2023

5 CONSEILS POUR CONSTRUIRE VOTRE CYBERDÉFENSE

RÉDIGÉ PAR

LES EXPERTS UBCOM

www.ubcom.eu
contact@ubcom.eu

PRÉFACE

LES CYBERATTAQUES, LE MAL DU XXI SIÈCLE

Depuis l'émergence des cryptomonnaies au tournant des années 2010, les cyberattaques (vols de données et attaques par rançongiciels) ont connu une très forte augmentation. Cette recrudescence s'explique par le fait que les cyberattaquants peuvent désormais revendre facilement les données volées, sur le darkweb. Le contexte cyber s'est donc particulièrement tendu.

La place des technologies du numérique n'a cessé de croître. Il est désormais indispensable de se protéger face aux nombreuses menaces cyber. Être en mesure d'évoluer dans un environnement sécurisé nécessite d'avoir été formé à des gestes spécifiques en matière de cybersécurité. Rien n'est naturel quand il s'agit de technologie, et les pratiques visant à garantir une protection de ses données non plus. C'est pourquoi UBCOM vous propose une nouvelle vision des actions à mettre en œuvre pour protéger votre vie numérique, qu'elle soit privée ou professionnelle.

Ce guide rassemble les gestes essentiels à connaître et nous vous invitons à vous y référer comme un pense-bête.

INTRODUCTION

Tel que nous l'entendons, la cybersécurité correspond à la mise en œuvre de moyens techniques pour protéger la confidentialité, l'intégrité et la disponibilité d'une information.

Ces informations peuvent concerner un mail, un SMS, une conversation téléphonique ou même un post sur un forum ou un réseau social. Ces informations personnelles doivent être sécurisées tout au long de leur «cycle de vie» ; depuis leur création dans un milieu sécurisé, à leur destruction totale quand cela est possible. Entre temps, leur stockage, leur transfert et leur accessibilité sont des questions de cybersécurité.

Entreprises, particuliers, professions libérales, informaticiens, novices, prestataires de services ou agents gouvernementaux ; nous sommes tous concernés par les menaces numériques.

Ces cybermenaces prennent de nombreuses formes, dont la seule limite se trouve dans l'imagination des hackers.

Les 5 règles pour construire votre cyberdéfense ne peuvent garantir une protection absolue. Autrement notre métier serait beaucoup trop simple. Cependant, elles sont les mesures de protection minimum pour mettre à l'abri vos informations. Toute forme de défense constitue un obstacle face aux pirates informatiques et génère de la résistance, indispensable pour éviter le pire.

Dans la majorité des cas, les hackers utilisent des attaques automatisées (*bots*) qui sont de plus en plus intelligents, mais incapables d'improviser. Leur efficacité repose sur l'erreur humaine et les comportements à risque.

Supprimez-les et vous aurez fait un grand pas vers votre cybersécurité !

