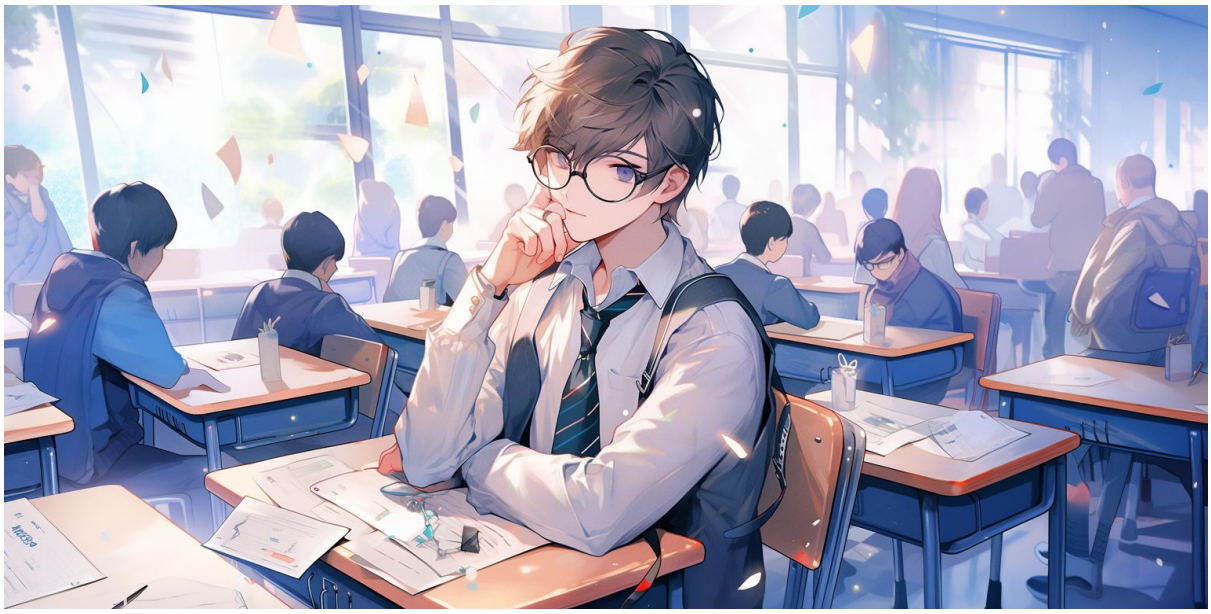
Formation sécurité web digitale



Objectif

L'objectif d'une formation sur la sécurité numérique est de fournir aux participants les connaissances, les compétences et les bonnes pratiques nécessaires pour protéger les systèmes informatiques, les données et les réseaux contre les menaces potentielles.

