9 astuces pour éviter la FRAUDE sur Internet

Avec toutes les histoires de fraude et de vol d'identité qui se déroulent sur Internet, il est normal d'avoir peur et d'être intimidé par ce vaste monde numérique. Et pourtant, Internet rend la vie plus agréable dans la mesure que l'on sache comment naviguer sécuritairement.

Avec les informations qui suivent vos renseignements personnels seront mieux à l'abri des fraudeurs et vous pourrez désormais naviguer l'esprit tranquille sur Internet.

ASTUCE #1

Créer des mots de passe sécuritaires

C’est la base! Pour protéger vos renseignements personnels, vos comptes bancaires et votre vie privée, il vous faut des mots de passe robustes. Voici la liste des erreurs communes à éviter.

- **Trop court** : Un mot de passe de 8 caractères et moins est deviné par un ordinateur en seulement quelques secondes. (Référence)

- **Contient des renseignements personnels** : Évitez dans vos mots de passe d’inclure le nom d’un membre de la famille ou d’un animal de compagnie, une adresse, une date de naissance, les paroles d’une chanson que vous aimez, etc. Ces informations sont facilement accessibles sur les réseaux sociaux et les fraudeurs les utilisent pour deviner les mots de passe.

- **Trop évident** : Les termes comme "password'', ‘’123456’, “qwerty”, “1234567890” font partie de la liste des 200 mots de passe les plus utilisés. Changez au besoin l’un de vos mots de passe s’il ressemble ou se retrouve dans cette liste.

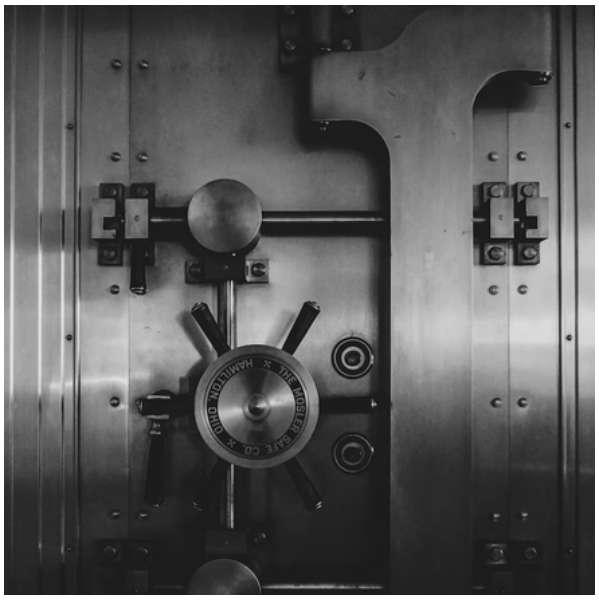
- **Un seul mot de passe pour tous les comptes** : Si votre mot de passe est deviné, alors tous vos comptes en ligne sont compromis. L’idéal est d’en utiliser un pour chaque compte que vous possédez.

Saviez-vous que 81% des brèches informatiques sont causées par des mots de passe faibles?

ASTUCE #1 - SUITE

Créer des mots de passe sécuritaires

Pour avoir un mot de passe sûr, robuste et sécuritaire, il est fortement recommandé d'avoir un **minimum de 16 caractères**. Pour y arriver, la recette magique est toute simple. Il vous suffit d'utiliser une **combinaison de trois ou quatre mots**. Voici quelques exemples:



"AimerPoutineGaspésie!"

“DimancheC4féChevrolet”

“HamburgerKetchupMay0”

“B@teauAtlantiqueAfrique"

"BatmanVilainJ0ker"

Inspirez-vous de votre environnement ou d'un certain passage de votre vie. Ainsi, vos futurs mots de passe vont être simples à retenir et vraiment sécuritaires dus à leur longueur. Au final, assurez-vous que votre mot de passe:

- Est composé d'un minimum de 16 caractères
- Ne contient aucun renseignement personnel
- Est unique pour chacun de vos comptes en ligne
- Contient une variation de lettres, chiffres et symboles (optionnel)

ASTUCE #2

Activez l'authentification à deux facteurs

Termes similaires: Validation en deux étapes, la double authentification, authentification à double facteur, authentification multifactorielle ou vérification en deux étapes.