À RETENIR

01 **Choisir un pare-feu (*firewall*) sécurisé**

02 **Installer un VPN sur vos outils numériques**

03 **Renforcer la sécurité de vos mots de passe**

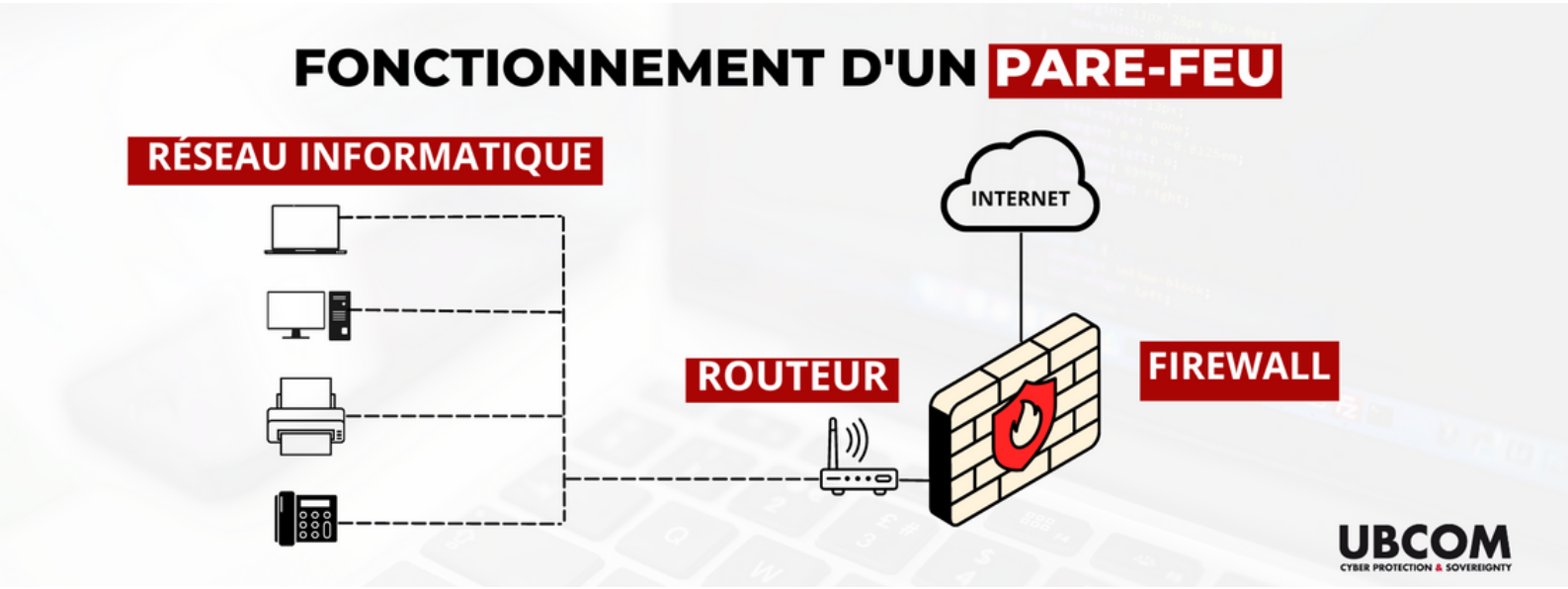
04 **Utiliser un cloud sécurisé souverain**

05 **Sécuriser ses moyens de communication**

01 Choisir un pare-feu (*firewall*) sécurisé

Un pare-feu peut être logiciel, matériel ou hybride. Il permet de filtrer les communications autorisées, entrantes et sortantes, sur votre réseau informatique. **Son objectif est de faire respecter la politique de sécurité du réseau.**

Le terme français « pare-feu » renvoie à un mur virtuel qui bloque toute connexion, non autorisée, considérée comme malveillante. Ce mur virtuel constitue une barrière de protection essentielle pour se prémunir des intrusions et des attaques extérieures. Il convient donc de choisir son pare-feu avec le plus grand soin tout en veillant à ce qu'il corresponde au mieux à vos besoins.



3 CONSEILS POUR CHOISIR SON PARE-FEU

- **DIFFÉRENCIEZ LES TYPES DE PARE-FEU EXISTANTS** :
  Pare-feu virtuel ou physique ? Installation pour protéger tout votre réseau, ou installation d'applications sur chacun de vos appareils ? Présence d'IoT, d'objets connectés, d'automates ?

  Chaque type de pare-feu présente ses avantages et ses inconvénients. La première chose à faire est d'identifier vos besoins avec le plus de précision possible.

- **IDENTIFIEZ LA PUISSANCE DE VOTRE LIAISON INTERNET ET LE NOMBRE D'ÉQUIPEMENTS À PROTÉGER PAR VOTRE FUTUR PARE-FEU**
  En effet, le débit du réseau dépend du nombre de périphériques et d'utilisateurs connectés permettant ainsi de déduire le nombre d'IP à protéger.

- **DÉTERMINEZ LES RÈGLES DE FILTRAGE DE VOTRE PARE-FEU**
  Il vous faudra établir la liste de toutes les applications qui communiquent avec Internet. Les modèles « Next Generation » incorporent également des critères intelligents pour détecter et bloquer les menaces. Des règles bien définies demandent du temps et de la compétence mais assurent une sécurité accrue.

