LIGUE DES CADETS DE L'AIR DU CANADA · ÉDITION 2026

Formation en cybersécurité

Reconnaître l'hameçonnage d'aujourd'hui et protéger vos comptes Microsoft 365, Outlook et Gmail

K2E Security

Pourquoi c'est important en 2026

8,3 milliards

courriels d'hameçonnage détectés par Microsoft dans les trois premiers mois de 2026

Microsoft Threat Intelligence

86 %

des attaques d'hameçonnage sont maintenant rédigées ou améliorées par l'IA

KnowBe4, 2026

704 M$

perdus à la fraude par les Canadiens en 2025, et seulement 5 à 10 % des fraudes sont signalées

Centre antifraude du Canada

Objectifs de la séance

Repérer l'hameçonnage

Codes QR, faux CAPTCHA, codes d'appareil, courriels écrits par l'IA

Verrouiller vos comptes

Phrases de passe solides et validation en deux étapes

Savoir quoi faire

Comment signaler, et quoi faire si vous avez déjà cliqué

PARTIE 1

L'hameçonnage et l'ingénierie sociale

Les attaquants ciblent d'abord les gens

L'ingénierie sociale vous pousse à donner de l'information, de l'argent ou un accès. L'hameçonnage en est la forme la plus courante, et il arrive maintenant par tous les moyens de communication:

- **Courriel** Hameçonnage
- **Texto** Hameçonnage par texto
- **Appel téléphonique** Hameçonnage vocal, maintenant avec des voix clonées par l'IA
- **Code QR** Hameçonnage par code QR
- **Invitations Teams et calendrier** Fausses réunions et faux fichiers partagés

Les leviers émotionnels utilisés

Urgence
« Votre compte sera fermé dans 24 heures »

Peur
« Facture impayée », « avis juridique », « connexion suspecte »

Cupidité
« Vous avez gagné une carte-cadeau »

Curiosité
« Découvrez qui a partagé un fichier avec vous »

Empathie
« La famille d’un cadet a besoin d'aide d'urgence »

Vérifiez trois choses dans chaque message

Un courriel d'hameçonnage peut sembler venir d'une personne de confiance. Ralentissez et vérifiez ces points avant d'agir.

L'expéditeur

Qui envoie vraiment ce message ?

- Vient-il du vrai domaine de notre organisation ?
- Un collègue écrit-il d'une adresse Gmail ou Outlook.com personnelle ?
- L'adresse correspond-elle au nom affiché ?

Le contexte

Pourquoi l'envoie-t-on ?

- Attendiez-vous ce message ?
- Cette personne demanderait-elle normalement cela ?
- Vous pousse-t-on à agir vite ou à garder le secret ?

Le contenu

Est-ce que ça a du sens ?

- Où mènent vraiment les liens ? Survolez-les d'abord.
- Demande-t-on un mot de passe, un code ou un paiement ?
- Y a-t-il une pièce jointe, un code QR ou un fichier partagé inattendu ?

Un doute ? Contactez la personne au numéro ou à l'adresse que vous avez déjà, jamais ceux du message.

Vérifiez l'adresse exacte de l'expéditeur

Le nom affiché peut être n'importe quoi. Lisez toujours l'adresse après le « @ ».

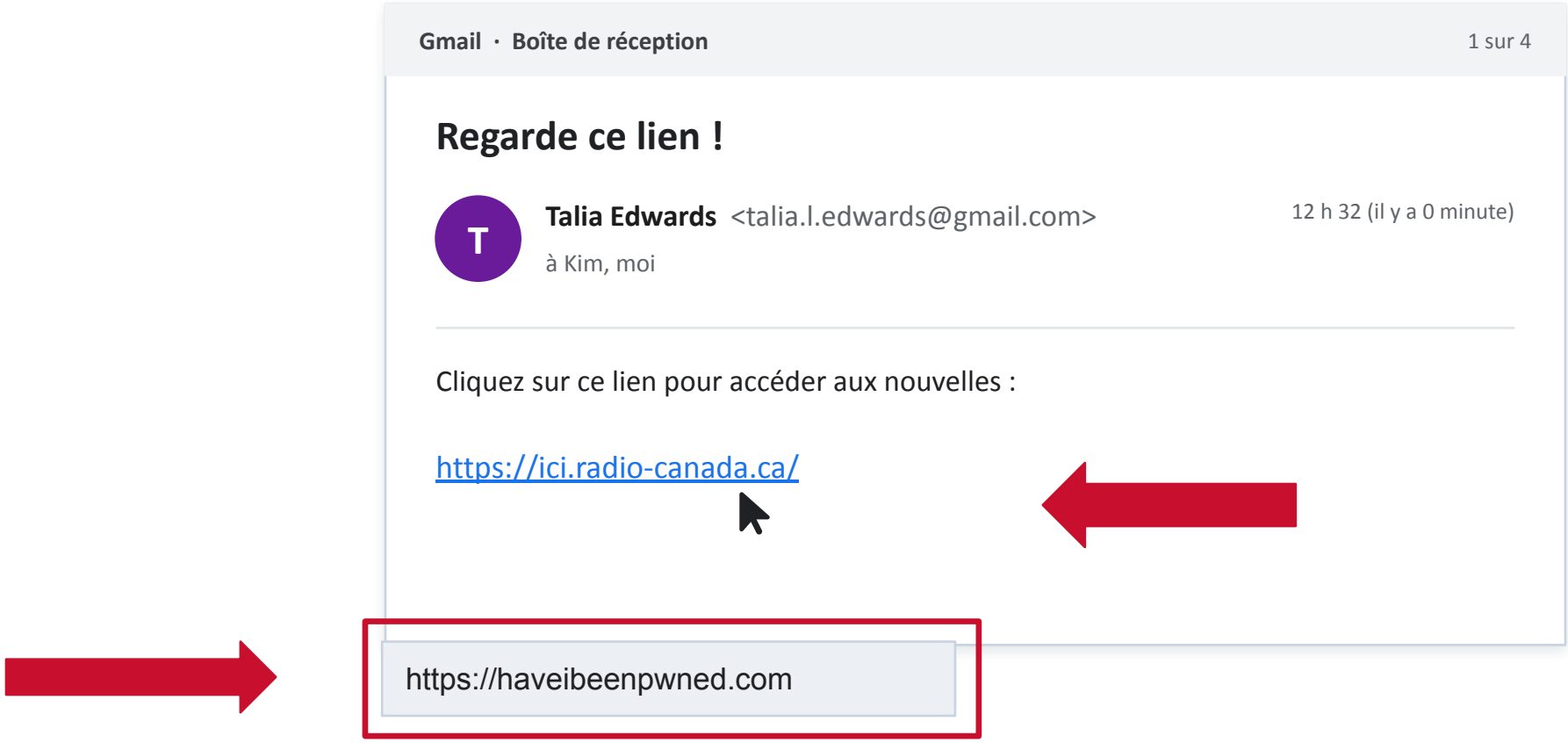
Type	Ce que vous voyez	Verdict
Officielle	`execdir@aircadetleague.com`	✓ **Légitime**
Typosquattage	`execdir@aircadet-league.com`	✕ **Faux : trait d'union en trop**
Extension changée	`execdir@aircadetleague.co`	✕ **Faux : il manque le « m »**
Lettre semblable	`execdir@aircadetIeague.com`	✕ **Faux : « I » majuscule au lieu du « l »**
Nom usurpé	`"Pierre Forgues" <pierre.forgues@gmail.com>`	✕ **Faux : compte personnel**

Sur votre téléphone

Les applications Outlook et Gmail n'affichent que le nom. Touchez le nom de l'expéditeur pour voir l'adresse complète avant de lui faire confiance.

Un nom connu venant d'une adresse Gmail ou inconnue est un signal d'alarme, même si c'est celui du directeur général.

Comment survoler un lien ?



Le lien affiche radio-canada.ca, mais l'aperçu en bas montre la vraie destination. Ils ne correspondent pas : ne cliquez pas.

Survolez avant de cliquer : lisez le vrai domaine

Survolez (souris) ou appuyez longuement (mobile). Le vrai domaine précède la première « / » simple.

