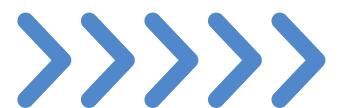
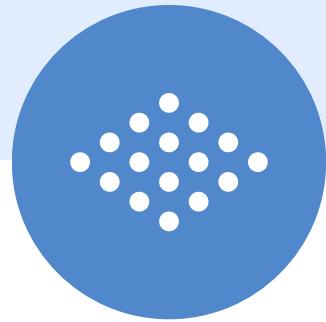


INFORMER LES UTILISATEURS

Ladrière Valentine





>>> CYBERCAFE <<<

Filtrer les connexions internet: OpenDNS FamilyShield

C'est la solution la plus simple et efficace pour filtrer les sites web inappropriés dans un cybercafé. En modifiant les paramètres DNS sur le routeur du réseau local, OpenDNS FamilyShield bloque automatiquement l'accès aux sites pornographiques, discriminatoires et à d'autres catégories sensibles.



Facile à configurer et à gérer, même sans connaissances techniques avancées.



Pas besoin d'installer de logiciel sur chaque machine.



Fonctionne au niveau du réseau, donc couvre tous les appareils connectés.



Gratuit et fiable.



Traitemen~~t~~t de la demande de connexion

Demande de connexion à un site

Lorsqu'un utilisateur dans le cybercafé tente de se connecter à un site web, l'ordinateur envoie une requête DNS pour résoudre l'adresse du site (c'est-à-dire pour traduire le nom du site en adresse IP).

Filtrage de la requête DNS

Cette requête DNS est envoyée vers les serveurs DNS d'OpenDNS FamilyShield au lieu des serveurs DNS classiques de votre fournisseur d'accès Internet (FAI). Les serveurs DNS d'OpenDNS analysent la demande. OpenDNS a une base de données de sites web classés selon des catégories (pornographie, violence, discours haineux, etc.).

Filtrage automatique

OpenDNS FamilyShield a des filtres prédéfinis qui bloquent automatiquement les catégories sensibles sans nécessiter d'intervention manuelle. Les catégories bloquées incluent la pornographie, la violence, la haine, les jeux d'argent, etc. Il n'y a pas besoin de configurer chaque site manuellement, car tout le filtrage est basé sur les catégories de contenu.



Traitemet de la demande de connexion

Décision d'autoriser ou de bloquer

Si le site demandé appartient à une catégorie de contenu bloquée par OpenDNS FamilyShield (par exemple, un site pornographique ou discriminatoire), les serveurs DNS renvoient une réponse qui empêche la connexion à ce site. L'utilisateur recevra un message d'erreur ou une page indiquant que l'accès à ce site est bloqué.

Si le site appartient à une catégorie autorisée, les serveurs DNS renvoient l'adresse IP du site, permettant à l'utilisateur de se connecter normalement.

OpenDNS FamilyShield autorise ou bloque les connexions en fonction de la catégorie du site. Si un site fait partie d'une catégorie bloquée, la connexion est refusée, et si le site est jugé sûr, la connexion est autorisée. Cela permet une gestion efficace du contenu tout en simplifiant le processus pour le gérant du cybercafé.

Prise en charge MP3, vidéos



Sites partage illégaux

Il utilise des filtres par catégories de contenu, incluant des catégories qui bloquent l'accès à des sites populaires de téléchargement illégal de musique, vidéos, et autres fichiers.

Tentative pour accéder à un site de partage illégal = OpenDNS empêchera la connexion