  Il ne vous reste plus qu'à déterminer les bons critères, selon vos besoins, pour choisir votre pare-feu. Les experts UBCOM se tiennent à votre disposition pour vous accompagner dans l'évaluation de ces critères et vous proposer la solution la plus adaptée à vos usages.

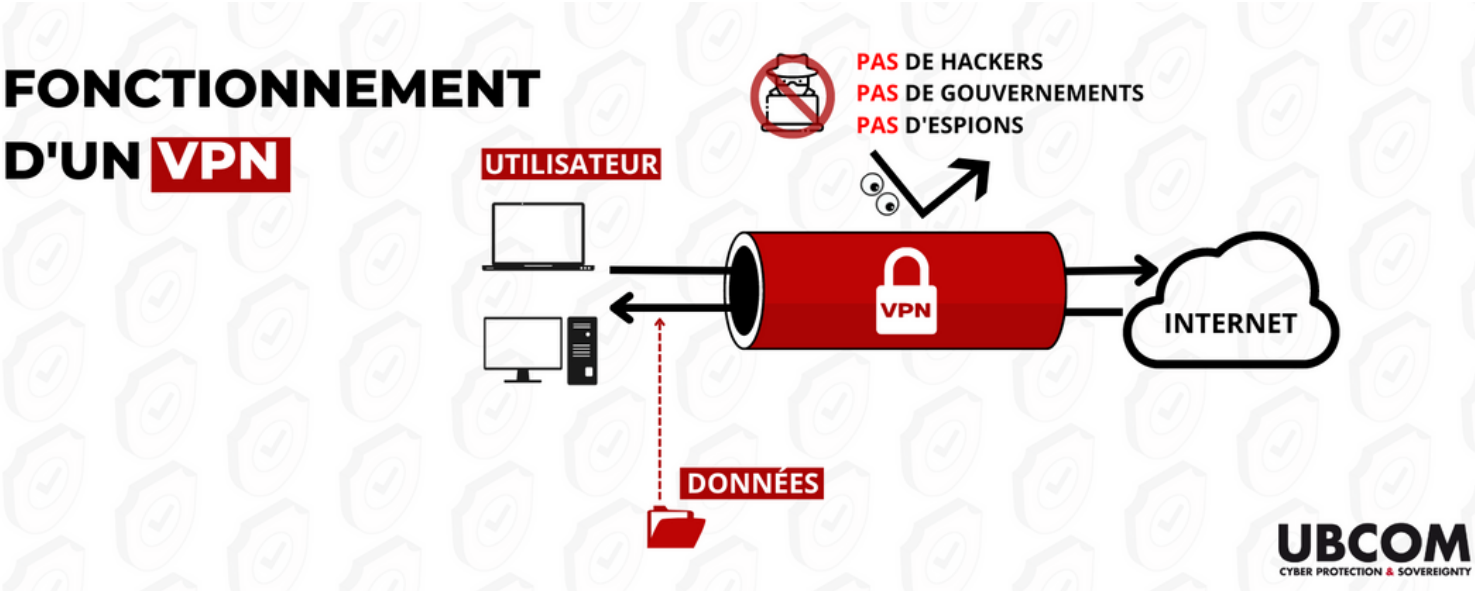
02 Installer un VPN sur vos outils numériques

Un VPN (*virtual private network)*, est un service qui protège votre identité en ligne, en masquant votre IP. Le VPN renforce ainsi la sécurité de votre connexion à internet. Il crée un tunnel chiffré, à travers lequel transitent toutes vos données en particulier votre adresse IP et donc votre identité en ligne. Il vous donne la possibilité de choisir un point d'accès réseau (nouvelle adresse IP) partout dans le monde. Dans certains pays, le recours à un VPN est nécessaire pour accéder à certains sites et contourner la censure.

Recourir à un VPN peut avoir divers objectifs : empêcher votre fournisseur d'accès à internet de recueillir vos informations personnelles, débloquer des contenus géo-bloqués (contournement de la censure), limiter le tracking de vos activités en ligne ou encore protéger vos données lorsque vous vous connectez à un Wi-Fi public. Le VPN, traitant de vos données, doit être choisi avec précaution.

