Trousse de sensibilisation à la cybersécurité

Une communauté fière d'adopter un comportement cyberprudent

UNIVERSITÉ LAVAL

Objectif de la trousse

La trousse de sensibilisation est un outil destiné aux gestionnaires de l'Université Laval et vise le partage d'informations sur les bons comportements à adopter en matière de cybersécurité. Cet outil permet également d'encourager les discussions au sein des équipes de travail afin d'élargir leurs connaissances pour se protéger des cyberattaques.

Quels sont les outils de la trousse ?

Voici les outils présentés dans cette trousse :

- 7 fiches thématiques résumant les points essentiels à retenir pour développer un comportement numérique responsable
- Liens vers des vidéos de sensibilisation
- Résumé des bonnes pratiques à adopter
- Quiz pour tester les connaissances du personnel

Comment utiliser la trousse ?

Vous pouvez débuter l'utilisation de la trousse lors d'une réunion d'équipe déjà prévue à l'agenda. Allouez environ 15 minutes, au début de votre rencontre, pour parler des thèmes de la cybersécurité. Il est conseillé d'aborder deux ou trois thèmes par rencontre. Utilisez également les outils tels que les vidéos et le quiz afin de tester les connaissances du personnel.

Retrouvez davantage d'informations et de ressources sur la page Web destinée à la cybersécurité. Il est aussi possible d'y signaler un incident et d'y trouver les coordonnées des centres de services TI afin d'obtenir de l'aide.

ulaval.ca/cybersecurite

Les thèmes clés de la cybersécurité

Les thèmes abordés dans cette trousse sont les suivants:

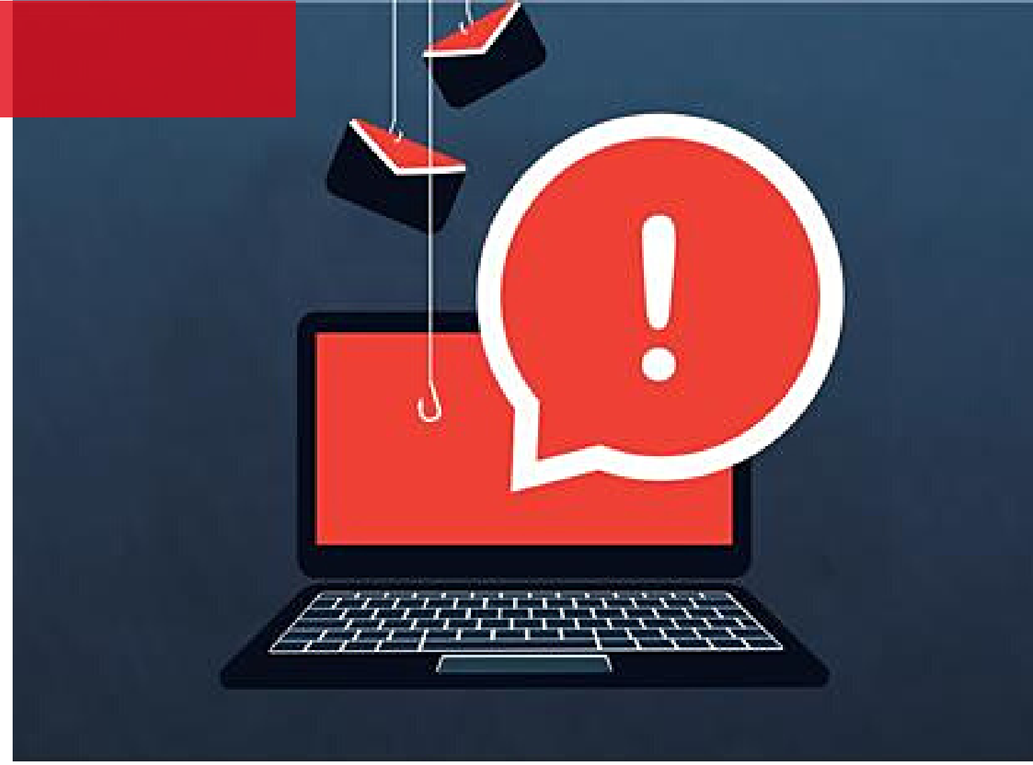
1. **Hameçonnage**
2. **Virus et rançongiciels**
3. **Mots de passe**
4. **Authentification multifactorielle**
5. **Sécurité des appareils mobiles**
6. **Sécurité Wi-Fi**
7. **Ingénierie sociale ou l'art de la manipulation**

1. Hameçonnage

Comment reconnaître une tentative d’hameçonnage ?