Restrictions streaming

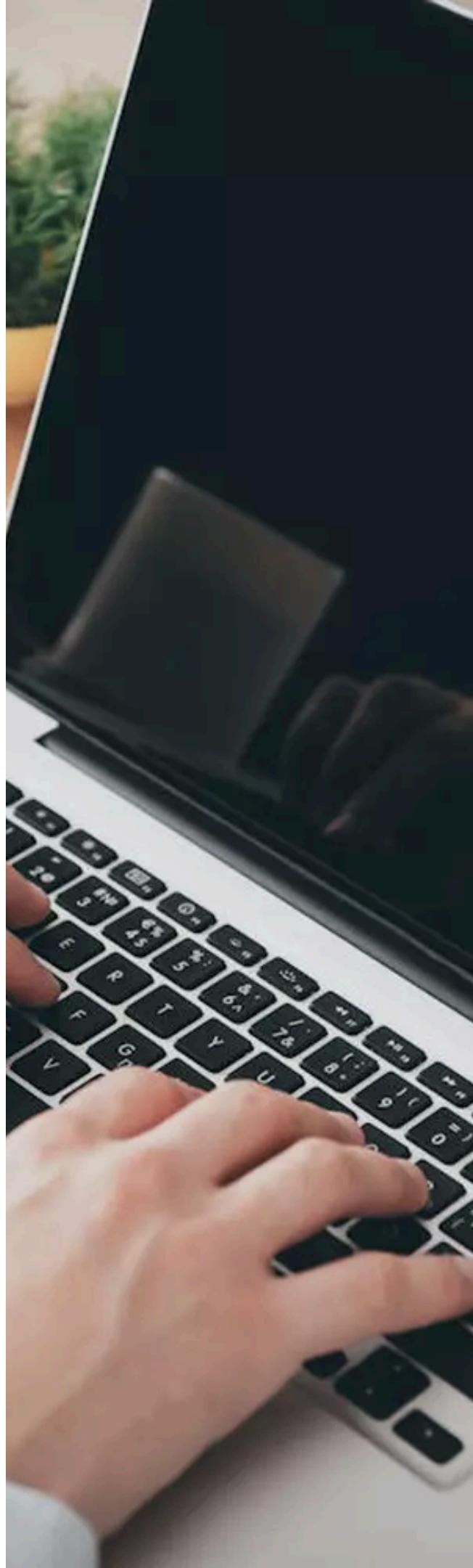
De nombreux sites de streaming non autorisés, qui offrent des vidéos ou de la musique en streaming sans licence, sont également bloqués par OpenDNS. Cela réduit la possibilité de visionner ou télécharger des fichiers protégés par des droits d'auteur de manière illégale.



Sites malveillants

Il dispose également d'une base de données de menaces qui inclut les sites connus pour distribuer des malwares. Lorsqu'un utilisateur tente de se connecter à un site dangereux, OpenDNS bloque automatiquement l'accès à ce site avant même que l'utilisateur n'ait pu télécharger un fichier infecté.





Prise en charge MP3, vidéos



Contenus non sécurisés

OpenDNS FamilyShield est conçu pour filtrer non seulement les sites sensibles en termes de contenu, mais aussi pour empêcher l'accès à des sites et services qui ne respectent pas les standards de sécurité, réduisant ainsi le risque d'intrusions malveillantes via des sites non fiables.



Filtrage des URL (phishing)

OpenDNS peut aussi bloquer les sites de phishing (sites frauduleux visant à voler des informations personnelles). Les utilisateurs sont protégés contre ces types d'attaques en étant empêchés d'accéder à des sites malveillants qui tentent de les tromper.

Utilisation des supports USB

Pour empêcher les utilisations frauduleuses des supports USB, le responsable du cybercafé peut mettre en place plusieurs mesures de sécurité, permettant de bloquer ou restreindre l'accès aux périphériques USB de manière automatisée, sans nécessiter une intervention quotidienne.



Désactivation des ports USB via le BIOS/UEFI

En désactivant les ports USB, les utilisateurs ne pourront pas brancher de périphériques USB. Une fois configuré, cette option ne nécessite aucune gestion quotidienne.

Outil de gestion de groupe (Windows)

L'éditeur de stratégie de groupe (Gpedit.msc) permet de configurer une politique de restriction des périphériques USB.

Logiciels de gestion des périphériques USB

Ils permettent de bloquer l'accès aux ports USB ou de limiter l'accès à certains types de périphériques. Permettent de contrôler quels types de périphériques sont autorisés et d'effectuer la journalisation des tentatives de connexion de périphériques.

Logiciel antivirus

Certains logiciels antivirus offrent des fonctionnalités permettant de bloquer ou de limiter l'accès aux périphériques USB. L'antivirus peut aussi assurer une protection contre les malwares qui pourraient être transférés via des clés USB.