12 CRITÈRES POUR CHOISIR SON VPN

- les protocoles de chiffrements,
- les protocoles VPN,
- la gestion des logs,
- la bande-passante du VPN,
- le nombre de serveurs,
- la localisation des serveurs,
- l'accès aux plateformes de streaming,
- le nombre d'appareils supportés,
- le prix,
- le service client,
- la réputation du VPN,
- La nationalité de l'éditeur.



03 Renforcer la sécurité de vos mots de passe

62% des entreprises déclarent ne pas prendre les mesures nécessaires pour sécuriser correctement les données mobiles.

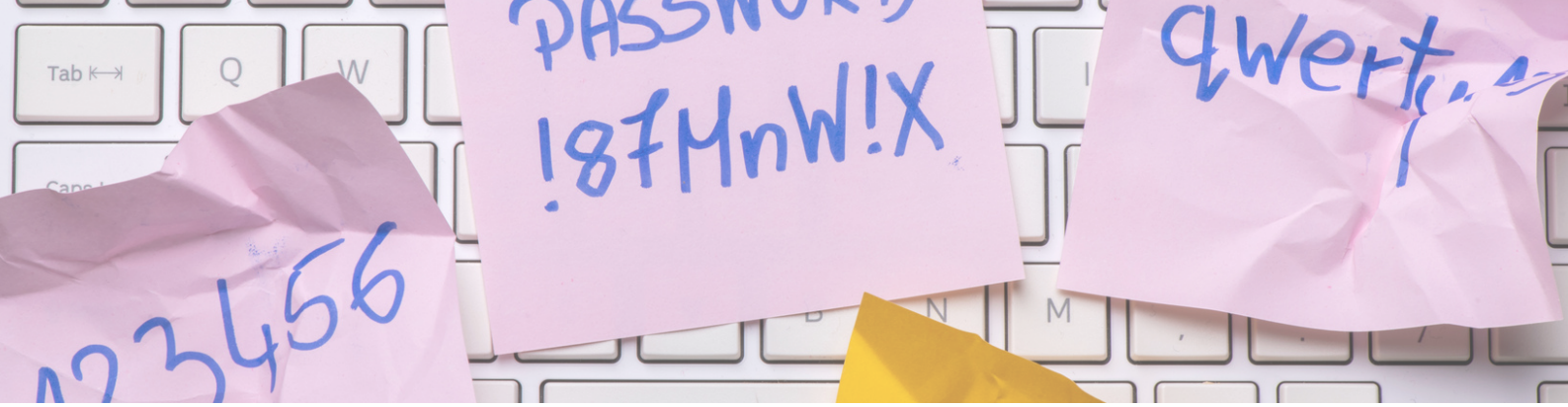
Que 45% des victimes disent qu'elles changeraient leur mot de passe après avoir été piratées.

Seulement 37% ont utilisé l'authentification à deux facteurs pour sécuriser leurs mots de passe en 2020.

Source : Insitute Ponemon et Google

Ces chiffres sont alarmants pour la sécurité informatique et demandent de se pencher sur la question de la sécurisation des mots de passe. Une dernière statistique nous révèle en effet que **80% des brèches** lors de piratage ou de cyberattaques, **sont liées aux mots de passe** (source : Verizon).

Ainsi, il conviendra de veiller avec un soin tout à fait particulier à la configuration des mots de passe. Généralement construits avec des mots ou des noms faciles à retenir, nous vous recommandons au contraire de choisir un mot de passe avec des mots complexes et différents à chaque fois.



5 RÈGLES POUR CONSTRUIRE SON MOT DE PASSE

CHOISIR UN MOT DE PASSE FORT ET COMPLEXE
Un minimum de 12 caractères, comprenant des lettres majuscules et minuscules, des chiffres et des symboles, renforcera la complexité de vos mots de passe.

CRÉER UN MOT DE PASSE UNIQUE
Oubliez les dates de naissance de vos proches ou bien les noms propres de votre entourage : privilégiez des mots de passe composés d'une suite unique de caractères aléatoires.