- Les tentatives d’hameçonnage prennent généralement la forme d’un courriel ou d’un texto contenant un hyperlien à cliquer ou une pièce jointe inconnue à télécharger.
- L’expéditeur du message vous est souvent inconnu et s’adresse à vous avec une formule d’appel générale telle que «Madame, Monsieur» ou «Cher client».
- Le message vous demande de confirmer des renseignements personnels en évoquant diverses raisons: éviter la fermeture d’un compte bancaire, replanifier la livraison d’un colis, confirmer un abonnement, etc.
- Un contexte d’urgence est souvent établi dans le message afin de vous inciter à agir rapidement. Un ton menaçant peut également être utilisé.
- L’expéditeur utilise souvent une formule générale telle que «Secteur de la sécurité informatique» ou «Département du service à la clientèle» pour signer le message.

De la fausse information visant à vous piéger peut aussi circuler dans les médias sociaux. Faites preuve de vigilance et ne cliquez pas sur des hyperliens douteux menant à un site que vous ne connaissez pas.



Saviez-vous que...

Pour signaler un courriel d’hameçonnage dans Outlook, vous pouvez utiliser le bouton Signaler le message (ou Report Message) situé dans le menu Message. Sélectionnez ensuite Hameçonnage (Phishing). Ainsi, vous ne recevrez plus de courriels provenant de cet expéditeur. Si vous avez mordu à l'hameçon, informez votre centre de services TI.

Vidéo

Se prémunir contre l'hameçonnage

Lien Youtube

2. Virus et rançongiciels

Comment reconnaître une tentative d’attaque de rançongiciel ?

- Le rançongiciel se cache habituellement dans un fichier joint à un courriel ou peut être téléchargé dans une fausse page Web accessible par un hyperlien.
- Avant de cliquer sur un hyperlien, survolez-le avec votre souris pour en voir l’URL et vous assurer qu’il s’agit d’une adresse fiable. Si vous ne connaissez pas le site ou que les mots de l’adresse sont mal orthographiés, méfiez-vous et n’ouvrez pas l’hyperlien.
- Les fausses pages Web créées par les fraudeurs copient les couleurs et les logos d’organismes ou entreprises reconnus pour vous faire croire qu’il s’agit de sites légitimes et vous incitent à télécharger le logiciel ou le document.
- Les sites frauduleux contiennent généralement des fautes d’orthographe et de grammaire ainsi que des typographies et couleurs d’écriture différentes.
- L’expéditeur du courriel utilise souvent une signature générale telle que «Secteur de la sécurité informatique» pour donner de la crédibilité à son contenu.

Saviez-vous que…

Lorsque le rançongiciel a terminé son travail, une fenêtre s’affiche. On y mentionne que vos fichiers ont été chiffrés et que vous devez verser un montant d’argent pour récupérer vos données. Ne payez pas la rançon demandée et contactez rapidement votre centre de services TI qui saura vous aider.