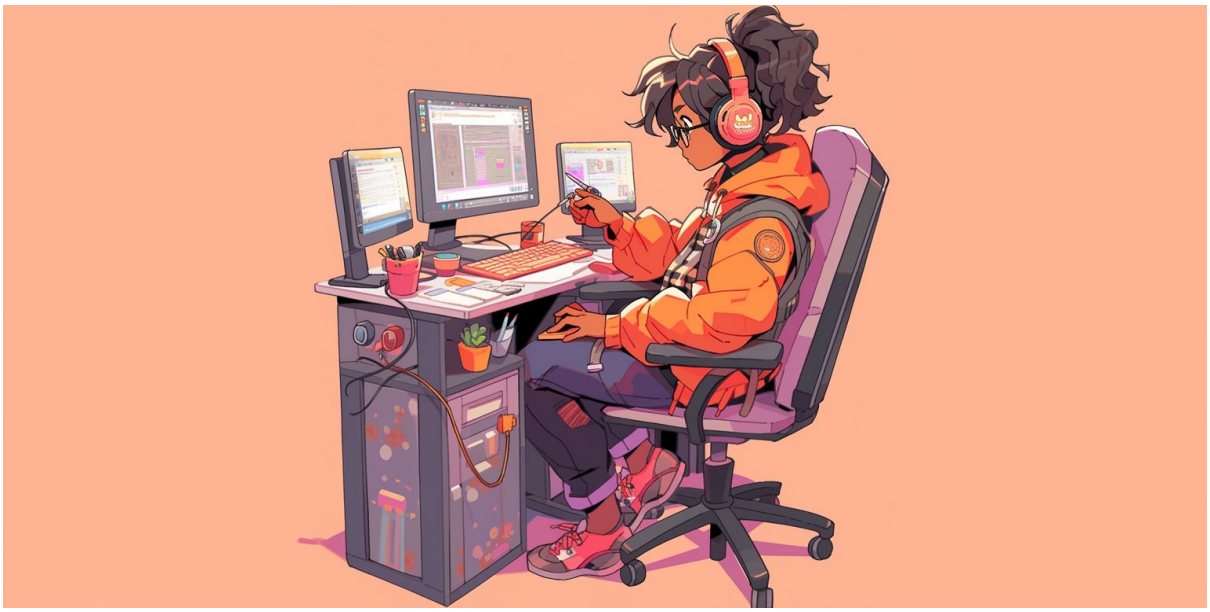
Compréhension des menaces et des vulnérabilités : Apprendre à identifier les différentes menaces potentielles auxquelles les systèmes informatiques sont confrontés, ainsi que les vulnérabilités qui pourraient être exploitées par des attaquants.

Connaissance des technologies de sécurité : Acquérir une compréhension approfondie des technologies de sécurité, telles que les pare-feu, les antivirus, les systèmes de détection d'intrusion, la cryptographie, etc.

Gestion des identités et des accès : Apprendre à mettre en œuvre des politiques de gestion des identités et des accès pour assurer que seules les personnes autorisées ont accès aux informations sensibles.

Sensibilisation à la sécurité : Éduquer les utilisateurs sur les meilleures pratiques en matière de sécurité, y compris la création et la gestion de mots de passe forts, la détection des tentatives de phishing, et la prudence lors de l'utilisation de périphériques et de services en ligne.

Sécurité des réseaux : Comprendre les principes de base de la sécurité des réseaux, y compris la sécurisation des connexions, la détection des intrusions, et la protection contre les attaques de déni de service.



Lexique sécurité

Antivirus : Un logiciel conçu pour détecter, prévenir et éliminer les logiciels malveillants, tels que les virus, les vers et les chevaux de Troie.

Attaque par force brute : Une méthode d'attaque où un attaquant tente de deviner un mot de passe en suggérant différentes combinaisons de caractères jusqu'à ce que le mot de passe correct soit trouvé.

Authentification à deux facteurs (A2F) : Un mécanisme de sécurité qui exige deux formes d'identification distinctes avant de permettre l'accès, généralement quelque chose que l'utilisateur sait (mot de passe) et quelque chose qu'il possède (comme un code généré par une application sur son téléphone).

Cryptographie : La pratique de sécuriser les communications en convertissant l'information en un code difficile à intercepter ou à comprendre sans la clé de décodage appropriée.

Firewall : Un dispositif ou un logiciel qui surveille et contrôle le trafic réseau, décident quels paquets de données peuvent entrer ou sortir d'un réseau.

Hameçonnage (Phishing) : Une technique d'attaque où un attaquant se fait passer pour une entité de confiance pour tromper les utilisateurs et les inciter à divulguer des informations sensibles, comme des identifiants ou des mots de passe.

Ingénierie sociale : L'utilisation de techniques psychologiques pour manipuler des personnes afin qu'elles divulguent des informations confidentielles.

Logiciel malveillant (Malware) : Un terme générique qui englobe tout logiciel conçu pour causer des dommages à un ordinateur, un réseau ou à des données, y compris les virus, les vers, les chevaux de Troie et les ransomwares.