✓ SÛR

`https://login.microsoftonline.com/common/oauth2`

Vrai domaine de connexion Microsoft. Ce qui suit la « / » n'a pas d'importance.

✕ FAUX

`https://login.microsoftonline.verify-acct.ru/`

Le vrai domaine est verify-acct.ru. « microsoftonline » n'est qu'un leurre.

✕ FAUX

`https://ACCOUNTS.GO0GLE.COM/signin`

Un zéro remplace un « o ». Les majuscules le rendent plus difficile à repérer.

Les liens raccourcis et les codes QR cachent la destination. Si vous ne voyez pas où ça mène, ne l'ouvrez pas.

PARTIE 2

Quoi de neuf : les ruses d'hameçonnage de 2026

Six tendances d'hameçonnage à connaître

Hameçonnage rédigé par l'IA

86 % de l'hameçonnage est maintenant généré ou peaufiné par l'IA. Une orthographe parfaite ne veut plus dire que c'est sécuritaire.

Hameçonnage par code QR

En hausse de 146 % au début de 2026. Le balayage vous fait passer au téléphone, hors des protections du travail.

Faux CAPTCHA (« ClickFix »)

Une page « Prouvez que vous êtes humain » vous fait coller et exécuter une commande cachée.

Codes d'appareil et contournement de l'AMF

Vous vous connectez sur la vraie page Microsoft, mais avec le code de l'attaquant : c'est lui qui entre.

Pièges Teams et calendrier

Hameçonnage par invitation de calendrier en hausse de 49 % et les attaques Teams sont en hausse de 41 % (KnowBe4).

Fausses alertes et faux rappels

Faux courriels d'« alerte de sécurité Google », suivis d'appels d'un faux « soutien technique ».

Exemple : le code QR « mot de passe qui expire »

Outlook · Boîte de réception

1

Action requise : votre mot de passe expire aujourd'hui

Sécurité Microsoft 365 <no-reply@m365-securenotice.com>

À : kim@aircadetleague.com

Bonjour Kim,

2

Votre mot de passe Microsoft 365 expire aujourd'hui. Pour garder votre mot de passe actuel, balayez le code ci-dessous avec votre téléphone.

Cette demande expire dans 2 heures.

3



1

Expéditeur imitateur

Ce n'est pas microsoft.com. Le nom affiché fait tout le travail.

2

Urgence et offre étrange

« 2 heures » et « garder votre mot de passe actuel » sont des pressions classiques.

3

Le code QR est le piège

Il vous fait passer au téléphone, où vous ne pouvez pas survoler le lien et où les protections du travail ne s'appliquent pas. L'hameçonnage par code QR a bondi de 146 % au début de 2026.

Ne balayez jamais un code QR pour vous connecter, « vérifier » ou garder un mot de passe.

Exemple : le faux « Je ne suis pas un robot »



1 **Cocher la case copie une commande**

La page place discrètement une commande malveillante dans votre presse-papiers (la mémoire de l'ordinateur).

2 **Les « étapes » l'exécutent**

Windows + R, coller, puis Entrée.
Sur un Mac, la page vous demande de coller (Commande ⌘ + V) dans le Terminal.

3 **Ce que ça installe**

Habituellement un voleur d'information qui récupère les mots de passe enregistrés et les sessions ouvertes, y compris Microsoft 365 et Gmail.

Aucun vrai site ne vous demande de coller quoi que ce soit dans Exécuter, PowerShell ou le Terminal. Fermez l'onglet.

Exemple : l'hameçonnage par code d'appareil

La page de connexion est réelle : vérifier l'adresse Web ne suffit donc pas. Une campagne de 2026 a touché plus de 340 organisations, notamment au Canada.

1 Un « fichier partagé »

« Kim a partagé Budget escadron 2026.xlsx. Pour l'afficher, entrez le code WQ7K-DM4P sur microsoft.com/devicelogin. »

2 Connexion sur la vraie page

Vous tapez le code sur le vrai site de Microsoft, puis vous approuvez votre demande d'AMF comme d'habitude.