Vidéo

Protégez-vous des virus et rançongiciels

Lien Youtube

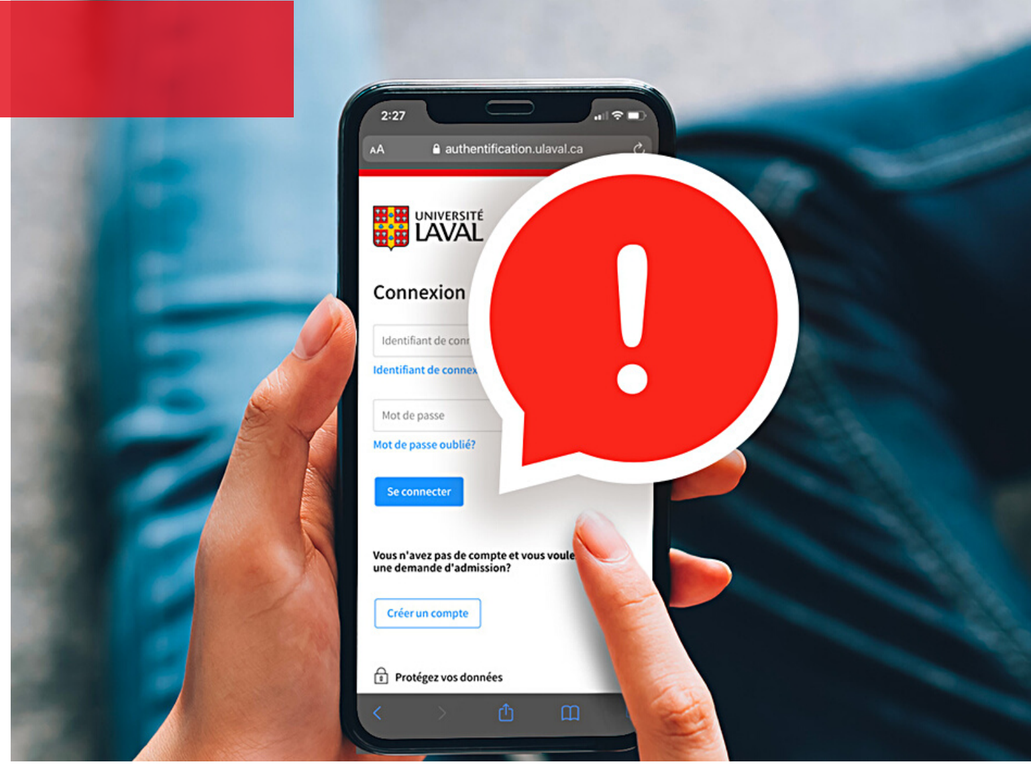
3. Mots de passe

Choisir un mot de passe robuste

Le choix d'un mot de passe ne doit pas être négligé et différents éléments sont à prendre en compte afin de configurer un mot de passe fort et impossible à trouver.

- Composez des mots de passe d'au moins 12 caractères. Utilisez un mélange de lettres, chiffres, caractères spéciaux, majuscules.
- N'utilisez pas d'informations liées à votre vie personnelle dans vos mots de passe. Votre adresse, date de naissance ou le nom de votre animal de compagnie sont à proscrire.
- Évitez d'insérer une lettre majuscule au début du mot de passe et de remplacer des lettres par des symboles qui leur ressemblent (exemple: S par $). Ces pratiques, largement répandues, sont faciles à retenir, mais aussi faciles à deviner.
- Puisqu'il devient de plus en difficile de se souvenir de tous les mots de passe, pensez à utiliser un gestionnaire de mots de passe. Vous n'aurez alors qu'à retenir le mot de passe principal, qui déverrouille le gestionnaire. Ce mot de passe doit bien sûr être très robuste et totalement unique.

Si vous pensez que l'un de vos mots de passe a été dérobé, modifiez-le sans tarder et communiquez avec votre centre de services TI.

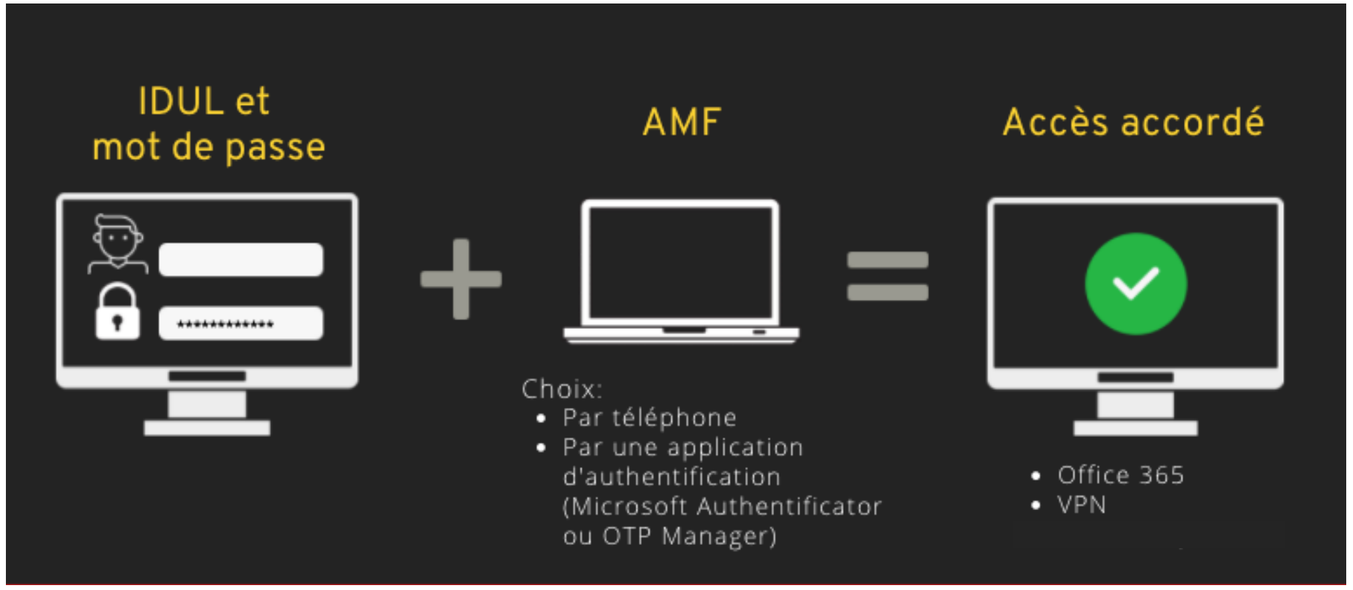


Saviez-vous que...

Il est préférable d'utiliser un mot de passe robuste et différent pour chacun de vos comptes. Refusez aussi l'option de connexion automatique lorsqu'elle vous est proposée par un navigateur, un logiciel ou une application.

4. Authentification multifactorielle (AMF)

L’authentification multifactorielle (AMF) renforce la protection de vos comptes. En exigeant, en plus du mot de passe, au moins une autre méthode d’authentification, elle permet de vérifier que c’est bel et bien le propriétaire d’un compte qui tente de s’y connecter. Ainsi, un pirate informatique qui aurait réussi à dérober l’un de vos mots de passe ne parviendrait quand même pas à accéder à vos comptes puisqu’il ne pourrait passer la deuxième étape d’authentification.



Saviez-vous que…

L'Université Laval rendra disponible l'authentification multifactorielle (AMF) aux membres de sa communauté, à l'automne 2021. Celle-ci sera d'abord offerte sur la base d'une participation volontaire. Ensuite, l'AMF deviendra obligatoire pour l'ensemble de la communauté universitaire, à partir de l'hiver 2022.

5. Sécurité des appareils mobiles

Avant de télécharger une application, recherchez des informations complémentaires sur celle-ci et validez sa provenance. La source de téléchargement doit être fiable.

Prenez aussi soin de sécuriser tous vos appareils mobiles, particulièrement lorsque vous en configurez un nouveau, en mettant en pratique quelques actions simples:

- Définissez un code d’accès à votre appareil et activez le verrouillage après un délai d’inactivité.
- Désactivez les connexions Bluetooth et le Wi-Fi lorsque vous n’en avez pas besoin.
- Mettez régulièrement à jour les applications et le système d’exploitation de vos appareils.
- Ne partagez pas d’informations sensibles par texto ou courriel.
- Bloquez les numéros de téléphone qui vous envoient des messages non désirés.
- Synchronisez vos appareils avec un ordinateur pour sauvegarder vos données.

Saviez-vous que...

Saviez-vous qu'un appareil mobile contient autant de renseignements personnels qu'un ordinateur ? Les appareils mobiles sont de plus en plus la cible des fraudeurs puisque nous les utilisons tous les jours. Surtout, la plupart du temps, ces derniers ne présentent pas des mesures de sécurité équivalentes à votre environnement de travail.

6. Sécurité Wi-Fi

- Ne vous connectez jamais à un réseau public non sécurisé. Méfiez-vous d'un réseau offert gratuitement et sans mot de passe dans un endroit public.
- Privilégiez l'usage du réseau VPN lorsque vous êtes à l'extérieur du campus.
- Assurez-vous que vos mises à jour de logiciels et anti-virus sont effectuées afin que les pirates ne profitent pas des failles des versions antérieures.

Que faire si vous êtes victime d'une cyberattaque par l'entremise d'un réseau Wi-Fi ?

- Ne débranchez ou n'éteignez pas votre ordinateur ou votre appareil. Gardez-le ouvert afin de préserver des traces et des preuves de l'attaque.
- Déconnectez votre appareil du réseau Wi-Fi qui était utilisé.
- Si l'attaque a infecté un appareil de l'Université, avertissez rapidement votre centre de services TI. Si votre appareil personnel est attaqué, communiquez avec un informaticien.
- Mémorisez et notez le plus d'éléments possibles à propos de l'attaque. Ils seront utiles pour les personnes qui prendront l'incident en charge.

Saviez-vous que...

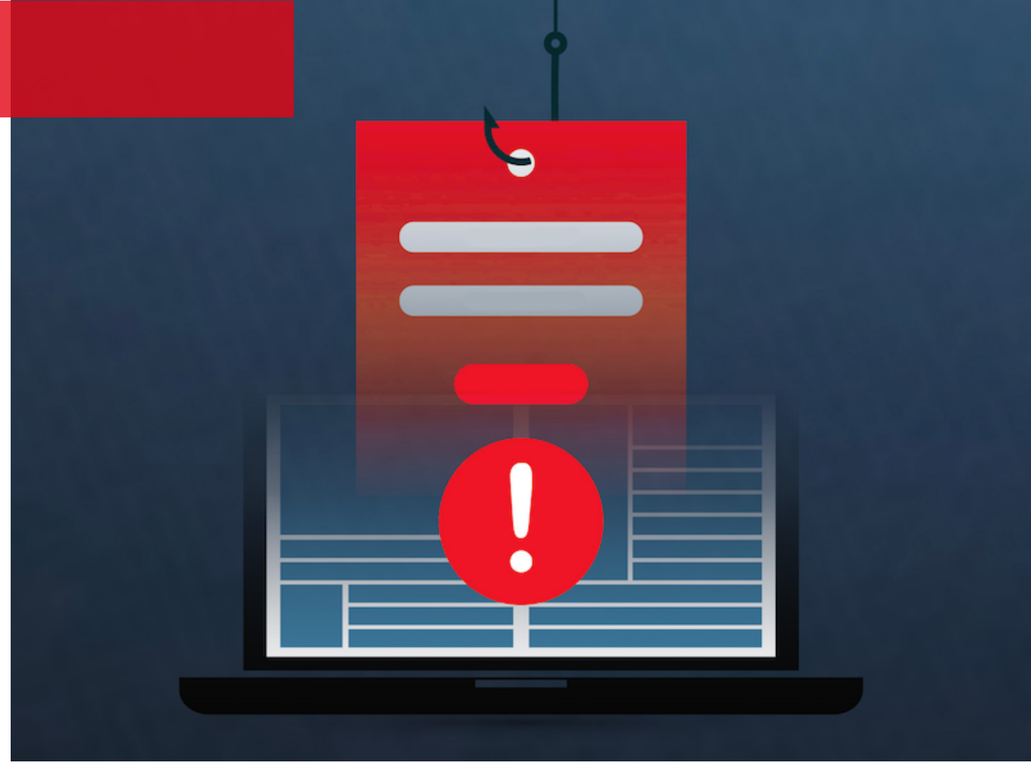
Les réseaux publics peuvent être mal protégés. Un réseau public d'apparence légitime peut cacher un réseau parrallèle mis en place par un cybercriminel. Ce dernier pourra alors intercepter les communications des personnes qui s'y connectent.

7. Ingénierie sociale ou l'art de la manipulation

L’ingénierie sociale est une technique de manipulation utilisée pour inciter une personne à transmettre elle-même des données sensibles.

Comment reconnaître l’ingénierie sociale?

- Dans le contexte d’un courriel ou d’un échange de plusieurs messages, la personne avec qui vous discutez pourrait vous amener à ouvrir une pièce jointe ou à cliquer sur un hyperlien. Un programme malveillant peut alors être installé et le fraudeur peut prendre le contrôle de votre ordinateur à distance.
- Vous pourriez recevoir un appel téléphonique au cours duquel votre interlocuteur cherche à vous soutirer des informations confidentielles.
- Les fraudeurs peuvent abandonner volontairement une clé USB ou un autre dispositif électronique contenant un virus ou un programme malveillant dans un espace public. Une fois branché à un ordinateur, le virus ou le logiciel s’active et permet au cybercriminel de s’infiltrer dans le système d’une organisation.
- Le cybercriminel peut tenter d’accéder à une zone de travail sécurisée par la technique de talonnage. Il pourrait entrer en contact avec vous et se faire passer pour un partenaire externe de l’organisation ou suivre un employé autorisé.



Saviez-vous que...

Les réseaux sociaux sont de plus en plus utilisés par les cybercriminels qui tentent de connaître vos comportements, vos habitudes et de voir vos liens avec d’autres personnes. Faites preuve de vigilance, ces renseignements pourraient être utilisés pour vous manipuler.

Avez-vous un comportement cyberprudent ?