Pare-feu (Firewall) : Un système de sécurité qui contrôle le trafic réseau en autorisant ou en bloquant certaines communications en fonction d'un ensemble de règles prédéfinies.

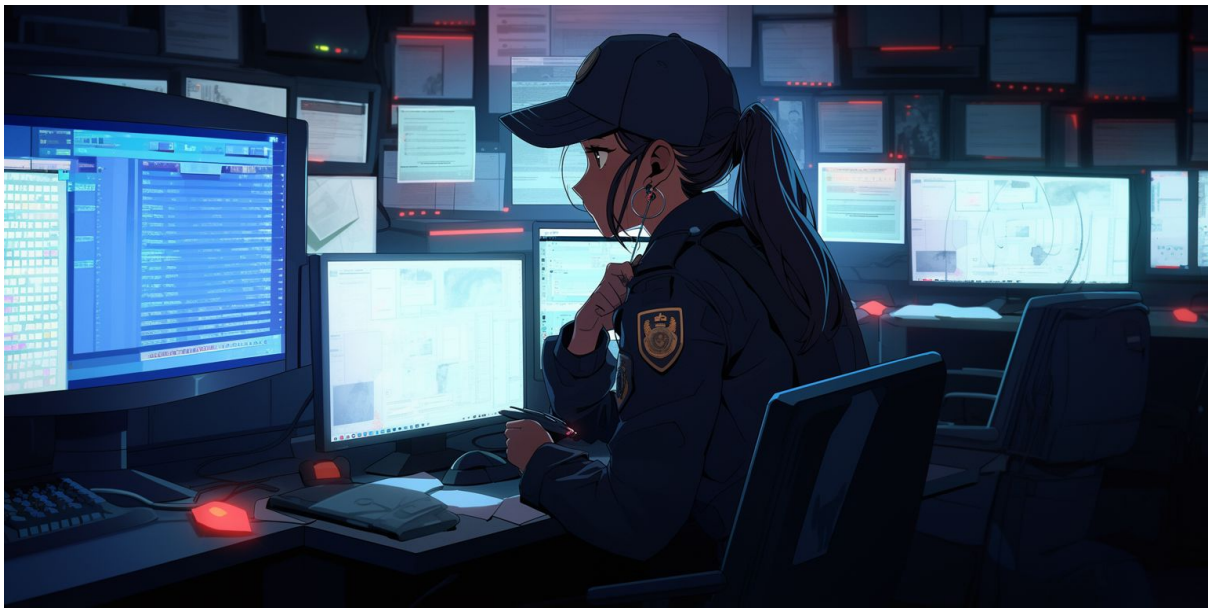
Ransomware : Un type de logiciel malveillant qui chiffre les fichiers d'un utilisateur et demande le paiement d'une rançon en échange de la clé de déchiffrement.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) : Protocoles de sécurité qui garantissent la confidentialité et l'intégrité des données échangées entre un navigateur web et un serveur.

Virus : Un type de logiciel malveillant capable de se propager en infectant d'autres programmes ou fichiers, généralement en modifiant leur code.

VPN (Virtual Private Network) : Un réseau virtuel privé qui permet à des utilisateurs distants de se connecter à un réseau sécurisé via une connexion chiffrée sur Internet.

Zero-Day Exploit : Une attaque qui exploite une vulnérabilité avant qu'un correctif ne soit disponible, laissant les utilisateurs sans défense.



Sécuriser son site Internet

Mises à jour régulières : Assurez-vous que tous les logiciels, y compris le système d'exploitation, le serveur web, les applications et les plugins, sont à jour avec les derniers correctifs de sécurité.

Certificat SSL/TLS : Installez un certificat SSL/TLS pour chiffrer les données entre le navigateur des utilisateurs et votre serveur, assurant ainsi la confidentialité des informations échangées.

