e-Enfance 3018

Association Reconnue d'Utilité Publique

Escroqueries et arnaques en ligne

Phishing, chantage à la webcam, usurpation d'identité

Explosion des arnaques en ligne pendant le confinement :
22 % des problèmes rencontrés par les jeunes pendant le Grand Confinement sont des arnaques en ligne (vs 7 % hors confinement)*

Les escroqueries en ligne sont nombreuses ! Elles reposent sur la crédulité et le manque de connaissance des internautes. Les plus jeunes sont particulièrement vulnérables.

L'hameçonnage (phishing) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (mots de passe etc.) et/ou bancaires en se faisant passer pour un tiers de confiance.
Le scamming consiste à faire croire à l'internaute qu'il a reçu un prix, et qu'il devra verser une somme pour le recevoir.
Le chantage à la webcam (sextorsion) consiste à menacer de publier une vidéo (souvent à caractère sexuel) de la victime, si une rançon n'est pas versée.

Que dit la Loi ? Différentes infractions peuvent être retenues…

Une escroquerie (article 313-1 du code pénal) est le fait d'obtenir un bien, un service ou de l'argent par une tromperie. La victime donne volontairement son argent car elle est trompée sur les intentions de l'auteur = 5 ans d'emprisonnement et 375 000€ d'amende.
Usurpation d'identité (article 226-4-1 du code pénal) = un an d'emprisonnement et 15 000€ d'amende. **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite** (article 226-18 du code pénal) = 5 ans d'emprisonnement et 300 000€ d'amende.

Comment éviter les pièges ?

- **Expliquez à vos enfants l'existence de telles escroqueries ou arnaques en ligne :** en connaissant ces phénomènes, le but recherché par leurs auteurs, ils seront plus vigilants,
- **Apprenez à votre enfant les bons usages numériques :**
  - Être vigilant sur les informations partagées : ne pas divulguer ses coordonnées,
  - Être méfiant sur les sollicitations reçues : les personnes qui nous contactent ne sont pas toujours celles qu'elles prétendent être et leurs intentions ne sont pas toujours sincères,
  - Ne jamais acheter seul quelque chose,
  - Parler à un adulte au moindre doute ou à l'occasion d'un événement inhabituel !
- **N'enregistrez pas de moyen de paiement sur le smartphone, la tablette ou la console de jeu utilisés** par votre enfant afin d'éviter tout acte d'achat non autorisé,
- **Protégez vos outils numériques :** effectuez des mises à jour régulières, choisissez des mots de passe différents et suffisamment complexes pour chaque site et application.

Que faire si votre enfant est victime ?

- **Rassurez votre enfant :** il est important de le déculpabiliser, et de partager avec lui ses émotions,
- **Conservez des preuves en faisant des copies d'écran,**
- **Appelez votre banque pour tenter de faire opposition,** si votre enfant a transmis des éléments sur vos moyens de paiement ou réalisé des achats,
- **Déposez plainte au commissariat de police ou à la gendarmerie.**

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.

*Etude OpinionWay réalisée par l'Association e-Enfance pendant le confinement en Mai 2020

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