FICHE DE CONTROLE SÉCURITÉ NUMÉRIQUE

Avant de compléter cette fiche de contrôle, il est important de lire le document "Un guide de sécurité numérique pour tous".

Sécurité numérique

- ○ Je suis capable de faire la différence entre la sécurité numérique et la cybersécurité, et je comprends l'importance de ces concepts pour ma protection en ligne.
- ○ Je suis conscient de la croissante numérisation de nos vies et des dangers qui en découlent.
- ○ Je veille à ce que mes logiciels soient fréquemment mis à jour afin de corriger les failles connues, réduisant ainsi les risques de piratage par des cybercriminels.
- ○ Je suis au courant des évolutions dans le domaine de la sécurité numérique en m'informant par la lecture de sources crédibles d'information.
- ○ Je reste vigilant quant à ma présence sur Internet en surveillant régulièrement mes applications, programmes et informations personnelles divulguées en ligne.

Logiciel

- ○ J'ai conscience de détenir une empreinte numérique, autrement appelée la trace de mes activités en ligne, qui influence mon identité numérique même quand je ne suis pas activement connecté.
- ○ J'ai conscience que mes activités en ligne, comme publier, rechercher ou partager, laissent des traces de données pouvant révéler des éléments de mon identité.
- ○ Je reconnais que l'utilisation d'Internet génère des données qui sont collectées par les moteurs de recherche, les réseaux sociaux et les entreprises, ce qui engendre des risques comme la fraude et la violation de la vie privée.
- ○ Je me conforme aux bonnes pratiques de sécurité informatique, telles que l'utilisation d'un antivirus et la mise à jour fréquente des logiciels.
- ○ Si besoin est, je sais comment supprimer mes traces en ligne en désactivant mes comptes sur les réseaux sociaux et en demandant la suppression de mes informations personnelles.

Mots de passe

- ○ Je sais comment composer un mot de passe sécurisé en utilisant des mots, phrases, lettres, chiffres et symboles spéciaux.
- ○ Je suis au courant des différentes techniques utilisées par les pirates pour décoder les mots de passe.
- ○ Pour éviter toute faille de sécurité, je ne réutilise jamais le même mot de passe sur plusieurs sites.
- ○ Je change fréquemment mon mot de passe pour renforcer ma sécurité.
- ○ Je renforce la sécurité de mes comptes en utilisant des techniques supplémentaires telles que l'authentification à deux facteurs (2FA), l'authentification à plusieurs facteurs (MFA) et les mots de passe à usage unique (OTP).

DOCUMENT ÉLABORÉ PAR
cameco+
Communication Consultancy for the Common Good

FICHE DE CONTROLE SÉCURITÉ NUMÉRIQUE

Avant de compléter cette fiche de contrôle, il est important de lire le document "Un guide de sécurité numérique pour tous".

Intelligence artificielle qui crée (IA générative)

- ○ Je sais que l'IA générative produit des textes, des images et d'autres contenus en s'appuyant sur son processus d'apprentissage.
- ○ Je garde un œil sur les progrès de l'IA générative et ses dangers éventuels.
- ○ Je suis au courant des dangers de sécurité numérique, liés aux usurpations d'identité numérique à des fins d'escroquerie, aux logiciels malveillants complexes et aux failles de sécurité des données.
- ○ Je vérifie les informations que je reçois en consultant plusieurs sources fiables pour contrer la désinformation crée par l'IA.
- ○ Je signale les contenus suspects générés par l'IA aux plateformes et aux autorités compétentes.
- ○ Je mets régulièrement à jour les paramètres de confidentialité de mes comptes en ligne.

Aspects socioculturels de la sécurité numérique

- ○ Je reconnais que le contexte, qu'il soit personnel, social ou professionnel, peut avoir un impact sur la façon dont les gens perçoivent et pratiquent la sécurité numérique.
- ○ Je suis conscient que certaines personnes peuvent être plus vulnérables en ligne en raison de leur race, leur ethnie, leur genre, leur nationalité ou leur religion.
- ○ Je suis au courant des différentes formes de harcèlement en ligne, telles que la diffamation, l'usurpation d'identité, l'extorsion, la traque, la surveillance sexuelle, le harcèlement, les dommages émotionnels et les menaces de violence.
- ○ Je reconnais que les défis liés au bien-être, à la culture de l'annulation et à l'autocensure, sont des dangers qui impactent la sécurité en ligne de tout un chacun.
- ○ Je supporte la promotion de l'empathie numérique, la compréhension et la dénonciation du harcèlement en ligne pour améliorer la sécurité virtuelle.

