Blueprint

Cybersécurité pour TPE & PME

Un guide pratique et accessible pour renforcer votre sécurité informatique, même sans service IT dédié.

Avril 2025

Edition spéciale TPE & PME

Pour plus d'infos :
Rendez-vous sur www.creativminds.ch ou réservez un appel gratuit pour parler de votre situation : Parlons CyberSécurité > Par où commencer ?


ACCESS
GRANTED

Édition 2025

Nadège FARALLI

Fondatrice de CreativMinds, une entreprise spécialisée dans l'accompagnement au changement et la cybersécurité.

Stop aux idées reçues

Bienvenue dans ce blueprint conçu spécialement pour les TPE et PME qui souhaitent comprendre et anticiper les risques liés à la cybersécurité. Ce guide n'est pas réservé aux spécialistes : il s'adresse aux dirigeants, aux collaborateurs, aux référents informatiques improvisés… à tous ceux qui veulent protéger leur activité, sans jargon ni usine à gaz.

🚨 **Pourquoi ce guide ?**

Chaque jour, des entreprises comme la vôtre sont victimes d'attaques informatiques.
Pas parce qu'elles sont mal gérées. Pas parce qu'elles sont négligentes.

Mais parce qu'elles sont **faciles à attaquer, et rentables** pour les cybercriminels.

Une simple erreur (clic sur un lien piégé, mot de passe trop simple, fichier partagé sans protection) peut entraîner :

💸 Des pertes financières importantes

⛔ Un blocage complet de votre activité

🕵️ Une atteinte à votre réputation

Et pourtant… la plupart de ces attaques auraient pu être évitées avec quelques gestes simples.

Depuis 2019, j'ai aidé des dizaines de structures à sécuriser leurs usages numériques, de la start-up aux institutions publiques.

Ce blueprint est une synthèse des bonnes pratiques que je partage au quotidien :

- accessibles,
- efficaces,
- et validées sur le terrain.

Prenez ce document comme un point de départ. Une prise de conscience. Un déclic.

Les 5 dangers à ne pas sous-estimer

La cybersécurité n'est pas qu'un sujet d'informaticiens. En tant que dirigeant·e, indépendant·e, ou collaborateur·trice d'une TPE/PME, vous êtes exposé·e à des risques concrets.

Voici les 5 menaces les plus fréquentes qui ciblent les petites structures :

Chiffres à retenir :

- **88%** des cyberattaques démarrent par un e-mail piégé
- **52%** des PME touchées font faillite dans les 6 mois
- **70%** n'ont pas de responsable cybersécurité

Et pourtant, la majorité des attaques pourraient être évitées par quelques gestes simples.t

Ce que vous pouvez faire dès maintenant

- Sensibilisez vos équipes au phishing
- Activez l'authentification à 2 facteurs
- Ne partagez jamais vos mots de passe
- Faites des sauvegardes automatiques
- Mettez à jour vos appareils régulièrement

Besoin d'aide ?

Vous n'avez pas à faire tout ça seul.
Nous accompagnons les petites structures à mettre en place des protections simples et efficaces, sans jargon inutile.
👉 **Prenez rendez-vous :** Parlons Cybersécurité > Par où commencer ?

Les erreurs qu'on voit (trop) souvent

Une journée type... ou presque !

🕘 9h00

1

J'ouvre mes mails sans me méfier

📩 Erreur #1 : Je clique sur un lien sans vérifier

Un mail de livraison ? Une pièce jointe suspecte ? Le piège classique du phishing. Un clic peut suffire à installer un logiciel malveillant.

🕘 11h00

2

On me demande un mot de passe...

🔑 Erreur #2 : J'utilise toujours le même mot de passe

Et souvent... il est trop simple. Une fois compromis, il ouvre toutes les portes de votre entreprise.

🕘 14h00

3

Je travaille depuis mon téléphone perso

📱 Erreur #3 : J'utilise un appareil non sécurisé

Pas de code, pas de protection, pas de sauvegarde. Or, ces appareils accèdent souvent à vos données professionnelles.

🕘 17h00

4

Je ne sauvegarde rien

💾 Erreur #4 : Si ça plante, je perds tout

Pas de sauvegarde automatisée = risque de perte de fichiers ou de blocage total (ransomware, suppression involontaire...).

Ce sont ces petites erreurs du quotidien qui provoquent **les plus gros dégâts**.

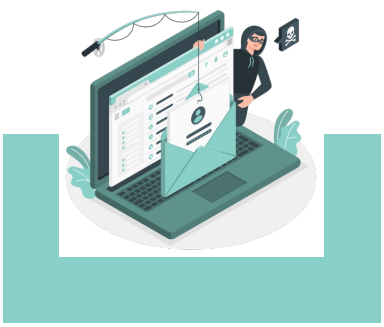
Mais la bonne nouvelle, c'est qu'elles peuvent être évitées facilement.