3 L'attaquant devient vous

Le code appartenait à l'appareil de l'attaquant. Il obtient votre boîte courriel et votre OneDrive, sans mot de passe.

N'entrez un code d'appareil que si vous configurez une télé, une console ou un appareil devant vous.

Exemple : la fausse alerte de sécurité Google

Gmail · Boîte de réception

Alerte de sécurité : une assignation a été émise pour votre compte Google

1 **Google** <no-reply@google.com>

À : kim.cadets@gmail.com

Une demande des forces de l'ordre nous oblige à leur transmettre une copie du contenu de votre compte. Pour consulter la demande ou la contester, visitez :

2 sites.google.com/view/support-case-48213

Vous avez 48 heures pour répondre.

1 **L'adresse peut sembler parfaite**

Des attaquants ont réutilisé de vrais messages de Google pour afficher no-reply@google.com et passer les contrôles de Gmail.

2 **Sites.google.com : ouvert à tous**

Une adresse Web de Google ne prouve pas que Google a créé la page.

3 **Puis vient l'appel**

Un faux « soutien Google » ou « soutien Microsoft » appelle et demande le code envoyé à votre téléphone.

Vérifiez les alertes vous-même sur myaccount.google.com ou account.microsoft.com, et ne partagez jamais un code.

Exemple : le « petit service » et la fraude au paiement

Outlook · Boîte de réception

Petit service

Maj J. Tremblay <co.tremblay.squadron@gmail.com>

À : kim@aircadetleague.com

Es-tu disponible ? J'ai besoin que tu achètes 5 cartes-cadeaux de 100 $ pour la remise des prix des cadets ce soir.

Je suis en réunion et je ne peux pas prendre d'appels. Envoie-moi juste des photos des codes des cartes, je te rembourse demain.

Envoyé de mon iPhone

L'harponnage a coûté aux Canadiens plus de **68 millions de dollars** en 2025, et environ 31 millions dans les trois premiers mois de 2026 seulement (Centre antifraude du Canada).

Signes à surveiller

- Le nom d'un dirigeant avec une adresse personnelle
- Cartes-cadeaux, virements bancaires ou virements Interac
- « Nouvelles coordonnées bancaires » d'un fournisseur
- « Je ne peux pas parler » et le secret

Vérifiez toute demande de paiement par téléphone, à un numéro connu. Exigez deux approbations pour les fonds.

Signalez-le, et agissez vite si vous avez cliqué

Comment signaler

Outlook / Microsoft 365

Sélectionnez le message, puis Signaler > Signaler l'hameçonnage.

Gmail

Ouvrez le message, puis le menu ⋮ > Signaler un hameçonnage.

Textos suspects

Transférez le texte au 7726 (SPAM), chez tous les fournisseurs canadiens.

Fraude ou argent perdu

Centre antifraude du Canada : 1-888-495-8501 ou en ligne, ainsi que votre police locale.

Vous avez déjà cliqué ?

1. Pas de panique, et ne le cachez pas. La rapidité compte plus que le blâme.
2. Changez ce mot de passe immédiatement, à partir d'un appareil fiable.
3. Déconnectez toutes les sessions dans la page de sécurité de votre compte Microsoft ou Google.
4. Avisez la personne-ressource TI de votre escadron ou votre superviseur.
5. Si de l'argent ou des coordonnées bancaires sont en jeu, appelez votre banque maintenant.

PARTIE 3

Mots de passe et validation en deux étapes

Long et unique

Les mots de passe piratés suivent presque toujours des modèles prévisibles. La longueur l'emporte.

✕ MOT DE PASSE FAIBLE

Piraté en quelques minutes par dictionnaire ou force brute.

`CadetsAir2024!`

nom de l'organisation · année · symbole à la fin

- ✕ Moins de 12 caractères
- ✕ Basé sur des noms, des années, des saisons ou des animaux
- ✕ Réutilisé sur d'autres sites

✓ PHRASE DE PASSE SOLIDE

Long et aléatoire, donc beaucoup plus difficile à pirater.