Comptes utilisateurs restreints

Les comptes utilisateurs limités (avec des priviléges d'administrateur restreints), les adolescents ne pourront pas apporter des modifications aux paramètres du système, notamment en ce qui concerne les périphériques USB.

Configuration pérenne

Pour garantir que la configuration réalisée soit pérenne, le responsable du cybercafé doit prendre plusieurs précautions supplémentaires. Ces actions visent à assurer la stabilité de la configuration, à éviter toute manipulation ou contournement, et à maintenir un environnement sécurisé sans nécessiter une surveillance quotidienne.



Verrouillage des paramètres système

**Mot de passe administrateur sécurisé:
mot de passe fort et unique**

**Restreindre l'accès aux paramètres de
configuration : Bloquer l'accès aux
outils de configuration du système**



Mises à jour automatiques

**Mises à jour automatiques des logiciels
de sécurité**

**Mises à jour automatiques du système
d'exploitation**



Verrouillage paramètres BIOS/UEFI

**Si vous avez désactivé les ports USB au
niveau du BIOS/UEFI: l'accès doit être
protégé par un mot de passe BIOS fort**



Surveillance et audits réguliers

**Outils de journalisation : Utilisez des
outils de journalisation pour surveiller
les événements importants**

Contrôles périodiques: audits



Environnement d'utilisateur limité

**Les utilisateurs utilisent des comptes
utilisateurs standard plutôt que des
comptes administrateurs.**

**Utilisation de logiciels de gestion des
utilisateurs (Active Directory...)**



Configuration pérenne

Pour garantir que la configuration réalisée soit pérenne, le responsable du cybercafé doit prendre plusieurs précautions supplémentaires. Ces actions visent à assurer la stabilité de la configuration, à éviter toute manipulation ou contournement, et à maintenir un environnement sécurisé sans nécessiter une surveillance quotidienne.



Sauvegardes régulières

Sauvegarde des paramètres système et de sécurité : Assurez-vous de sauvegarder régulièrement les configurations du système



Formation et sensibilisation

Règles et protocoles d'utilisation: Expliquez clairement les règles d'utilisation des équipements



Verrouillage paramètres BIOS/UEFI

Si vous avez désactivé les ports USB au niveau du BIOS/UEFI: l'accès doit être protégé par un mot de passe BIOS fort



Windows Update

L'application native sous Windows qui permet de garantir que le système d'exploitation reste à jour et sécurisé est Windows Update.

Fonctionnement de Windows Update

Mises à jour automatiques : permet de télécharger et d'installer automatiquement les mises à jour

Gestion des versions récentes : assure que le système est toujours à jour en matière de sécurité et de fonctionnalités

En assurant que Windows Update fonctionne correctement et que les mises à jour sont appliquées régulièrement, le responsable du cybercafé garantit que les systèmes d'exploitation restent sécurisés, sans faille de sécurité, et toujours à jour avec les dernières fonctionnalités et protections.

Comment l'utiliser:

Ouvrir les paramètres Windows : Allez dans Paramètres > Mise à jour et sécurité.

Vérifier les mises à jour : Cliquez sur Vérifier les mises à jour pour voir s'il y a des mises à jour disponibles.

Configurer les mises à jour automatiques : Vous pouvez configurer Windows Update pour télécharger et installer automatiquement les mises à jour

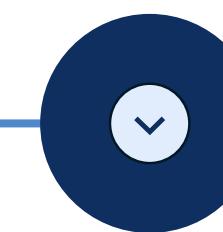


Windows Update et les failles de sécurité

Windows Update joue un rôle clé dans la protection contre les failles de sécurité en fournissant des mises à jour critiques de sécurité qui corrigent les vulnérabilités du système d'exploitation.