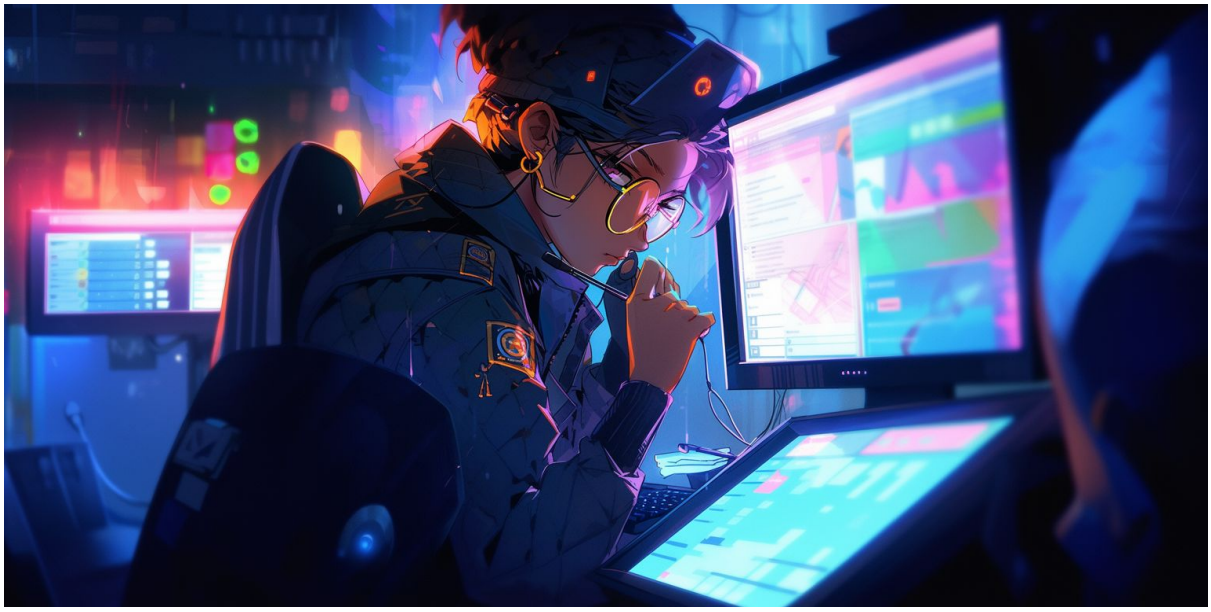
Sauvegardes régulières : Effectuez des sauvegardes fréquentes des données du site et assurez-vous que les procédures de restauration fonctionnent correctement en cas de besoin.

Gestion des accès : Utilisez des méthodes d'authentification forte, implémentez une politique de gestion des accès et révoquez rapidement les droits d'accès des utilisateurs qui n'en ont plus besoin.

Surveillance du site : Utilisez des outils de surveillance pour détecter les activités suspectes, les tentatives d'intrusion et les comportements anormaux sur le site.

Pare-feu applicatif web (WAF) : Installer un pare-feu applicatif web pour filtrer le trafic HTTP et détecter et bloquer les attaques web courantes.

Sécurisation des fichiers et répertoires : Restreignez les permissions d'accès aux fichiers et répertoires sensibles, et assurez-vous que les utilisateurs n'ont accès qu'aux ressources nécessaires.



Sécuriser son ordinateur

Mises à jour régulières : Assurez-vous que votre système d'exploitation, les logiciels et les applications sont toujours à jour avec les derniers correctifs de sécurité.

Logiciel antivirus/antimalware : Installer un logiciel antivirus/antimalware fiable et conserver-le à jour. Effectuez régulièrement des analyses de votre système.

**** Pare-feu :**** Activez le pare-feu intégré de votre système d'exploitation ou installez un pare-feu tiers pour contrôler le trafic réseau et bloquer les connexions non autorisées.

