Cybersécurité en entreprise

8 RÉFLEXES CLÉS

les clés de la banque

LES GUIDES BANCAIRES
N°6 / Sécurité

CE GUIDE VOUS EST OFFERT PAR :

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 : mars 2024

SOMMAIRE

8 RÉFLEXES CLÉS

Si vous êtes victime de cyberattaque, des conseils pratiques et un annuaire de professionnels labellisés sont disponibles sur cybermalveillance.gouv.fr, le site national d'assistance et de prévention en sécurité numérique.

Introduction

Les cyberattaques se multiplient menaçant toute entreprise, quelle que soit sa taille. Une faille de sécurité ou une fuite de données peut avoir de lourdes conséquences sur votre activité et votre réputation. Nombreuses, les fraudes se renouvellent constamment. Voici les plus fréquentes :

- fraude au RIB (45%)
- fraude au président (41%)
- intrusion dans le système informatique (41%)
- usurpation d'identité (30%)
- fraude au faux client (25%)

** Chiffres Cybermalveillance.gouv.fr*

Ce guide présente des réflexes simples pour votre sécurité numérique.

1. Je sensibilise les collaborateurs

La plupart des fraudes en entreprise ciblent les collaborateurs. Ils peuvent être contactés afin d'obtenir des informations sur l'entreprise, des identifiants de comptes bancaires, leur faire réaliser des paiements...

Pour protéger votre entreprise :

- **Sensibilisez vos collaborateurs** à la cybersécurité dans leur quotidien professionnel avec des exemples concrets.
- **Adoptez une charte informatique** pour préciser les règles d'utilisation du matériel informatique, de la messagerie, y compris lors des déplacements professionnels ou en cas d'utilisation mixte de l'ordinateur (usage professionnel et personnel)…
- **Organisez des formations spécifiques** pour les postes les plus exposés (ex : personnes habilitées à réaliser des paiements) et planifiez des séances de rappel car les fraudes se renouvellent régulièrement.
- **Mettez en place des protocoles et des consignes de sécurité**, particulièrement pour les paiements, les changements de coordonnées bancaires et contrôlez leur bonne application.

Réagir rapidement en cas d'escroquerie :

- **Contactez votre banque** pour stopper les transactions frauduleuses.
- **Faites opposition** à votre carte bancaire.
- **Changez vos mots de passe ou codes**, s'ils ont été révélés.
- **Surveillez vos comptes bancaires** pour détecter toute anomalie et la contester.

2. J'établis des procédures avec mes partenaires

Les liens que vous entretenez avec vos partenaires (clients, fournisseurs, comptables, banquiers, etc.) sont autant d'opportunités pour les fraudeurs de tenter de vous escroquer. L'identité de l'un d'entre eux peut être usurpée et on peut vous faire croire à un changement de domiciliation bancaire à des fins de paiement, ou encore vous faire réaliser une action pour pirater votre système informatique.

Pour protéger votre entreprise :

- **Établissez des protocoles précis** pour la réalisation de toutes vos opérations bancaires.
- En cas de demande suspecte, vérifiez son authenticité en contactant le partenaire à ses coordonnées habituelles et **respectez les procédures établies**.
- Face à un « rappel pour impayé », assurez-vous que la prestation a été réalisée et facturée. Puis consultez les factures antérieures pour en **vérifier la cohérence**.
- **Contrôlez les informations diffusées** sur votre entreprise notamment sur Internet et n'échangez pas d'informations sensibles avec vos partenaires en dehors de circuits sécurisés.

Réagir rapidement en cas d'escroquerie :

- **Informez votre partenaire** aux coordonnées habituelles de toute tentative de fraude utilisant son identité.
- **Surveillez vos comptes** bancaires pour détecter des opérations frauduleuses et les contester.
- Nettoyez votre système informatique (cf. infra).

3. Je sécurise mon site Internet

Sur Internet, les fraudes peuvent concerner vos transactions et le vol de données clients. Votre site peut également être piraté et bloqué (c'est le « déni de service »). Vous devez assurer la sécurité de votre site et des données de vos clients. Il en va de votre crédibilité professionnelle et donc de la survie de votre activité.

Pour protéger votre entreprise :

- **Installez un certificat de sécurité en « https »**, choisissez un hébergement sécurisé avec une assistance 24h/24.
- **Assurez-vous**, auprès de votre banque ou prestataire de paiement, **de la sécurité des solutions de paiement proposées** pour la vente à distance.
- **Mettez en place l'authentification forte** pour vos clients en e-commerce comme la réglementation l'exige.
- **Chiffrez les données de vos clients** et ne conservez que les données utiles : évitez de stocker les numéros de carte bancaire.
- **Changez régulièrement vos mots de passe**, mettez à jour vos antivirus, vos logiciels…

Réagir rapidement en cas d'escroquerie :

- **Déposez plainte** auprès de la police en communiquant les informations recueillies (type de carte, adresse IP...) et prévenez votre banque/prestataire de paiement.
- En cas d'attaque informatique, **demandez l'assistance d'un professionnel labellisé** sur cybermalveillance.gouv.fr. Contactez aussi le CSIRT de votre région (Computer Security Incident Response Team). Ce centre de réponse aux incidents cyber propose notamment aux PME et associations une assistance gratuite de 1er niveau, complémentaire à celle proposée par les prestataires de cybermalveillance.
- En cas de violation des données personnelles de vos clients, **signalez l'incident à la CNIL** (Commission Nationale de l'Informatique et des Libertés) dans les 72 heures.