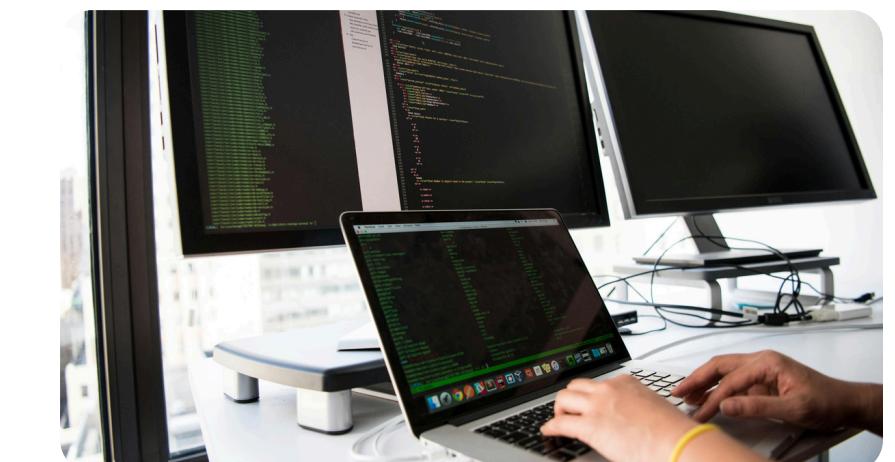
Mises à jour de sécurité:
Correction des vulnérabilités critiques (Microsoft publie un patch de sécurité si une faille est découverte)



Mises à jour de fonctionnalités de sécurité: Amélioration de la sécurité, propose des fonctionnalités de sécurité améliorées



Réduction de la surface d'attaque: Certaines mises à jour apportent des améliorations au niveau des composants internes de Windows, réduisant ainsi la surface d'attaque en corrigeant les failles

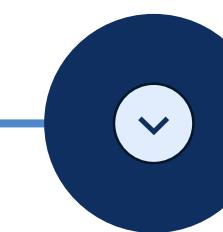


Windows Update et les failles de sécurité

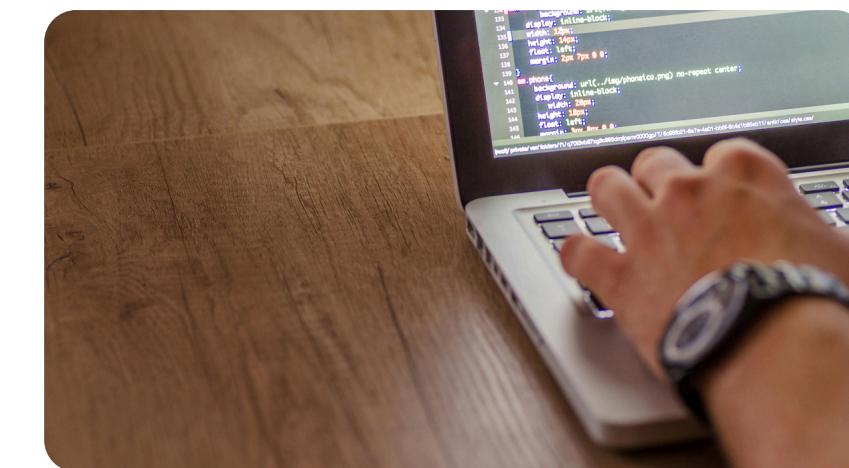
Windows Update joue un rôle clé dans la protection contre les failles de sécurité en fournissant des mises à jour critiques de sécurité qui corrigent les vulnérabilités du système d'exploitation.



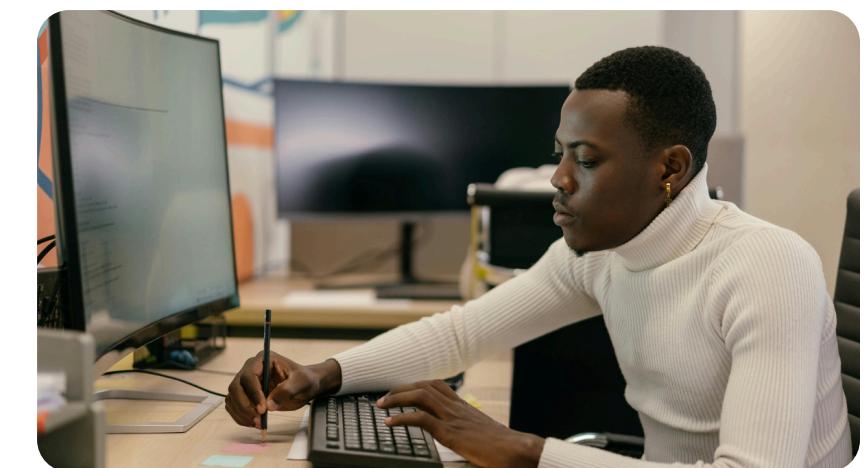
Protection contre les attaques 0-day: Réponse rapide aux vulnérabilités découvertes Windows Update diffuse rapidement des patchs de sécurité pour réduire l'impact des attaques



