Cybersolide

GUIDE GRATUIT · ÉDITION DE NOVEMBRE 2026

Dix problèmes de sécurité des PME

Une page par problème, une histoire, des gestes concrets.

AU SOMMAIRE

01 Un escroc écrit en votre nom

02 Un mot de passe volé ouvre la messagerie

03 Un faux RIB ou un faux ordre de virement

04 Un faux message pousse à cliquer

05 Les fichiers sont chiffrés, la sauvegarde aussi

06 Un appareil resté sans mise à jour

07 Le même mot de passe partout

08 Une porte laissée ouverte sur internet

09 Un ancien salarié garde ses accès

10 Le jour où l'attaque arrive

Par où commencer : trois gestes, la première semaine

Dix problèmes suivent, classés par priorité. Si vous n'avez qu'une semaine, ces trois gestes protègent le plus pour le moins d'effort.

LUNDI

01

Protégez votre nom de domaine

Lancez le diagnostic gratuit, puis faites publier SPF, DKIM et DMARC. C'est le geste qui permet aux messageries de refuser les faux e-mails envoyés à votre nom.

Détail page 3

MERCREDI

02

Exigez une seconde preuve à la connexion

Activez-la sur la messagerie de l'entreprise. Une demi-journée, et un mot de passe volé cesse de suffire.

Détail page 4

VENDREDI

03

Écrivez la règle du rappel

Aucun changement de RIB, aucun virement pressant sans rappeler au numéro connu. Une ligne, une heure, aucun coût.

Détail page 5

Comment lire ce guide. Chaque page tient seule : le problème, une histoire qui pourrait être la vôtre, les gestes, le temps et le coût, et de quoi vérifier que c'est fait. Votre prestataire informatique peut appliquer la plupart d'entre eux : donnez-lui la page. Ces gestes recoupent les mesures de base de la directive européenne NIS2, si votre entreprise en relève.

Un escroc écrit en votre nom

Tant que votre nom de domaine (ce qui suit le @ de vos adresses) n'est pas protégé, n'importe qui peut envoyer un e-mail qui semble venir de vous.



Un faux e-mail
signé de votre nom

SPF, DKIM, DMARC
sur votre domaine

Votre client
ne le reçoit pas

> UNE HISTOIRE · UNE ENTREPRISE DE MAÇONNERIE, DOUZE SALARIÉS
>
> Un mardi, trois clients reçoivent une facture de « compta@votre-entreprise.fr » avec un nouveau RIB. L'adresse et le logo sont les bons, et aucune boîte n'a été piratée : rien n'indiquait aux messageries comment reconnaître les vrais e-mails de l'entreprise. Deux clients paient.

CE QU'IL FAUT FAIRE

1. **SPF : déclarez les expéditeurs autorisés.** Ajoutez une ligne TXT dans la zone DNS, le carnet d'adresses du domaine. Pour Microsoft 365 seul : `v=spf1 include:spf.protection.outlook.com -all`.
2. **DKIM : faites signer chaque e-mail.** Activez la signature chez chaque expéditeur, puis publiez dans le DNS ce qu'il demande (deux CNAME chez Microsoft 365, une clé TXT chez Google).
3. **DMARC : dites quoi faire des faux.** Publiez `_dmarc` avec `v=DMARC1; p=none; rua=mailto:...` pour recevoir des rapports. Après quelques semaines de corrections, passez à `p=quarantine`, puis à `p=reject`.

À savoir. Un domaine réservé mais muet reçoit `v=spf1 -all`. Ces réglages n'arrêtent ni un domaine sosie (`votre-entreprlse.fr`, avec un l à la place du i), ni une boîte réellement piratée : voir les problèmes 2 et 4.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Une demi-journée pour SPF et DKIM, puis 4 à 6 semaines avant `p=reject`	Aucun logiciel à acheter	SPF, DKIM et DMARC en `p=reject` sont publiés, et vos factures arrivent toujours.

Un mot de passe volé ouvre la messagerie

Un mot de passe se devine, se réutilise ou se saisit sur une fausse page. S'il est le seul verrou, qui le tient est chez vous.



Un mot de passe volé

Une seconde preuve sur le téléphone

Votre messagerie reste fermée

UNE HISTOIRE · UN CABINET COMPTABLE, QUINZE PERSONNES

Lundi, une collaboratrice reçoit « Votre boîte est pleine, reconnectez-vous » et saisit son mot de passe sur la fausse page. Le soir, quelqu'un lit ses échanges avec les clients. Avec une seconde preuve à la connexion, le mot de passe seul n'aurait rien ouvert.

