GUARDIEN

GUIDE PRATIQUE

CYBERSÉCURITÉ POUR LES PROFESSIONNELS

10

Principes essentiels de cybersécurité pour les TPE, les indépendants et les professions libérales

Protégez votre activité sans jargon technique.
Des actions concrètes, immédiatement applicables,
pour sécuriser l'essentiel sans budget dédié.

Édition 2026 | Guardien — Cybersécurité accessible

Sommaire

Les 10 principes essentiels — navigation rapide

Pourquoi ce guide ?

La cybersécurité n'est pas réservée aux grandes entreprises

Les TPE, indépendants et professions libérales représentent aujourd'hui **43 % des cibles d'attaques informatiques** — et pourtant, la grande majorité n'a ni responsable sécurité, ni budget dédié, ni plan d'action clair. En 10 principes concrets et actionnables, ce guide vous donne les outils pour vous protéger efficacement, sans jargon technique ni investissement massif.

Pourquoi les TPE, indépendants et professions libérales sont ciblés

En 2025, le coût moyen d'un incident de cybersécurité pour une structure de moins de 50 personnes s'élevait à **50 000 €** — entre temps d'arrêt, perte de données, coûts de remédiation et atteinte à la réputation. Pour beaucoup d'entreprises et d'indépendants, c'est une somme qui peut mettre en péril la survie de l'activité.

43%

Des cibles d'attaques

Sont des TPE, indépendants et professions libérales malgré leur petite taille

50k€

Coût moyen

D'un incident de cybersécurité pour une structure de moins de 50 personnes

21j

Interruption moyenne

Suite à un ransomware sans sauvegardes testées en place

Résumé exécutif — Les 10 principes

PRINCIPE	PRIORITÉ	EFFORT	IMPACT
1. Mots de passe & gestionnaire	Critique	Moyen	Très élevé
2. Double authentification (MFA)	Critique	Faible	Très élevé
3. Mises à jour systématiques	Critique	Faible	Élevé
4. Protection de la messagerie	Critique	Faible	Très élevé

PRINCIPE	PRIORITÉ	EFFORT	IMPACT
5. Formation anti-phishing	Haute	Moyen	Élevé
6. Verrouillage des appareils	Haute	Faible	Élevé
7. Sauvegardes régulières	Haute	Moyen	Très élevé
8. Séparation des accès	Moyenne	Moyen	Élevé
9. Réduction surface d'attaque	Moyenne	Faible	Moyen
10. Plan de réponse incidents	Haute	Moyen	Très élevé

⚡ **RECOMMANDATION IMMÉDIATE**

Commencez par les **principes 1, 2 et 4**. Ces trois actions seules couvrent la majorité des incidents courants contre les TPE, indépendants et professions libérales.

01

PRINCIPE CRITIQUE

Utilisez un mot de passe unique et fort pour chaque compte critique

> ⚡ **PREMIER RÉFLEXE — FAITES CE TEST MAINTENANT**
>
> Vérifiez sur **haveibeenpwned.com** si vos adresses email professionnelles ont été compromises dans une fuite de données connue *(ainsi que vos adresses personnelles utilisées à des fins professionnelles)*.
>
> C'est gratuit, immédiat et souvent révélateur. Si votre adresse apparaît dans les résultats, vos identifiants ont peut-être déjà circulé — agissez dès aujourd'hui.

Le problème

Un seul mot de passe réutilisé sur plusieurs services est une bombe à retardement. Quand une base de données est compromise quelque part (et cela arrive des dizaines de fois par jour dans le monde), les identifiants sont testés automatiquement sur des centaines d'autres services — c'est ce qu'on appelle le *credential stuffing*.

En TPE ou en tant qu'indépendant, un seul compte compromis peut donner accès à votre messagerie, vos fichiers partagés, vos outils de facturation ou vos systèmes clients.

> ⚡ **ACTION CONCRÈTE — PRIORITÉ IMMÉDIATE**
>
> Déployez un **gestionnaire de mots de passe** pour vous et votre équipe. Les options les plus solides pour les TPE et indépendants incluent **1Password Teams**, **Bitwarden Business** ou **Dashlane Business**. Ils créent et stockent des mots de passe longs et uniques pour chaque service, sans mémorisation.