Renforcement de la protection des applications et des navigateurs: Mise à jour des applications natives,



Vérification des configurations et des outils de sécurité: Amélioration continue des configurations de sécurité Windows Update met à jour des outils de sécurité... qui renforcent la sécurité du système



Outil supplémentaire

Je recommande d'installer est un logiciel antivirus fiable, comme Windows Defender Antivirus
Pourquoi?

Protection contre les malwares

déetecter, prévenir et supprimer les menaces malveillantes

Analyse en temps réel

déetecter un fichier exécutable malveillant

Les menaces sur le web

bloque l'accès à des sites web malveillants, pages susceptibles de distribuer des malwares.

Contrôle périphériques externes

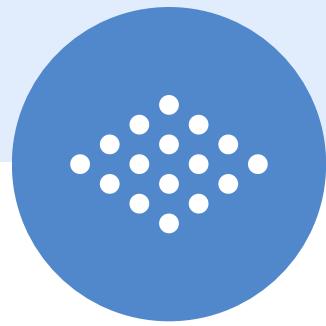
Scan des périphériques externes

Pare-feu

Protection contre les attaques réseau
filtre le trafic réseau et bloque les tentatives d'intrusion

Fonctions supplémentaires

Gestion des mots de passe ou VPN



LYCEE



La création des mots de passe



Longueur et complexité des mots de passe (au moins 12 caractères)

Utilisation de phrases de passe (des séquences de mots choisis aléatoirement)

Authentification multifacteur (code envoyé sur un téléphone...)

Gestionnaire de mots de passe

Renouvellement des mots de passe: imposer un délai d'expiration des mots de passe

Protection des mots de passe: pas de partage, éviter de noter les mots de passe sur des supports non sécurisés

Modification des mots de passe par défaut

Recommandations: gestion des mots de passe durant les deux années de BTS



Utiliser des mots de passe robustes



Ne jamais partager ses mots de passe

Ne pas réutiliser les mêmes mots de passe

Éviter d'enregistrer des mots de passe dans des navigateurs non sécurisés.



Mettre à jour les mots de passe régulièrement



Utiliser un gestionnaire de mots de passe sécurisé



En cas de compromission: Signaler immédiatement



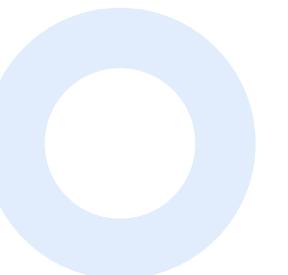
Participer aux ateliers ou formations proposés par l'établissement





La méthode basée sur une phrase ou une expression significative

- Choisir une phrase mémorable : Exemple : "Le ciel est bleu aujourd'hui"
- Personnaliser la phrase :
Ajouter des majuscules et des caractères spéciaux :
"LeCielEstBleu@joud'hui!"
Remplacer certains caractères par des chiffres ou des symboles : "L3C!elEstBl3u@joud'hui!"
- Résultat : Une passphrase robuste et facile à retenir.



Manipulations non souhaitables >>>



Enregistrer les mots de passe dans le navigateur

Peuvent être compromis si l'appareil est piraté ou si quelqu'un d'autre y accède.



Réutiliser le même mot de passe

Si un service est compromis, tous les autres comptes utilisant le même mot de passe sont également exposés.



Partager ses identifiants

Cela va à l'encontre des principes de responsabilité individuelle en matière de cybersécurité.



