Cybersécurité au quotidien

9 RÉFLEXES CLÉS

les clés de la banque

LES GUIDES BANCAIRES
N°7 / Sécurité

CE GUIDE VOUS EST OFFERT PAR :

les clés de la banque

Pour toute information complémentaire, nous contacter : info@lesclesdelabanque.com

Éditeur : FBF - 18 rue La Fayette 75009 Paris - Association Loi 1901
Directeur de publication : Maya Atig
Imprimeur : Concept graphique,
ZI Delaunay Belleville - 9 rue de la Poterie - 93207 Saint-Denis
Dépôt légal : octobre 2024

SOMMAIRE

9 RÉFLEXES CLÉS

Si vous pensez être victime, des conseils pratiques sont disponibles sur www.cybermalveillance.gouv.fr le site national d'assistance et de prévention du risque numérique. Pour porter plainte ou signaler une fraude (faux site, piratage de messagerie électronique, chantage, demande de rançon, etc.), utilisez la plateforme THESEE sur service-public.fr.

Pour plus de réflexes sécurité, par moyen de paiement notamment, consultez notre collection de guides « sécurité » sur lesclesdelabanque.com.

Introduction

Avec Internet, les fraudes se multiplient avec toujours plus d'ingéniosité. Pour vous protéger, il est crucial de rester vigilant, surtout pour accéder à votre banque en ligne et pour vos paiements... Ce guide vous propose des réflexes simples de cybersécurité à appliquer au quotidien.

1. Je ne réponds pas aux sollicitations

Un courriel (phishing) ou SMS (smishing), peut vous conduire sur un faux site où vos informations de connexion bancaire ou de paiement, pourraient être récupérées et utilisées à votre insu.

Pour vous protéger :

- **Ne cliquez pas sur les liens ni sur les pièces jointes** d'un message que vous n'attendiez pas.
- **Prenez votre temps** pour faire les vérifications nécessaires, surtout si le message est alarmiste et demande une action urgente (paiement, envoi d'informations personnelles…).
- **Ne donnez pas suite** à un SMS vous incitant à un appel ou une connexion depuis votre téléphone. En cas de doute, transférez le SMS au 33700 ou sur www.33700.fr.

Réagir rapidement en cas d'escroquerie :

- **Faites opposition** au plus vite si vous avez divulgué des informations de paiement.
- **Prévenez votre banque**, aux coordonnées habituelles, si vous avez fourni vos codes d'accès de banque à distance.
- **Changez vos mots de passe** ou codes si vous les avez communiqués à un tiers.
- **Informez l'organisme** dont semble provenir le message pour lui signaler la tentative de fraude utilisant son identité afin de stopper toute escroquerie en cours.
- **Surveillez vos comptes** pour détecter et contester toute opération frauduleuse.

2. Je protège mes données personnelles

Sur Internet, sites e-commerce, sites de rencontre ou réseaux sociaux par exemple, vos données personnelles peuvent être volées et ensuite utilisées à votre insu. Un escroc pourrait même tenter de vous séduire à seule fin de les récupérer. L'usurpation d'identité est en forte hausse.

Pour vous protéger :

- **Maîtrisez les données que vous partagez et avec qui**. Vos données, c'est vous. Soyez aussi vigilant qu'avec vos papiers d'identité ou vos clés.
- **Sauvegardez régulièrement vos fichiers** ou autres documents importants sur un support externe (disque dur ou coffre-fort électronique) et sécurisé.
- **Mettez à jour vos systèmes et anti-virus** sur tous vos appareils… et verrouillez-les par des mots de passe ou codes.
- **Variez et changez régulièrement vos mots de passe**, choisissez-les avec soin. Privilégiez des phrases de passe sans informations personnelles (date de naissance). Ne les notez pas. Si besoin, enregistrez-les dans un gestionnaire de mots de passe sécurisé.
- **Utilisez des adresses e-mail 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 régulièrement votre historique** de navigation et supprimez les cookies.
- **Limitez au nécessaire les autorisations demandées** par les applications que vous installez.

Réagir rapidement en cas d'escroquerie :

- **Portez plainte** auprès de la police ou de la gendarmerie et signalez l'usurpation d'identité.
- Demandez, au site concerné, à **récupérer/effacer vos données**, et opposez-vous à leur utilisation.
- Vous pouvez **contacter la CNIL** (Commission nationale de l'informatique et des libertés) pour faire valoir vos droits : accès, rectification, etc.
- En cas de chantage à la webcam (menace de diffusion de photos/vidéos soi disant compromettantes), ne répondez pas et **ne payez pas** la rançon réclamée. En effet, il est très peu probable que les escrocs détiennent des choses sur vous.

3. J’utilise des sites sûrs pour mes achats en ligne

De faux sites imitent les grands sites marchands pour voler vos données personnelles, dont vos identifiants de connexion bancaire ou informations de paiement.