Mots de passe forts : Utilisez des mots de passe forts, uniques et changez-les régulièrement. Utilisez des gestionnaires de mots de passe pour simplifier la gestion de vos identifiants.

Authentification à deux facteurs (A2F) : Activez l'authentification à deux facteurs lorsque cela est possible pour ajouter une couche supplémentaire de sécurité.

Cryptage : Chiffrez les données sensibles, en particulier si vous stockez des informations sur des supports amovibles comme des clés USB.

Sauvegardes régulières : Effectuez des sauvegardes régulières de vos données importantes et vérifiez que vous pouvez restaurer ces sauvegardes en cas de besoin.

Réseau sécurisé : Utilisez des connexions sécurisées (WPA2/WPA3) pour votre réseau Wi-Fi domestique et évitez les réseaux Wi-Fi publics pour des activités sensibles.

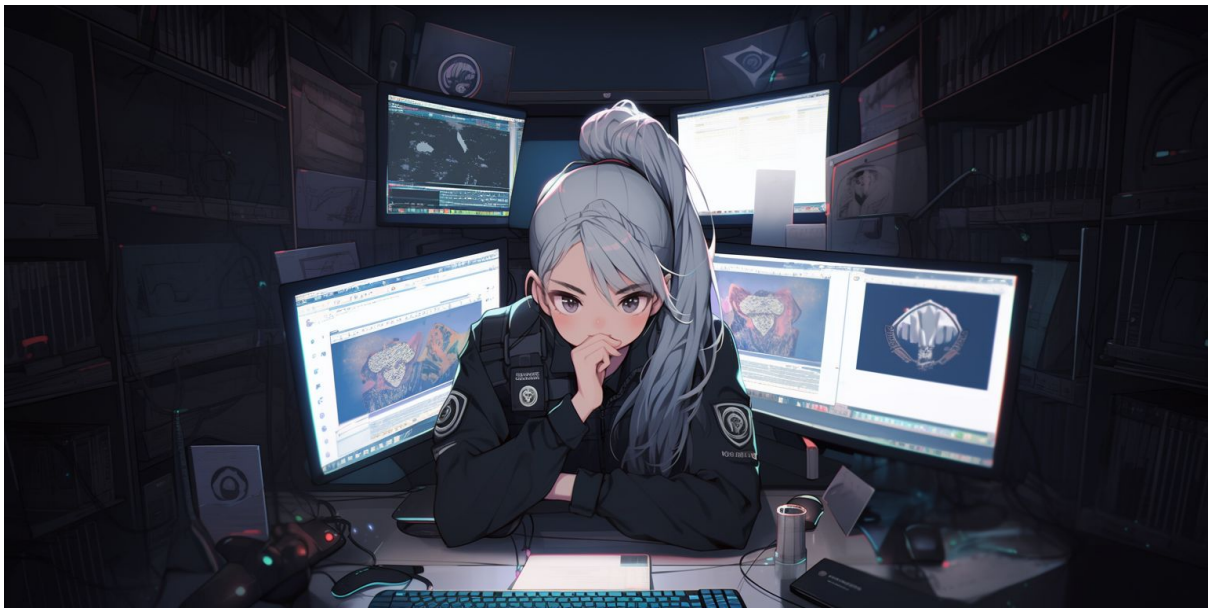
Sécurisation du navigateur : Utilisez les fonctionnalités de sécurité du navigateur, activez le blocage des pop-ups, et évitez les extensions non nécessaires.

Mises à jour du navigateur : Gardez votre navigateur web à jour pour bénéficier des dernières fonctionnalités de sécurité.

Éviter les téléchargements suspects : Ne téléchargez des fichiers que depuis des sources fiables. Évitez les sites web douteux et les liens non sollicités.

Suppression des logiciels inutiles : Désinstallez les logiciels que vous n'utilisez pas pour réduire les vulnérabilités potentielles.