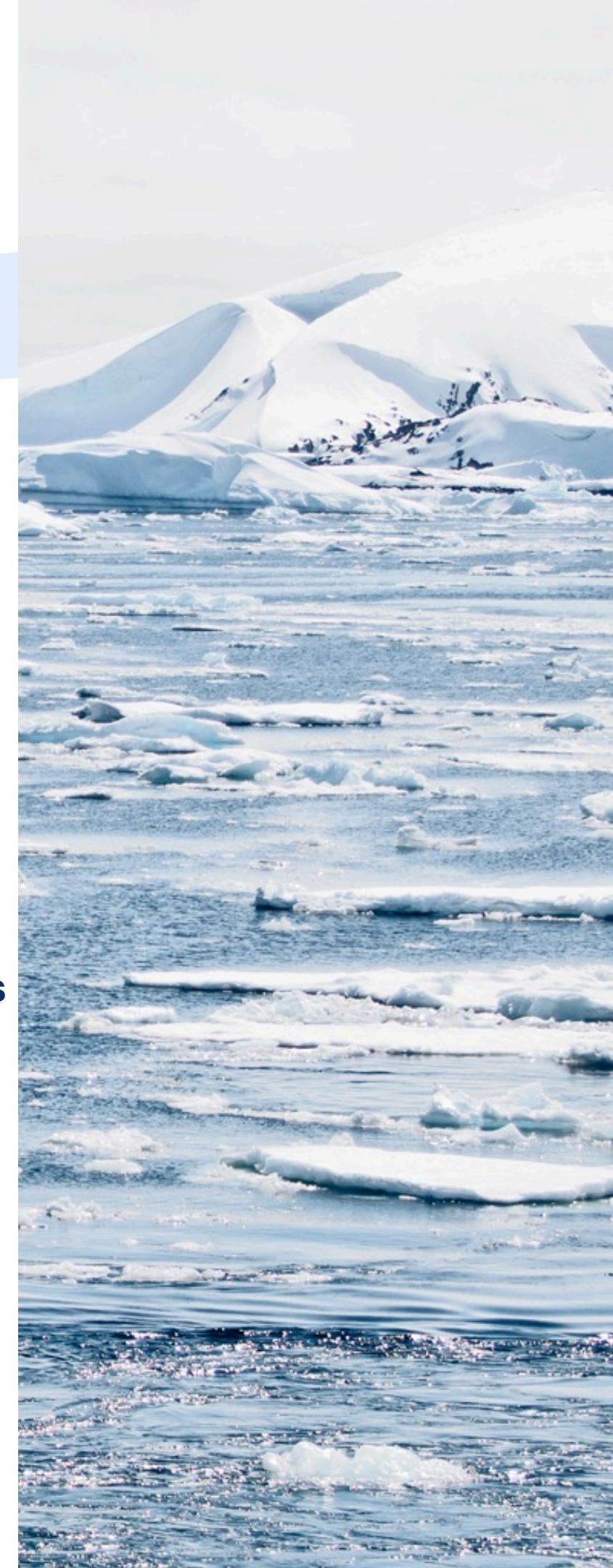
Réseaux Wi-Fi publics

Les réseaux publics sont souvent vulnérables aux attaques



Liens non vérifiés

Cela peut mener à des sites de phishing imitant des plateformes légitimes pour voler des identifiants.



Manipulations non souhaitables>>>>



Désactiver l'authentification multifacteur

La MFA fournit une couche de sécurité supplémentaire, et sa désactivation réduit significativement la protection contre les accès non autorisés.