Checklist d'application

- ✓ Vérifier sur **haveibeenpwned.com** si vos adresses email professionnelles ont été compromises (ainsi que vos adresses personnelles utilisées à des fins professionnelles)
- ✓ Choisir et déployer un gestionnaire de mots de passe pour toute l'équipe
- ✓ Remplacer en priorité les mots de passe de : email professionnel, banque, ERP/CRM, hébergement web, administration système
- ✓ Interdire les mots de passe partagés entre collaborateurs

- ✓ Définir une politique de mots de passe (longueur minimum 16 caractères, renouvellement annuel ou après incident)

> 💡 **POURQUOI C'EST CRITIQUE**
>
> *En 2024, plus de **80 % des violations de données** liées aux identifiants provenaient de mots de passe réutilisés ou trop faibles. Un gestionnaire de mots de passe élimine ce vecteur d'attaque quasi intégralement.*

02

PRINCIPE CRITIQUE

Activez la double authentification (MFA) partout

Le problème

Même avec un bon mot de passe, un compte peut être compromis si le mot de passe fuite, est deviné ou intercepté. La double authentification (MFA ou 2FA) ajoute un second verrou : même si quelqu'un connaît votre mot de passe, il ne peut pas se connecter sans le second facteur.

> ⚡ **ACTION CONCRÈTE — PRIORITÉ IMMÉDIATE**
>
> Activez le MFA **immédiatement** sur tous vos outils sensibles. Services prioritaires :
>
> → Microsoft 365 ou Google Workspace
>
> → Outils de comptabilité et facturation
>
> → CRM et outils commerciaux
>
> → Accès VPN et administration réseau
>
> → Hébergement web et noms de domaine
>
> → Réseaux sociaux professionnels

Checklist d'application

- ✓ Activer le MFA sur Microsoft 365 / Google Workspace pour tous les utilisateurs
- ✓ Choisir une méthode MFA robuste : application d'authentification (Google Authenticator, Authy, Microsoft Authenticator) plutôt que SMS
- ✓ Documenter les codes de secours dans un endroit sécurisé
- ✓ Imposer le MFA comme règle obligatoire dans votre politique de sécurité interne
- ✓ Vérifier que les comptes administrateurs ont systématiquement le MFA activé

> 💡 **POURQUOI C'EST CRITIQUE**
>
> *Selon Microsoft, le MFA bloque **99,9 % des attaques automatisées** sur les comptes. C'est la mesure au meilleur ratio effort/efficacité qui existe en cybersécurité.*

03

PRINCIPE CRITIQUE

Maintenez tous vos systèmes et logiciels à jour

Le problème

Les mises à jour de sécurité corrigent des failles connues. Quand une faille est publiée, les attaquants l'exploitent souvent dans les heures suivantes. Les systèmes non mis à jour sont des cibles faciles, même pour des attaquants peu sophistiqués.

La grande majorité des ransomwares et intrusions réussies exploitent des vulnérabilités pour lesquelles un correctif existait depuis plusieurs semaines ou mois.

> ⚡ **ACTION CONCRÈTE — ACTIVEZ LES MISES À JOUR AUTOMATIQUES**
>
> Périmètre à couvrir :
>
> → Systèmes d'exploitation (Windows, macOS, Linux)
>
> → Navigateurs web
>
> → Applications métier et SaaS
>
> → Antivirus et solutions de protection des postes
>
> → Équipements réseau (routeurs, switches, points d'accès Wi-Fi)
>
> → Serveurs et infrastructures hébergées

Checklist d'application

- ✓ Activer les mises à jour automatiques sur tous les postes de travail
- ✓ Définir une fenêtre de maintenance mensuelle pour les serveurs
- ✓ Tenir un inventaire des logiciels utilisés et de leurs versions
- ✓ Abonner un responsable aux alertes de sécurité des éditeurs clés (ANSSI, CERT-FR)
- ✓ Éliminer les logiciels en fin de vie qui ne reçoivent plus de mises à jour

