

La cybersécurité

La **cybersécurité** c'est comme à la maison, on ne laisse pas entrer n'importe qui chez soi ! On fait attention à nos données sur ordinateur et sur internet et cela commence par une bonne hygiène numérique.

Mon ordi me propose une mise à jour, à quoi ça sert ?

Installe-la ! Elle colmate les failles de sécurité pour tenir les hackers à distance.

Télécharger sans risques, c'est possible ?

Toujours depuis des sources sûres pour éviter les virus.

Le VPN c'est magique !

Pas vraiment. Il ne te protège pas contre les virus et conserve les traces en ligne.

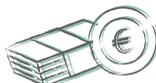
La cybersécurité



Mets-toi à jour !

Les mises à jour de tes appareils peuvent parfois te sembler inutiles, voire une perte de temps, mais en réalité elles jouent un rôle crucial en comblant les failles de sécurité et en les protégeant contre les attaques de pirates qui exploitent ces

vulnérabilités. Ne pas les installer, c'est laisser la porte ouverte aux cybercriminels qui guettent ces occasions. Alors, pour rester protégé, pense à les installer !



Quand c'est gratuit, c'est toi le produit

Télécharger des films, de la musique ou des livres sur internet peut exposer tes appareils et tes données à des risques cachés. Si télécharger illégalement semble facile et inoffensif, il y a en réalité des conséquences sérieuses. En effet, des logiciels malveillants peuvent s'infiltrer

avec les fichiers illégaux.

Conséquence : un appareil plus lent ou pire, le vol de tes données personnelles !

Alors pour rester en sécurité, privilégie les téléchargements depuis des sources légales et sécurisées.

À la pêche aux infos

L'hameçonnage est une cyberattaque très commune au cours de laquelle les pirates envoient des messages, souvent par mail ou SMS. Ils se font passer pour des organismes fiables pour te duper et te faire cliquer sur des liens ou télécharger des pièces jointes malveillantes, volant au passage tes données. Ils exploitent tes émotions et l'urgence, se faisant

même passer pour des organisations humanitaires.

Il y a même des arnaques aux QR codes : un simple scan d'un menu au restaurant est désormais susceptible d'infecter ton téléphone !

Protège-toi en vérifiant toujours l'expéditeur de tes messages et en évitant de cliquer sur les liens ou téléchargements suspects.



Le mot de passe, c'est comme la clé de ta maison !



Avec des machines de plus en plus douées pour craquer les mots de passe, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) recommande désormais entre 12 et 14 caractères variés pour une meilleure sécurité. Mais n'utilise pas le même mot de passe-partout ! Pour t'aider, pense au coffre-fort

numérique : tu mémorises un seul mot de passe et il s'occupe du reste en te connectant automatiquement sur un site et en toute sécurité. Autre solution : lorsque cela t'est proposé, utilise l'authentification multi facteurs ! C'est en empilant les couches de protection que tu deviens très difficile à craquer !

Le VPN, la protection miracle ?



Le VPN ou Réseau privé virtuel, est souvent vendu par les influenceurs comme la couche de protection infaillible pour naviguer tranquillement sur le net. On a simplement oublié de te dire qu'il n'immunise en rien contre les virus ni ne rend tes

actions totalement anonymes. Son seul rôle est de masquer ton adresse IP en te connectant via un serveur distant. Le VPN reste tout de même une couche supplémentaire de protection, mais à relativiser.



On ne met pas tous ses œufs dans le même panier

Pour mieux te protéger des cyberattaques, fais des sauvegardes régulières de tes fichiers importants. Utilise des disques amovibles, comme une clé USB ou un disque dur externe, pour les données confidentielles. Pour tes documents moins sensibles, le cloud (« nuage » en français) comme

l'application ENT « Mes données » sont pratiques : tes fichiers sont sur un serveur en ligne, accessibles avec ton identifiant.

Ainsi, tes données essentielles restent en sécurité, même en cas de problème ! sur ton appareil.



Traces numériques

Chaque action en ligne laisse des traces numériques, un peu comme des empreintes digitales dans le monde virtuel. Pour minimiser les risques de cyberattaques, adopte une bonne hygiène numérique : sois prudent avec les informations que tu partages sur les réseaux sociaux, utilise des paramètres de confidentialité stricts et pense à

effacer régulièrement ton historique de navigation et tes cookies. Cela aide à réduire ton empreinte en ligne tout en te protégeant contre le suivi indésirable et les menaces potentielles. Pour cela, consulte la fiche « e-réputation ».



Le savais-tu ?



Pour un mot de passe unique et mémorable, crée ta propre « passphrase » avec une suite de mots significatifs pour toi (souvenir marquant ou phrase amusante de ton quotidien). Cela rend ton mot de passe à la fois complexe et personnel, difficile à deviner pour les autres mais facile à retenir pour toi.

Par exemple, « Il fait beau dans le Nord et pas dans le sud depuis 2004 ! » :
lfaitbodsleN&pasdsleSd2004!

Sitographie



[Cano.pe/CoffreFortNumerique](https://cano.pe/CoffreFortNumerique)

Coffre-fort numérique pour stocker tous ses mots de passe sans tracas.



[Cano.pe/RessourcesEducativesInternet](https://cano.pe/RessourcesEducativesInternet)

Des ressources éducatives pour naviguer sur internet en sécurité.



[Cano.pe/MalletteCybersecurite](https://cano.pe/MalletteCybersecurite)

Une mallette cybersécurité à utiliser et imprimer !



[Cano.pe/TelecrochetFictifCybersecurite](https://cano.pe/TelecrochetFictifCybersecurite)

Télécrochet fictif qui aborde la cybersécurité avec humour.



[Cano.pe/PourAllerPlusLoin](https://cano.pe/PourAllerPlusLoin)

10 pratiques pour se protéger davantage.



[Cano.pe/SiteOfficielANSSI](https://cano.pe/SiteOfficielANSSI)

Pour des conseils officiels sur la sécurité des systèmes d'information et des guides pratiques.



[Cano.pe/ProtectionDonnees](https://cano.pe/ProtectionDonnees)

Pour tout savoir sur la protection des données personnelles et la réglementation.

Ce QR est fiable !
Scannez-moi pour
accéder à la dernière
version de la fiche

