Petit guide Quick-Wins Cyber pour les indépendants et TPE

La cybersécurité représente un défi majeur pour les indépendants et les TPE, souvent confrontés à un manque de temps, de personnel et de ressources financières pour investir dans des solutions coûteuses.

Ce guide " **Quick-Wins Cyber** " a été conçu pour vous offrir une aide gratuite et accessible. En prenant le temps de vérifier au moins une à deux fois par an les points essentiels mentionnés, vous pouvez significativement renforcer votre protection contre les menaces cybernétiques, et ce, sans nécessiter d'investissements majeurs.

Il ne se veut pas exhaustif. Si vous avez besoin d'aide, nous sommes là pour vous accompagner.

Ce guide sera organisé par thème, composé d'une section succincte explicative, d'une check-liste et traitera des points suivants:

01 - Mettre à jour vos équipements / logiciels

Limitez les failles de sécurité en gardant tous vos appareils et logiciels à jour régulièrement.

Les logiciels, qu'ils soient commerciaux ou développés en interne, comportent inévitablement des vulnérabilités. Ces failles de sécurité peuvent être exploitées par des cybercriminels pour accéder à votre système, voler des données sensibles, installer des logiciels malveillants ou perturber vos opérations.
Il est donc essentiel de maintenir tous vos logiciels, y compris votre système d'exploitation, à jour. Les mises à jour de sécurité publiées par les éditeurs de logiciels corrigent les vulnérabilités connues et réduisent considérablement le risque d'attaques informatiques.

Notes importantes concernant votre situation:

Liste des logiciels métiers installés:

- ☐ .....
- ☐ .....
- ☐ .....

Équipement supplémentaire (ex. NAS, pare-feu, ...):

- ☐ .....
- ☐ .....
- ☐ .....

Autres notes:

- ☐ .....
- ☐ .....
- ☐ .....

1 - Équipements à mettre à jour

Système d'exploitation	Logiciels
☐ Windows / MacOS / Linux ☐ Android / iOS	☐ Navigateurs (Chrome / Edge / Firefox) ☐ Suite bureautique (Office, Acrobat, ...) ☐ Logiciels métier

2 - Étapes simples pour faire les mises à jour

Activez les mises à jour automatiques	Vérifiez les mises à jour manuellement Utilisez des outils gratuits
☐ Windows Update / MacOS Update / Linux package manager ☐ Google Play Store / iOS App Store	☐ Accédez aux paramètres de l'application > Mises à jour ☐ PatchMyPC Home Updater / Ninite

3 - Points importants

Redémarrez vos équipements	Liens utiles
☐ Il est recommandé de redémarrer les équipements (ordinateur/téléphone) au moins une fois par jour. ☐ Les mises à jour sont généralement effectuées et appliquées au démarrage	Mettre à jour Windows Mettre à jour MacOS Mettre à jour Android Mettre à jour iOS Mettre à jour Adobe PDF Reader Mettre à jour Microsoft Office Mettre à jour les applications sur Android Mettre à jour les applications sur iOS

02 - Sécurité des comptes: Mots de Passes et MFA

Sécurisez vos comptes grâce à aux bonnes pratiques de mots de passe et l'authentification multifactorielle.

Les comptes utilisateurs constituent souvent le premier point d’entrée pour les cybercriminels. Une mauvaise gestion des identifiants – mots de passe faibles, comptes partagés, ou absence de contrôle d’accès – facilite grandement les intrusions.

Il est donc primordial de renforcer la sécurité des comptes en adoptant des pratiques simples mais efficaces. Utilisez des mots de passe complexes et uniques pour chaque compte, comportant au moins 12 caractères, et évitez d’utiliser des informations personnelles ou des mots communs. Pour ne pas avoir à les mémoriser tous, un gestionnaire de mots de passe est une solution idéale : il permet de stocker et générer des mots de passe forts et différents pour chaque service.

La mise en place de la double authentification (MFA) ajoute une couche de sécurité essentielle. Même si un mot de passe venait à être compromis, le pirate ne pourrait pas accéder au compte sans le second facteur d’authentification — généralement un code temporaire envoyé par application ou SMS.

Enfin, il est important de limiter les accès : chaque utilisateur doit avoir son propre compte, avec les droits minimums nécessaires. Supprimez ou désactivez les comptes inutilisés et surveillez régulièrement les accès aux outils et aux données sensibles.

On vous décrit ci-dessous **3 niveaux de protection.** Même si on recommande fortement la 3ème stratégie, si pour quelconque raison vous ne pouvez pas la suivre, nous vous donnons les bonnes pratiques à mettre en place en fonction.