La Commission Nationale de l'Informatique et des Libertés (CNIL) propose de nombreuses publications pour vous aider dans vos démarches, notamment pour la mise en conformité de votre site au règlement européen sur la protection des données (RGPD).

4. Je maîtrise la diffusion des données relatives à ma société

De nombreuses escroqueries sont rendues possibles grâce aux informations récupérées sur Internet (annonces légales, site de l'entreprise ou de ses partenaires commerciaux, réseaux sociaux...). Elles peuvent aussi être recueillies auprès des collaborateurs par téléphone par exemple. Ces pratiques sont appelées « ingénierie sociale ».

Pour protéger votre entreprise :

- Assurez-vous que **les contenus publiés** sur votre site et sur les réseaux sociaux **ne révèlent pas d'informations sensibles** (exemple : organigramme de votre entreprise).
- **Contrôlez** régulièrement **les informations disponibles** en tapant le nom de votre entreprise dans les moteurs de recherche.
- **Sensibilisez vos salariés** à ce risque spécifique, notamment sur les réseaux sociaux : informations, photos… pourraient être utilisées de façon malveillante et détournées grâce à l'intelligence artificielle (« deepfake »).
- **Attirez leur attention sur les appels** téléphoniques visant à récupérer des informations sur votre entreprise ou les personnes en charge des paiements.

Réagir rapidement en cas d'escroquerie :

Contactez vos partenaires ou les sites concernés, si vous souhaitez faire modifier les informations concernant votre société. Vous pouvez **contacter la CNIL** pour faire valoir vos droits : accès, rectification des données, etc.

5. Je choisis mes mots de passe avec soin

Les attaques informatiques reposent souvent sur le déchiffrage d'un mot de passe que ce soit pour compromettre ou accéder à un logiciel, un site marchand, un site Internet, une application bancaire...

Pour protéger votre entreprise :

- **Définissez un mot de passe spécifique** pour chaque service, appareil, logiciel, application utilisée par votre entreprise.
- **Il ne doit contenir aucune information professionnelle ou personnelle** qui pourrait être découverte facilement par un tiers, à partir de votre k-bis par exemple (date de création de l'entreprise, votre date de naissance…).
- Il doit **combiner** si possible des **lettres** (majuscules, minuscules), des **chiffres** et des **caractères spéciaux** et être **suffisamment long**.
- Les mots de passe **ne doivent jamais être enregistrés** sur vos appareils, utilisez plutôt un gestionnaire de mots de passe ou un fichier chiffré.

Réagir rapidement en cas d'escroquerie :

- **Changez le mot de passe** pour le service concerné.
- Concernant votre messagerie, si des codes confidentiels figurent dans votre boite de réception, modifiez-les également.

Ne notez pas vos mots de passe sur des post-it ou des carnets.

6. Je sécurise l'accès à mes services bancaires

Les escrocs essaieront de récupérer vos informations de connexion pour réaliser des opérations en leur faveur. Vous devez identifier les tentatives de phishing et protéger vos codes et mots de passe.

Pour protéger votre entreprise :

- **Ne divulguez pas** votre **identifiant** et votre **mot de passe** de connexion. Ils sont strictement personnels.
- Changez le mot de passe provisoire fourni par votre banque, dès réception.
- En cas de délégation à un tiers (expert-comptable, service financier…), assurez-vous qu'ils disposent de leur propre code personnel et vérifiez que les opérations (consultation, virement, montant…) sont conformes aux habilitations.
- Ne vous connectez pas depuis un appareil ou un réseau Wi-Fi public.
- **Tapez directement l'adresse du site** de votre banque dans votre navigateur et ne suivez jamais un lien ou QR Code envoyé par mail.
- **Suivez les consignes de sécurité** du prestataire pour votre matériel informatique et votre connexion (cf. infra).
- **Consultez régulièrement les messages de sécurité (informations, alertes…) de votre banque**, sur le site ou l'application et appliquez ses conseils.

Votre banque ne vous demandera jamais votre mot de passe de connexion.

Réagir rapidement en cas d'escroquerie :

- **Informez votre banque** en utilisant le n° de téléphone habituel ou la messagerie sécurisée de son site ou application. Demandez un nouveau mot de passe.
- **Vérifiez les dernières opérations** effectuées sur votre compte.
- **Consultez votre compte quotidiennement** pour détecter toute anomalie et contester les opérations frauduleuses s'il y a lieu.
- **Signalez le faux site** sur la plateforme Thésée et déposez plainte en cas de débit frauduleux. Vous pouvez aussi échanger avec un gendarme en ligne 7j/7, 24h/24.