CE QU'IL FAUT FAIRE

1. **Activez la seconde preuve, d'abord sur la messagerie.** Sans coût. Microsoft 365 : les « paramètres de sécurité par défaut » de Microsoft Entra. Google Workspace : la validation en deux étapes, avec un début dans 2 à 4 semaines pour que chacun s'inscrive.
2. **Préférez une application au SMS.** Microsoft Authenticator ou Google Authenticator, gratuites, sur le téléphone de chacun.
3. **Donnez une clé aux comptes sensibles.** Administrateurs et personnes qui valident des paiements : une clé physique ou une passkey, qu'une fausse page ne trompe pas.
4. **Prévoyez un secours.** Une deuxième clé ou des codes de secours, au bureau et non dans la boîte qu'ils protègent.

À savoir. Selon Microsoft, la double authentification bloque plus de 99,9 % des attaques sur les comptes.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Une demi-journée de prestataire, puis dix minutes par salarié	Gratuit avec une application, quelques dizaines d'euros par clé physique	Chaque messagerie demande une seconde preuve, et les comptes d'administration et de paiement ont une clé.

Un faux RIB ou un faux ordre de virement

Une fausse facture, ou un faux dirigeant qui réclame un virement « urgent et confidentiel », peut vider un compte d'un coup. L'argent parti revient rarement.



Un nouveau RIB
reçu par e-mail

Un rappel au numéro
de votre dossier

Le virement part
au bon compte

UNE HISTOIRE · UNE SOCIÉTÉ DE NÉGOCE, TRENTE PERSONNES

> « Suite à un changement de banque, merci d'utiliser ce RIB pour votre prochain règlement de 18 400 €. » Le message vient de l'adresse habituelle du fournisseur, dont la messagerie a été piratée. La comptable rappelle le fournisseur au numéro de son dossier : il n'a jamais changé de banque.

CE QU'IL FAUT FAIRE

1. **Écrivez une règle d'une ligne.** Tout changement de RIB se vérifie en rappelant le numéro de votre dossier, jamais celui du message, même si la demande vient d'un chef.
2. **Demandez une double validation.** Dans la banque en ligne, au-delà d'un montant fixé, 5 000 € par exemple.
3. **Lisez l'alerte de votre banque.** Depuis le 9 octobre 2025, elle compare le nom du bénéficiaire et l'IBAN à chaque virement SEPA. Une « correspondance partielle » ou une absence de correspondance se règle par un appel.
4. **Si le virement est parti, agissez dans l'heure.** Appelez la banque pour demander le retour des fonds, gardez les messages, portez plainte.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Une heure	Gratuit	La règle est écrite et connue de ceux qui paient, et la banque demande une seconde validation au-delà du montant fixé.

Un faux message pousse à cliquer

L'hameçonnage est un faux message qui vous fait saisir un mot de passe ou un numéro de carte sur une fausse page, par e-mail, SMS ou messagerie.



Un message pressant
et une petite somme

Vous lisez l'adresse
avant de cliquer

Vous ne saisissez
rien, vous signalez

UNE HISTOIRE · UN GARAGE, HUIT SALARIÉS

> « Votre colis n'a pas pu être livré. Réglez 1,99 € de frais sous 24 heures sur colis-suivi-fr.info. » L'assistante saisit le numéro de la carte de l'entreprise, et des débits partent à l'étranger. Trois signes auraient dû l'arrêter : l'urgence, la petite somme, une adresse qui n'est pas celle du transporteur.

CE QU'IL FAUT FAIRE

1. **Regardez l'adresse réelle.** Celle de l'expéditeur, pas son nom affiché, et celle du lien : survolez-le, ou appuyez longuement sur téléphone.
2. **Ne saisissez jamais un mot de passe depuis un lien reçu.** Passez par vos favoris ou l'application.
3. **Méfiez-vous de la pression.** Urgence, menace, bonne affaire : au moindre doute, rappelez l'organisme à un numéro que vous connaissez.
4. **Formez l'équipe une fois par an.** SensCyber, de Cybermalveillance.gouv.fr, est gratuit : trois modules de 25 à 45 minutes.

À savoir. Pour signaler : signal-spam.fr (e-mails), 33700 (SMS), Phishing Initiative (faux sites).

TEMPS	COÛT	✓ C'EST FAIT QUAND
Une demi-heure par an et par salarié	Gratuit	Chacun sait à qui signaler un message douteux, et une séance a eu lieu dans l'année.

