul recours est de **porter plainte** auprès de la police ou de la gendarmerie.

- Sur une plateforme légale, saisissez la [médiation de l'AMF](#) qui peut intervenir pour résoudre votre litige à l'amiable.
- **Signalez rapidement toute anomalie sur votre compte bancaire** et si une opération ne vous concerne pas, prévenez immédiatement votre banque.

## 7. Je vérifie l'identité de mes interlocuteurs

*La fraude aux coordonnées bancaires, qui concernait surtout les entreprises, touche désormais de plus en plus les particuliers. Un ordre de virement (transfert de compte à compte) ne peut pas être annulé, la somme ne peut donc pas être restituée par un transfert en sens inverse.*

**Pour me protéger :**

- **Vous devez être particulièrement vigilant** quand vous émettez un ordre de virement si un de vos correspondants habituels vous informe d'un changement de coordonnées bancaires (ex : bailleur).
- Assurez-vous de la véracité de l'information en contactant la personne (ou organisme) au numéro de téléphone (ou adresse) que vous utilisez habituellement.
- Si un proche vous demande de l'assistance par courriel, contactez-le directement sans répondre à son message et posez-lui des questions précises auxquelles lui seul peut répondre.

**Réagir en cas d'escroquerie :**

- **Prévenez la personne** dont l'identité a été usurpée.
- **Signalez rapidement toute anomalie** et si une opération bancaire ne vous concerne pas, prévenez immédiatement votre banque.
- Selon la nature de l'opération anormale relevée, votre banque pourra faire des recherches et vous indiquera la marche à suivre.

## 8. Je protège mon matériel

*Un logiciel malveillant pourrait infecter votre matériel (téléphone, tablette, ordinateur...) :*

- vos données pourraient être récupérées pour être ensuite utilisées à votre insu,
- votre matériel pourrait se retrouver bloqué et vos fichiers encryptés, avec une demande de rançon (ransomware) pour les récupérer,
- votre matériel pourrait être utilisé pour en attaquer d'autres ou envoyer du spam.

**Pour me protéger :**

- Ne téléchargez que les programmes et contenus (photos, vidéos, sonneries, thèmes pour mobile et jeux) provenant d'une source fiable. N'ouvrez pas de fichier joint à un courriel suspect.

- Ne branchez pas de clé usb sur votre poste si ce n'est pas quelqu'un de confiance qui vous l'a remise.
- **Téléchargez régulièrement les mises à jour système**, installez sur votre ordinateur, tablette et téléphone, un antivirus et un pare-feu efficaces avec des mises à jour automatiques.
- **N'utilisez pas de matériel dont vous ne maîtrisez pas le niveau de sécurité** (cybercafé, libre-service...).
- **Verrouillez votre mobile** (smartphone, tablette) par un code de sécurité (mieux qu'un schéma) en plus du mot de passe de la carte Sim.
- N'enregistrez pas vos codes et mots de passe.
- Ne laissez pas votre matériel sans surveillance.

#### Réagir en cas d'escroquerie :

- En cas de virus ou d'attaque, **lancez votre antivirus**. N'effectuez aucune opération de banque à distance (connexion, virement, opposition...).
- **Déconnectez votre appareil** de votre réseau pour éviter la contagion sur les autres ordinateurs connectés à votre Wi-Fi.
- **Ne faites plus de transaction en ligne** et ne vous connectez pas sur le site de votre banque jusqu'à désinfection de votre matériel.
- Utilisez un autre matériel sécurisé pour changer au plus vite vos codes et mots de passe.
- **Vérifiez les dernières opérations effectuées** sur votre compte.
- En cas de dysfonctionnement de votre ligne téléphonique, signalez-le à votre opérateur, la ligne a pu être détournée et être utilisée pour effectuer des tentatives de fraudes bancaires sur vos comptes.
- En cas de perte ou de vol d'un terminal (tablette, ordinateur, téléphone...), **changez immédiatement vos mots de passe** (applications bancaires et non bancaires), y compris vos codes d'accès de messagerie électronique.

## 9. Je protège mes connexions

*Votre connexion pourrait être utilisée à votre insu pour :*

- *recupérer vos données personnelles et les utiliser ensuite,*
- *bloquer votre ordinateur et encrypter vos fichiers, avec une demande de rançon (ransomware) pour les récupérer.*

#### Pour me protéger :

- Choisissez un fournisseur d'accès internet reconnu et suivez ses conseils de sécurité.
- Vérifiez la présence de « https » devant l'adresse du site, icône d'une clé ou d'un cadenas dans la fenêtre du navigateur Internet.
- Contrôlez qu'aucune autre fenêtre internet n'est ouverte, tapez vous-même l'adresse exacte du site.
- Configurez votre réseau Wi-Fi domestique en choisissant une clé de sécurité complexe (WPA2 ou WPA-AES) depuis l'interface de votre fournisseur d'accès.

- N'activez la fonction Bluetooth ou WI-FI que lorsque c'est nécessaire et désactivez-la dès la fin d'utilisation.
- Ne réalisez pas de transaction et ne consultez votre compte en banque depuis un ordinateur public ou connecté à un réseau Wi-Fi public.
- Si la date de votre dernière connexion est affichée, vérifiez-la. Quand vous avez terminé, utilisez le bouton « déconnexion » et effacez l'historique dès que vous avez fini.
- Si vous avez supprimé des documents, n'oubliez pas de vider la corbeille.

**Réagir en cas d'escroquerie :**

- Ne payez pas la rançon : rien ne garantit que les pirates vous fournissent la clé qui permettra de déchiffrer vos fichiers ou débloquer votre ordinateur.
- Débranchez votre équipement d'internet pour éviter la propagation.
- Selon que l'ordinateur est bloqué ou pas, sauvegardez les données qui ne sont pas contaminées grâce à un périphérique dédié (disque dur externe, clé USB...) et attendez la résolution du problème avant de les installer à nouveau.
- Désinfectez votre matériel.
- Utilisez des logiciels spécialisés de récupération des fichiers.