



LIVRE BLANC · OCTOBRE 2026

Cybersécurité des petites entreprises

L'essentiel pour artisans, commerçants et TPE :
des gestes simples, des outils gratuits,
et qui appeler quand on est dépassé.

Avant de commencer

Ce petit livre s'adresse à ceux qui font tourner une petite entreprise sans service informatique : artisans, commerçants, professions libérales, gîtes et petites structures. Il se lit en un quart d'heure. Il ne demande aucune connaissance technique et ne vous vend rien : tout ce qu'il recommande est gratuit ou déjà dans votre ordinateur.

Le constat d'abord. Les attaques qui touchent les petites entreprises ne sont presque jamais des opérations spectaculaires. Ce sont des messages bien imités, un mot de passe réutilisé, une sauvegarde qui n'existait pas le jour où l'ordinateur est tombé en panne. Les mêmes erreurs reviennent, et les mêmes gestes simples les évitent.

Ce qu'il faut retenir en cinq lignes

1	Un mot de passe différent par compte, rangé dans un gestionnaire.
2	La double authentification sur la messagerie, la banque et les comptes importants.
3	Les mises à jour automatiques, et pas de machine dont le support est terminé.
4	Une sauvegarde qu'on a déjà testée, dont une copie est débranchée.
5	Le réflexe de rappeler avant de payer, de cliquer ou de changer un RIB.

Les pages suivantes détaillent chaque geste, avec l'outil gratuit qui convient. Si, en route, vous vous dites que ce n'est pas pour vous, la dernière page vous explique comment me demander un coup de main. Ce n'est pas une honte : l'informatique est mon métier, pas le vôtre.

Où en est la menace ?

Quelques chiffres tirés des deux sources publiques de référence en France : Cybermalveillance.gouv.fr (rapport d'activité 2025, publié en mars 2026) et l'ANSSI, l'agence de l'État chargée de la sécurité informatique (panorama de la cybermenace 2025, présenté le 11 mars 2026).

Plus de 500 000

victimes assistées par Cybermalveillance.gouv.fr en 2025, soit 20 % de plus qu'en 2024.

+ 73 %

de demandes d'assistance venant d'entreprises et d'associations en un an (particuliers : + 47 %). Les entreprises sont la catégorie dont les demandes progressent le plus vite.

21 % · 16 % · 13,5 %

Les trois premières menaces pour les entreprises et associations : piratage de compte (21 %), hameçonnage (16 %) et faux ordres de virement (13,5 %). Viennent ensuite les rançongiciels (8,1 %) et les violations de données (6,6 %).

+ 170 %

de fraudes au virement : elles s'étendent à la facturation électronique et à la paie. Les faux conseillers bancaires progressent de 159 %.

1 366

incidents traités par l'ANSSI en 2025, dont 128 compromissions par rançongiciel. Les PME, TPE et ETI restent la catégorie la plus touchée par ces attaques.

Ce que cela dit

Deux enseignements. Le premier : les attaques visent les habitudes de gestion courantes (un virement, une facture, un RIB qui change) bien plus que des failles techniques compliquées. Le second : une petite entreprise est souvent touchée sans avoir été piratée elle-même, parce que ses coordonnées figurent dans une fuite de données survenue ailleurs et servent à rendre un message plausible. L'ANSSI note aussi que l'intelligence artificielle abaisse le niveau d'entrée des attaquants, notamment pour fabriquer des messages d'hameçonnage convaincants : un texte bien écrit n'est plus un gage de sérieux.

Les parts ci-dessus sont des parts de demandes d'assistance : elles mesurent ce que les victimes ont signalé, pas le nombre réel d'attaques.

Les huit gestes qui comptent

Dans l'ordre où je vous conseille de les faire. Les trois premiers suffisent déjà à écarter une grande partie des mauvaises surprises.

1

Un mot de passe par compte, rangé dans un gestionnaire

Cybermalveillance.gouv.fr recommande au minimum 12 signes et un mot de passe différent pour chaque compte. Personne ne retient cinquante mots de passe de ce genre : c'est le rôle d'un gestionnaire. Vous ne reprenez qu'une seule phrase de passe, celle qui l'ouvre, et il fabrique et range les autres.

