OCTOBRE 2021

CYBER-SÉCURITÉ EN ENTREPRISE

8 RÉFLEXES CLÉS

N°6
LES GUIDES
SÉCURITÉ BANCAIRE

les clés de la banque

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 : octobre 2021

SOMMAIRE

INTRODUCTION

Si vous êtes victime de cybermalveillance, des conseils pratiques sont disponibles sur www.cybermalveillance.gouv.fr **le site national d'assistance et de prévention du risque numérique.**

2020 a été l'année de l'explosion des cyberattaques avec une multiplication par 4 des signalements et demandes d'assistance, tous publics confondus.

Les tentatives d'escroqueries sont nombreuses et les modes opératoires constamment renouvelés. Il s'agit ainsi :

- **de rançongiciels (17%),**
- **de piratage informatique (16%),**
- **de piratage de compte (11%),**
- **d'usurpation d'identité (8%),**
- **de virus (7%),**
- **de violation de données (7%),**
- **d'hameçonnage ou phishing (7%),**
- **de faux support technique (7%),**
- **de dénis de service (4 %),**
- **de faux ordre de virement (3%)...***

Internet et les outils numériques sont aujourd'hui incontournables dans l'exercice de votre activité, avec vos collaborateurs comme avec vos partenaires. Une faille de sécurité ou encore la communication de données confidentielles peut avoir de lourdes conséquences sur votre activité, voire sur la réputation de votre entreprise.

Ce guide vous présente quelques réflexes simples à adopter pour votre sécurité numérique, tant au niveau du matériel que du comportement de chacun (employé, collaborateur, partenaire...).

**Chiffres Cybermalveillance.*

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... ou encore pour leur faire réaliser des paiements.

1

Je sensibilise mes collaborateurs

POUR PROTÉGER VOTRE ENTREPRISE :

- **Sensibilisez** chacun de **vos collaborateurs** à la cybersécurité dans leur quotidien professionnel avec des exemples concrets.
- Adoptez une **charte informatique** pour préciser à l'ensemble de vos collaborateurs les conditions d'utilisation du matériel informatique de l'entreprise, de la messagerie, lors de déplacements professionnels ou encore pour l'utilisation mixte d'un matériel (usage professionnel et personnel).
- Développez 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 évoluent régulièrement (ex : fraude au président, fraude au changement de coordonnées bancaires).
- Mettez en place des **protocoles** et des **consignes** de sécurité, particulièrement pour les paiements, les changements d'IBAN d'un fournisseur et contrôlez-en la bonne application.

Cybermalveillance propose sur son site Internet un annuaire de professionnels labellisés « expert cyber » pour vous accompagner dans votre sécurité numérique.

RÉAGIR EN CAS D'ESCROQUERIE :

- Si vous pensez que des **données bancaires** ont été **récupérées frauduleusement, signalez-le immédiatement à la banque** pour stopper au plus vite toute escroquerie en cours. Faites opposition immédiatement à votre carte bancaire ou bloquer les virements/ prélèvements au débit de votre compte.
- Si des **mots de passe ou codes** ont été **révélés, changez-les** immédiatement.
- **Surveillez régulièrement vos comptes bancaires** pour détecter des opérations frauduleuses et les contester.

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

2

J'établis des procédures avec mes partenaires

POUR PROTÉGER VOTRE ENTREPRISE :

- **Établissez**, pour vos collaborateurs, **des protocoles précis** pour la réalisation de toutes vos opérations bancaires.
- Si une demande est inhabituelle ou concerne un changement d'IBAN, **vérifiez directement avec un contre appel auprès du partenaire** en utilisant toujours les coordonnées et procédures habituelles de contact.
- En cas de « rappel pour impayé », **prenez le temps d'effectuer des vérifications** sur la réalité de la prestation facturée et 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 EN CAS D'ESCROQUERIE :

- **Informez votre partenaire habituel** (banque, comptable, etc.), dont semble provenir le message frauduleux, pour lui signaler des tentatives de fraude utilisant son identité.
- **Surveillez** régulièrement **vos comptes bancaires** pour détecter des opérations frauduleuses et les contester.
- **Nettoyez régulièrement votre système informatique** (cf. page 16).

Sur un site Internet, les fraudes peuvent concerner le paiement d'articles commandés et le vol de données clients (coordonnées, mél, etc.). Votre site peut également être piraté et bloqué (c'est ce qu'on appelle le « déni de service »). Si vous disposez d'un site, vous devez en assurer la sécurité, notamment celle des données de vos clients. Il en va de votre crédibilité professionnelle et donc de la survie de votre activité.