7. Je sécurise mes équipements numériques et mes données

L'accès à vos équipements (ordinateur, smartphone, tablette) et à vos logiciels doit vous être réservé. Vous devez aussi vous protéger des attaques et virus qui pourraient bloquer votre réseau ou corrompre vos fichiers pour obtenir une rançon (ransomware) ou détourner votre matériel de son utilisation normale (machine zombie) pour effectuer du spam par exemple.

Pour protéger votre entreprise :

- Mettez en place des **mots de passe complexes** pour chaque équipement ou logiciel.
- **Verrouillez votre appareil** dès que vous cessez de l'utiliser et activez l'identification par code, schéma, empreinte… de votre smartphone/tablette, en plus du code PIN.
- **Utilisez un antivirus** et un système informatique de détection des menaces (EDR).
- Limitez l'installation de logiciels aux personnes habilitées (votre référent informatique par exemple ou la personne désignée comme administrateur).
- **Sauvegardez** régulièrement vos données sur des supports externes (disques durs de préférence).
- **Installez les mises à jour** proposées par les fabricants de matériel informatique et les éditeurs de logiciels, depuis les sources officielles, pour corriger les failles de sécurité détectées.
- Limitez, pour vos collaborateurs ou vous-même, l'utilisation à des fins professionnelles des appareils personnels, souvent moins sécurisés.
- Évitez d'introduire des contenus en provenance de sources inconnues ou peu fiables (clé USB trouvée, site Internet, pièce jointe d'un courriel suspect…).

Réagir rapidement en cas d'escroquerie :

- 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.
- En cas de virus ou d'attaque, **lancez votre antivirus** et déconnectez votre appareil de votre réseau informatique pour éviter une propagation.
- **Ne réalisez aucune opération** bancaire en ligne tant que votre appareil n'est pas désinfecté.
- **Vérifiez les dernières transactions** sur votre compte bancaire.
- **Signalez les dysfonctionnements** de votre ligne téléphonique à votre opérateur pour vous assurer que votre ligne n'a pas été détournée.

8. Je protège ma connexion Internet

La connexion Internet peut constituer un accès au réseau de votre entreprise et à vos données professionnelles, voire personnelles. Vous devez la sécuriser pour éviter toute utilisation non autorisée.

Pour protéger votre entreprise :

- Choisissez un fournisseur d'accès Internet reconnu et consultez ses avertissements de sécurité.
- Configurez votre réseau Wi-Fi avec **une clé de sécurité complexe** depuis l'interface de votre fournisseur.
- Si vous mettez un réseau Wi-Fi à disposition de vos clients ou partenaires, utilisez **une clé de sécurité spécifique**, différente de la clé principale.
- Vérifiez que les sites que vous visitez commencent par **https**, et affichent l'**icône d'une clé** ou d'un **cadenas** dans la barre d'adresse.
- **Ne transmettez pas d'informations sensibles** et ne vous connectez pas à votre site de banque à distance depuis un ordinateur public ou connecté à un réseau Wi-Fi public.
- En cas de connexion depuis un Wi-Fi public (hôtel, train…), **utilisez un VPN** (réseau privé virtuel) qui sécurise et chiffre vos échanges.

Réagir rapidement en cas d'escroquerie :

- **Modifiez le mot de passe de votre Wi-Fi,** si vous suspectez une utilisation non autorisée, en utilisant un autre terminal (réseau de votre téléphone mobile par exemple).
- En cas de blocage de votre ordinateur et demande de rançon, **prévenez la police et ne payez pas** : en effet, rien ne garantit que les pirates vous fournissent la clé qui permettra de déchiffrer vos fichiers ou débloquer votre ordinateur.
- Pour éviter la propagation, **déconnectez votre équipement** du réseau mais sans l'éteindre ni le redémarrer.
- Si possible, **sauvegardez sur un support externe** (disque dur) **les données** qui ne sont pas corrompues.
- **Utilisez votre antivirus et des logiciels spécialisés** de récupération des fichiers.

Pour aller plus loin, vous trouverez sur le site de l'ANSSI, des guides détaillés et bonnes pratiques pour renforcer votre sécurité numérique.

Vous pouvez réaliser un auto-diagnostic de cybersécurité de votre système d'information via le site ssi.economie.gouv.fr

Concernant la fraude aux ordres de virement, consultez le guide « Ordres de virement des entreprises – 9 réflexes sécurité ».

LES RÉFLEXES CLÉS

La cybersécurité en entreprise

1. Je sensibilise mes collaborateurs
2. J'établis des procédures avec mes partenaires
3. Je sécurise mon site Internet
4. Je maîtrise la diffusion des données relatives à ma société
5. Je choisis mes mots de passe avec soin
6. Je sécurise l'accès à mes services bancaires
7. Je sécurise mes équipements numériques et mes données
8. Je protège ma connexion Internet

lesclesdelabanque.com

FÉDÉRATION
BANCAIRE
FRANÇAISE

BAC DE TRI