Autres aspects

- ○ Je veille à avoir un téléphone ou un ordinateur portable dédié uniquement au travail pour renforcer la sécurité.
- ○ Je suis conscient des réglementations spécifiques à chaque pays en matière de pratiques numériques, comme l'interdiction.
- ○ Je suis informé des lois propres à chaque pays que je visite concernant les pratiques numériques, telles que l'interdiction de l'utilisation de VPN personnels dans certaines régions.
- ○ Je reconnais que bien que je ne sois pas une célébrité, je reste susceptible d'être victime de cybermenaces.
- ○ Je suis conscient que de simples comportements, tels que la mise à jour fréquente des logiciels et l'utilisation de mots de passe robustes, peuvent considérablement améliorer la sécurité en ligne.
- ○ Je concède qu'il est impossible d'atteindre une sécurité numérique à 100 % en raison de la constante évolution des menaces et des aspects humains.

DOCUMENT ÉLABORÉ PAR
cameco+
Communication Consultancy for the Common Good

FICHE DE CONTROLE SÉCURITÉ NUMÉRIQUE

Avant de compléter cette fiche de contrôle, il est important de lire le document "Un guide de sécurité numérique pour tous".

Navigateurs

- ○ Je suis conscient du fait qu'utiliser un navigateur web non sécurisé peut me mettre en danger en raison du risque de piratage, de vol de données, de pistage, de logiciels malveillants et d'autres menaces.
- ○ Je comprends que même avec l'usage des navigateurs sécurisés, la sécurité n'est pas totale, donc il est important d'appliquer de bonnes pratiques d'hygiène en ligne.
- ○ Je mets régulièrement à jour mon navigateur web et j'utilise le moins d'extension web possible pour éviter de mettre en danger mes informations.
- ○ Je télécharge et installe un bloqueur de publicités (adblocker) fiable afin de bloquer les annonces nuisibles, les désagréments, les atteintes à la vie privée et les traqueurs.
- ○ Je bloque les fenêtres pop-up pour éviter d'être exposé à des contenus gênants et dangereux sur des sites web malveillants.
- ○ Je supprime régulièrement les cookies indésirables afin d'empêcher le traçage et de protéger la vie privée.
- ○ Je désactive la fonction web de remplissage automatique pour éviter de fournir des informations sensibles dans des formulaires en ligne, potentiellement malveillants.

Réseaux privés virtuels (VPN)

- ○ J'admets qu'un VPN, également connu sous le nom de "réseau privé virtuel", sécurise ma connexion internet en assurant la confidentialité en ligne grâce à un tunnel de données chiffrées.
- ○ Je comprends l'importance d'avoir un VPN personnel pour me connecter à un réseau Wi-Fi public, accéder à des contenus restreints, protéger mes données personnelles et cacher mon adresse IP.
- ○ Je fais régulièrement une évaluation de mes activités en ligne pour voir si l'utilisation d'un VPN est nécessaire pour renforcer ma sécurité et préserver ma vie privée.

Médias sociaux

- ○ Je comprends que les médias sociaux ont à la fois des avantages, comme l'apprentissage et la communication, mais aussi des risques comme la cyberintimidation et la dépendance.
- ○ Je règle consciemment mes paramètres de confidentialité afin de définir les personnes qui peuvent voir mes messages sur les réseaux sociaux.
- ○ Je suis conscient(e) de la permanence des messages en ligne et je veille à préserver ma réputation en choisissant avec soin les contenus que je partage
- ○ J'adapte ma présence en ligne dans des lieux à risques, en évitant de trop publier ou partager des informations.
- ○ J'accorde une grande importance à la confidentialité des informations personnelles pour prévenir les cas d'usurpation d'identité.
- ○ Je suis conscient(e) des mesures adéquates à prendre dans des cas précis, y compris la suppression et le blocage des harceleurs, le signalement aux administrateurs du site et l'implication des autorités si nécessaire.
- ○ Je suis prudent sur les réseaux sociaux, en évitant les messages, les liens douteux et les tentatives d'hameçonnage.
- ○ J'évite de partager des informations sensibles par le biais de systèmes de messagerie afin de réduire les risques de piratage, de violation de données et d'interception.

DOCUMENT ÉLABORÉ PAR
cameco+
Communication Consultancy for the Common Good