Limitation des droits d'administration : Utilisez un compte d'utilisateur standard au lieu du compte administrateur pour réduire les risques liés aux logiciels malveillants.



Sécuriser sa messagerie

Mots de passe forts : Utilisez des mots de passe robustes, combinant lettres majuscules et minuscules, chiffres et caractères spéciaux. Ne réutilisez pas le même mot de passe pour plusieurs comptes.

Authentification à deux facteurs (A2F) : Activez l'authentification à deux facteurs pour renforcer la sécurité de l'accès à votre compte.

Mises à jour régulières : Assurez-vous que votre client de messagerie est à jour avec les derniers correctifs de sécurité.

Vérification des liens : Méfiez-vous des liens dans les courriels. Vérifiez toujours l'authenticité des liens avant de cliquer, en survolant-les pour afficher l'URL réelle.

Éviter les pièces jointes suspectes : N'ouvrez pas les pièces jointes provenant d'expéditeurs inconnus, et assurez-vous que les fichiers provenant de sources connues sont sécurisés.

Crainte du hameçonnage : Soyez vigilant face aux tentatives de hameçonnage. Vérifiez l'authenticité des courriels, en particulier ceux demandant des informations sensibles.

Protection antivirus : Utilisez un logiciel antivirus fiable pour scanner les pièces jointes et les liens dans les courriels afin de détecter les menaces potentielles.

Mise en quarantaine des spams : Configurez votre filtre anti-spam pour identifier et isoler les courriels indésirables dans un dossier dédié.

Gestion des contacts : Supprimez les contacts inutiles et marquez les contacts de confiance pour éviter de recevoir des courriels indésirables.

Sécuriser sa box Internet

Changer les identifiants par défaut : Modifiez les identifiants de connexion par défaut de votre box (nom d'utilisateur et mot de passe) pour des valeurs uniques et robustes.

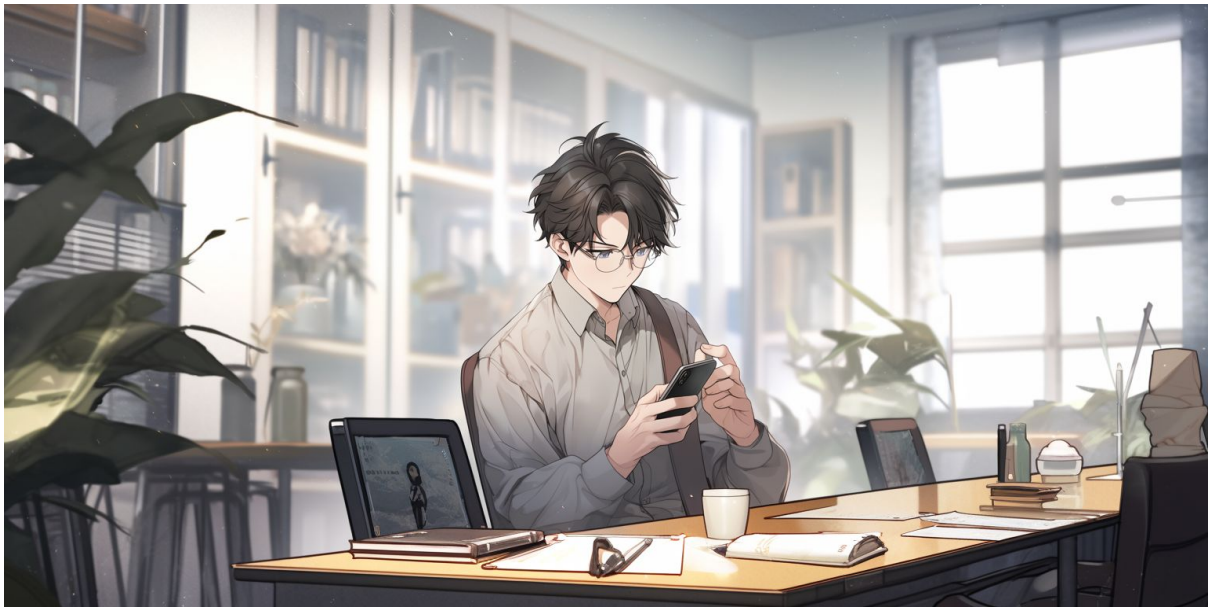
Mises à jour régulières : Assurez-vous que le firmware de votre box est à jour en installant les dernières mises à jour fournies par le fabricant pour corriger les vulnérabilités de sécurité.