3

Je sécurise mon site Internet

POUR PROTÉGER VOTRE ENTREPRISE :

- **Faites installer un certificat de sécurité en « https »**, choisissez un hébergement sécurisé avec une assistance 24h/24.
- Assurez-vous, auprès de votre banque ou de votre prestataire de paiement, de la **sécurité des solutions de paiement** proposées pour la vente à distance ainsi que des fonctionnalités de contrôle, analyse de risque, conformité à la réglementation sur l'authentification forte.
- Mettez en place une **solution d'authentification forte** de vos clients en e-commerce comme la réglementation l'exige. Cela vous permettra de limiter vos risques d'impayés liés à l'usurpation d'identité/fraude à la carte bancaire, mais également d'offrir une expérience de paiement fluide pour vos clients.
- **Sécurisez les données de vos clients** en les chiffrant, en changeant régulièrement les mots de passe, en mettant à jour vos antivirus…
- **Conservez uniquement les données utiles** de vos clients et évitez de stocker les numéros de carte bancaire.

RÉAGIR EN CAS D'ESCROQUERIE :

- En cas de fraude, **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, **consultez le site www.cybermalveillance.gouv.fr**. Une assistance pourra vous être fournie par les prestataires partenaires.
- En cas de violation des données personnelles de vos clients, vous devez **effectuer un signalement 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) a pour mission d'informer le public et de protéger les données personnelles.
Elle 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).

De nombreuses escroqueries sont rendues possibles grâce aux informations accessibles sur Internet (annonces légales, publications sur les sites de l'entreprise ou de ses partenaires commerciaux, réseaux sociaux professionnels ou personnels) ou encore recueillies directement auprès des collaborateurs par téléphone par exemple. Ce procédé qui consiste à obtenir et utiliser des informations à des fins frauduleuses s'appelle « l'ingénierie sociale ».

4

Je maîtrise la diffusion des données relatives à ma société

POUR PROTÉGER VOTRE ENTREPRISE :

- **Vérifiez** que **les contenus** que vous publiez sur votre site/page sur les réseaux sociaux ne sont pas sensibles (exemple : organigramme de votre entreprise).
- **Contrôlez** régulièrement **les informations disponibles** sur votre entreprise en tapant son nom dans un moteur de recherche.
- **Sensibilisez vos salariés** à ce risque spécifique, notamment en attirant leur attention sur les dangers des réseaux sociaux : informations, photos… qui pourraient être utilisées de façon malveillante et sur les enquêtes téléphoniques qui cherchent à recueillir des informations sur votre entreprise ou sur les personnes en charge des paiements.

RÉAGIR 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** (Commission Nationale de l'Informatique et des Libertés) pour faire valoir vos droits : accès, rectification, etc.

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

5

Je choisis mes mots de passe avec soin

POUR PROTÉGER VOTRE ENTREPRISE :

- **Définissez un mot de passe unique** pour chaque service, appareil, logiciel, application utilisée par votre entreprise…
- **Il ne doit contenir aucune information professionnelle ou personnelle** qui pourrait être découverte 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.**
- Le mot de passe **ne doit jamais être enregistré** sur votre équipement.

ATTENTION

Un mot de passe ne doit pas être écrit (post-it, carnet…) mais peut être enregistré dans un fichier chiffré.

RÉAGIR EN CAS D'ESCROQUERIE :

- En cas de divulgation de votre mot de passe, **changez-le immédiatement** pour le service concerné.
- Concernant votre messagerie, si des codes confidentiels d'autres applications figurent dans les courriels de votre boite de réception, modifiez-les également.

Sites et applications bancaires sont l'objet de nombreuses attaques/tentatives de fraudes que ce soit par des courriels de type phishing (hameçonnage) ou encore par des attaques informatiques de type virus ou cheval de Troie.

6

Je sécurise l'accès à mes services bancaires

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 votre expert-comptable ou à votre service financier par exemple :
  - demandez à votre banque, un code personnel pour chacun,
  - vérifiez que les opérations autorisées (consultation, virement, montant…) sont conformes aux habilitations.
- Ne vous connectez pas depuis un appareil ou un réseau Wi-Fi public.
- Pour votre navigation, **tapez vous-même l'adresse du site** de votre banque et ne suivez jamais un lien qui vous a été envoyé dans un courriel.
- **Suivez les consignes de sécurité** pour votre matériel informatique et votre connexion (cf. infra).