SÉLECTIONNER UN GESTIONNAIRE DE MOT DE PASSE
Un gestionnaire de mot de passe vous permet de générer un mot de passe robuste, complexe et unique, de transférer des comptes, de sauvegarder tous vos mots de passes dans un coffre fort accessible depuis tous vos outils et applications, mais aussi de les partager de manière permanente ou instantanée et enfin d'y accéder n'importe où et n'importe quand.

ACTIVER L'AUTHENTIFICATION À DEUX FACTEURS
Elle rajoute une couche supplémentaire de sécurité contre les tentatives d'intrusion.

VÉRIFIER LES FUITES DE MOTS DE PASSE
Il est possible que vos mots de passe soient compromis sans que vous ne le sachiez. Cette fonctionnalité disponible chez les éditeurs de solution de gestion des mots de passe permet de vérifier la non-compromission de vos mots de passe et donc, de renforcer la sécurité de vos comptes. D'autres sites comme *haveibeenpwned.com* permettent également ce service.

Retrouvez les conseils des experts UBCOM
pour renforcer la sécurité de vos mots de passe en vidéo ici !

04 Utiliser un cloud sécurité souverain

Sauvegarder vos données dans un cloud c'est bien.

Sécuriser le cloud sélectionné c'est mieux.

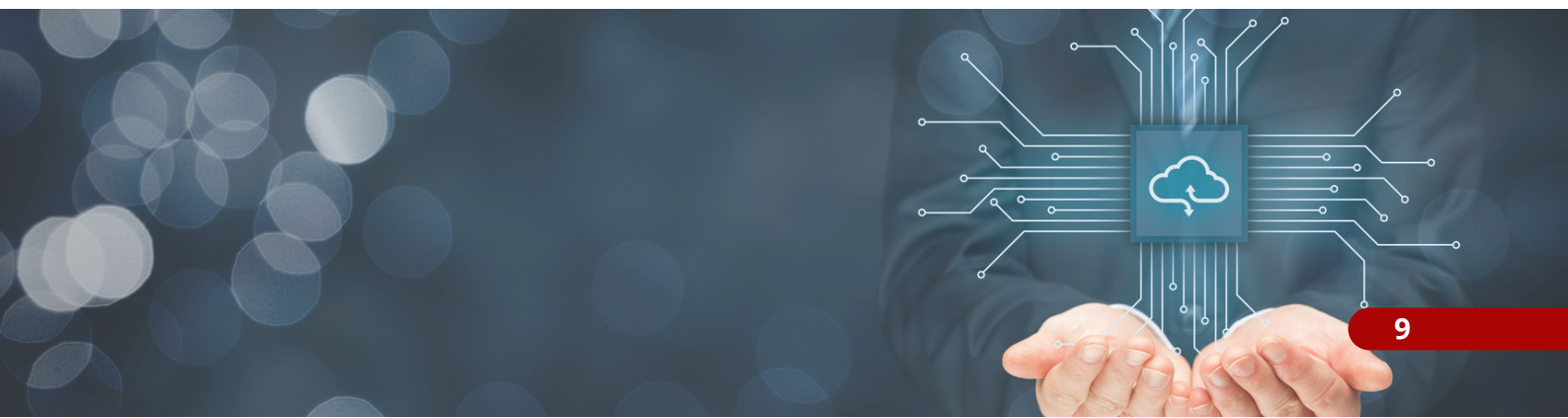
Choisir un cloud souverain, c'est presque parfait !

Au moment de choisir un service cloud, assurez-vous qu'il garantisse votre sécurité à différents niveaux : sécurité physique des datacenters, accessibilité des serveurs, duplication et chiffrement des données... Il existe plusieurs technologies de chiffrement des données. Notez que certains services cloud offrent un niveau de sécurité supplémentaire en proposant un chiffrement de bout en bout dit « sans connaissance ».

Qu'est ce qu'un cloud souverain ? Selon le guide sur le cloud computing et les data center à l'attention des collectivités locales, le cloud souverain est un «modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de cloud sont physiquement réalisés dans les limites du territoire national, par une entité de droit français et en application des lois et normes françaises».