Les fichiers sont chiffrés, la sauvegarde aussi

Un rançongiciel, programme qui bloque vos fichiers contre rançon, chiffre aussi les sauvegardes branchées. Sans copie hors d'atteinte, il ne reste qu'à payer ou tout perdre.



Vos fichiers
au bureau

Une copie
sur un autre support

Une copie hors
des locaux

> UNE HISTOIRE · DEUX BUREAUX D'ÉTUDES VOISINS
>
> Tous deux sauvegardent chaque nuit. Le premier sur un disque réseau toujours branché : le rançongiciel le chiffre avec le reste. Le second change de disque chaque vendredi et emporte l'ancien chez le dirigeant : il perd quelques jours de travail, au lieu de tout.

CE QU'IL FAUT FAIRE

1. **Gardez plusieurs copies, dont une ailleurs.** Trois copies, sur deux supports, dont une hors des locaux.
2. **Déconnectez ou verrouillez une copie.** Un disque débranché après chaque sauvegarde, ou une sauvegarde en ligne « immuable », que personne ne peut effacer pendant trente jours.
3. **Sauvegardez aussi ce qui est en ligne.** Messagerie et fichiers de Microsoft 365 ou Google : leur corbeille ne protège pas d'une suppression en masse.
4. **Restaurez pour de vrai chaque trimestre.** Un dossier remis en place, le temps noté. Une sauvegarde jamais testée est une hypothèse.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Une demi-journée de prestataire, puis une heure par trimestre	Souvent quelques dizaines d'euros par mois, selon le volume	Une copie hors ligne ou immuable existe, et une restauration a réussi il y a moins de trois mois.

Un appareil resté sans mise à jour

Une mise à jour ferme des failles que les attaquants connaissent déjà. Un seul appareil en retard suffit à ouvrir une porte.



Des robots testent
la faille publiée

Votre appareil,
déjà mis à jour

La faille est fermée,
rien à exploiter

UNE HISTOIRE · UN CABINET D'ARCHITECTES, VINGT PERSONNES

> Le fabricant d'un pare-feu publie un correctif pour une faille grave. Dans les jours qui suivent, des programmes automatiques essaient tous les appareils de ce modèle visibles sur internet. Le cabinet qui installe le correctif le lendemain passe à côté. Celui qui attend la revue du trimestre reste ouvert des semaines.

CE QU'IL FAUT FAIRE

1. **Automatisez ordinateurs et téléphones.** Mises à jour automatiques de Windows, macOS, des navigateurs et des téléphones, et un redémarrage chaque semaine.
2. **Traitez à part pare-feu, box et VPN.** Visibles de l'extérieur, ils installent leurs correctifs de sécurité dès leur publication.
3. **Remplacez ce qui n'est plus pris en charge.** Windows 10 n'a plus de mises à jour de sécurité gratuites depuis le 14 octobre 2025 : passez à Windows 11 si l'ordinateur le permet, sinon remplacez-le.
4. **Pensez au site web.** WordPress, son thème et ses modules se mettent à jour chaque mois, après une sauvegarde.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Une heure de prestataire, puis un quart d'heure par mois	Aucun logiciel à acheter, hors remplacement des appareils trop anciens	Aucun appareil en service n'est privé de correctifs, et les appareils exposés se mettent à jour sous quelques jours.

Le même mot de passe partout

Personne ne retient quarante mots de passe. On en réutilise un, et la fuite d'un seul site ouvre alors tous les autres.



Vous retenez
une seule phrase

Le gestionnaire
garde tous les autres

Un mot de passe
différent par site

UNE HISTOIRE · UN COMMERCIAL, UNE PME DE SERVICES

> Il utilise « Lyon2019! » pour sa messagerie et pour le site d'un salon professionnel. Le salon se fait voler sa base de comptes, et trois semaines plus tard quelqu'un se connecte à sa messagerie depuis l'étranger. Avec un mot de passe par site, la fuite n'aurait ouvert que le salon.