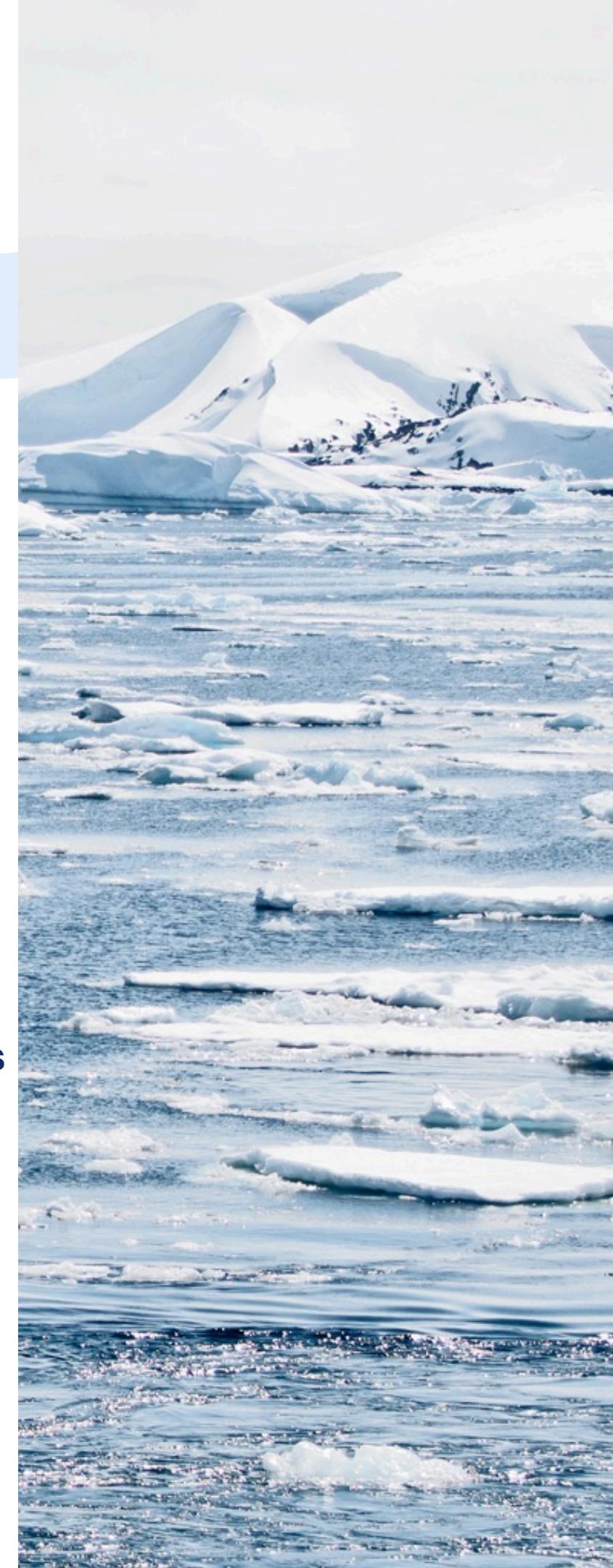
Oublier de se déconnecter des sessions

Si l'utilisateur oublie de se déconnecter, d'autres personnes peuvent accéder à ses comptes.

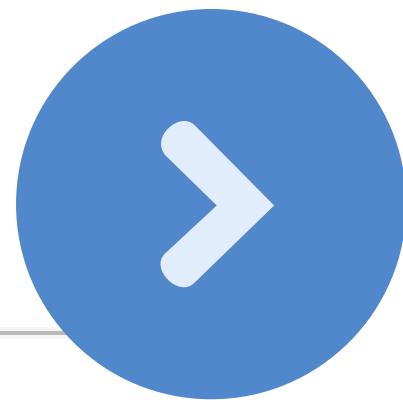


Enregistrer les identifiants

Les fichiers texte ou tableurs stockant des identifiants sont facilement accessibles en cas de piratage ou de perte de l'appareil.



Stratégies de sécurité locales



Stratégie

- Audit de la longueur minimale du mot de passe
- Conserver l'historique des mots de passe
- Durée de vie maximale du mot de passe
- Durée de vie minimale du mot de passe
- Enregistrer les mots de passe en utilisant un chiffrement réversible
- Le mot de passe doit respecter des exigences de complexité
- Longueur minimale du mot de passe

Audit de la longueur minimale du mot de passe: Permet de surveiller si les mots de passe définis respectent la longueur minimale requise.

Conserver l'historique des mots de passe: Empêche la réutilisation des anciens mots de passe

Durée de vie maximale du mot de passe: Définit le nombre maximal de jours pendant lesquels un mot de passe peut être utilisé avant qu'il ne doive être changé.

Durée de vie minimale du mot de passe: Empêche les utilisateurs de changer immédiatement leur mot de passe plusieurs fois

Enregistrer les mots de passe en utilisant un chiffrement réversible: Permet de stocker les mots de passe dans un format qui peut être décrypté.

Le mot de passe doit respecter des exigences de complexité: Oblige les utilisateurs à créer des mots de passe robustes

Longueur minimale du mot de passe: Définit le nombre minimal de caractères requis pour un mot de passe