Pour vous protéger :

- **Vérifiez que l'adresse du site est correcte** surtout si quelque chose vous semble inhabituel (page d'accueil, modalités de fonctionnement…). Différez vos achats en cas de doute.
- **Tapez vous-même l'adresse du site** et vérifiez les signes de sécurité (https, cadenas ou clé dans le navigateur). Cela garantit le cryptage des données échangées. Attention cependant, ça ne garantit pas que le site est officiel.
- **Vérifiez les informations du marchand** : nom, adresse, service clients, les garanties de livraison, les modalités de paiement, de retour, de contact, les CGV, les avis…
- **N'effectuez pas de paiement si le site est hébergé en dehors de l'Union européenne.** L'absence de fenêtre d'authentification forte doit vous alerter, sauf en cas de faible montant ou d'opération récurrente.
- **N'enregistrez pas vos données** de paiement sur le site.
- **Ne divulguez à personne votre identifiant et mot de passe** de portefeuille électronique.
- **Ignorez les courriels douteux** imitant des sites marchands.

Réagir rapidement en cas d'escroquerie :

- Si vous pensez avoir communiqué vos données bancaires à un faux commerçant, **contactez votre banque** pour lui signaler.
- En cas de fraude avérée, **faites opposition, déposez plainte** et contestez l'opération auprès de votre banque.
- **Signalez la fraude** sur le site du service public (Perceval) pour aider les enquêteurs.
- **Vérifiez régulièrement votre compte bancaire**. Pour une opération que vous considérez ne pas avoir faite, vous avez, à compter du débit en compte :

  – 13 mois pour **contester un paiement** dans l'Espace Économique Européen (EEE) ;

  – 70 jours (ou 120 jours selon le contrat), pour un paiement hors de l'EEE.

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

De faux sites imitent les sites bancaires afin de récupérer vos données personnelles, identifiants de connexion ou informations de paiement.

Pour vous protéger :

- **Vérifiez que l'adresse du site est correcte** surtout si quelque chose vous semble inhabituel (page d'accueil, modalités de fonctionnement…). Contactez votre conseiller en cas de doute.
- **Tapez vous-même l'adresse du site** bancaire.
- **Consultez les messages de sécurité de votre banque** dans sa rubrique dédiée.
- **N'enregistrez pas vos identifiants** de connexion ni sur le site ni sur l'application.
- Ne vous authentifiez sur l'appli de votre banque qu'à votre initiative. Et prenez le temps de vérifier ce que vous êtes en train de valider.
- Ne validez jamais une opération suite à un appel, un SMS ou un courriel.

Réagir rapidement en cas d'escroquerie :

- **Avertissez votre banque** aux coordonnées habituelles et signalez le site ou le courrier frauduleux sur PHAROS et signal-spam.fr.
- **Vérifiez 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 :

  – 13 mois pour **contester un paiement** dans l'Espace Économique Européen (EEE) ;

  – 70 jours (ou 120 jours selon le contrat) pour un paiement hors de l'EEE.

5. J'ignore les remboursements inattendus/ offres trop exceptionnelles

Le plus souvent, un message (courriel ou publicité sur Internet ou sur les réseaux sociaux) vous annonce un remboursement inattendu d'un organisme public (ex : Caisses d'allocations familiales, Sécurité sociale, impôts, etc.) ou une offre irrésistible (ex : un smartphone à 1 € alors que tous les sites le proposent à 700 €)...

Pour vous protéger :

- **Ne donnez pas suite.** Si c'est trop beau pour être vrai, alors c'est sûrement faux.
- **Méfiez-vous : certaines offres comprennent des abonnements cachés** qui impliquent d'autres prélèvements plus élevés.
- **Vérifiez l'information** en contactant la personne (ou organisme) aux coordonnées habituelles et non celles fournies dans le message.

Réagir rapidement en cas d'escroquerie :

- **Prévenez votre banque et faites opposition** si vous pensez avoir fourni vos données à un escroc.
- **Ne partagez pas ces messages** pour éviter de répandre la fraude.
- **Signalez les messages et sites suspects** via la plateforme PHAROS. Ils seront traités par les autorités compétentes.
- **Signalez toute anomalie sur votre compte** à votre banque.

6. **Offre rentable et sans risque ? Je passe**

Investissements très rentables et sans risque (diamants, cryptos, Forex, etc.), crédits à taux imbattable et sans frais, promesses de gains irréalistes, faux conseillers financiers, fausses autorités publiques, placements atypiques… : les fraudes sont très variées et les chances de récupérer votre argent sont quasi inexistantes.

Pour vous protéger :

- **Ne donnez pas suite.** Si c'est trop beau pour être vrai, c'est sûrement faux.
- **Vérifiez l'agrément de l'intermédiaire** sur Orias et celui de l'entreprise sur Regafi. En cas de doute, contactez l'AMF ou l'ACPR.
- **Tapez vous-même l'adresse du site** et vérifiez qu'il est sécurisé (https, cadenas, etc.). Cela garantit le cryptage des données échangées. Attention cependant, ça ne garantit pas que le site est officiel.
- **Méfiez-vous d'un « conseiller » insistant** qui ne s'intéresse pas à votre situation financière, ne cherche pas à déterminer votre taux d'endettement…
- Ignorez les « professionnels » qui vous proposeraient de récupérer votre argent perdu sur les sites de trading.
- **Posez des questions** et exigez une documentation écrite.
- **Ne versez pas d'argent, ne donnez pas votre numéro de carte bancaire** et ne signez aucun document.