Évitez de noter vos mots de passe sur papier, dans un courriel ou dans un fichier non protégé.

Gratuit : KeePassXC (logiciel libre, en français ; sa version 2.7.9 est certifiée par l'ANSSI selon Cybermalveillance.gouv.fr) ou Bitwarden, dont la version gratuite n'est limitée ni en nombre de mots de passe ni en nombre d'appareils.

2

La double authentification partout où c'est possible

Même si quelqu'un découvre votre mot de passe, il lui manque le second élément : un code reçu par SMS ou généré par une application, une clé dédiée ou votre empreinte. Commencez par la messagerie (c'est elle qui permet de réinitialiser tout le reste), la banque, vos comptes Google ou Microsoft, la fiche Google de votre établissement et vos réseaux sociaux.

Le piratage de compte est la première menace signalée par les entreprises : c'est le geste qui rapporte le plus pour le moins d'efforts.

Gratuit : l'option est incluse dans tous les grands services. Pour générer les codes, 2FAS est une application gratuite, sans création de compte.

3

Les mises à jour, et rien qui soit hors support

Chaque mise à jour de sécurité ferme une faille que les attaquants connaissent déjà. Activez le téléchargement et l'installation automatiques sur les ordinateurs, les téléphones, mais aussi la box, l'imprimante réseau et les caméras s'il y en a.

Point d'actualité : Microsoft a mis fin au support de Windows 10 le 14 octobre 2025. Passé cette date, il ne fournit plus de mises à jour de sécurité gratuites, sauf programme payant pour les entreprises. Un ordinateur qui l'utilise encore doit passer à Windows 11 s'il en est capable, ou être remplacé. Vérifiez aussi la date de fin de support avant tout achat.

Gratuit : les mises à jour automatiques de Windows, de macOS, d'Android et d'iOS.

4

Des sauvegardes qui existent, qui sont débranchées, et qu'on a testées

Un rançongiciel chiffre vos fichiers et réclame de l'argent pour les rendre. Une panne, un vol, un incendie ont le même effet. La parade est la même : une copie récente. Deux précautions que Cybermalveillance.gouv.fr met en avant : déconnecter le support de sauvegarde quand on ne s'en sert pas (un programme malveillant détruit aussi les copies restées branchées), et vérifier régulièrement qu'on sait restaurer un fichier.

On résume souvent la bonne pratique par la règle dite « 3-2-1 » : trois copies, sur deux supports différents, dont une hors de l'entreprise.

Gratuit : la sauvegarde intégrée à Windows ou à macOS (Time Machine) vers un disque externe, qu'on débranche ensuite. Un disque externe coûte quelques dizaines d'euros, une seule fois.

5

Un antivirus à jour

Un antivirus, gratuit ou payant, reste une protection de base utile à condition d'être à jour. Sous Windows, Microsoft Defender est déjà installé et gratuit : vérifiez simplement qu'il est actif. N'installez jamais un second antivirus par-dessus, et méfiez-vous des fenêtres qui vous annoncent un virus et vous poussent à télécharger quelque chose : ce sont souvent elles, le piège.

Gratuit : Microsoft Defender (Windows) ou la protection native de macOS.

6

Le réflexe du rappel : on vérifie avant de cliquer, payer ou changer un RIB

Les signes d'un message d'hameçonnage : une offre trop belle ou un remboursement inattendu, une pièce jointe que vous n'attendiez pas, une adresse d'expéditeur étrange, un lien dont l'adresse diffère d'une lettre du site réel, une urgence. Aucune banque ne demande vos identifiants par message ou téléphone.

Le cas qui coûte le plus cher : le « changement de RIB ». Un message, en apparence de votre fournisseur ou de votre expert-comptable, annonce de nouvelles coordonnées bancaires. Règle simple : rappelez la personne au numéro que vous avez déjà, jamais à celui du message.

Gratuit : il suffit d'un téléphone et d'un numéro que vous connaissez.