💡 **POURQUOI C'EST CRITIQUE**

*L'attaque **WannaCry de 2017** a paralysé des centaines de milliers de systèmes dans 150 pays — en exploitant une faille pour laquelle un correctif existait depuis deux mois. Les systèmes mis à jour n'ont pas été affectés.*

04

PRINCIPE CRITIQUE

Sécurisez en priorité votre messagerie d'entreprise

Le problème

Votre messagerie est la **clé maîtresse** de votre entreprise numérique. Elle permet de réinitialiser quasiment tous vos autres comptes, de recevoir des informations confidentielles, d'autoriser des virements et de communiquer avec vos clients. Si elle est compromise, tout le reste peut l'être aussi.

Action 1 — Vérifier SPF, DKIM et DMARC sur mxtoolbox.com

Ces 3 protocoles protègent votre domaine contre l'usurpation d'identité (spoofing). Voici ce que vous devez trouver pour chacun d'eux.

SPF *Sender Policy Framework*

Ce que c'est : déclare quels serveurs ont le droit d'envoyer des emails en votre nom.

COMMENT VÉRIFIER SUR MXTOOLBOX

Aller sur **mxtoolbox.com** → onglet **"SPF Record Lookup"** → entrer votre domaine (ex : votreentreprise.fr).

CE QUE VOUS DEVEZ TROUVER

Un enregistrement TXT commençant par `v=spf1` suivi des serveurs autorisés, et se terminant par `-all` (strict) ou `~all` (souple).

EXEMPLE — GMAIL / GOOGLE WORKSPACE

```
v=spf1 include:_spf.google.com -all
```

⚠ Signe d'alerte : "SPF record not found" → votre domaine est non protégé, n'importe qui peut usurper votre adresse

DKIM *DomainKeys Identified Mail*

Ce que c'est : signature cryptographique qui prouve que l'email n'a pas été altéré depuis son envoi.

COMMENT VÉRIFIER SUR MXTOOLBOX

Aller sur **mxtoolbox.com** → **"DKIM Lookup"** → entrer votre domaine + le sélecteur de votre fournisseur email (`google` pour Google Workspace, `k1` pour Mailchimp).

CE QUE VOUS DEVEZ TROUVER

Un enregistrement TXT avec une longue clé publique :

```
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOC...
```

⚠ Signe d'alerte : "DKIM record not found" → emails non signés, facilement falsifiables

DMARC *Domain-based Message Authentication*

Ce que c'est : politique qui dit aux serveurs destinataires quoi faire si SPF ou DKIM échouent.

COMMENT VÉRIFIER SUR MXTOOLBOX

Aller sur **mxtoolbox.com** → **"DMARC Lookup"** → entrer votre domaine.

CE QUE VOUS DEVEZ TROUVER — POLITIQUE P=

→ `p=none` → surveillance seulement (acceptable pour commencer, mais insuffisant)

→ `p=quarantine` → les emails suspects vont en spam **(bonne protection)**

→ `p=reject` → les emails suspects sont bloqués **(protection maximale — recommandée)**

EXEMPLE D'UN BON ENREGISTREMENT DMARC

```
v=DMARC1; p=reject; rua=mailto:reports@votre-domaine.fr
```

⚠ Signe d'alerte : "DMARC record not found" ou p=none → aucune politique, domaine facilement usurpable

Récapitulatif — ce que vous devez voir

PROTOCOLE	CE QU'ON DOIT VOIR ✅	SIGNE D'ALERTE ❌
SPF	v=spf1 ... -all	"SPF not found"
DKIM	v=DKIM1; k=rsa; p=...	"DKIM not found"
DMARC	p=reject ou p=quarantine	"DMARC not found" ou p=none

Si l'un de ces 3 enregistrements est absent ou mal configuré, contactez votre hébergeur ou administrateur DNS — la correction prend **moins de 30 minutes** mais protège définitivement votre domaine contre l'usurpation d'identité.