Voici un résumé des bonnes pratiques pour se protéger des cyberattaques

Mots de passe

Choisissez des mots de passe complexes, difficiles à deviner et évitez de les réutiliser.

Courriels

Restez vigilant face aux courriels que vous recevez. Vérifiez l'identité de l'expéditeur.

Hyperliens

Ne cliquez pas sur un hyperlien dont vous ne connaissez pas l'origine ou que vous n'avez pas sollicité.

Pièces jointes

N'ouvrez pas de pièce jointe dont vous n'êtes pas sûr de la source, ni de quoi il s'agit.

Données personnelles

Ne partagez pas vos données personnelles, à moins qu'il soit vraiment nécessaire de le faire.

Wi-Fi

Utilisez des réseaux sécurisés pour vous connecter et préférez le VPN de l'Université Laval.

Mises à jour

Effectuez régulièrement les mises à jour de vos systèmes et logiciels.

Réseaux sociaux

Protégez votre identité numérique en mettant à jour vos préférences. Ne cliquez pas sur des liens douteux.

Sauvegardes

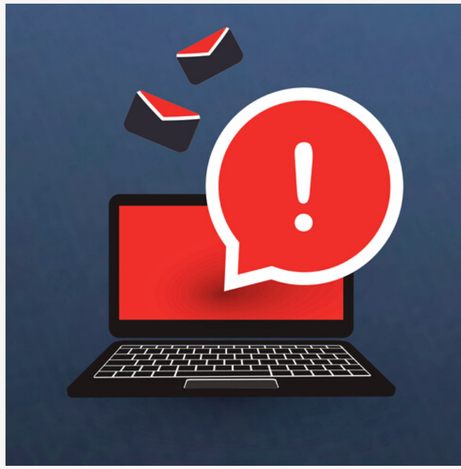
Sauvergardez vos données et fichiers et assurez-vous d'avoir une copie, par exemple, sur One Drive.

Anti-virus

Protégez tous vos appareils avec un anti-virus.

Signalez une fraude

Contactez votre centre de services TI pour signaler une fraude.



QUIZ

10 QUESTIONS

Partagez les questions à l'écran et invitez l'équipe à y répondre. Trouvez le corrigé suite à chaque question.

Sources des questions: imaa.ca, avast.com

QUESTION 1

Il est important de vérifier régulièrement les mises à jour à effectuer sur mes appareils électroniques et de les faire sans tarder.

A) Vrai

B) Faux

Réponse : Vrai

Les mises à jour doivent être effectuées régulièrement, car elles contiennent souvent des correctifs aux failles de sécurité présentes dans le code initial. En téléchargeant les dernières versions des logiciels de sécurité, des navigateurs Web et des systèmes d'exploitation, vous prenez les meilleures mesures de protection contre les virus, les maliciels et les autres menaces en ligne.

QUESTION 2

Laquelle ou lesquelles des mesures ci-dessous vous semblent importantes en matière de cybersécurité ?

A) L'installation d'un anti-virus
B) L'utilisation de mots de passe robustes
C) L'utilisation de l'authentification multifactorielle
D) La formation pour le développement d'un comportement cyberprudent
E) Toutes ces réponses

Réponse : E

Plusieurs éléments sont importants en matière de cybersécurité. Que ce soit les antivirus, les mots de passe robustes, l'authentification multifactorielle et bien sûr nos comportements numériques. Ces derniers sont souvent la porte d'entrée utilisée par les cybercriminels. La formation est alors un élément essentiel pour l'adoption d'un comportement cyberprudent.

QUESTION 3

Un ordinateur ne peut être victime d'une cyberattaque si l'utilisateur dispose d'un réseau privé virtuel actif (VPN - virtual private network).

- Vrai
- Faux

Réponse : Faux

Un VPN est un "tunnel virtuel" entre votre appareil et Internet. Lorsqu'il est actif, il est plus difficile d'intercepter vos données. Toutefois, il ne constitue pas une solution de cybersécurité à lui seul. Les appareils peuvent être infectés ou attaqués lorsqu'un VPN est actif, surtout s'il est le seul outil de protection dont dispose l'organisation (ce qui n'est pas le cas pour l'Université Laval).

QUESTION 4

Quel type de Wi-Fi est sécuritaire pour se connecter lorsque vous êtes à l'extérieur du bureau ? Plusieurs choix possibles.

