Hygiène numérique et 6 conseils pour protéger votre vie privée en ligne

Qu’est-ce que l’hygiène numérique ?
C’est l’ensemble des comportements responsables à adopter et des précautions à prendre pour améliorer votre sécurité en ligne et vous protéger contre la fraude.
De nombreux stratagèmes existent pour obtenir vos renseignements personnels, mais l’utilisation de pratiques sécuritaires en ligne peut freiner les cybercriminels.
En voici un survol.

6 conseils essentiels à retenir :

1. Utilisez des mots de passe robustes.
2. Protégez vos renseignements personnels et bancaires.
3. Contrôlez l’information que vous publiez sur les réseaux sociaux.
4. Protégez votre activité sur le Web.
5. Effectuez des achats en ligne sécurisés.
6. Sachez reconnaître la fraude financière en ligne.

Cybersécurité et protection des données personnelles

1. Utilisez des mots de passe robustes.

Un mot de passe robuste devrait comprendre entre 10 à 14 caractères et inclure des lettres minuscules et majuscules, des chiffres ainsi que des caractères spéciaux.
Ne le divulguez à personne, pas même à vos proches.

Évitez les mots de passe faciles à deviner comme ceux qui sont basés sur le nom de votre animal de compagnie ou d'un membre de votre famille.
Mémorisez plutôt une phrase logique qui n'est connue que de vous.
Par exemple, utilisez des chiffres et les premières lettres de chaque mot d'une phrase secrète que vous aurez inventée afin de créer un mot de passe qui n'aura du sens que pour vous.

Chaque appareil ou compte devrait être associé à un mot de passe différent afin d'éviter qu'une seule fuite d'information compromette la sécurité de plusieurs services à la fois.

Enfin, lorsque c'est possible, activez la validation à deux étapes (aussi appelée « authentification à deux facteurs ») à titre de protection supplémentaire.
La validation à deux étapes vous donne ainsi un second moyen de vous authentifier, en plus de votre mot de passe, en utilisant par exemple l'entrée d'un code de sécurité à usage unique transmis par courriel ou par message texte.

2. Protégez vos renseignements personnels et bancaires.

À moins que ça vous soit demandé dans un contexte officiel, évitez de divulguer des informations personnelles ou confidentielles telles que votre nom complet, votre adresse, votre numéro de téléphone, votre numéro d'assurance sociale (NAS), votre date de naissance et des renseignements en lien avec vos divers comptes et services, qu'ils soient bancaires, financiers ou autres.
Certaines informations, comme les mots de passe, ne doivent pas être dévoilées à qui que ce soit, même dans un contexte officiel.

Questionnez-vous sur la légitimité d'une demande ou sur la façon dont celle-ci est effectuée.
Prenez un pas de recul et posez des questions afin de mieux comprendre la raison de la demande. Par exemple : « Pourquoi la personne a-t-elle besoin de cette information? », « Est-ce que je peux seulement montrer mes pièces d'identité? », « Est-ce nécessaire que mes renseignements soient conservés? », « Comment mes renseignements sont-ils protégés? », etc.
Dans le doute, faites une recherche en vous référant à une source fiable et/ou contactez l'entreprise afin confirmer de la légitimité de la demande.

Ces questions peuvent aussi s'appliquer avant de partager volontairement des renseignements, que ce soit lors de l'inscription à un concours ou d'une publication sur les médias sociaux, par exemple.

Avant de remplir un formulaire en ligne — y compris lors d'un achat sur le Web —, vérifiez que vos données sont adéquatement protégées par le protocole HTTPS.
Pour savoir si le site que vous consultez est bien sécurisé, un symbole de cadenas doit accompagner l'adresse

de la page Web dans votre navigateur.
Celle-ci doit également commencer par *http**s*** : le « S » indique la présence de cette mesure de sécurité.

Dans la mesure du possible, connectez-vous à des réseaux Wi-Fi sécurisés lorsque vous naviguez en ligne.
De plus, ne partagez jamais de données personnelles et n'accédez pas à des sites qui en contiennent lorsque vous utilisez un réseau sans-fil public.
Bien que ces réseaux publics soient pratiques, n'importe qui peut s'y connecter, y compris des personnes malintentionnées.

Vie privée en ligne

3. Contrôlez l'information que vous publiez sur les réseaux sociaux.

Le piratage psychologique (ou « ingénierie sociale ») est une technique de manipulation utilisée par des personnes malveillantes afin de gagner votre confiance et de vous pousser à divulguer des informations confidentielles à des fins de fraude.
Les informations partagées sur les médias sociaux peuvent donc être une mine d'or pour les cybercriminels afin de rendre leurs tactiques encore plus vraisemblables à vos yeux.

