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

Gendarmerie nationale

LA LETTRE CYBER *en région Grand Est*

Janvier 2024

La thématique du mois
Les bonnes résolutions

Le début d'année est toujours marqué par les bonnes résolutions. Afin d'assurer sa cybersécurité, il est primordial si cela n'a pas encore été fait, d'en prendre en observant les règles d'or suivantes sur les bonnes pratiques de l'outil numérique. Tenir ses bonnes résolutions est encore plus important afin de se prémunir de cyberattaques souvent préjudiciables à votre image ou à celle de votre institution.

SÉPAREZ STRICTEMENT VOS USAGES À CARACTÈRE PERSONNEL DE CEUX À CARACTÈRE PROFESSIONNEL

Avec l'avènement d'Internet et l'évolution des usages, la frontière entre vie professionnelle et vie personnelle devient de plus en plus poreuse. Pour sécuriser au mieux vos usages numériques dans ces différents environnements, appliquez ces quelques bonnes pratiques :

- Evitez d'utiliser vos moyens personnels (adresse mail, téléphone mobile, clé USB, etc.) à des fins professionnelles et inversement.
- Ne connectez pas d'équipements personnels, ou non fournis par votre service informatique, au réseau de votre entité ou à un équipement professionnel (téléphone mobile personnel, clé USB ou gadget électronique offert, etc.).
- À l'inverse, ne connectez vos équipements professionnels sur votre réseau personnel que dans les conditions prévues par votre service informatique.
- N'utilisez pas votre adresse mail professionnelle pour vous inscrire sur des sites Internet à titre personnel et réciproquement.

METTEZ RÉGULIÈREMENT À JOUR VOS OUTILS NUMÉRIQUES.

Un appareil ou un logiciel qui n'est pas à jour devient vulnérable et davantage exposé aux risques informatiques. Les quelques conseils qui suivent permettent de réduire significativement ce risque.

- Identifiez l'ensemble de vos appareils et logiciels.
- Lorsque l'on vous propose une mise à jour, effectuez-la immédiatement.
- Téléchargez les mises à jour uniquement depuis les sites officiels des éditeurs.
- Sur vos appareils, activez l'option de téléchargement et d'installation automatique des mises à jour quand elle existe.

PROTÉGEZ VOS ACCÈS PAR UNE AUTHENTIFICATION DOUBLE-FACTEUR LORSQUE C'EST POSSIBLE OU A MINIMA PAR DES MOTS DE PASSE COMPLEXES.

Utilisez un mot de passe différent pour chaque accès (messagerie, banque en ligne, comptes de réseaux sociaux, etc.) : en cas de compromission de l'un de vos comptes, cela évitera l'effet boule de neige.

- Créez un mot de passe suffisamment long, complexe et inattendu : de 8 caractères minimum et contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux.
- Ne communiquez jamais votre mot de passe à un tiers : aucune organisation ou personne de confiance ne vous demandera de lui communiquer votre mot de passe.

Utilisez un gestionnaire de mots de passe : pas simple de retenir tous ses codes de connexion ! Heureusement des outils de type « coffres forts de mots de passe » existent. Ces derniers mémorisent tous vos mots de passe et vous permettent d'en générer de manière aléatoire.

NE LAISSEZ PAS VOS ÉQUIPEMENTS SANS SURVEILLANCE LORS DE VOS DÉPLACEMENTS PROTÉGEZ VOTRE ESPACE DE TRAVAIL ET VOS DONNÉES

- Pensez à équiper votre écran d'un filtre de confidentialité lorsque vous utilisez vos équipements dans les espaces publiques (train, café, restaurant…)
- Verrouillez votre poste de travail lorsque vous n'êtes pas à votre bureau et placez en lieu sûr tout matériel sensible (support de stockage).

Sous peine de les voir manipulés, compromis à votre insu et vos données volées.

PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES EN LIGNE

Préservez votre identité numérique en vous montrant vigilant sur Internet et les réseaux sociaux.

Chacun doit se sentir responsable de ce qu'il diffuse sur Internet. Ne communiquez jamais d'informations sensibles sur des sites qui ne vous semblent pas suffisamment protégés, surtout lorsque la mention "Non sécurisé" apparaît à gauche de l'adresse du site Internet.
Veillez également à bien identifier les personnes avec qui vous communiquez sur Internet. Si vous avez un doute sur une identité, contactez cette personne par un autre moyen avant d'effectuer la moindre action ou de répondre à une requête.

PROTÉGEZ VOTRE MESSAGERIE PROFESSIONNELLE

L'hameçonnage (ou phishing en anglais) désigne une technique frauduleuse qui consiste à usurper l'identité d'un organisme connu (banque, opérateurs, etc) ou d'un proche pour récupérer des informations. Quelques règles simples permettent de l'éviter.

- Ne cliquez jamais sur un lien ou une pièce jointe qui vous semblent douteux. En cas de suspicion, passez la souris sur le lien pour voir apparaître l'adresse vers laquelle il dirige et appréciez sa légitimité.
- Ne répondez jamais à un mail suspect. Au moindre doute, contactez l'expéditeur par un autre canal.
- Vérifiez les paramètres de sécurité de votre compte de messagerie.
- Si le fournisseur de messagerie le permet, activez la double authentification pour sécuriser vos accès.

NE FAITES PAS CONFIANCE AUX RÉSEAUX NON MAITRISÉS POUR CONNECTER VOS ÉQUIPEMENTS

S'ils peuvent s'avérer très utiles, les réseaux Wi-Fi publics sont une aubaine pour les attaquants. Très faciles d'accès, ces réseaux peuvent être contrôlés pour intercepter vos informations personnelles.

- Désactivez les connexions sans-fil (Wi-Fi, Bluetooth, NFC, …) lorsque vous ne vous en servez pas pour éviter que vos appareils s'y connectent automatiquement.
- Lorsque c'est possible, privilégiez la connexion privée associée à votre abonnement mobile. Et n'oubliez pas de sécuriser le partage de connexion de vos appareils à l'aide d'un mot de passe.
- Si vous n'avez d'autre choix que d'utiliser un Wi-Fi public, veillez à ne jamais y réaliser d'opérations à caractère sensible (paiement par carte bancaire, déclaration d'impôts, renseignement d'informations confidentielles, etc.) et si possible utilisez un réseau privé virtuel (VPN).

FAITES PREUVE DE VIGILANCE LORS DE VOS ÉCHANGES TÉLÉPHONIQUES OU EN VISIOCONFÉRENCE

La confidentialité des conversations n'est pas assurée sur les réseaux publics.
Ne donnez jamais d'informations confidentielles au téléphone. Privilégiez le contre appel afin de vous assurez de l'identité de votre interlocuteur.

SAUVEGARDEZ REGULIEREMENT VOS DONNES

Effectuez des sauvegardes régulières de vos données personnelles et professionnelles sur des supports placés en sécurité vous protège en cas de panne, de perte, de vol, de destruction de votre matériel ou d'attaque informatique. Selon vos besoins, plusieurs solutions de sauvegarde s'offrent à vous.

VEILLEZ À LA SÉCURITÉ DE VOTRE SMARTPHONE

Évitez de prendre votre smartphone pendant les réunions sensibles. Il peut être utilisé pour enregistrer vos conversations, y compris à votre insu.

+ 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

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
Rédacteurs : ADC D. MUNSCH – 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