A) Les réseaux Wi-Fi payant dans les transports et les hôtels
B) Les réseaux Wi-Fi privés (ex.: chez un ami)
C) Les réseaux Wi-Fi ouverts et gratuits dans les cafés, les restaurants, les musées, les bâtiments publics, les aéroports et les gares.

Réponse : B

Utiliser un réseau Wi-Fi public gratuit ou prépayé comporte des risques, que vous vous connectiez depuis un appareil personnel ou professionnel. Lorsque vous utilisez un réseau Wi-Fi privé, vous savez qui l'a configuré et vous avez la quasi-certitude que les personnes qui s'y connectent (collègues, famille, amis) ne sont pas mal intentionnées.

QUESTION 5

Lequel des mots de passe suivant est le plus robuste ?

A) B44C9490
B) 2x3b4y8m
C) laCyberSecurite
D) Du&Vine#Fa63Ka

Réponse : D

Le mot de passe Du&Vine#Fa63Ka présente plus de 12 caractères et n'utilise pas de mots isolés du dictionnaire, de combinaisons clavier prévisibles ou de chiffres répétés. Également, il ne présente pas d'éléments relatifs à la vie privée d'une personne.

QUESTION 6

Il est important de changer ses mots de passe 2 à 3 fois par année.

- Vrai
- Faux

Réponse : Faux

En changeant trop souvent vos mots de passe, vous augmentez vos chances de les oublier. Les études démontrent que les personnes à qui on demande de changer les mots de passe fréquemment vont en sélectionner des plus faibles ou vont utiliser des modèles similaires. Il vaut mieux privilégier une phrase de passe robuste, sécurisée dans un gestionnaire de mots de passe et que l'on change uniquement en cas de compromission.

QUESTION 7

Un cybercriminel a réussi sa tentative d'hameçonnage auprès d'un membre du personnel. Quelle est la conséquence possible de cette cyberattaque ?

A) Un rançongiciel peut être déployé au sein de l'organisation
B) La personne peut être victime d'un vol d'identité ou d'une fraude
C) Le cybercriminel peut s'infiltrer dans les réseaux de l'organisation
D) Toutes ces réponses

Réponse : D

Plusieurs conséquences sont possibles à la suite d'une attaque par hameçonnage comme le vol d'identité et la fraude bancaire. L'infiltration d'un cybercriminel dans l'organisation peut aussi causer des dommages à l'aide d'un rançongiciel qui peut bloquer l'accès à des données importantes. Sachez que la majorité des cyberattaques débutent par un courriel d'hameçonnage.

QUESTION 8

Que faut-il faire pour reconnaître un courriel frauduleux ?
Plusieurs choix possibles.

A) Vérifier l'adresse de l'expéditeur
B) Vérifier l'orthographe
C) Dans le doute, valider par un autre canal de communication
D) Rechercher les éléments douteux dans le message
E) Identifier si on me demande d'agir dans un contexte d'urgence
F) Toutes ces réponses

Réponse : F

Il est important de toujours vérifier l'adresse d'envoi et l'orthographe du message, mais aussi d'identifier les éléments douteux et si le message présente un contexte d'urgence. Attention, vous pouvez aussi recevoir un message d'une vraie adresse courriel qui a été compromise. Dans ce cas, si le courriel provient d'une personne que vous connaissez, contactez-la par un autre canal de communication et informez un centre de services TI.

QUESTION 9

Les courriels frauduleux ont pour objectif de soutirer de l'argent.

- Vrai
- Faux

Réponse : Faux

Les cyberattaques ont très souvent pour objectif de récolter vos informations personnelles. Elles peuvent aussi avoir pour objectif d'installer des logiciels malveillants, des virus ou des rançongiciels sur vos appareils. Il est important de se méfier de tout courriel d'apparence frauduleuse.

QUESTION 10

Vous avez trouvé une nouvelle application intéressante, mais elle n'est pas dans le magasin d'Apple ou de Google Apps.

A) Vous pouvez la télécharger.
B) Vous devez vous méfier.

Réponse : B

Il faut toujours privilégier les applications vérifiées dans des magasins d'applications. Une arnaque a eu lieu pendant la crise du COVID-19. Une application rendue disponible disait pouvoir suivre le nombre de cas au Canada, mais elle était plutôt un rançongiciel qui chiffrait le contenu des cellulaires. L'application demandait ensuite une rançon pour que les victimes puissent retrouver leurs données.

Merci de contribuer au développement d'un comportement numérique responsable au sein de votre communauté universitaire.