7

Séparer le professionnel et le personnel

Un compte, un ordinateur ou un espace de stockage utilisé pour tout est un point faible : si l'un est piraté, tout tombe. Gardez une messagerie, des appareils et un espace de fichiers distincts pour l'activité de l'entreprise et pour la vie de famille. C'est l'une des dix mesures essentielles de Cybermalveillance.gouv.fr.

Gratuit : rien à acheter : c'est une habitude.

8

Savoir à l'avance qui appeler

Le jour où cela arrive, on perd ses moyens. Notez dès maintenant, près de l'ordinateur, les contacts de la page « En cas d'incident », et dites à vos salariés à qui signaler un message louche : l'important n'est pas de ne jamais se tromper, mais de le dire tout de suite.

Gratuit : 17Cyber, le dispositif d'assistance de la Police, de la Gendarmerie et de Cybermalveillance.gouv.fr.

Les aides publiques gratuites

L'État propose plusieurs services, gratuits et sérieux, que presque personne ne connaît. Je vous conseille de commencer par le premier.

MonAideCyber	Un diagnostic gratuit de premier niveau, d'une durée d'1 h 30, réalisé par un « Aidant cyber » formé par l'ANSSI. Il couvre six thèmes (organisation, accès, postes, infrastructures et données, sensibilisation, réaction à une attaque) et débouche sur six mesures à mettre en œuvre dans les six mois, avec un point de suivi à six mois.	monaide.cyber.gouv.fr
17Cyber	Dispositif d'assistance de la Police nationale, de la Gendarmerie nationale et de Cybermalveillance.gouv.fr, accessible à toutes les victimes d'infractions numériques, entreprises comprises. Quelques questions en ligne conduisent à des conseils adaptés ; en cas d'urgence, appeler le 17 ou le 112.	17cyber.gouv.fr
Cybermalveillance .gouv.fr	Le site de référence : fiches pratiques, fiches réflexes par type de problème, et deux outils de sensibilisation gratuits. SensCyber (trois modules de 25 à 45 minutes avec attestation) et MalletteCyber Pro, un kit clé en main pour animer un atelier avec vos salariés.	cybermalveillance.gouv.fr
SecNumacadémie	Un cours en ligne gratuit de l'ANSSI, en quatre modules d'1 h 30 à 2 h, avec des exemples tirés de la vie des entreprises.	à rechercher par son nom
CSIRT régionaux	Quatorze centres régionaux de réponse aux incidents, à contacter en cas d'attaque, pour les PME, collectivités et associations. Ils font aussi de la prévention.	à rechercher par son nom
France Num	L'initiative de l'État pour le numérique des petites entreprises : guides, rubrique « Protéger mon entreprise » et liste de formations gratuites.	à rechercher par son nom

Ces dispositifs évoluent : vérifiez leur adresse et leurs conditions sur les sites officiels avant d'y recourir.

Où en êtes-vous ?

Cochez ce qui est vrai aujourd'hui, sans vous raconter d'histoires : personne ne regarde.

- ☐ Chacun de mes comptes a un mot de passe différent, d'au moins 12 signes.
- ☐ J'utilise un gestionnaire de mots de passe.
- ☐ La double authentification est activée sur ma messagerie et sur ma banque.
- ☐ Mes ordinateurs se mettent à jour automatiquement.
- ☐ Aucun de mes ordinateurs n'utilise un système dont le support est terminé (par exemple Windows 10).
- ☐ J'ai sauvegardé les fichiers de l'entreprise au cours du dernier mois.
- ☐ Une copie de ma sauvegarde est débranchée, ou conservée hors de l'entreprise.
- ☐ J'ai déjà essayé de restaurer un fichier depuis ma sauvegarde.
- ☐ Avant de modifier un RIB, je rappelle le fournisseur à un numéro que je connais.
- ☐ Mes salariés (ou moi-même) savons reconnaître un faux message.
- ☐ Mes comptes et mes appareils professionnels sont séparés des personnels.
- ☐ Je sais qui appeler si je suis victime d'une attaque.

