MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

LA LETTRE CYBER *en région Grand Est*

Octobre 2023

La thématique du mois
LA SECURITE SUR LES RESEAUX SOCIAUX (RS)

? Protégez votre monde en ligne

A l'ère du numérique, les réseaux sociaux (RS) ont révolutionné nos interactions avec le monde. Ces plateformes (Facebook, Instagram, X, Snapchat…) nous permettent de rester en contact avec des amis, découvrir de nouvelles idées, s'intégrer à des communautés… Cependant à tout avantage, il y a son lot d'inconvénients, que ce soit pour un usage personnel ou professionnel. L' utilisation accrue de ces plateformes comporte des risques potentiels en matière de sécurité en ligne.

• Quels sont les risques sur les RS ?

Les RS représentent des outils de communications et de diffusion d'informations puissants, aisément accessibles à tous. Ils font désormais partie intégrante de la vie personnelle des internautes et sont également devenus un outil incontournable pour les entreprises souhaitant promouvoir leurs activités. Cependant ils ne sont pas à l'abri d'activités malveillantes. Parmi les risques auxquels les utilisateurs de ces plateformes sont exposés, on peut citer l'escroquerie, l'usurpation d'identité, le chantage, le vol d'informations, le cyberharcèlement, la désinformation et la diffamation.

Les cyberattaquants ont divers objectifs lorsqu'ils ciblent les réseaux sociaux, tels que :
- la collecte de données personnelles, ils peuvent alors chercher à collecter des informations personnelles comme les noms,adresses,numéros de téléphone… et les utiliser pour l'usurpation d'identité ou la fraude.
- l'escroquerie financière, certains cybercriminels cherchent à tromper les utilisateurs en leur faisant croire à des opportunités d'investissement, des offres de vente frauduleuse….Ils peuvent également tenter de voler des informations financières, telles que les numéros de carte de crédit.
- chantage, les cyberattaquants peuvent menacer de divulguer des informations embarrassantes ou compromettantes sur les victimes si elles ne paient pas une rançon. Cela peut inclure la menace de révéler des messages privés, des photos intimes ou d'autres contenus sensibles.
- phishing, les RS sont souvent utilisés pour lancer des attaques de phishing, où les cybercriminels tentent d'obtenir des informations de connexion ou d'autres données sensibles en se faisant passer pour une entité de confiance, comme une entreprise ou une organisation gouvernementale.
- propagation de logiciels malveillants, les cyberattaquants peuvent utiliser les réseaux sociaux pour diffuser des liens vers des sites web ou des fichiers malveillants qui infectent les ordinateurs ou les appareils mobiles des utilisateurs.
- manipulation de l'opinion publique, les acteurs malveillants peuvent utiliser les réseaux sociaux pour propager de la désinformation, manipuler les opinions politiques, sociales, ou encore créer la discorde en ligne.

Les 10 bonnes pratiques à adopter

- **Protégez l'accès à votre compte :** vos comptes de RS sont des mines d'or pour les cybercriminels. Ils contiennent de nombreuses informations personnelles sensibles pouvant être convoitées. Utilisez des mots de passe différents et robustes. (15 caractères contenant des chiffres, majuscules, minuscules, et caractères spéciaux selon les recommandations de l'ANSSI). Si le service le propose, activez la double authentification.

- **Vérifiez vos paramètres de confidentialité :** par défaut, les paramètres de visibilité de vos informations personnels (tph,adresse,mail…) et des publications sont souvent ouverts. Il est généralement possible de restreindre cette visibilité en réglant la configuration du compte. Vérifiez régulièrement ces paramètres de confidentialité qui peuvent être modifiés sans que vous le sachiez.

- **Maîtrisez vos publications :** Ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire. Et respectez la loi.

- **Faites attention à qui vous parlez :** vos contacts peuvent avoir été piratés et vous partager du contenu malveillant ou vous soutirer des données, photos, argent...

- **Contrôlez les applications tierces :** certaines applications, tels que des jeux, quiz…, proposent d'interagir avec votre compte de RS. Analyser les demandes d'autorisation avec attention car une fois activée, elles peuvent avoir accès à vos informations personnels, contacts...

- **Evitez les ordinateurs et les réseaux Wifi publics :** Evitez dans la mesure du possible de renseigner des informations sensibles dans un ordinateur ou matériel qui n'est pas le votre. Si vous y êtes contraints, pensez à vous déconnecter de votre compte après utilisation.

- **Vérifiez régulièrement les connexions à votre compte :** Si vous détectez une session ou connexion inconnue ou que vous ne l'utilisez plus, déconnectez là. Au moindre doute, changez immédiatement de mot de passe.

- **Faites preuve de discernement avec les informations publiées :** Tout le monde peut publier n'importe quelle information, elles peuvent être partiellement ou totalement fausses. Ces « fake news » peuvent avoir de graves conséquences sur les personnes qui en sont victime. Avant tout partage, vérifier la véracité.

- **Utilisez en conscience l'authentification avec votre compte de réseau social sur d'autres sites :** si votre RS a été piraté et qu'il est associé à un site internet, le cyberattaquant aura également accès à tout le sites internet où votre RS a été associé.Vérifiez les autorisations que vous délivrez.t

- **Supprimez votre compte si vous ne l'utilisez plus,** afin d'éviter que vos informations soient récupérées par des tiers ou votre compte utilisé à votre insu.

Que faire en cas de problème ?

-en cas de piratage de votre RS ou demander la suppression d'une publication compromettante : conseils de la CNIL → www.cnil.fr
-être conseillé face à une situation de cyberharcèlement : contacter gratuitement 3018
-signaler un contenu illicite sur les RS : plateforme Pharos → www.internet-signalement.gouv.fr

+ D'INFOS

CYBER MALVEILLANCE .GOUV.FR

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-Enfance 3018
Ensemble, agissons pour un monde numérique responsable

CNIL.
PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Région de gendarmerie du Grand Est
LA LETTRE CYBER en région Grand Est

Directeur de la publication : GCA S. OTTAVI
Responsable éditorial : COL L. GRAU
Rédacteurs : ADJ M. KNOBLOCH – ADJ E. DUBOIS

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
laurent.grau@gendarmerie.interieur.gouv.fr
mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie :