



CHECKLIST IMPRIMABLE

Cybersécurité petite entreprise : les priorités à cocher

Protégez l'activité de votre entreprise avec des actions concrètes, à vérifier une par une. Cette checklist aide à réduire les risques qui peuvent bloquer les e-mails, les paiements, les fichiers ou la relation client.

Au sommaire

- 1 Les 4 réflexes à retenir
- 2 1. Sécuriser les accès et les comptes
- 3 2. Préserver les données et la continuité d'activité
- 4 3. Déjouer les fraudes courantes
- 5 Risques prioritaires : le bon contrôle à appliquer
- 6 4. Réagir sans improviser en cas d'incident

Les 4 réflexes à retenir

La cybersécurité protège les comptes, les données, les appareils, les logiciels et les usages numériques de l'entreprise.

La protection repose sur des règles simples, des outils correctement configurés et une réaction préparée.

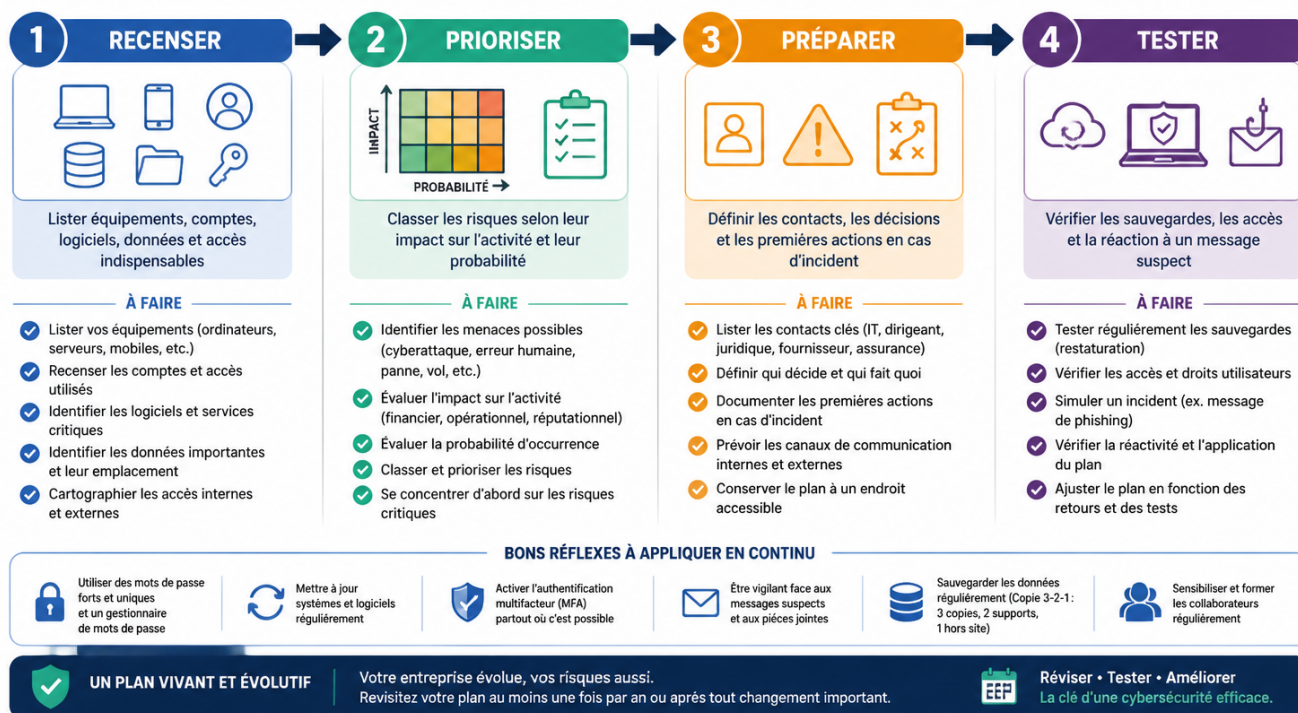
Une messagerie, un outil de comptabilité ou des fichiers indisponibles peuvent interrompre rapidement l'activité.

Les premières priorités sont les accès, les mises à jour, les sauvegardes testées et la vérification des demandes sensibles.



PLAN DE CYBERSÉCURITÉ EN 4 ÉTAPES

Un plan simple et efficace pour protéger votre entreprise, vos données et assurer la continuité de votre activité.



SCHEMA Les quatre étapes d'un plan de cybersécurité adapté à une petite entreprise.

1. Sécuriser les accès et les comptes

Utiliser un mot de passe unique pour chaque compte professionnel

Éviter de réemployer un même mot de passe entre messagerie, outils métier et services en ligne.

- ☐ **Activer l'authentification à plusieurs facteurs**
À prioriser pour la messagerie et les comptes donnant accès à des données ou à des paiements.
- ☐ **Séparer les comptes administrateurs des comptes utilisés au quotidien**
Limiter l'usage des droits étendus aux tâches qui les nécessitent réellement.
- ☐ **Revoir la liste des administrateurs**
Retirer les accès qui ne sont plus nécessaires.
- ☐ **Limitier les droits d'accès aux outils et aux documents**
Donner à chaque personne uniquement les accès utiles à son activité.

2. Préserver les données et la continuité d'activité

- ☐ **Mettre à jour les appareils, logiciels et sites utilisés par l'entreprise**
Les outils non mis à jour peuvent être ciblés par des campagnes automatisées.
- ☐ **Prévoir une sauvegarde des données essentielles**
Inclure notamment les devis, factures, contrats, dossiers clients et documents de travail importants.
- ☐ **Conserver une sauvegarde séparée de l'environnement de travail**
Une sauvegarde connectée en permanence au même réseau qu'un poste infecté peut aussi devenir indisponible.
- ☐ **Tester la restauration d'un fichier ou d'un dossier**
Une sauvegarde est réellement utile si les données peuvent être restaurées.
- ☐ **Identifier les outils indispensables à l'activité**
Messagerie, comptabilité, commandes, caisse, stock, rendez-vous et stockage de documents.

3. Déjouer les fraudes courantes

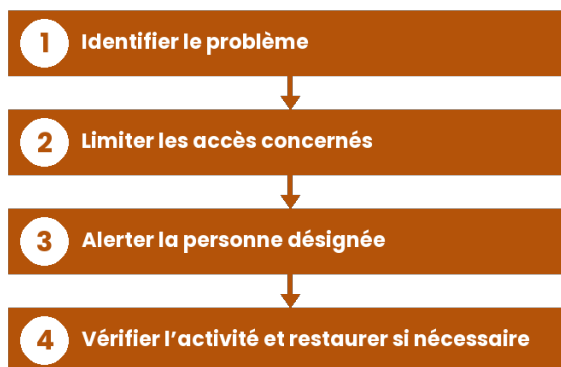
- ☐ **Se méfier des messages urgents demandant une action immédiate**
Un faux e-mail, SMS ou site peut chercher à récupérer un mot de passe ou un code.
- ☐ **Vérifier toute demande de paiement ou de changement d'IBAN**
Utiliser un canal indépendant, par exemple un appel vers un numéro déjà connu.
- ☐ **Ne pas se fier uniquement à l'apparence d'un e-mail ou d'un expéditeur**
Une messagerie compromise peut servir à envoyer de faux messages à des clients ou partenaires.
- ☐ **Prévoir une procédure simple de signalement interne**
Chaque personne doit savoir à qui transmettre un message ou un comportement suspect.
- ☐ **Sensibiliser les personnes qui utilisent les outils de l'entreprise**
La vigilance face aux demandes inhabituelles complète les protections techniques.

Risques prioritaires : le bon contrôle à appliquer

Risque	Impact possible	Contrôle à vérifier
Hameçonnage	Vol de compte, fraude ou diffusion de faux messages	Authentification à plusieurs facteurs et procédure de signalement
Rançongiciel	Fichiers ou logiciels indisponibles	Sauvegarde séparée, mises à jour et test de restauration

Risque	Impact possible	Contrôle à vérifier
Fraude au virement	Perte financière directe	Double validation et contrôle de l'IBAN par un canal indépendant
Compte administrateur compromis	Accès étendu aux outils et aux données	Comptes séparés, droits limités et revue des administrateurs

4. Réagir sans improviser en cas d'incident



1 Identifier le problème

Repérez un compte inaccessible, un message suspect, une demande de paiement inhabituelle ou des fichiers devenus indisponibles.

2 Limiter les accès concernés

Évitez de poursuivre une action douteuse et protégez les comptes ou outils potentiellement touchés.

3 Alerter la personne désignée

Appliquez la procédure interne prévue afin de centraliser la réaction et les vérifications.

4 Vérifier l'activité et restaurer si nécessaire

Contrôlez les demandes sensibles, les accès et la disponibilité des données essentielles à partir de sauvegardes testées.

! Point de vigilance

Une petite entreprise peut être ciblée sans être particulièrement connue : les attaques automatisées recherchent notamment des identifiants divulgués, des adresses e-mail, des sites non mis à jour ou des pièces jointes malveillantes.

Cette checklist constitue un point de départ opérationnel. Adaptez les accès, les sauvegardes et la procédure de réaction aux outils réellement utilisés par votre entreprise.