Lorsque vous vous connectez à l'un de vos comptes, en plus de votre mot de passe, l'authentification à deux facteurs exige une deuxième preuve d'identité comme :

- une question de sécurité dont vous connaissez la réponse
- un code envoyé à votre téléphone
- un NIP
- une authentification ou confirmation par message texte

Vous êtes **le SEUL** à détenir ces informations et c'est pour cette raison que cette deuxième barrière augmente de façon significative votre sécurité en ligne. En plus, elle vous protège contre :

- les vols de vos mots de passe
- 100% des bots informatiques
- 96% des attaques par hameçonnage
- et 76% des attaques ciblées

ASTUCE #2 - SUITE

Activez l'authentification à deux facteurs

La plupart des réseaux sociaux, institutions bancaires et autres comptes en ligne offrent la possibilité d'activer l'authentification à deux facteurs. À chaque fois qu'un site web, un appareil ou une application vous le propose, activez-le! En voici quelques uns:

- Google / YouTube
- Facebook
- Instagram
- TikTok
- Desjardins - Acces D

ASTUCE #3

Attention aux réseaux Wi-Fi publics non sécurisés

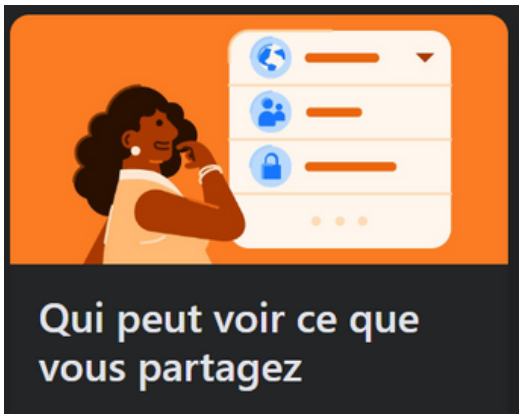
Puisqu'il est facile de se connecter à ces réseaux sans mot de passe, les pirates sont en mesure de les intégrer et d'espionner les données personnelles qui transitent. En d'autres mots, lorsque vous êtes connecté à un réseau Wi-Fi public **non sécurisé** de votre café du coin, un fraudeur peut savoir TOUT ce que vous faites sur Internet : les pages web que vous consultez, les mots de passe que vous saisissez, les cartes de crédit que vous utilisez, etc 😱😱😱.

Saviez-vous qu'en 2019, les sommes perdues au Canada contre la fraude s'élèvent à 96 163 328$ (Référence)

ASTUCE #4

Compléter l'assistance de confidentialité de Facebook

Les réseaux sociaux sont une mine d'or pour les fraudeurs. Toutes les informations que vous publiez peuvent être accessibles par n'importe qui et utilisées à votre insu. Pour protéger votre compte Facebook, il existe un outil qui permet en seulement quelques clics de protéger votre compte rapidement. Cliquez ici et complétez les trois sections suivantes:



Assurez-vous de choisir qui peut voir les informations de votre profil tel que : numéro de téléphone, adresse courriel, date d'anniversaire, relation, amis et autres.

Mettez à jour votre mot de passe si ce dernier n'est pas robuste, configurez l'authentification à deux facteurs et activez les alertes de connexion.

Vous pouvez contrôler qui peut vous envoyer des invitations. Préférez-vous tout le monde ou seulement les amis de vos amis?

HAMEÇONNAGE

L’hameçonnage est le troisième type de fraude en ligne le plus courant au Canada. C’est quand un cybercriminel prétend être une organisation légitime et qui va essayer de voler des données confidentielles.

