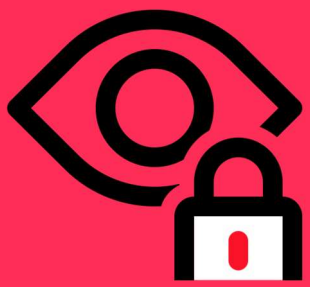
Je travaille dans un lieu public



Je renforce ma sécurité

Je protège ma vie privée

Travailler dans un lieu public, c'est s'exposer à des risques liés à la nature ouverte des réseaux et à la proximité d'autres personnes. En utilisant un VPN, des mots de passe solides, un verrouillage automatique, en restant vigilant sur les données que tu manipules et en gardant ton système à jour, tu protèges tes données et ta vie privée.

Évite de travailler sur des **informations sensibles** si possible.

01

. **Protection** des accès

Utilise un **VPN pour protéger ta connexion** internet, surtout si tu utilises un Wi-Fi public non sécurisé. C'est comme créer un tunnel sécurisé entre ton ordinateur et le site ou service que tu utilises.

- *Le Wi-Fi public n'est pas sûr : Beaucoup de lieux publics (cafés, gares, bibliothèques) offrent du Wi-Fi gratuit, mais souvent non sécurisé. Cela veut dire que **d'autres utilisateurs connectés au même réseau peuvent intercepter les données** que tu envoies ou reçois.*
- *Evil Twin (Faux point d'accès Wi-Fi). Un attaquant **crée un faux point d'accès Wi-Fi** qui imite un réseau public légitime (par exemple, "Free_Coffee_Shop_WiFi"). Les utilisateurs se connectent à ce réseau croyant qu'il est authentique.*

Verrouille ton écran dès que tu t'éloignes, même pour un court instant pour empêcher quelqu'un de voir ce que tu fais ou d'accéder à tes fichiers.

- *Accès non autorisé. Consiste à **accéder à un ordinateur ou un système informatique sans l'autorisation de son propriétaire.***

Active l'authentification à deux facteurs (2FA) quand c'est possible : cela ajoute une couche de sécurité en demandant un code supplémentaire (par SMS, app ou email) en plus du mot de passe.

Utilise un **mot de passe fort** (combinant lettres, chiffres, caractères spéciaux) pour protéger ta session et tes comptes en ligne et ne le partage jamais.

02
Prudence avec les données sensibles

Évite de consulter ou saisir des informations très sensibles (numéros de carte bancaire, documents confidentiels, mots de passe, données profes-sionnelles critiques) quand tu es connecté à un réseau public.

Si tu dois le faire, vérifie que le site est sécurisé (adresse commençant par **https://** avec un **petit cadenas** dans la barre d'adresse).

03
Protection physique

Même si tu t'absentes **juste pour quelques minutes** (ex : aller aux toilettes ou commander un café), **emporte toujours ton ordinateur avec toi**.

Sois **vigilant à ton environnement** et aux personnes autour de toi.

Attention aux liquides (ex : café renversé).

04
Confidentialité visuelle

Utilise un filtre de confidentialité pour écran afin d'empêcher les regards indiscrets.

- *Shoulder Surfing. Consiste à **observer discrètement une personne** pendant qu'elle saisit des **informations sensibles** (comme un mot de passe, un code PIN, ou des données personnelles)*

Sois discret dans la gestion de tes mots de passe ou informations personnelles.

05
Surveille ton environnement

Installe-toi dans un endroit **où tu peux voir les gens autour de toi**.

Ne t'assois **pas dos à un espace ouvert** si tu veux garder un œil sur ce qui se passe.

Méfie-toi des comportements suspects (quelqu'un qui tourne autour de ta table, regarde ton écran par-dessus ton épaule, etc.).

Conseils de prévention

Pourquoi **utiliser le 2FA** (authentification à deux facteurs)

Plus de sécurité
Même si quelqu'un vole ton mot de passe, il ne pourra pas se connecter sans le deuxième facteur (ex. : code SMS, appli, empreinte digitale).

Protège contre le piratage
Le 2FA empêche les hackers d'accéder à tes comptes, même s'ils trouvent ton mot de passe avec une attaque ou un phishing.

Facile à utiliser
Tu reçois juste un code par SMS ou via une appli (comme Google Authenticator ou Microsoft Authenticator).

Recommandé par les experts
Les sites les plus sécurisés (banques, mails, réseaux sociaux) l'utilisent et te le proposent.

Fonctionne partout
Tu peux l'activer sur presque tous tes comptes : Gmail, Facebook, Instagram, Amazon, etc.

Pour toutes questions ou suggestions d’amélioration.

ubik-infosec.ca @michel-panouillot

A propos de l’auteur

Professionnel chevronné en sécurité de l'information, je cumule plus de dix ans d’expérience dans des environnements complexes et diversifiés, incluant les secteurs gouvernementaux, de la formation et militaire. Mon expertise est centrée sur l’analyse en cybersécurité, avec une spécialisation en gouvernance et conformité réglementaire.