Comptez vos cases cochées

10 à 12 : vous avez une bonne base. Vérifiez surtout que votre sauvegarde se restaure vraiment. **6 à 9** : il reste quelques priorités ; commencez par celles qui sont décochées parmi les gestes 1, 2 et 4. **0 à 5** : rien d'irréversible, mais ne remettez pas à demain : faites d'abord les gestes 1, 2 et 4, puis demandez le diagnostic gratuit MonAideCyber.

Ce petit test est indicatif : il ne remplace pas un véritable audit.

En cas d'incident

Un message cliqué trop vite, un compte qui ne répond plus, des fichiers devenus illisibles. Dans l'ordre :

1	Gardez votre calme et isolez. Coupez l'appareil concerné du réseau (câble, Wi-Fi) pour limiter les dégâts. Ne payez aucune rançon sans avis.
2	Conservez les preuves. Gardez le message, la capture d'écran, la demande de rançon : ils serviront à la plainte et à l'assurance.
3	Prévenez votre banque si vous avez communiqué des coordonnées bancaires ou constaté un prélèvement frauduleux : faites opposition tout de suite.
4	Changez vos mots de passe du compte touché et de tous ceux où vous aviez le même, depuis un appareil sain ; activez la double authentification.
5	Demandez de l'aide. 17Cyber (17cyber.gouv.fr) pose quelques questions et oriente. En cas d'urgence, appelez le 17 ou le 112. Le 114 par SMS si vous ne pouvez pas parler ou entendre.
6	Déposez plainte auprès de la police ou de la gendarmerie, ou par écrit au procureur de la République.
7	Signalez. Courriels : Signal Spam. SMS : 33700 (gratuit). Faux sites : Phishing Initiative. Conseils sur la marche à suivre : Info Escroqueries, 0 805 805 817 (appel gratuit, en semaine de 9 h à 18 h 30).

Pour un message d'hameçonnage cliqué, ces étapes suivent les conseils de la fiche réflexe de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr).

Si cela vous paraît trop technique

Beaucoup de mes clients ont commencé ainsi : ils savaient ce qu'il fallait faire, ils n'avaient simplement ni le temps ni l'envie de s'y mettre. Je peux le faire avec vous ou à votre place, à un prix annoncé d'avance, sans surprise.

Selon votre situation, trois façons d'avancer :

Faire le point. Je regarde votre informatique (postes, messagerie, box, accès, sauvegardes, abonnements) et je vous remets un état des lieux écrit, sans jargon, avec les actions classées par priorité.

Sécuriser. Je mets en place l'essentiel de ce livre sur vos postes : mots de passe, double authentification, mises à jour, sauvegardes testées.

Former votre équipe. Une heure, avec des exemples réels, pour que chacun reconnaisse les arnaques et sache quoi faire.

Vous préférez commencer par le diagnostic public gratuit ? Faites-le, puis revenez vers moi : je vous aide à appliquer les six mesures qui en ressortent.

La Fibre Alpine

Conseil informatique pour TPE, artisans et commerçants de Savoie et de Haute-Savoie, et à distance dans toute la France.

fibre-alpine.fr · contact@fibre-alpine.fr

Les prestations et leurs tarifs sont présentés dans la rubrique « Catalogue » du site.

Sources et précisions

Chiffres des menaces : [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), rapport d'activité 2025 (communiqué de mars 2026) ; répartition des menaces par public rapportée par Le Monde Informatique (27 mars 2026) et TPE Actu (7 avril 2026) ; ANSSI, panorama de la cybermenace 2025 (11 mars 2026), rapporté par Le Monde Informatique. Recommandations : fiches « 10 mesures essentielles », « Mots de passe », « Sauvegardes », « Mises à jour » et fiche réflexe « Hameçonnage » de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr). Dispositifs publics : economie.gouv.fr (17 juillet 2025), page de MonAideCyber et de 17Cyber. Fin de support de Windows 10 : Microsoft, 14 octobre 2025. Consultés le 24 octobre 2026.

Ce document donne des repères généraux, à jour à la date indiquée. Il ne constitue ni un audit, ni un conseil juridique, ni une garantie de protection. Les marques citées appartiennent à leurs propriétaires ; leur mention n'implique aucun partenariat.