

VOTRE LIVRE BLANC

Sensibilisation aux bonnes pratiques informatiques

Protéger votre entreprise face aux cybermenaces : les fondamentaux expliqués simplement, avec les chiffres 2025 de l'ANSSI et de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr).

CEMATYS

L'essentiel de l'informatique

Sommaire

01

Chiffres clés

Prenons conscience de la réalité

02

Protégez votre messagerie

La première porte d'entrée des attaques

03

Sauvegardez vos données

La règle 3-2-1, simplement expliquée

04

Séparez vos usages pro / perso

Une frontière à ne pas laisser s'effacer



Chiffres clés

Prenons conscience de la réalité, avec les derniers chiffres officiels

En 2025, l'ANSSI a traité 3 586 événements de sécurité en France. Les TPE, PME et ETI représentent désormais 48 % des victimes de cyberattaques, contre 37 % un an plus tôt — une hausse qui confirme que les petites structures sont devenues une cible de choix, non pas pour leur valeur, mais parce qu'elles sont perçues comme moins bien protégées.

48 %

des victimes de cyberattaques en 2025 sont des TPE/PME/ETI

16 %

des entreprises déclarent avoir subi une cyberattaque dans l'année

43 %

des attaques identifiées sont liées à l'hameçonnage (phishing)

+73 %

d'entreprises assistées par Cybermalveillance.gouv.fr en un an

Malgré cette pression croissante, trois quarts des TPE-PME consacrent encore moins de 2 000 € par an à leur sécurité informatique. La prise de conscience progresse, mais la protection concrète peine encore à suivre.



Protégez votre messagerie

En 2025, l'hameçonnage (phishing) reste la menace numéro un, tous publics confondus, avec une hausse de 70 % des signalements traités par [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — soit plus de 108 000 demandes d'assistance sur la seule année. Un e-mail frauduleux, un clic, et c'est l'accès à vos messageries, vos fichiers partagés et vos identifiants qui se retrouve compromis.

Le piratage de compte, première menace pour les professionnels

Le piratage de comptes en ligne arrive en tête des menaces touchant spécifiquement les entreprises en 2025, en progression de 45 %. Une fois un compte de messagerie compromis, l'attaquant peut usurper l'identité de l'entreprise, contacter ses clients ou fournisseurs, et déclencher des fraudes au virement.

3 réflexes simples à adopter

- Ne jamais cliquer sur un lien ou une pièce jointe inattendue, même si l'expéditeur semble connu.
- Vérifier l'adresse e-mail complète de l'expéditeur, pas seulement le nom affiché.
- Installer une solution antispam et sensibiliser régulièrement vos équipes, par exemple avec de faux e-mails de test.

03

Sauvegardez vos données

Après une accalmie en 2024, les attaques par rançongiciel repartent nettement à la hausse en 2025 : +10 % de demandes d'assistance, dont une progression de 7 % pour les seuls professionnels. Près de la moitié des attaques par rançongiciel recensées par l'ANSSI visent désormais des structures de taille petite ou moyenne.

La règle 3-2-1, pour dormir tranquille

3

copies de vos données au total (l'original et deux sauvegardes)

2

supports de stockage différents (disque, serveur, cloud...)

1

copie conservée en dehors de votre réseau habituel

Une sauvegarde n'a de valeur que si elle a déjà été testée : beaucoup d'entreprises ne découvrent une sauvegarde corrompue ou incomplète qu'au moment précis où elles tentent de s'en servir — c'est-à-dire trop tard.

04

Séparez vos usages pro / perso

Avec le développement du télétravail et des outils numériques, la frontière entre vie professionnelle et personnelle s'est nettement estompée. On consulte ses messages personnels depuis son poste de travail, et ses fichiers professionnels depuis son téléphone personnel. Ce mélange des usages, s'il n'est pas encadré, devient une porte d'entrée supplémentaire pour les attaquants.

Quelques bonnes pratiques simples

- Ne jamais utiliser de service de stockage en ligne personnel (cloud grand public) pour des fichiers professionnels.
- Ne pas mélanger messagerie professionnelle et messagerie personnelle sur le même compte.
- Éviter de se connecter aux outils professionnels depuis un réseau Wi-Fi public non sécurisé.
- Utiliser des mots de passe différents entre comptes personnels et professionnels.

Ce qu'il faut retenir : un système d'information bien séparé entre usages professionnels et personnels limite la surface d'attaque de votre entreprise, sans complexifier le quotidien de vos équipes.

**Votre système d'information est
l'élément central de votre entreprise.
N'attendez plus pour le protéger.**

TÉLÉPHONE

07 60 03 82 82

SITE WEB

cematys.fr

SIÈGE SOCIAL

33 Quai Arloing, CS10306, 69337 Lyon Cedex 09

CENTRE TECHNIQUE

6 Avenue Karl Marx, 69120 Vaulx-en-Velin

CEMATYS

L'essentiel de l'informatique