Senior Informatique

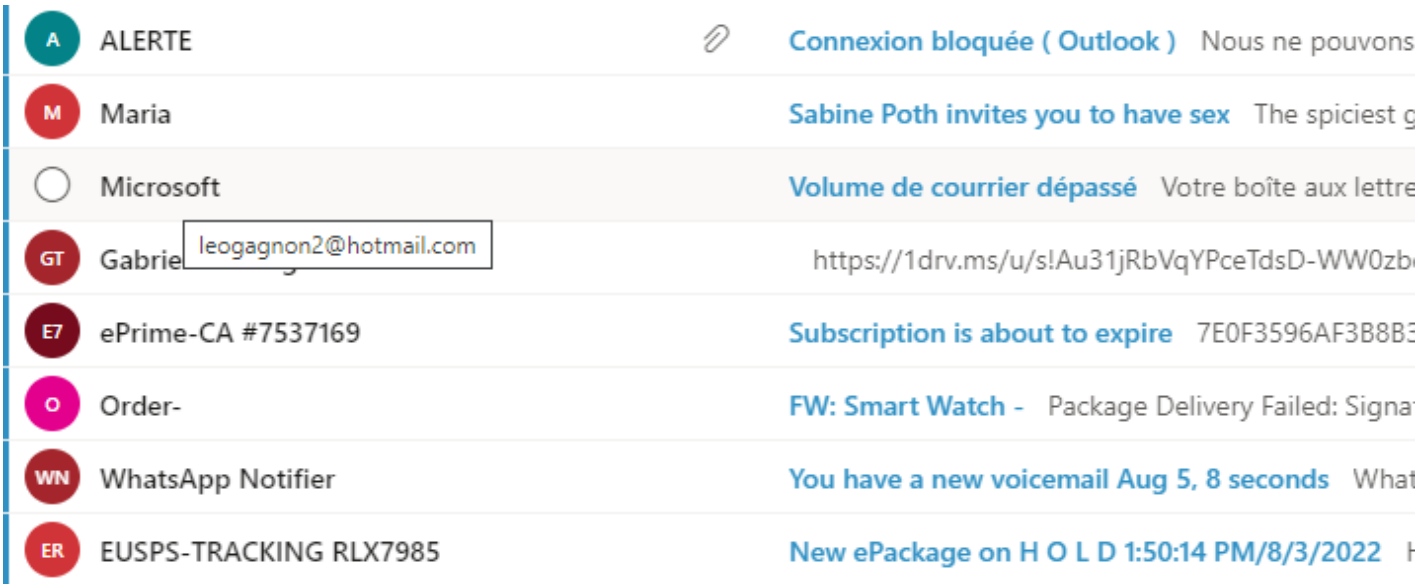
twinmolloy@gmail.com
seniorinformatique.ca

À quoi ressemble un message d'hameçonnage?

Comme pour un pécheur qui essaie divers hameçons, un fraudeur aussi essaiera différentes approches. L'hameçonnage peut prendre la forme d'un courriel, d'un SMS ou d'une page web. Il peut se faire passer pour votre banque, votre organisation et même vos amis. En règle générale, les tentatives d'hameçonnage ont pour objectif de **jouer avec vos émotions** et vous **inciter à passer à l'action**. En voici quelques exemples :

- Fermeture imminente de votre compte en banque
- Vous avez GAGNÉ à la loterie, réclamez votre prix!
- Une offre IRRÉSISTIBLE se déroule en ce moment
- Tentative échouée pour vous livrer un colis
- Un ami vous demande de l'aide

Exemples d'hameçonnage par courriel dans lequel il y a soi un lien ou une pièce jointe ... sûrement un virus!!!



Les scénarios sont infinis. Lorsque vous recevez un message, prenez votre temps et appliquez les astuces suivantes :

ASTUCE #5

Ne cliquez sur aucun lien et pièce jointe

Elles paraissent inoffensives à première vue, mais ces liens peuvent contenir des logiciels malveillants, des ransomwares ou d'autres menaces en ligne. Par exemple, il existe des virus dont leur seul objectif est de voler vos mots de passe enregistrés sur votre navigateur (Edge, Chrome, Firefox, etc). Méfiez-vous!

Pour vérifier la légitimité d'un lien, vous pouvez survoler votre curseur dessus (**sans cliquer**) et l'url devrait apparaître en bas à gauche de votre écran.

ASTUCE #6

Validez l'adresse courriel

L'adresse courriel peut aussi être trompeuse et contenir des variations de caractères. Exemple: support@tech.com versus supp0rt@tech.com sont deux adresses visiblement pareilles mais complètement différentes.

ASTUCE #7

Vérifier l'authenticité du message

Que le contenu du message soit véridique ou pas, au moindre doute contactez l'expéditeur par le moyen que vous utilisez normalement. Et notez bien ceci, **NE RÉPONDEZ PAS** au message tant que son authenticité n'est pas validé.

Anecdote : Ma mère a envoyé un avertissement par courriel à tous ses contacts. Je l'ai contactée par téléphone et non par courriel pour valider qu'elle va bien et constater que son compte de messagerie s'est fait pirater. En protégeant son compte à nouveau, j'ai remarqué que le pirate a obtenu l'adresse courriel de tous ceux et celles qui ont répondu au message.

ASTUCE #8

Trouvez des incohérences

Les messages contenant des fautes d'orthographe, et même des images floues sont à éviter.