Chaque renseignement sur vous devenant accessible à tous représente un morceau de casse-tête.
Si des fraudeurs en assemblent suffisamment, ils pourraient obtenir un portrait détaillé de votre identité.
Les données recueillies peuvent servir à usurper votre identité, à créer de faux sites Web ou encore, à envoyer des courriels frauduleux personnalisés et d'une grande crédibilité.

Prenez garde de ne pas diffuser, même accidentellement ou sous forme d'images, des informations personnelles ou confidentielles.
Par exemple, ne publiez pas une photo où l'on voit la plaque d'immatriculation de votre véhicule ou votre adresse.

Méfiez-vous aussi des jeux, des **sondages** et des **questionnaires ludiques** sur les réseaux sociaux, même si les questions ou les réponses semblent anodines.
Certaines personnes utilisent les renseignements recueillis pour mettre en place des stratagèmes frauduleux ou pour tenter de deviner vos mots de passe ou les réponses à vos questions de sécurité.

Selon la plateforme, ajustez vos paramètres de confidentialité et de sécurité afin de contrôler qui a accès à vos publications et à vos informations.
Les réglages par défaut permettent souvent à un grand nombre de personnes d'en apprendre beaucoup à votre sujet.

Présence sur le Web

4. Protégez votre activité sur le Web.

En utilisant des logiciels spécialisés ou des témoins (*cookies*), les cybercriminels et certains sites Web peuvent recueillir des données sur vos habitudes virtuelles, par exemple les pages que vous visitez, les recherches que

vous effectuez, les achats que vous faites en ligne et même l'identité de votre fournisseur Internet et votre emplacement géographique approximatif.

L'utilisation d'un réseau privé virtuel (*Virtual Private Network* ou *VPN*) vous permet d'encoder vos informations de connexion et de protéger votre confidentialité.
Ce système brouille également votre adresse IP, ce qui complique l'identification de votre géolocalisation.

Effacez vos données de navigation sur une base régulière afin de limiter votre empreinte sur le Web et ainsi réduire les risques de vous faire épier ou de devenir la cible d'une cyberattaque.

Faites une coupure entre votre vie personnelle et vos activités professionnelles.
Si vous avez accès dans le cadre de votre travail à un courriel, à un ordinateur ou à un téléphone fourni par votre employeur, évitez de les utiliser pour des raisons personnelles. À l'inverse, n'utilisez pas vos appareils personnels pour partager de l'information professionnelle.

Achats en ligne

Assurez-vous de transiger sur un site de confiance en repérant le symbole de cadenas associé au protocole HTTPS au début de l'adresse Web, les mentions légales obligatoires et les conditions générales de vente.

Privilégiez les modes de paiement sécurisés tels que votre carte de crédit plutôt que les virements électroniques ou l'envoi postal d'argent comptant.
Votre carte de crédit Desjardins bénéficie également de la protection Responsabilité zéro : celle-ci vous permet d'obtenir un remboursement en cas de transaction frauduleuse dans la mesure où votre convention d'utilisation est respectée.

Faites preuve de vigilance sur les plateformes d'achat de seconde main et les petites annonces.
Bien que ces transactions aient souvent lieu en personne ou hors de la plateforme de vente, certains bons comportements peuvent être adoptés.
Lisez nos conseils pour prévenir et repérer les fraudes liées aux petites annonces.

Escroqueries en ligne

6. Sachez reconnaître la fraude financière en ligne.

Hameçonnage (faux courriels, textos frauduleux, etc.), messages privés provenant de personnes inconnues, appels téléphoniques : les cybercriminels ont recours à de multiples tactiques dans le but de soutirer les renseignements personnels et bancaires de leurs victimes.

Bien que les méthodes utilisées varient grandement, certains signes courants peuvent aider à reconnaître une tentative de fraude.
Par exemple :

- On vous demande de fournir des informations, d'effectuer un remboursement ou d'intervenir concernant un problème quelconque dans un délai très court.
  Une raison est mentionnée afin de justifier **cette urgence**.

- Le message comporte des **fautes d’orthographe** ou une mise en page peu professionnelle qui intègre le logo d’une marque connue.
- Vous avez remporté un prix, reçu un transfert d’argent **inattendu** ou on vous propose une offre qui semble **trop belle pour être vraie**.

De façon générale, les fraudeurs essaient de créer un sentiment d’urgence ou de piquer votre curiosité pour vous pousser à réagir sans réfléchir et ainsi tromper votre vigilance.

Une saine hygiène numérique contribue à renforcer votre sécurité sur le Web.
Choisir des mots de passe robustes, protéger vos informations personnelles et confidentielles et en limiter la diffusion, faire preuve de vigilance et de discrétion en ligne : voilà autant de façons de réduire votre exposition aux cybermenaces.
Adoptez ces bonnes habitudes dès maintenant pour naviguer l’esprit tranquille.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231015
"C'est ensemble qu'on avance"