Choisissez votre stratégie - .....

Stratégie 1 : Sans gestionnaire de mots de passe, sans MFA

**** Ce que vous pouvez faire pour limiter les risques*

Dans ce scénario, vous devez **mémoriser ou noter manuellement** chacun de vos mots de passe. Cela demande une certaine discipline, car il est impératif de ne **pas réutiliser les mêmes mots de passe** sur plusieurs services, et de choisir des mots de passe longs, complexes et uniques.

Bonnes pratiques à suivre :

- Choisissez des mots de passe d'au moins **12 caractères** avec un mélange de lettres (majuscules et minuscules), chiffres et symboles.
- Évitez les noms, dates de naissance, ou mots évidents.
- N'utilisez jamais le même mot de passe pour des services sensibles (comme votre boîte mail, vos outils de gestion client ou votre banque).
- Gardez une **copie papier sécurisée** (coffre, tiroir fermé à clé) si vous avez vraiment besoin d'écrire vos mots de passe, mais ne les stockez jamais dans un fichier texte ou une feuille Excel non protégée.

Cette stratégie **exige rigueur et mémoire**, et reste vulnérable si un mot de passe est compromis.

Stratégie 2 : Avec MFA, sans gestionnaire de mots de passe

**** Une sécurité renforcée, même si les mots de passe ne sont pas parfaits*

Ici, vous ajoutez une **double authentification (MFA)** : un code temporaire demandé à chaque connexion ou lors d'un accès sensible. Ce code est généralement généré par une **application mobile** (Google Authenticator, Authy...) ou reçu par SMS.

Même si vos mots de passe ne sont pas tous parfaits, le MFA protège vos comptes : **un attaquant ne pourra pas se connecter sans ce second facteur.**

Bonnes pratiques à suivre :

- Utilisez des mots de passe solides malgré tout.
- Activez le MFA sur **tous les services qui le permettent**, surtout ceux liés à vos clients ou à vos finances.
- Ne stockez pas vos codes MFA uniquement sur votre téléphone principal : pensez à enregistrer les clés de secours (ou un appareil de secours).

Cette stratégie **renforce grandement la sécurité**, mais demande de jongler avec plusieurs mots de passe à retenir ou à noter.

Stratégie 3 : Gestionnaire de mots de passe + MFA

**** La solution la plus simple, efficace et sécurisée*

Le **gestionnaire de mots de passe** (comme Bitwarden, 1Password ou Dashlane) permet de **générer, stocker et remplir automatiquement** des mots de passe forts et uniques pour chaque service. Il vous suffit de **retenir un seul mot de passe maître** pour y accéder. Avec la MFA activée, même si ce mot de passe est volé, vos données restent protégées.

Les avantages :

- Vous n'avez plus à créer ou mémoriser des dizaines de mots de passe.
- Le gestionnaire les remplit automatiquement dans vos navigateurs et applis.
- Vous n'avez qu'à retenir **trois mots de passe en tout** :
  - celui de votre **ordinateur**
  - celui de votre **boîte mail de récupération**
  - celui de votre **gestionnaire de mots de passe**

Conseils supplémentaires :

- Choisissez un mot de passe maître **long, unique et que vous ne pouvez pas oublier** (mais difficile à deviner !).
- Activez le MFA pour le gestionnaire lui-même.
- Sauvegardez votre mot de passe maître dans un endroit sûr, comme un coffre physique ou une copie papier codée.

C'est **le meilleur compromis** entre sécurité, confort et efficacité.

1 - Gestionnaire de mot de passe

Choix du gestionnaire	Choix du mot de passe
☐ Bitwarden ☐ 1Password ☐ Dashlane ☐ LastPass ☐	☐ Créer un mot de passe robuste ☐ Conservez le mdp dans un lieu sécurisé ☐ Installez l'extension pour votre navigateur principal (chrome, edge, firefox, ...) ☐ Activer le MFA

2 - Authentification multifactorielle (MFA)

Choix de l'application MFA	Activez le MFA

☐ Authy
☐ Google Authenticator
☐ .....
 	
Profitez d'activer le MFA pour changer le mot de passe des comptes.
 	
☐ Adresses e-mail
☐ Réseaux sociaux
☐ .....
	☐ Gestionnaire de mot de passe
	☐ Adresse e-mail
	  ☐ Personnelle
	  ☐ Professionnelle
	☐ Réseaux sociaux
	  ☐ Facebook
	  ☐ LinkedIn
	  ☐ Instagram
	  ☐ .....
	☐ Dès que possible

3 - Bonus

- ☐ Importez tous vos mots de passes dans votre gestionnaire
- ☐ Installez l'application sur votre smartphone
- ☐ Listez les comptes importants dans le tableau ci-dessous
- ☐ Prenez le temps de changer les mdp de ces comptes, générez et enregistrez les dans le gestionnaire de mdp
- ☐ Pour vos adresses e-mail, aller vérifier sur https://haveibeenpwned.com/ si votre compte a potentiellement été compromis sur un site. Assurez-vous de vous connecter aux services listés sur le site et d'aller changer immédiatement votre mot de passe. Ensuite, inscrivez vous sur https://haveibeenpwned.com/NotifyMe pour être notifié de toute nouvelle compromission.
- ☐ Prenez l'habitude lorsque vous êtes devant une page de connection de déverrouiller votre extension du gestionnaire de mot de passe avant de vous authentifier, si le mot de passe est déjà sauvegardé, celui-ci sera automatiquement pré rempli, s'il n'est pas enregistré, le gestionnaire de mot de passe vous proposera de le sauvegarder. Si c'est le cas, prenez le temps d'aller directement modifier le mot de passe, pour ne plus devoir vous en soucier à l'avenir.
- ☐ Prenez le temps de suivre les quelques recommandations ci-dessus vos avantages
  - ☐ Vous n'avez qu'à retenir **trois mots de passe en tout** :
    - ☐ celui de votre **ordinateur**
    - ☐ celui de votre **boîte mail de récupération**
    - ☐ celui de votre **gestionnaire de mots de passe**

    Plus de prise de tête pour choisir et retenir des mots de passes

Comptes Professionnels	Comptes Personnels

☐ Adresses e-mail
  ☐ Principale
  ☐ Secondaire
  ☐ .....
☐ Réseaux sociaux
  ☐ Linkedin
  ☐ Facebook
  ☐ Instagram
  ☐ TikTok
  ☐ .....
☐ Banque
☐ Logiciels métier
☐ .....
☐ .....
☐ .....
☐ .....
☐ .....
☐ .....
☐ .....
☐ .....
	☐ Adresses e-mail
	  ☐ Principale
	  ☐ Secondaire
	  ☐ .....
	☐ Réseaux sociaux
	  ☐ Linkedin
	  ☐ Facebook
	  ☐ Instagram
	  ☐ TikTok
	  ☐ .....
	☐ Banque
	☐ Logiciels
	☐ .....
	☐ .....
	☐ .....
	☐ .....
	☐ .....
	☐ .....
	☐ .....
	☐ .....

03 - Connexions sécurisées : Wi-Fi public & VPN

**** Protégez vos données lors de vos déplacements ou connexions hors du bureau.*

Dans notre quotidien numérique, il est tentant – et parfois nécessaire – de se connecter à un réseau Wi-Fi public : à la terrasse d'un café, dans une gare, un hôtel ou un espace de coworking. C'est pratique, rapide, et souvent gratuit. Mais derrière cette facilité d'accès se cache un véritable terrain de jeu pour les cybercriminels. Ces réseaux sont rarement sécurisés correctement, et parfois même créés volontairement par des attaquants dans le but de piéger les utilisateurs.

Lorsque vous vous connectez à un Wi-Fi public, toutes les données que vous échangez peuvent être interceptées : identifiants de connexion, emails professionnels, fichiers en cours d'envoi, informations de carte bancaire, etc. Ce type d'attaque, appelé "man-in-the-middle", permet à un tiers connecté au même réseau d'observer, modifier ou détourner votre trafic sans que vous vous en rendiez compte.

Pire encore, certains cybercriminels mettent en place de faux réseaux portant des noms rassurants comme "Wi-Fi_Hotel_Gratuit" ou "Café_Secure". Si vous vous y connectez, ils peuvent non seulement espionner vos échanges, mais aussi rediriger votre navigation vers de faux sites ressemblant à vos services habituels (banque, messagerie, réseaux sociaux) pour y voler vos identifiants en toute discrétion.

Utiliser un VPN (Virtual Private Network). C'est un outil qui chiffre toutes les données entre votre appareil et Internet, même si vous êtes sur un réseau non sécurisé. Le VPN rend votre activité illisible pour toute personne extérieure.