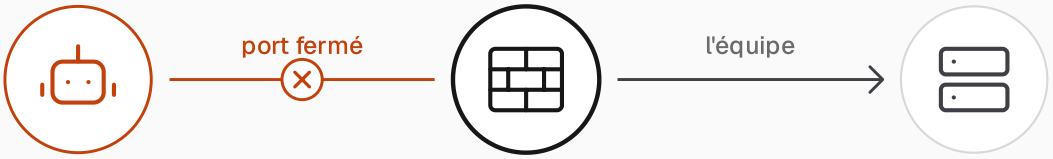
CE QU'IL FAUT FAIRE

1. **Équipez chacun d'un gestionnaire, protégé par une longue phrase.** Bitwarden, 1Password ou Dashlane, en offre entreprise qui permet de partager des accès. KeePassXC, gratuit, suffit pour deux ou trois personnes. Une phrase longue, jamais utilisée ailleurs, protège le gestionnaire.
2. **Laissez-le inventer les mots de passe.** Un par site, de 12 signes au moins, que personne n'a besoin de connaître.
3. **Changez d'abord les comptes qui comptent.** Messagerie, banque, comptabilité. Les autres suivent au fil des connexions.
4. **Vérifiez les fuites.** Saisissez les adresses de l'entreprise sur haveibeenpwned.com, et changez les mots de passe des comptes touchés.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Deux heures pour l'installer, quelques semaines pour tout y ranger	Quelques euros par utilisateur et par mois, gratuit avec KeePassXC	Chaque salarié se sert du gestionnaire, et aucun mot de passe ne traîne dans un tableur ou sur un post-it.

Une porte laissée ouverte sur internet

Un bureau à distance, un ancien site, une caméra ou une imprimante restent visibles de l'extérieur, où des robots les essaient jour et nuit.



Des robots frappent à la porte

Une seule entrée, le VPN protégé

Postes et fichiers invisibles

UNE HISTOIRE · UNE PME DE TRANSPORT, VINGT-CINQ PERSONNES

> Pour dépanner pendant un confinement, le prestataire a ouvert sur internet le bureau à distance d'un serveur. Quatre ans plus tard, plus personne ne s'en souvient. Un robot trouve l'accès, essaie des mots de passe, entre et lance un rançongiciel un samedi soir.

CE QU'IL FAUT FAIRE

1. **Demandez la liste de ce qui est visible.** Chaque service joignable depuis internet, et pourquoi. Ce qui n'a pas de raison se coupe. L'accès d'un fournisseur se ferme dès qu'il a fini.
2. **Pas de bureau à distance en direct.** L'accès passe par un VPN (tunnel chiffré) à jour, avec la double authentification, jamais par un port ouvert (RDP, 3389).
3. **Changez les mots de passe d'origine.** Box, routeurs, imprimantes, caméras : ceux du carton sont connus de tous les robots.

À savoir. L'ANSSI note que l'accès à distance (RDP) reste l'une des portes d'entrée préférées des rançongiciels.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Deux à quatre heures de prestataire	Aucun logiciel à acheter	La liste des services visibles est écrite et justifiée, et aucun bureau à distance n'est ouvert sans VPN.

Un ancien salarié garde ses accès

Un compte oublié est une porte que personne ne surveille : celle d'un ancien salarié, d'un stagiaire, d'un prestataire dont la mission est finie.



Un salarié
quitte l'entreprise

La liste
de ses accès

Tout est fermé
le dernier jour

UNE HISTOIRE · UN CABINET DE CONSEIL, DIX-HUIT PERSONNES

> Un commercial part chez un concurrent. Trois mois plus tard, son compte du logiciel clients fonctionne encore, et il consulte le fichier depuis chez lui. Personne ne le voit : personne ne savait qu'il avait ce compte.

CE QU'IL FAUT FAIRE

1. **Tenez la liste des accès de chaque personne.** Outils, comptes partagés, badges, ordinateurs et téléphones prêtés.
2. **Le dernier jour, tout se ferme.** Comptes bloqués, matériel rendu, mots de passe partagés qu'elle connaissait changés. Un prestataire a son propre compte, fermé à la fin de sa mission.
3. **Traitez la messagerie avec méthode.** La personne retire ses messages personnels, ses fichiers de travail passent à un responsable, puis l'adresse est supprimée.
4. **À l'arrivée, le strict nécessaire.** Chacun reçoit les accès de son poste, notés dans la liste.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Une heure pour la liste, un quart d'heure par départ	Gratuit	La liste est à jour, et une check-list de départ est appliquée à chaque sortie.

Le jour où l'attaque arrive

Le jour d'une attaque, on perd les premières heures à chercher un numéro et à hésiter. Une page préparée à l'avance les fait gagner.



Écrans bloqués, rançon demandée

La page du classeur : qui appeler

Plainte sous 72 h, CNIL si besoin

UNE HISTOIRE · UNE ENTREPRISE DE FOURNITURES, QUARANTE PERSONNES

Un matin, les écrans affichent une demande de rançon. La responsable administrative sort la page du classeur, fait débrancher les câbles réseau sans éteindre les machines, appelle le prestataire et l'assureur, et dépose plainte avant le soir.