Checklist d'application

- ✓ Vérifier SPF, DKIM et DMARC sur **mxtoolbox.com** et corriger tout enregistrement absent ou en `p=none`
- ✓ Activer le MFA sur toutes les boîtes email (cf. Principe 2)
- ✓ Désactiver le protocole IMAP/POP3 si non nécessaire (vecteur d'attaque fréquent)
- ✓ Activer la journalisation des connexions pour détecter les connexions anormales
- ✓ Former l'équipe : aucun changement de RIB ou virement urgent ne doit se faire sans confirmation téléphonique

💡 **POURQUOI C'EST CRITIQUE**

*La **fraude au président (BEC)** est l'une des arnaques les plus coûteuses pour les TPE et indépendants. Elle exploite presque toujours une messagerie insuffisamment sécurisée ou un manque de procédure de vérification.*

05

PRIORITÉ HAUTE

Formez vos équipes à reconnaître le phishing

Le problème

La technologie seule ne suffit pas. Le phishing — emails, SMS ou messages trompeurs qui imitent des expéditeurs légitimes — reste la **première porte d'entrée** des cyberattaques dans les TPE et chez les indépendants. Un seul clic d'un collaborateur peut suffire à compromettre tout le système.

⚡ **ACTION CONCRÈTE — SIGNES D'ALERTE À ENSEIGNER**

- → Adresse email de l'expéditeur légèrement différente du domaine officiel
- → Urgence artificielle ("agissez dans l'heure", "votre compte sera suspendu")
- → Demande inhabituelle de la hiérarchie par email (virement, changement de RIB)
- → Lien qui ne correspond pas à ce qu'il prétend être (survol avec la souris)
- → Pièce jointe inattendue d'un expéditeur connu

Checklist d'application

- ✓ Organiser une session de sensibilisation courte (30 min) pour toute l'équipe
- ✓ Diffuser des exemples réels d'emails de phishing récents
- ✓ Mettre en place une adresse email interne pour signaler les emails suspects
- ✓ Réaliser des simulations de phishing (outils : KnowBe4, Proofpoint, ou services ANSSI)
- ✓ Définir une procédure claire : toute demande de virement doit être confirmée par téléphone

💡 **POURQUOI C'EST IMPORTANT**

95 % des incidents de cybersécurité *impliquent une erreur humaine. La formation est l'investissement au meilleur ROI en cybersécurité — quelques heures pour protéger l'ensemble de l'activité.*

06

PRIORITÉ HAUTE

Verrouillez et protégez tous vos appareils professionnels

Le problème

Un ordinateur portable volé dans un café, un téléphone professionnel oublié dans un taxi, ou simplement un poste laissé déverrouillé pendant une absence — chaque appareil non sécurisé est une porte ouverte sur vos données d'entreprise.

Pour les TPE, indépendants et professions libérales, les appareils contiennent souvent des informations critiques : données clients, contrats, accès aux systèmes, emails confidentiels.

⚡ **ACTION CONCRÈTE — MESURES FONDAMENTALES**

- → Code PIN ou mot de passe solide (pas 0000 ou 1234)
- → Biométrie si disponible (empreinte ou Face ID)
- → Verrouillage automatique après 5 minutes d'inactivité maximum
- → Chiffrement du disque activé (BitLocker sur Windows, FileVault sur Mac)
- → Solution de gestion à distance (**MDM**) pour les appareils mobiles

📖 **DÉFINITION**

MDM (Mobile Device Management) : outil logiciel qui permet à une entreprise de gérer, configurer, sécuriser et surveiller à distance l'ensemble des appareils mobiles utilisés par ses collaborateurs (smartphones, tablettes, ordinateurs portables). Un MDM permet, par exemple, de verrouiller ou d'effacer à distance un téléphone perdu ou volé, d'imposer un code PIN, ou d'empêcher l'installation d'applications non autorisées.

Exemples d'outils MDM accessibles aux TPE : Microsoft Intune, **Jamf Now** (pour Apple), **ManageEngine Mobile Device Manager Plus** (version gratuite disponible pour moins de 25 appareils).

