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

LA LETTRE CYBER en Région Grand Est

Gendarmerie nationale

GENDARMERIE

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

OCTOBRE 2024

LA THEMATIQUE DU MOIS:
HALLOWEEN

Les « fantômes » du web :
Comment éviter les pièges numériques effrayants

Virus, ransomware, phishing

Alors que l'ombre d'Halloween s'étend en cette période, il n'y a pas que les monstres et les sorcières qui rôdent dans la nuit…Sur internet aussi, les esprits malveillants sont à l'affût. Les pirates informatiques, semblables à des vampires numériques, cherchent à siphonner vos informations personnelles et financières. En cette période effrayant, il est plus que jamais essentiel de se protéger contre les « fantômes » du web : virus, ransomware et phishing.

Dans cette lettre, nous allons partager avec vous quelques conseils simples pour éloigner ces créatures digitales et vous assurer une cybersécurité à toute épreuve.

1. Méfiez vous des emails « fantômes » (phishing)

Les pirates se déguisent souvent en contact de confiance pour vous envoyer des emails frauduleux. Avant de cliquer sur un lien ou d'ouvrir une pièce jointe, vérifiez toujours l'adresse des emails de l'expéditeur. Ne donnez jamais d'informations sensibles par email.

2. Utilisez des mots de passe « ensorcelés » (robustes et uniques)

Choisissez des mots de passe complexes et uniques pour chaque compte. Combinez des lettres, des chiffres et des symboles. Pour plus de sécurité, utilisez un gestionnaire de mots de passe pour ne pas avoir à vous souvenir de tous.

3. Doublez la protection avec une amulette magique (authentification à 2 facteurs)

Activez l'authentification à deux facteurs (2FA) sur vos comptes. Même si un pirate obtient votre mot de passe, cette couche supplémentaire de sécurité (comme un code envoyé sur votre téléphone) l'empêchera d'accéder à vos données.

4. Mettez à jour vos sorts (logiciels) régulièrement

Les « failles de sécurité » sont comme des portes laissées ouvertes aux attaques. Assurez-vous que votre système d'exploitation, vos logiciels et vos antivirus sont toujours à jour pour bénéficier des dernières protections.

5. Utilisez un bouclier de protection (antivirus et pare feu)

Un bon logiciel antivirus et un pare-feu vous protègent des virus et malwares. Ils surveillent en continu votre ordinateur et bloquent toute activité suspecte avant qu'elle ne puisse causes des dégâts.

6. Evitez les lieux hantés (réseaux Wi-Fi publics non sécurisés)

Les réseaux Wi-Fi publics, comme ceux des cafés ou des hôtels, sont souvent non sécurisés. Si vous devez les utiliser, évitez d'y consulter des informations sensibles. Utilisez un VPN pour masquer votre activité en ligne et la sécuriser.

7. Sauvegardez vos données pour éviter la malédiction des ransomwares

Faites régulièrement des sauvegardes de vos données importantes sur un support externe ou dans le cloud. En cas d'attaque de ransomware, vous pourrez restaurer vos fichiers sans payer de rançon.

+ D'INFOS

CYBER MALVEILLANCE .GOUV.FR

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

e-enfance 3018

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

ANSSI Agence nationale de la sécurité des systèmes d'information

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

Directeur de la publication: GCA O.KIM
Responsable éditorial: COL L. GRAU
Rédacteur: 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: