
Staying connected with friends, family, and coworkers has been challenging, especially over the last year. Through the internet and social media, we've been able to stay present in each other's lives – whether it be to attend a loved one's wedding, work on projects, or participate in games nights. However, increasing the time we spend online has made us more vulnerable to cyber threats and scams. With October being Cybersecurity Awareness month, here are some ways you can protect yourself online while remaining in touch.

**Be mindful of what you share**

Part of the fun of social media is sharing our lives with others, but sharing too much can make you a target for someone to steal your identity or hack your account. To keep yourself safe, customize the security settings on your social media accounts, limit the personal information you post or have in your profile (such as phone numbers or addresses), and be cautious about accepting requests and invites from people you don't know in real life.

**Recognize phishing scams so you're not the bait**

Phishing is the act of acquiring sensitive information (such as usernames, passwords, or even credit card numbers) by pretending to be someone you know or trust. If you receive a questionable email, text, or even direct message on social media promising you a grand prize (for a contest you never entered), using threatening language, asking for personal information, or containing typos or bizarre language, ignore it and do not click on any suspicious links or downloads.

## Keep it complicated

One of the best ways to keep your information safe is to use unique, complex passwords or passphrases for your online accounts. A strong password is at least 12 characters (letters, numbers, or symbols) while a strong passphrase should be at least 15 characters and 4 or more random words. Consider using a password manager to protect your passwords and keep them in a secure place so you don't have to memorize or write them down (only to lose it soon after).

For an added layer of protection, use two-factor authentication or multi-factor authentication whenever available. Doing so adds an extra step to your login process (by receiving a PIN to your phone or email, for example), but helps prevent cybercriminals from gaining access to your account without confirming the PIN, thumbprint, or facial recognition.

For more information on Cybersecurity Awareness Month and ways to stay safe online, use the resources below.

### Resources

- Government of Canada | Get Cyber Safe
- Microsoft | Why is Cybersecurity Awareness Month important?
- Government of Canada | Password managers
- KnowBe4 | Phishing blog


Rester en contact avec les amis, la famille et les collègues a été difficile,

surtout au cours de la dernière année. Grâce à Internet et aux médias sociaux, nous avons pu rester présents dans la vie de notre entourage, que ce soit pour assister au mariage d'un proche, pour travailler sur des projets ou pour participer à des soirées de jeux. Cela dit, puisque nous passons plus de temps en ligne, nous sommes plus vulnérables aux cybermenaces et aux escroqueries. Comme octobre est le Mois de la sensibilisation à la cybersécurité, voici quelques façons de vous protéger en ligne sans nuire à vos relations sociales.

### Faites attention à ce que vous publiez

L'un des aspects amusants des médias sociaux est le fait de montrer des moments de notre vie aux autres. Par contre, en publiant trop d'informations, vous risquez de devenir la cible d'un vol d'identité ou d'un piratage de compte. Pour assurer votre sécurité, personnalisez les paramètres de sécurité de vos comptes de médias sociaux, limitez les renseignements personnels que vous publiez ou dont vous faites part dans votre profil (numéro de téléphone, adresse, etc.), et faites preuve de prudence quand vous acceptez des demandes et des invitations de personnes que vous ne connaissez pas dans la vraie vie.

### Repérez les escroqueries par hameçonnage pour éviter d'être un appât

L'hameçonnage consiste à obtenir des renseignements sensibles (par exemple des noms d'utilisateur, des mots de passe ou même des numéros de carte de crédit) en se faisant passer pour une connaissance ou une personne de confiance. Si vous recevez un courriel, un message texte ou même un message privé sur les médias sociaux qui est louche et qui vous promet un grand prix (dans le cadre d'un concours auquel vous n'avez jamais participé), utilise un langage menaçant, demande des renseignements personnels ou encore contient des coquilles ou une formulation bizarre, n'en tenez pas compte et ne cliquez pas sur des liens ou des fichiers suspects à télécharger.

### Optez pour la complexité

L'une des meilleures façons d'assurer la protection de vos renseignements est d'utiliser des mots de passe ou des phrases de chiffrement uniques et complexes pour vos comptes en ligne. Pour être robuste, un mot de passe doit compter au moins 12 caractères (lettres, chiffres ou symboles), tandis qu'une phrase de chiffrement doit compter au moins 15 caractères et quatre mots aléatoires. Songez à utiliser un gestionnaire de mots de passe pour protéger vos mots de passe et les conserver en lieu sûr. De cette façon, vous n'aurez pas à les mémoriser ou à les mettre par écrit (au risque de les égarer peu de temps après).

Pour plus de sécurité, utilisez l'authentification à deux facteurs ou

l’authentification multifactorielle dans la mesure du possible. Cette mesure ajoute une étape supplémentaire à votre processus d’ouverture de session (en recevant un NIP sur votre téléphone ou par courriel, par exemple), mais elle contribue à empêcher les cybercriminels d’accéder à votre compte sans authentification au moyen d’un NIP, d’une empreinte digitale ou de la reconnaissance faciale.

Pour en savoir plus sur le Mois de la sensibilisation à la cybersécurité et sur les façons de vous protéger en ligne, utilisez les ressources ci-après.

### Ressources

- Governement du Canada | Pensez cybersécurité
- Microsoft | Why is Cybersecurity Awareness Month important?
- Governement du Canada | Gestionnaires de mots de passe
- KnowBe4 | Phishing blog

**The Manion Living Well Team**

www.manionwilkins.com