Mot de passe Wi-Fi fort : Utilisez un mot de passe Wi-Fi robuste et évitez d'utiliser des informations personnelles évidentes. Un mélange de lettres, chiffres et caractères spéciaux est recommandé.

Pare-feu intégré : Activez le pare-feu intégré à votre box pour contrôler le trafic entrant et sortant. Configurez-le correctement en fonction de vos besoins de sécurité.

Désactivation des services inutiles : Désactivez les services et les fonctionnalités de votre box qui ne sont pas nécessaires. Cela réduit la surface d'attaque potentielle.

Gestion des administrateurs : Restreignez l'accès administrateur à votre box en utilisant un nom d'utilisateur et un mot de passe fort. Évitez d'utiliser des identifiants faciles à deviner comme "admin".



Sécuriser son Smartphone

Verrouillage par mot de passe ou code PIN : utilisez un mot de passe robuste ou un code PIN pour verrouiller l'accès à votre smartphone. Évitez les schémas de déverrouillage simples.

Empreintes digitales ou reconnaissance faciale : Activez les méthodes de déverrouillage biométriques telles que la reconnaissance des empreintes digitales ou faciales si votre smartphone les prend en charge.

Mises à jour régulières : Assurez-vous que votre smartphone dispose des dernières mises à jour logicielles pour bénéficier des correctifs de sécurité.

Applications uniquement depuis des sources fiables : Téléchargez des applications uniquement à partir de magasins d'applications officiels tels que Google Play Store (Android) ou App Store (iOS).

Permissions d'application : Vérifiez et limitez les autorisations accordées aux applications. N'accordez que les autorisations nécessaires à leur fonctionnement.

Code d'accès aux applications sensibles : Si possible, configurez des codes d'accès individuels pour les applications sensibles, comme les applications de messagerie et de banque.

Chiffrement du téléphone : Activez le chiffre du stockage sur votre smartphone pour protéger vos données en cas de perte ou de vol.

Sauvegardes régulières : Effectuez régulièrement des sauvegardes de vos données pour minimiser la perte en cas de problème avec votre smartphone.

Réseau Wi-Fi sécurisé : Évitez de vous connecter à des réseaux Wi-Fi non sécurisés. Utilisez un réseau virtuel privé (VPN) lorsque vous vous connectez à des réseaux Wi-Fi publics.

Désactivation du Bluetooth et du Wi-Fi : Désactivez le Bluetooth et le Wi-Fi lorsque vous ne les utilisez pas pour réduire les risques liés aux attaques potentielles.

Notification de verrouillage : Activez les notifications de verrouillage pour être informé en cas de tentative d'accès non autorisé à votre smartphone.

Antivol : Activez les fonctionnalités antivol intégrées à votre smartphone, telles que la localisation à distance et le verrouillage à distance.

Suppression des applications inutilisées : Supprimez les applications que vous n'utilisez plus pour réduire la surface d'attaque potentielle.

Gestion des mises à jour des applications : Assurez-vous que toutes les applications installées sur votre smartphone sont à jour avec les dernières versions, y comprennent les correctifs de sécurité.