Autrement dit, un cloud souverain est une notion complémentaire d'un service de stockage de données, focalisée sur le fait de protéger au maximum les données hébergées, en fonction du droit français.

Les experts d'UBCOM vous recommandent ainsi d'identifier les critères de stockage, les conditions de sécurité et la nationalité du cloud. Car avoir sa donnée en France, ne garantit pas qu'elle sera stockée dans un cadre souverain.



05 Sécuriser ses moyens de communication

La majorité des informations que vous exploitez sont partagées via des outils qui ne sont pas nécessairement sécurisés par défaut : messagerie instantanée, serveur mail, réseaux sociaux, etc. Au-delà de l'utilisation d'un pare-feu (*firewall*), d'un VPN et d'un mot de passe fort, vous pouvez également renforcer plus efficacement vos échanges grâce à des messageries chiffrées, qui permettent de sécuriser le contenu de vos communications.

Un service de messagerie chiffrée offre une solution de chiffrement de bout en bout. Cela réduit drastiquement les risques de vol de données et empêche la surveillance de vos conversations.

Nous vous recommandons d'éviter de recourir à des messageries non chiffrées, Facebook Messenger par exemple, ou à celles qui se disent chiffrées, mais exploitent vos métadonnées, tel que WhatsApp).

Enfin, privilégiez les solutions souveraines : ces solutions ne dépendent d'aucune loi extraterritoriale et garantissent une protection robuste de vos données. Nos experts peuvent aussi vous conseiller dans le choix de ces solutions innovantes et performantes.

"Si c'est gratuit,
c'est vous le produit, donc vos données"

Frans Imbert-Vier, PDG UBCOM

CONCLUSION

La cybersécurité est un secteur qui appelle à des compétences particulières et au respect de règles appropriées. Rien n'est inné et une formation à ces enjeux est essentielle pour protéger vos données. La pandémie de COVID-19, nous a collectivement fait prendre conscience de la vitesse à laquelle un virus particulièrement contagieux peut infecter l'ensemble de la population. Il convient d'appliquer ce raisonnement à l'univers du numérique, susceptible de devoir un jour faire face à une crise similaire. Au même titre que les gestes barrières furent indispensables pour empêcher la propagation du virus, les règles de cybersécurité énoncées ci-dessus revêtent aujourd'hui un caractère essentiel pour faire face à la recrudescence des cyberattaques.

Les virus informatiques existent sur l'ensemble des réseaux connectés. Quotidiennement, ils migrent pour infiltrer les systèmes de vos collègues, de vos amis et de vos familles et arriver jusqu'à vous. À partir de ce constat, il est urgent d'entendre la nécessité des gestes d'hygiène cyber pour vous protéger vous, mais aussi tout votre entourage. Grâce à divers outils, tels que les antivirus, les mots de passe et les VPN, il est possible de mettre en place des moyens concrets pour renforcer votre cyberdéfense et décourager les pirates informatiques de s'attaquer à vous.

Afin d'améliorer votre protection cyber, nous vous conseillons de faire appel à des experts dont c'est le métier. À l'écoute de vos problématiques et de leurs enjeux, ces experts seront capable d'analyser votre environnement et de vous apporter des conseils et de vous proposer des solutions adaptées.

Les experts UBCOM pourront ainsi vous présenter diverses solutions cyber, sélectionnées spécialement pour vous, qui renforceront la résilience de vos systèmes d'information. Ce guide des 5 conseils pour préparer votre cyberdéfense, réalisé par nos experts vous permettront de réduire considérablement votre niveau d'exposition aux attaques cyber.

N'hésitez pas à partager ces conseils autour de vous. Plus votre entourage sera sensibilisé, plus votre réseau immédiat sera à son tour sécurisé, et plus vos vulnérabilités diminueront. Nous sommes là pour vous aider à mettre en place ces solutions. N'attendez plus, **protégez-vous et contribuez à la protection de votre entourage !**

UBCOM

CYBER PROTECTION & SOVEREIGNTY

5 CONSEILS POUR CONSTRUIRE VOTRE CYBERSÉCURITÉ

www.ubcom.eu
contact@ubcom.eu