e-Enfance 3018

Association Reconnue d'Utilité Publique

Usurpation d'identité

Vol et utilisation de données personnelles propres à identifier la victime pour lui nuire

De quoi s'agit-il ?

L'usurpation d'identité est le fait de prendre délibérément l'identité d'une autre personne, et d'utiliser ses données personnelles propres à l'identifier. L'objectif ? Nuire à sa réputation, réaliser des opérations malveillantes ou frauduleuses en son nom.

Les usurpateurs peuvent voler les données via piratage ou escroquerie par exemple. Chez les jeunes, c'est souvent par négligence ou naïveté. L'échange de mots de passe ou le prêt de téléphone est fréquent entre copains. La création de profils au nom d'une personne, qu'elle soit ou non déjà inscrite sur Internet, pour s'amuser ou l'humilier, est également assez courante.

Que dit la loi ?

L'usurpation d'identité est un délit pénal (article 226-4-1 du code pénal), passible d'un an d'emprisonnement et de 15 000€ d'amende.

Comment éviter les pièges ?

- Donnez à votre enfant les bons usages numériques :

- **Ne jamais donner son mot de passe** même à son/sa meilleur(e) ami(e) ! Il doit rester personnel (comme sa brosse à dent !) et confidentiel,
- **Ne pas laisser son téléphone ou sa tablette sans surveillance,** surtout si sa session est ouverte
- **Lorsqu'il utilise une tablette ou un ordinateur partagé,** penser à se déconnecter de son compte après utilisation pour éviter que quelqu'un ne puisse y accéder,
- **Éviter de naviguer et de télécharger** des contenus sur des sites non sûrs ou illicites, **d'ouvrir des mails ou des pièces jointes d'expéditeurs inconnus,** de se connecter à un ordinateur ou à **un réseau Wi-Fi publics** afin de se prémunir du risque de piratage informatique.

- Renforcez sa sécurité numérique **en protégeant ses outils** avec un pare-feu solide, un programme antivirus complet, effectuez des mises à jour régulières du système et des logiciels installés.

Que faire si votre enfant est victime ?

- Le plus important est de faire cesser la diffusion des messages malveillants qui circuleraient en son nom ou de supprimer le compte frauduleux,
- Gardez des preuves : faites des captures d'écran,
- Faites un signalement en ligne (les réseaux sociaux proposent de signaler de manière anonyme un contenu ou un utilisateur abusif),
- Avertissez l'établissement scolaire si l'incident s'est produit avec un camarade de classe,
- En cas de piratage informatique, identifiez les origines possibles de l'intrusion (identifiants de connexion trop faibles, clic sur un lien malveillant, antivirus obsolètes) et les appareils touchés afin de prendre les mesures adéquates,
- Prévenez l'entourage que le contenu émanant du compte de votre enfant est frauduleux,
- Déposez plainte au commissariat de police ou à la gendarmerie, en fonction du préjudice subi.

Besoin d'aide ou de conseils personnalisés ? Contactez le 3018, le numéro national pour accompagner les jeunes, victimes de violences numériques, et leurs parents dans leur rôle d'éducation.

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS
Liberté Égalité Fraternité

SECRÉTARIAT D'ÉTAT CHARGÉ DE L'ENFANCE ET DES FAMILLES
Liberté Égalité Fraternité

3018.fr

gratuit - anonyme - confidentiel
du lundi au samedi de 9h00 à 20h00

3018

Co-funded by the European Union