`érable-ORBITE-mardi-47canot`

mots aléatoires · un en MAJUSCULES · chiffres · traits d'union

- ✓ 12 caractères minimum, plus c'est long, mieux c'est
- ✓ Des mots aléatoires sans lien, pas une citation ni un dicton
- ✓ Unique pour chaque compte

N'utilisez jamais un mot de passe vu sur une diapositive, y compris ces exemples.

Protégez vos mots de passe

À éviter

- ✕ Un seul mot du dictionnaire, ou des substitutions comme m0t2p@sse
- ✕ Noms, dates de naissance, noms d'utilisateur ou numéro d'escadron
- ✕ Écrire ses mots de passe sur des papillons adhésifs
- ✕ Utiliser le même mot de passe partout
- ✕ Partager ses mots de passe, même avec des collègues

À faire

- ✓ Utilisez un gestionnaire de mots de passe : Bitwarden, 1Password, ou celui intégré à Google ou Microsoft
- ✓ Utilisez une clé d'accès quand elle est offerte : aucun mot de passe à voler
- ✓ Vérifiez si votre adresse a été exposée sur haveibeenpwned.com



Ne le partagez jamais

Ni avec des collègues, ni par courriel ou clavardage.



Vrais sites seulement

Vérifiez la barre d'adresse avant de le taper.



Activez la validation

Un mot de passe volé ne suffit alors plus.



Exposé ? Agissez

Changez-le aussitôt et avisez votre personne-ressource TI.

Activez la validation en deux étapes dès aujourd'hui

Microsoft 365 et Outlook

Compte professionnel ou scolaire

Allez à mysignins.microsoft.com/security-info > Ajouter une méthode de connexion > Microsoft Authenticator.

Outlook.com personnel

Allez à account.microsoft.com/security > Gérer mon mode de connexion > activez la vérification en deux étapes.

Gmail et Google

Tout compte Google

Allez à myaccount.google.com/security > Comment vous connecter à Google > Validation en deux étapes > Activer.

Ajoutez ensuite une méthode de secours

Ajoutez l'application Google Authenticator ou une clé d'accès pour ne pas dépendre des textos.

Quelle deuxième étape choisir ?

Clé d'accès ou clé de sécurité

La plus solide. Impossible à hameçonner.

Application d'authentification

Solide. Utilise la correspondance de chiffres.

Code par texto

Mieux que rien.

Comment les attaquants contournent l'AMF

Fatigue de l'AMF

Avec votre mot de passe en main, l'attaquant envoie demande sur demande, ou appelle en se faisant passer pour les TI, jusqu'à ce que vous appuyiez sur Approuver pour que ça cesse.

Signal d'alarme : Une demande que vous n'avez pas lancée, surtout tard le soir.

Attaque de l'intercepteur

Une fausse page de connexion transmet en temps réel votre mot de passe et votre approbation AMF au vrai site Microsoft ou Google. Cette technique a bondi de 139 % en 2026.

Signal d'alarme : La barre d'adresse n'affiche pas microsoft.com ou google.com.

Lisez la demande avant d'appuyer

Microsoft Authenticator vous demande de taper le chiffre affiché à l'écran de connexion. Google affiche l'appareil et le lieu. S'il n'y a pas d'écran de connexion devant vous, ou si les détails ne correspondent pas, appuyez sur Refuser, changez votre mot de passe et avisez votre personne-ressource TI.

PARTIE 4

Appareils, Wi-Fi et partage de fichiers

Logiciels malveillants : entrée et protection

En 2026, le logiciel malveillant le plus courant est le voleur d'information : il copie discrètement les mots de passe enregistrés et les sessions ouvertes. Le rançongiciel verrouille vos fichiers et exige une rançon.