Liste d’utilitaires

Pour smartphone

Antivirus / Antimalware :
- Avast Mobile Sécurité et antivirus (Android/iOS)
- Bitdefender Mobile Sécurité (Android/iOS)
- Kaspersky Mobile Antivirus (Android/iOS)

Gestion des mots de passe :
- LastPass (Android/iOS)
- 1Mot de passe (Android/iOS)
- Dashlane (Android/iOS)

VPN (Réseau Privé Virtuel) :
- ExpressVPN (Android/iOS)
- NordVPN (Android/iOS)
- ProtonVPN (Android/iOS)

Sécurité Wi-Fi :
- Garde Wi-Fi (Android)
- Fing - Outils réseau (Android/iOS)
- Norton Secure VPN (Android/iOS)

Gestionnaire d'applications :
- AppLock (Android)
- Verrouillage d'application Norton (Android)
- Verrouillage de l'application Hexlock et coffre-fort de photos (Android)

Localisation et Antivol :
- Localiser mon iPhone (iOS)
- Trouver mon appareil (Android)
- Cerbère (Android)

Navigation sécurisée et anti-hameçonnage :
- Lookout Sécurité et antivirus (Android/iOS)
- McAfee Mobile Sécurité (Android/iOS)
- PhishTank (iOS)

Sécurité des messages et appels :
- Messagerie privée Signal (Android/iOS)
- Wickr Moi (Android/iOS)
- Téléphone silencieux (Android/iOS)

Analyse des candidatures :
- AppScan (Android)
- AppWatcher (Android)
- XPrivacyLua (Android, pour la gestion des autorisations)

Sauvegardes sécurisées :
- Google Drive (Android/iOS)
- iCloud (iOS)
- OneDrive (Android/iOS)

Navigateur sécurisé :

- Navigateur de confidentialité DuckDuckGo (Android/iOS)
- Navigateur de confidentialité Brave (Android/iOS)
- Firefox Focus (Android/iOS)

Pour ordinateur

Antivirus / Antimalware :

- Bitdefender
- Kaspersky Antivirus
- Norton Antivirus
- Antivirus McAfee
- Antivirus Avast

Pare-feu :

- Alarme de zone
- Pare-feu Comodo
- Fil de verre
- TinyWall (léger, pour Windows)

Antispyware / Antiransomware :

- Malwarebytes
- Spybot - Rechercher et détruire
- HitmanPro
- Cybereason RansomGratuit

Suite de sécurité tout-en-un :

- Kaspersky Internet Security
- Bitdefender Sécurité Totale
- Protection totale McAfee
- Norton360

VPN (Réseau Privé Virtuel) :

- ExpressVPN
- NordVPN
- CyberGhost
- ProtonVPN

Gestionnaire de mots de passe :

- Dernier passage
- 1Mot de passe
- Dashlane
- KeePass (open-source, pour les utilisateurs avancés)

Sauvegardes et Récupération :

- Acronis True Image
- Sauvegarde EaseUS Todo
- Macrium réfléchit
- Backup and Sync (Google, pour la sauvegarde dans le cloud)

Protection de la vie privée en ligne :

- CCleaner
- Privacy Badger (extension de navigateur)
- Ghostery (extension de navigateur)

- Déconnecter (extension de navigateur)

Outils d'analyse et de suppression de logiciels malveillants :

- HijackThis (analyse des logiciels malveillants)
- AdwCleaner (suppression des adwares)
- RogueKiller (anti-malware)
- ComboFix (spécialisé pour certains types d'infections, Windows uniquement)

Surveillance du réseau :

- Wireshark (analyseur de protocoles)
- Netcut (détection des intrusions réseau)
- GlassWire (surveillance du réseau)
- Nmap (scanner de réseau)

Cryptage des fichiers et disques :

- VeraCrypt (chiffrement de disque et de fichier)
- AxCrypt (chiffrement de fichier)
- BitLocker (intégré à Windows, pour le chiffrement de disque)

Gestion des mises à jour :

- Patch My PC (mise à jour des logiciels tiers)
- Secunia PSI (analyse des vulnérabilités)
- Ninite (installation et mise à jour automatique des logiciels)