Votre banque ne vous demandera jamais votre mot de passe.

RÉAGIR EN CAS D'ESCROQUERIE :

- En cas de doute, **informez** immédiatement **votre banque** en utilisant le n° de téléphone habituel et la messagerie sécurisée et demandez un nouveau mot de passe.
- **Vérifiez les dernières opérations** effectuées sur votre compte.
- **Consultez** ensuite **votre compte quotidiennement** pour détecter toute anomalie et contestez les opérations frauduleuses s'il y a lieu.

L'accès à vos équipements (ordinateur, smartphone, tablette) et à vos logiciels doit vous être réservé. Vous devez aussi vous protéger des menaces liées aux 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.

7

Je sécurise mon matériel informatique et mes données

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** régulièrement mis **à jour et un système informatique de détection des menaces** (EDR).
- Limitez la possibilité d'installation de logiciels aux seules personnes habilitées (votre référent informatique par exemple ou la personne désignée comme administrateur).
- **Effectuez régulièrement des sauvegardes** de vos données sur des supports externes (disques durs de préférence) stockés à un autre endroit.
- Installez **régulièrement** les **mises à jour** proposées par les fabricants de matériel informatique et les éditeurs de logiciels pour corriger les failles de sécurité détectées. Vérifiez leur origine en contrôlant par exemple le site Internet officiel du fabricant/éditeur.
- Limitez, pour vos collaborateurs ou vous-même, l'utilisation à des fins professionnelles des appareils privés souvent moins sécurisés.
- N'introduisez pas de contenus en provenance de sources à la fiabilité inconnue (clé USB trouvée, sites Internet, pièce jointe d'un courriel suspect…).

RÉAGIR 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.
- N'effectuez **aucune opération** de banque à distance (connexion, virement, opposition…) **jusqu'à désinfection** de votre matériel.
- **Vérifiez les dernières opérations** effectuées 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.

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 qu'elle soit utilisée à votre insu.

8

Je protège ma connexion Internet

POUR PROTÉGER VOTRE ENTREPRISE :

- Choisissez un fournisseur d'accès Internet reconnu et consultez ses avertissements de sécurité.
- Configurez votre réseau Wi-Fi en choisissant **une clé de sécurité complexe** (WEP, WPA, WPA2 ou WPA3) depuis l'interface de votre fournisseur d'accès.
- Si vous mettez un réseau Wi-Fi à disposition de vos clients ou partenaires, communiquez-leur **une clé de sécurité spécifique**, différente de la clé principale.
- Vérifiez la présence de **https** devant l'adresse du site auquel vous vous connectez, **icône d'une clé** ou d'un **cadenas** dans la fenêtre du navigateur Internet.
- **Contrôlez l'adresse exacte** du site et qu'aucune autre fenêtre Internet n'est ouverte.
- **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.

RÉAGIR EN CAS D'ESCROQUERIE :

- En cas de suspicion d'utilisation de votre connexion, **modifiez le mot de passe de votre réseau Wi-Fi** en utilisant un autre terminal et un autre accès à Internet (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** dédié (disque dur) les données qui ne sont pas corrompues.
- **Utilisez** votre **antivirus** et des **logiciels** spécialisés **de récupération** des fichiers.

Depuis juillet 2021, en cas de vulnérabilité ou de campagne d'attaque particulièrement critique, une notice succincte et compréhensible sera éditée par Cybermalveillance et l'ANSSI (agence nationale de la sécurité des systèmes d'information) et diffusée largement pour permettre une information et une réaction rapides au sein notamment des plus petites entreprises.

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

Pour aller plus loin, consultez nos autres mini-guides dédiés à la cybersécurité :

- **Ordres de virement des entreprises - 9 réflexes sécurité**
- **Cybersécurité au quotidien - 9 réflexes clés**

CYBERSÉCURITÉ EN ENTREPRISE
LES RÉFLEXES CLÉS

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 mon matériel informatique et mes données
8. Je protège ma connexion Internet

les clés de la banque

www.lesclesdelabanque.com

Le site pédagogique sur la banque et l'argent

www.cybermalveillance.gouv.fr

FÉDÉRATION
BANCAIRE
FRANÇAISE

Avec le soutien de l'ANSSI