Checklist d'application

- ✓ Inventorier tous les appareils professionnels (ordinateurs, téléphones, tablettes)
- ✓ Vérifier que le chiffrement du disque est activé sur tous les postes

- ✓ Définir une politique de verrouillage automatique
- ✓ Déployer une solution MDM si vous gérez plus de 5 appareils mobiles
- ✓ Documenter la procédure à suivre en cas de perte ou vol (effacement à distance)
- ✓ Interdire l'utilisation des appareils professionnels à des tiers

> 💡 **POURQUOI C'EST IMPORTANT**
>
> *En Europe, une perte d'appareils contenant des données personnelles doit être déclarée à la **CNIL sous 72 heures**. Le chiffrement supprime cette obligation de déclaration dans la plupart des cas — et protège vos données en toutes circonstances.*

07

PRIORITÉ HAUTE

Sauvegardez vos données régulièrement et testez vos restaurations

Le problème

Les ransomwares chiffrent vos données et réclament une rançon pour les déchiffrer. Même sans ransomware, une panne matérielle, une erreur humaine ou un sinistre peut vous faire perdre des mois ou des années de travail.

Une sauvegarde dont on n'a jamais testé la restauration n'est **pas une sauvegarde**.

⚡ ACTION CONCRÈTE — LA RÈGLE 3-2-1

3	2	1
copies de vos données	supports différents	copie hors site

Données à sauvegarder en priorité

- → Base de données clients et CRM
- → Données comptables et facturation
- → Contrats et documents juridiques
- → Emails critiques et configurations systèmes

Checklist d'application

- ✓ Identifier les données critiques et leur localisation
- ✓ Mettre en place une sauvegarde automatique quotidienne sur au moins deux supports
- ✓ Vérifier que les sauvegardes se font correctement (alertes en cas d'échec)
- ✓ Tester une restauration complète au moins une fois par trimestre
- ✓ Stocker au moins une copie hors site (cloud chiffré ou support physique)
- ✓ S'assurer que les sauvegardes ne sont pas accessibles depuis les postes infectés

💡 **POURQUOI C'EST CRITIQUE**

*La durée moyenne d'interruption suite à un ransomware est de **21 jours** sans sauvegardes testées. Les structures disposant de sauvegardes testées reprennent leur activité en moyenne en moins de **48 heures**.*

08

PRIORITÉ MOYENNE

Séparez les accès et cloisonnez les usages

Le problème

Dans beaucoup de structures de petite taille, tout le monde a accès à tout, et les usages personnels et professionnels se mélangent. Cette configuration amplifie considérablement les dégâts en cas d'incident : une seule compromission peut toucher l'ensemble du système.

> ⚡ **ACTION CONCRÈTE — PRINCIPE DU MOINDRE PRIVILÈGE**
>
> Chaque collaborateur n'accède qu'à ce dont il a besoin pour son travail. Séparations essentielles :
>
> → Comptes administrateurs séparés des comptes utilisateurs courants
>
> → Accès aux données sensibles limités aux personnes qui en ont besoin
>
> → Réseau Wi-Fi visiteurs séparé du réseau professionnel
>
> → Appareils professionnels distincts des appareils personnels

Checklist d'application

- ✓ Auditer les droits d'accès de chaque collaborateur
- ✓ Supprimer les droits administrateurs des postes utilisateurs standards
- ✓ Créer un réseau Wi-Fi invité séparé pour les visiteurs et les appareils personnels
- ✓ Mettre en place des groupes et permissions dans votre suite bureautique
- ✓ Définir une procédure d'onboarding/offboarding qui inclut la création/suppression des accès
- ✓ Révoquer immédiatement les accès lors d'un départ ou d'un changement de poste

> 💡 **POURQUOI C'EST IMPORTANT**
>
> *Les erreurs internes (accidentelles ou malveillantes) représentent une part significative des incidents dans les petites structures. Le cloisonnement des accès* ***limite les dégâts à un périmètre restreint*** *et facilite la détection.*

09

PRIORITÉ MOYENNE

Réduisez la surface d'attaque en supprimant ce que vous n'utilisez plus

Le problème

Chaque application, chaque compte, chaque intégration active est une porte potentielle. Au fil du temps, les TPE et les indépendants accumulent des accès oubliés, des applications abandonnées, des comptes ex-collaborateurs jamais désactivés. Chacun représente un risque silencieux.

