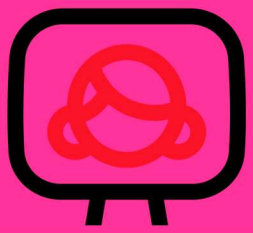
Je protège mon enfant des réseaux sociaux.



Je renforce ma sécurité

Je protège ma vie privée

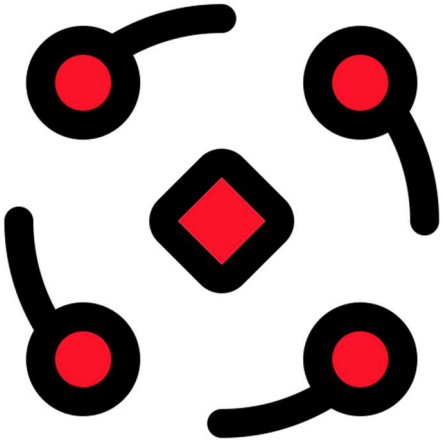
.ubik | infoSEC

Protéger les informations qui comptent pour vous.

“

Les réseaux sociaux font désormais partie du quotidien des jeunes. Bien qu’ils puissent être enrichissants, ils présentent aussi de réels dangers pour les enfants et adolescents.

”



a. Principaux risques

Risques **psychologiques**	**Cyberharcèlement :** insultes, moqueries, humiliations publiques (photos, commentaires, vidéos...). **Anxiété et dépression :** pression sociale, peur de manquer (FOMO), comparaison constante avec les autres. **Dépendance aux écrans :** perte de contrôle du temps passé, isolement social. **Baisse de l'estime de soi :** due aux likes, aux filtres, aux commentaires négatifs ou à l'exclusion numérique.
Risque **liés à la vie privée**	**Partage excessif d'informations personnelles :** nom, école, adresse, habitudes, géolocalisation... **Vol d'identité :** usurpation de profil ou collecte de données pour créer de faux comptes. **Exposition involontaire :** l'enfant peut être filmé ou pris en photo par d'autres sans consentement.
Risques **de manipulation ou de prédation**	**Prédateurs sexuels :** adultes se faisant passer pour des jeunes, utilisant la flatterie ou les menaces. **Grooming :** processus de manipulation visant à gagner la confiance d'un enfant pour l'exploiter (souvent à caractère sexuel). Escroqueries et arnaques : promesses de cadeaux, faux concours, liens malveillants
Risques **sociaux et réputationnels**	**E-réputation :** tout ce qu'un enfant publie peut rester en ligne indéfiniment, même supprimé. **Humiliation publique :** diffusion de vidéos ou d'images compromettantes. **Exclusion sociale :** l'enfant peut être mis à l'écart de certains groupes en ligne, ou au contraire exposé à des normes toxiques.
Risques **juridiques**	**Contenus inappropriés :** partage de contenu violent, sexuel, haineux, ou incitation à des comportements dangereux. **Responsabilité parentale :** en cas d'actes illégaux (harcèlement, insultes, piratage), les parents peuvent être tenus responsables
Risques **liés aux contenus**	**Contenus violents ou choquants :** facilement accessibles malgré les filtres. **Idéologies extrémistes :** certaines communautés en ligne diffusent des messages haineux ou sectaires. **Défis dangereux ("challenges") : incitation** à se mettre en danger pour attirer l'attention (ex : blackout challenge, blue whale, etc.)

b. Principales solutions 

Mettre en place des outils de contrôle parental

Utiliser des logiciels ou paramètres intégrés qui permettent de surveiller, filtrer et limiter l'accès :

Applications et logiciels recommandés :

- Windows / macOS : Contrôle parental intégré
- Google Family Link : Gestion des comptes Android et YouTube
- Apple Screen Time : Limites d'app usage et filtres de contenu
- Qustodio, Net Nanny, Norton Family, Kaspersky Safe Kids : Solutions tierces puissantes

Fonctionnalités utiles :

- Blocage de certaines apps (Snapchat, TikTok, etc.)
- Limitation du temps d'écran
- Surveillance des mots-clés ou comportements suspects
- Rapports d'activité hebdomadaires

Créer des comptes sécurisés pour les enfants

- Ne jamais laisser un enfant créer un compte seul.
- Utiliser une adresse e-mail parentale pour l'inscription.
- Configurer les paramètres de confidentialité (comptes privés, contrôle des abonnés, blocage des messages inconnus).
- Désactiver la géolocalisation et l'accès à l'appareil photo ou micro sauf nécessité.

Éducation et sensibilisation

Aucun outil technique ne remplace l'éducation numérique. Discutez avec l'enfant :

- Des risques : cyberharcèlement, prédateurs, fake news, dépendance
- Des bonnes pratiques : ne pas partager d'infos personnelles, ne pas accepter d'inconnus
- Du temps d'écran et de l'équilibre entre vie réelle et en ligne

Surveiller les applications utilisées

Certains réseaux sont plus risqués que d'autres. Informez-vous sur :

- TikTok, Snapchat, Instagram : très populaires mais peu filtrables
- YouTube : YouTube Kids est plus sûr, mais reste à surveiller
- Discord : surveiller les serveurs et interactions
- Vérifiez régulièrement les apps installées, les paramètres de confidentialité et les journaux d'activité.

Mettre à jour et sécuriser les appareils

- Activer les mises à jour automatiques
- Installer un antivirus ou suite de sécurité
- Configurer des comptes limités (non administrateurs) pour les enfants
- Utiliser un navigateur sécurisé (Brave, Firefox avec extensions de blocage, etc.)

Créer un climat de confiance

Les enfants doivent pouvoir parler s'ils vivent une mauvaise expérience en ligne. Évitez la surveillance intrusive, favorisez une approche bienveillante et activez des moments de dialogue réguliers.

- Surveillance douce mais active
- Dialogue régulier sur leurs expériences numériques
- Paramétrage des outils de sécurité et des comptes
- Accompagnement dans la compréhension de leurs droits et responsabilités

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.