CE QU'IL FAUT FAIRE

1. **Préparez une page, avec les vrais numéros.** Prestataire, assureur (à appeler avant d'engager des frais), banque, dirigeant et son remplaçant, plus 17cyber.gouv.fr qui guide les victimes pas à pas. Imprimée, rangée là où on la trouve sans ordinateur.
2. **Isolez, sans éteindre.** Débranchez le câble réseau et coupez le Wi-Fi des machines touchées, puis la box. Laissez-les sous tension : des preuves s'effacent à l'extinction.
3. **Portez plainte dans les 72 heures.** Avec une assurance cyber, c'est la condition pour être indemnisé de l'atteinte à vos systèmes. Faites-le avant de réinstaller, pour garder les preuves.
4. **Ne payez pas la rançon. Déclarez les fuites.** Si des données personnelles sont touchées, la CNIL se prévient dans les meilleurs délais, si possible sous 72 heures.

TEMPS	COÛT	✓ C'EST FAIT QUAND
Une heure de préparation	Gratuit	La page existe, avec les vrais numéros, elle est imprimée, et le dirigeant et son remplaçant savent où elle est.

Faire vérifier votre domaine, gratuitement

Le diagnostic de cybersolide.fr lit les données publiques de votre nom de domaine. Rien à installer, rien à demander à votre prestataire. Il répond à trois questions.

cybersolide.fr

Gratuit, sans inscription. Le résultat arrive en quelques secondes.

01

Un escroc peut-il écrire en votre nom ?

02

Des noms proches du vôtre sont-ils déjà réservés ?

03

Vos e-mails arrivent-ils bien chez vos clients ?

SI LE RÉSULTAT N'EST PAS AU VERT

Messagerie protégée

Nous mettons en place SPF, DKIM et DMARC pour vous, à distance et par écrit, jusqu'à `p=reject`, en 4 à 6 semaines, puis nous gardons le réglage douze mois.

LA PREMIÈRE ANNÉE

390 € HT

ENSUITE, LA GARDE

120 € HT par an

SI CE N'EST PAS ATTEINT

Remboursé, sous 60 jours, de notre fait

Sources

Chaque fait technique ou chiffré de ce guide a été relu dans ces pages le 10 novembre 2026. Les histoires sont des situations types, construites pour illustrer, pas des affaires réelles.

Faux ordres de virement (FOVI)
Cybermalveillance.gouv.fr · cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/escroquerie-faux-ordres-virement-fovi

Hameçonnage
Cybermalveillance.gouv.fr · cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Rançongiciels
Cybermalveillance.gouv.fr · cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Sauvegardes, mises à jour, mots de passe
Cybermalveillance.gouv.fr · cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques

SensCyber, formation gratuite
Cybermalveillance.gouv.fr · cybermalveillance.gouv.fr/tous-nos-contenus/senscyber-e-sensibilisation-cybersecurite

17Cyber, assistance aux victimes
Police, Gendarmerie, Cybermalveillance.gouv.fr · 17cyber.gouv.fr

Notifier une violation de données
CNIL · cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Générer un mot de passe solide
CNIL · cnil.fr/fr/generer-un-mot-de-passe-solide

Obligation de plainte sous 72 heures (art. L. 12-10-1 du code des assurances)
Direction générale du Trésor · tresor.economie.gouv.fr (FAQ sur l'obligation de dépôt de plainte)

La vérification du bénéficiaire d'un virement
La finance pour tous (Banque de France) · lafinancepourtous.com/2025/09/29/virement-la-verification-du-beneficiaire-par-la-banque-devient-obligatoire

État de la menace rançongiciel, 2021
ANSSI, CERT-FR · cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf

SPF, DKIM : configurer pour Microsoft 365
Microsoft Learn · learn.microsoft.com/defender-office-365/email-authentication-spf-configure

Exigences d'authentification des expéditeurs
Google Workspace, aide · support.google.com/a/answer/81126

RFC 7208 (SPF) et RFC 7489 (DMARC)
IETF · rfc-editor.org/rfc/rfc7208 et rfc7489

One simple action you can take to prevent 99.9 percent of account attacks
Microsoft Security, 20 août 2019 · microsoft.com/security/blog/2019/08/20

Windows 10 Home and Pro, cycle de vie
Microsoft Learn · learn.microsoft.com/lifecycle/products/windows-10-home-and-pro