> ⚡ **ACTION CONCRÈTE — AUDIT TRIMESTRIEL**
>
> Périmètre de nettoyage :
>
> → Comptes d'ex-collaborateurs ou ex-prestataires
>
> → Applications SaaS abandonnées ou en doublon
>
> → Extensions de navigateur non utilisées
>
> → Partages de fichiers publics ou trop larges
>
> → Accès de partenaires non revus depuis plus de 6 mois

Checklist d'application

- ✓ Lister tous les services SaaS actifs de l'entreprise
- ✓ Vérifier les accès tiers dans votre Google Workspace ou Microsoft 365
- ✓ Supprimer les comptes des ex-collaborateurs dans tous les systèmes
- ✓ Révoquer les partages de fichiers inutiles dans Google Drive ou SharePoint
- ✓ Désinstaller les logiciels non utilisés sur les postes de travail
- ✓ Documenter et revalider les accès prestataires tous les 6 mois

> 💡 **POURQUOI C'EST IMPORTANT**
>
> *Les "**actifs fantômes**" (Shadow IT) sont l'une des causes les plus fréquentes d'incidents non détectés. Moins vous avez d'entrées non surveillées, plus votre posture de sécurité est solide.*

10

PRIORITÉ HAUTE

Préparez un plan de réponse simple pour le jour J

Le problème

Sous la pression d'un incident — ransomware, compte compromis, fuite de données — les équipes improvisent et font souvent des erreurs qui aggravent la situation. Un plan de réponse simple, préparé à l'avance, change radicalement la façon dont une crise est gérée.

⚡ ACTION CONCRÈTE — VOTRE FICHE DE RÉPONSE AUX INCIDENTS

1. **Qui contacter en premier** : responsable IT ou prestataire, dirigeant, RSSI si applicable
2. **Quoi isoler immédiatement** : déconnecter le ou les postes affectés du réseau
3. **Quoi ne pas faire** : éteindre les machines, payer la rançon sans vérification, attendre trop longtemps
4. **Qui doit être informé** : clients si données compromises, CNIL sous 72h, assurance cyber
5. **Où sont les sauvegardes** et comment les restaurer
6. **Comment documenter** : journal des actions, captures d'écran, logs

Checklist d'application

- ✓ Rédiger la fiche de réponse aux incidents (une page suffit)
- ✓ La stocker hors ligne et dans le cloud (pas uniquement sur les postes)
- ✓ Identifier votre prestataire IT de confiance et noter son numéro d'urgence
- ✓ Vérifier votre couverture d'assurance cyber
- ✓ Former les collaborateurs à reconnaître un incident et à savoir à qui l'escalader
- ✓ Simuler une fois par an un scénario d'incident pour tester le plan

💡 **POURQUOI C'EST CRITIQUE**

*Les structures disposant d'un plan de réponse documenté réduisent en moyenne de **60 % le temps de remédiation** et de **40 % les coûts** associés à un incident. La préparation coûte quelques heures. L'improvisation coûte des semaines.*

Commencez maintenant, pas plus tard

La cybersécurité parfaite n'existe pas. Ce qui existe, c'est une protection suffisante pour rendre les attaques plus coûteuses que le gain espéré — et ainsi décourager la grande majorité des attaquants opportunistes.

1

Gestionnaire de mots de passe

Déployez pour toute l'équipe et remplacez les mots de passe critiques

2

Activez le MFA

Sur votre messagerie professionnelle et vos outils critiques

3

Vérifiez les sauvegardes

Testez une restauration complète dès cette semaine

Passez à l'étape suivante avec Guardien

Guardien accompagne les TPE, indépendants et professions libérales qui veulent aller plus loin sans se perdre dans la complexité. Notre diagnostic express vous donne en 72 heures :

- ✓ Un état des lieux de votre posture de sécurité actuelle
- ✓ 5 priorités concrètes adaptées à votre contexte
- ✓ Une feuille de route d'actions, classées par urgence et par effort
- ✓ Un email de suivi 7 jours plus tard pour vous aider à avancer

Pas de jargon. Pas de vente forcée de produits. Juste de la clarté et un plan.

Découvrir le Diagnostic Express →

guardien.nanocorp.app