Bonnes pratiques à suivre :

- Évitez autant que possible d'utiliser des Wi-Fi publics.
- Si vous devez absolument vous connecter à un Wi-Fi public:
  - Utilisez un VPN fiable avant d'accéder à vos outils professionnels ou données sensibles.
  - Évitez d'accéder à des services critiques (banque, back-office, outils clients) sans VPN.
- Préférez utiliser la connexion partagée (4G/5G) de votre téléphone si le VPN n'est pas disponible.
- Désactivez la connexion automatique au Wi-Fi sur votre appareil.
- Vérifiez que les sites web que vous visitez sont bien en HTTPS (avec le petit cadenas dans la barre d'adresse).

1 - Se connecter en toute sécurité en public

Forfait data mobile illimité	**Pas assez de data**
☐ En Europe ☐ Activez la 4G/5G ☐ Hors Europe (incl Suisse, ...) ☐ Activez le Wi-Fi + VPN	☐ Activez le Wi-Fi + VPN ☐ ProtonVPN ☐ Windscribe ☐ TunnelBear ☐ .....

04 - Sauvegardes : Protéger vos données en cas d'incident

**** Un bon système de sauvegarde est votre assurance contre la perte de données.*

Un disque dur qui tombe en panne, un ransomware, un vol d'ordinateur, une mauvaise manipulation : les causes de perte de données sont nombreuses, imprévisibles, et souvent irréversibles. Sans système de sauvegarde, la récupération est soit impossible, soit extrêmement coûteuse.

La mise en place d'un système de sauvegarde ne doit pas être complexe ni onéreuse. Il existe des solutions gratuites, fiables et automatisables, parfaitement adaptées aux indépendants et petites structures.

Parce que vos fichiers professionnels (documents clients, devis, factures, visuels, etc.) sont le cœur de votre activité. Une bonne sauvegarde doit être :

- **Automatique** (évite les oublis)
- **Redondante** (à deux endroits au minimum)
- **Hors ligne ou hors site** (en cas de piratage ou de perte physique)

Bonnes pratiques :

- Sauvegardez **automatiquement tous les jours**, ou au minimum une fois par semaine.
- Gardez **au moins une copie hors ligne** (ex : disque dur non branché en permanence).
- Si vos fichiers sont sensibles ou confidentiels, **chiffrez vos sauvegardes**.

Sauvegarde cloud gratuite:

- **OneDrive (Microsoft)** : 5 Go gratuits, intégré à Windows
- **Google Drive** : 15 Go gratuits (liés à votre compte Google)
- **Dropbox** : 2 Go gratuits (limité mais suffisant pour les documents légers)
- **iCloud Drive** : 5 Go gratuits (peut être étendu pour quelques euros)

1 - Sauvegarder ses données

Sauvegardes	Logiciels

☐ Sauvegardes
  ☐ Locale
  ☐ Cloud
  ☐ .....
☐ Dossiers importants
  ☐ Compta
  ☐ Liste client
  ☐ Documents importants
  ☐ .....
  ☐ .....
  ☐ .....
	☐ Windows
	  ☐ File History
	  ☐ Duplicati
	  ☐ FreeFileSync
	☐ MacOS
	  ☐ Time Machine
	  ☐ Duplicati
	  ☐ .....

05 - Conclusion

Ce guide a été conçu pour vous proposer **des actions simples, concrètes et accessibles à tous**, même sans connaissances techniques avancées. Il ne s'agit pas d'un manuel complet de cybersécurité, mais d'un **point de départ solide et gratuit**, basé sur les **bonnes pratiques essentielles** pour protéger votre activité.

Dans un monde où les cybermenaces évoluent rapidement, même les plus petites structures — indépendants, freelances, TPE — peuvent devenir des cibles. Pourtant, en appliquant **quelques principes de base**, il est tout à fait possible de **réduire considérablement les risques**, sans forcément investir beaucoup de temps ni d'argent.

Gardez à l'esprit que :

- La **sécurité numérique** est un processus continu, pas une action unique
- **Mieux vaut commencer petit mais maintenant**, que trop tard
- Et vous n'êtes pas seuls : **si vous avez des doutes, besoin d'aide ou de conseils personnalisés**, nous sommes là pour vous accompagner.

N'hésitez pas à nous contacter pour aller plus loin, former vos équipes, ou mettre en place des solutions adaptées à votre activité. Nous sommes labellisés par la Région Wallonne dans le cadre des **Chèques-Entreprises "Cybersécurité".**

> **La cybersécurité n'est pas un luxe. C'est une hygiène numérique, aussi essentielle que de verrouiller la porte de votre bureau.**