Les bons réflexes à adopter

Des gestes simples, mais puissants

Agir sans être expert·e

Mettre en place une culture de la cybersécurité ne nécessite pas d'être un pro de l'informatique.
Voici 3 bonnes pratiques à diffuser dans votre équipe dès aujourd'hui.



Réagir face à un mail suspect

Objectif : Apprendre à reconnaître un message de phishing

- ❑ Toujours vérifier l'expéditeur
- ❑ Ne jamais cliquer sur un lien douteux
- ❑ Signaler le mail à son responsable ou support IT

Créer des mots de passe solides

Objectif : Protéger l'accès à ses outils

- ❑ Utiliser une phrase de passe ou un générateur
- ❑ Ne jamais réutiliser le même mot de passe
- ❑ Activer l'authentification à deux facteurs

Sauvegarder automatiquement ses fichiers

Objectif : Ne jamais perdre de données critiques

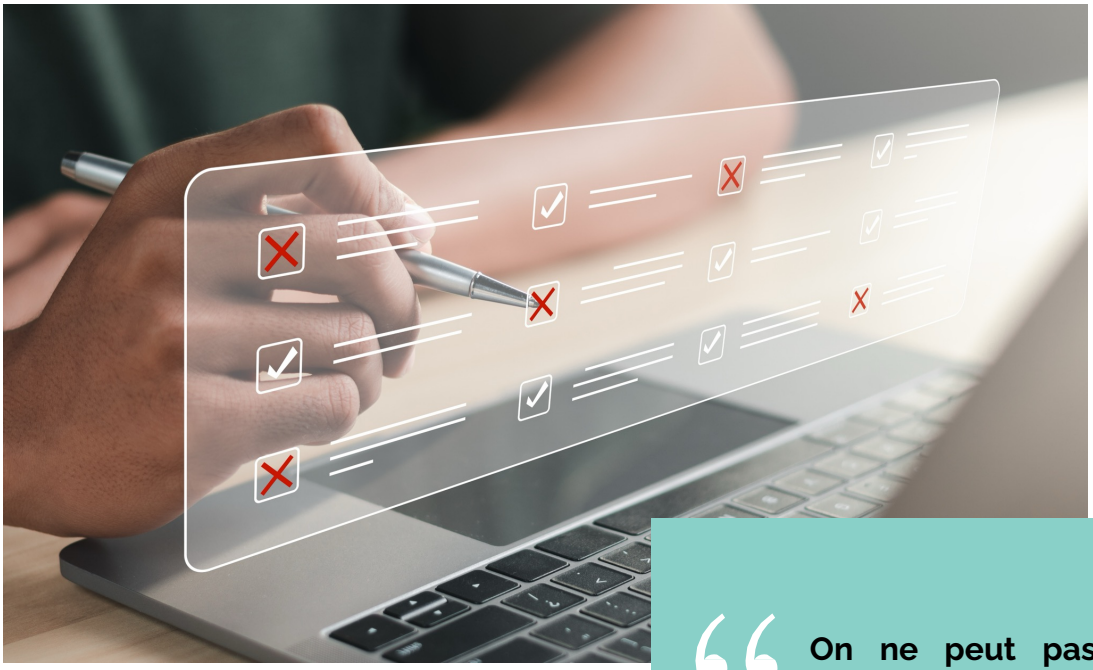
- ❑ Planifier des sauvegardes quotidiennes
- ❑ Stocker sur au moins 2 supports différents (ex : cloud + disque dur)
- ❑ Tester les restaurations de temps en temps

Où en êtes-vous ?

Faites le point sur votre cybersécurité en 2 minutes

Faites le point

Prenez 2 minutes pour évaluer votre posture cybersécurité.
Cochez ce qui est vrai aujourd'hui dans votre structure, puis comptez vos points !



> **On ne peut pas tout sécuriser, mais on peut éviter 90 % des risques avec les bons réflexes.**
>
> **Nadège Faralli,**
> consultante en cybersécurité TPE/PME

Les réflexes en place dans votre entreprise :

- ❑ Nos données sont sauvegardées automatiquement, de manière régulière.
- ❑ L'authentification à 2 facteurs est activée sur nos outils.
- ❑ Personne n'utilise le même mot de passe pour plusieurs services.
- ❑ Un plan d'action existe en cas de cyberattaque.
- ❑ Tous les collaborateurs ont reçu une sensibilisation récente.