Comment ils entrent

- Pièces jointes et fichiers partagés
- Faux CAPTCHA et fausses mises à jour du navigateur
- Logiciels piratés, mods de jeux et cracks
- Publicités et résultats de recherche malveillants
- Clés USB inconnues

Signes d'infection

- Fenêtres surgissantes, ou nouvelle page d'accueil
- Appareil lent, qui plante ou surchauffe
- Vos amis reçoivent des messages que vous n'avez pas envoyés
- Courriels de réinitialisation non demandés
- Programmes inconnus au démarrage

Protégez-vous

- Activez les mises à jour automatiques
- Gardez Microsoft Defender (Windows) ou XProtect (Mac) activé
- Installez les applications seulement à partir des boutiques officielles
- Sauvegardez vos fichiers importants, dont une copie hors ligne
- N'enregistrez pas vos mots de passe dans un navigateur partagé

Wi-Fi public et partage de fichiers

Sur un Wi-Fi public

- Confirmez le nom exact du réseau auprès du personnel : les faux points d'accès copient les vrais noms
- Utilisez le partage de connexion de votre téléphone ou un RPV fiable pour vous connecter
- Désactivez la connexion automatique aux réseaux ouverts
- Le cadenas veut seulement dire que la connexion est chiffrée, pas que le site est honnête

Pour partager des fichiers

- Utilisez OneDrive, SharePoint ou Google Drive de votre organisation, pas des comptes personnels
- Partagez avec des personnes précises, pas « Toute personne disposant du lien »
- Fixez une date d'expiration et retirez l'accès une fois terminé
- Ne mettez jamais l'information personnelle des cadets sur une clé USB non chiffrée

L'information des cadets est sensible : partagez le minimum, avec le moins de gens possible, le moins longtemps possible.

Huit habitudes qui bloquent la plupart des attaques

Vérifiez la vraie adresse de l'expéditeur

Survolez avant de cliquer

Ne balayez jamais un code QR pour vous connecter

Ne collez jamais une commande fournie par un site

N'entrez que les codes que vous avez demandés

Phrases de passe longues et uniques, et AMF

Vérifiez les demandes de paiement par téléphone

Signalez-le, même si vous avez cliqué

Des questions ?

K@K2ESEC.COM

En cas de doute, ne cliquez pas. Signalez-le.



ANNEXE

Guides de configuration et références

Administrateurs et propriétaires d'appareils

Admins Microsoft 365

- Exigez l'AMF pour tous : centre d'administration Microsoft Entra > activez les paramètres de sécurité par défaut, ou utilisez l'accès conditionnel
- Bloquez le flux de connexion par code d'appareil pour les utilisateurs qui n'en ont pas besoin (Accès conditionnel > Flux d'authentification)
- Activez Liens fiables, Pièces jointes fiables et la purge automatique zéro heure dans Defender pour Office 365

Admins Google Workspace

- Console d'administration > Sécurité > Authentification > Validation en deux étapes > Autoriser les utilisateurs à l'activer
- Faites inscrire tout le monde, puis activez l'application forcée pour que personne ne soit bloqué
- Activez la Protection avancée pour les comptes d'administration et des finances

Vérifiez votre propre ordinateur

- Windows : Démarrer > Sécurité Windows > Protection contre les virus et menaces. Un crochet vert signifie que vous êtes protégé; assurez-vous que la protection en temps réel est activée
- Mac : Réglages Système > Général > Mise à jour de logiciels > Mises à jour automatiques > activez « Installer les réponses de sécurité et les fichiers système » (garde XProtect à jour)

Références

1. Microsoft Threat Intelligence, “Email threat landscape: Q1 2026 trends and insights” and “Q2 2026 trends and insights,” Microsoft Security Blog, 2026.
2. KnowBe4, “Phishing Threat Trends Report, Volume 7,” 2026.
3. Google, “Our latest fraud and scams advisory,” June 2026.
4. Proofpoint, recherches sur l'hameçonnage par code d'appareil dans Microsoft 365, janvier et mai 2026.
5. The Hacker News, “Device code phishing hits 340+ Microsoft 365 organizations,” March 2026.
6. Centre antifraude du Canada, « Les 10 fraudes les plus courantes en 2025 » et « Tendances en matière de fraude : six premiers mois de 2026 ». antifraudcentre-centreantifraude.ca
7. Centre antifraude du Canada, communiqué sur une fraude par réacheminement de paiement, 13 mai 2026.
8. Federal Trade Commission des États-Unis, « How to spot a CAPTCHA scam », juin 2026.
9. Centre canadien pour la cybersécurité, conseils sur les phrases de passe et l'authentification multifacteur. cyber.gc.ca