Réagir rapidement en cas d'escroquerie :

- **Informez votre banque et faites opposition** si vous pensez avoir fourni vos données à un escroc.
- **Ne partagez pas ces messages** pour éviter de répandre la fraude.
- Selon les cas, **signalez les messages et sites suspects** à l'AMF ou l'ACPR et/ou via PHAROS.
- Si la plateforme est légale, saisissez la médiation de l'AMF pour résoudre votre litige à l'amiable. Sinon **portez plainte**.
- **Surveillez votre compte** et prévenez votre banque si vous remarquez des opérations que vous n'avez pas effectuées.

7. Je vérifie l'identité de mes interlocuteurs

La fraude aux coordonnées bancaires est devenue plus courante. Une fois un ordre de virement émis, il ne peut pas être annulé, la somme ne peut donc pas être restituée par un transfert en sens inverse.

Pour vous protéger :

- **Soyez vigilant** quand vous émettez un ordre de virement, surtout si un de vos créanciers vous informe d'un changement de RIB (ex : bailleur).
- **Vérifiez la véracité de l'information** en contactant la personne (ou organisme) aux coordonnées habituelles.

Réagir rapidement en cas d'escroquerie :

- **Informez votre banque** et la personne (ou organisme) dont l'identité a été usurpée.
- **Signalez toute anomalie** ou opération bancaire suspecte à votre banque.

8. Je protège mon matériel

Un logiciel malveillant peut infecter votre matériel (téléphone, tablette, ordinateur...) et :

- voler et utiliser vos données à votre insu ;
- bloquer l'appareil et crypter vos fichiers avec demande de rançon (ransomware) pour les récupérer ;
- utiliser votre appareil pour en attaquer d'autres ou envoyer du spam.

Pour vous protéger :

- **N'ouvrez pas les fichiers joints à un courriel suspect.** Téléchargez les programmes et contenus (photos, vidéos, thèmes, jeux…) provenant uniquement de sources fiables.
- Ne branchez pas de clé USB sur votre poste si ce n'est pas quelqu'un de confiance qui vous l'a remise.
- **Faites régulièrement les mises à jour système** et installez un antivirus et un pare-feu avec des mises à jour automatiques.
- **Evitez d'utiliser des appareils dont vous ne connaissez pas le niveau de sécurité** (cybercafé, libre-service…).
- **Verrouillez votre mobile** avec un code de sécurité en plus du mot de passe de la carte SIM.
- **N'enregistrez pas vos mots de passe** et ne laissez pas votre matériel sans surveillance.

Réagir rapidement en cas d'escroquerie :

- **Lancez votre antivirus**, en cas de virus ou d'attaque. N'effectuez aucune opération bancaire en ligne (connexion, virement, opposition…).
- **Déconnectez votre appareil du réseau** pour éviter la propagation 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.
- **Changez vos mots de passe** via un autre appareil sécurisé.
- **Vérifiez les dernières opérations effectuées** sur votre compte.
- En cas d'anomalie sur votre ligne téléphonique, contactez votre opérateur.

9. Je protège mes connexions

Sans protection, quelqu'un pourrait :

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

Pour vous protéger :

- **Choisissez un fournisseur d'accès Internet connu** et suivez ses conseils de sécurité.
- **Tapez vous-même l'adresse du site** et vérifiez qu'il est sécurisé (https, cadenas, etc.). Cela garantit le cryptage des données échangées. Attention cependant, ça ne garantit pas que le site est officiel.
- **Configurez votre Wi-Fi avec une clé de sécurité complexe.** Activez le Bluetooth que lorsque c'est nécessaire et désactivez-le dès la fin d'utilisation.
- **Ne réalisez pas de transaction** et ne consultez pas 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 »**.
- **Effacez régulièrement votre historique** de navigation et les cookies. Videz la corbeille après avoir supprimé des fichiers.

Réagir rapidement 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 appareil.
- **Débranchez votre équipement d'Internet** pour éviter la propagation.
- Si possible, **sauvegardez les documents non infectées** sur un support externe (disque dur, 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.

9 REFLEXES CLES

La cybersécurité au quotidien

1. Je ne réponds pas aux sollicitations
2. Je protège mes données personnelles
3. J'utilise des sites sûrs pour mes achats en ligne
4. Je suis vigilant quand je me connecte à ma banque
5. J'ignore les remboursements inattendus/ offres trop exceptionnelles
6. Offre rentable et sans risque ? Je passe
7. Je vérifie l'identité de mes interlocuteurs
8. Je protège mon matériel
9. Je protège mes connexions

lesclesdelabanque.com

FÉDÉRATION
BANCAIRE
FRANÇAISE