Votre score :

- 0–1 : 🟥 Il est urgent d'agir.
- 2–3 : 🟨 Vous avez posé les premières briques.
- 4–5 : 🟩 Vous êtes sur la bonne voie, continuez !

Les cyber risques en chiffres

Chaque jour, les TPE/PME sont exposées à des menaces. Voici quelques chiffres pour prendre conscience de la réalité… et passer à l'action.

60 %	des PME victimes d'une cyberattaque ferment dans les 6 mois.
90 %	des attaques réussies débutent par une erreur humaine.
14 jours	durée moyenne d'une interruption d'activité après une attaque.
1 clic	suffit pour compromettre un réseau entier.

Réagir ou subir : à vous de choisir

💥 **Des conséquences concrètes :**

- **Perte de données clients**

Impossible de récupérer des fichiers, contrats ou informations sensibles. Une perte de confiance immédiate de vos clients.

- **Blocage de la production (ransomware)**

Vos outils sont paralysés. Vous ne pouvez plus travailler, livrer, ni facturer. Chaque heure coûte cher.

- **Dépenses imprévues**

Paiement d'une rançon 💸, intervention en urgence de consultants, frais de communication de crise… des coûts qui explosent.

- **Impact sur la réputation**

Clients inquiets, partenaires méfiants. Une attaque peut nuire durablement à votre image… et ouvrir la porte à la concurrence.

✅ **Mais aussi des solutions :**

- **Formez vos équipes… régulièrement !**

Un seul atelier ne suffit pas : vos collaborateurs doivent savoir reconnaître une tentative de phishing, adopter les bons réflexes… et rester vigilants dans la durée.

- **Automatisez les sauvegardes**

Une bonne sauvegarde est automatique, régulière, testée… et stockée hors ligne. C'est votre assurance en cas de crise.

- **Choisissez les bons outils… et configurez-les bien**

Même les meilleurs logiciels sont inefficaces mal paramétrés. Une bonne configuration fait toute la différence.

- **Préparez un plan de réponse**

Chaque minute compte pendant une attaque. Un plan clair = moins de stress, moins de dégâts.

Les erreurs à éviter

01 🚫 Ne pas former ses équipes

Le risque ? Les collaborateurs deviennent la première faille de sécurité. Sans formation, ils ne savent pas reconnaître les tentatives d'attaque ni réagir efficacement.
Résultat :
- 👉 Une mauvaise manipulation déclenche une attaque (90 % des cas).
- 👉 Personne ne sait quoi faire en cas d'incident.
- 👉 Même les meilleurs outils ne suffisent pas si l'humain clique au mauvais endroit.

02 📦 Ne pas sauvegarder (ou mal)

Le risque ? Perte de données critiques malgré une impression de sécurité.
Résultat :
- 👉 Une sauvegarde connectée peut être chiffrée avec les fichiers principaux.
- 👉 Non testée = inutilisable en cas de crise.
- 👉 Sans sauvegarde récente, impossible de redémarrer l'activité.

03 🧩 Utiliser des outils mal configurés

Le risque ? Des portes laissées grandes ouvertes.
Résultat :
- 👉 Données visibles hors entreprise.
- 👉 Protections automatiques inopérantes.
- 👉 Trop de droits = accès trop large en cas de piratage.

04 📎 Partager des fichiers sans précaution

Le risque ? Une fuite de données à cause d'un simple lien mal géré.
Résultat :
- 👉 Liens publics trouvables sur Google.
- 👉 Accès pour d'anciens collaborateurs.
- 👉 Pas de mot de passe, ni de durée de validité.

Par où commencer ?

3 actions simples pour mieux vous protéger dès aujourd'hui

01

🛠️ Faites un point sur votre situation

→ Utilisez l'auto-diagnostic de la page 7 pour savoir où vous en êtes.

02

🔄 Appliquez les protections de base

→ Mettez à jour vos appareils et vos applications,
→ Activez la MFA,
→ Utilisez des mots de passe solides.

03

🎯 Sensibilisez vos équipes

→ 30 minutes suffisent pour apprendre à repérer les tentatives d'arnaques.

💬 ***Vous ne savez pas par quoi commencer ?***

Prenons 30 minutes ensemble pour définir vos priorités
→ [Parlons Cybersécurité > Par où commencer ?]

cre@tiv minds

Contactez-nous

Besoin d'aide pour démarrer ou évaluer vos pratiques cybersécurité ?
👉 Parlons-en ! Un appel de 30 minutes peut déjà tout changer.

📧 **contact@creativminds.ch**
🌐 www.creativminds.ch
📍 Basés à Nyon, intervention possible en ligne ou sur site.

🔗 **Prendre rendez-vous directement :**
Parlons CyberSécurité > Par où commencer ?