ASTUCE #9

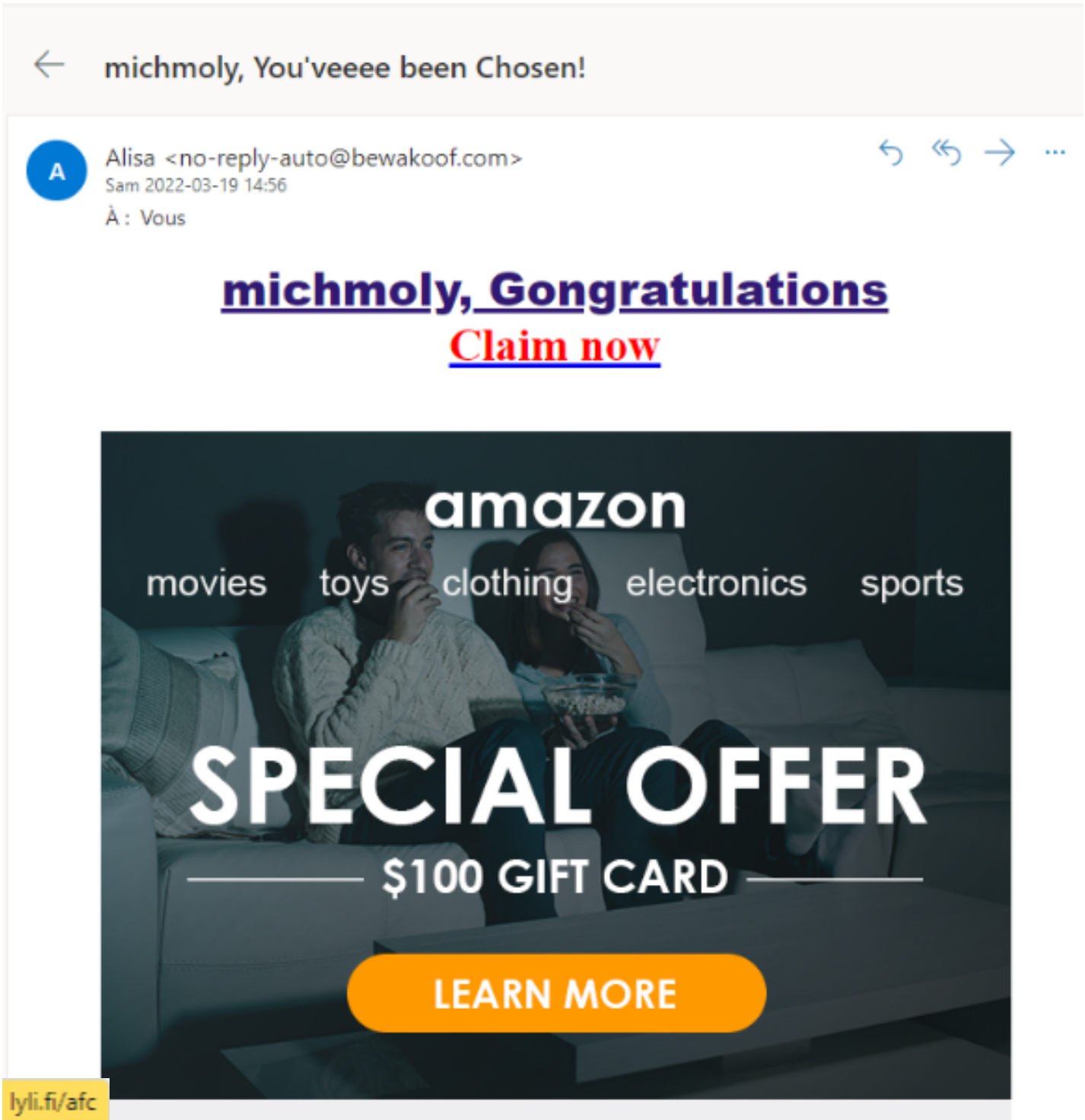
Méfiez-vous de vos ennemis et encore plus de vos amis

Une autre méthode d'hameçonnage couramment présente en ligne consiste à pirater un compte de l'un de vos contacts et de l'utiliser contre vous. Encore une fois, utilisez les astuces ci-haut pour protéger votre ami et vous.

Exemples d'hameçonnage

Par courriel

Ceci est un bon exemple d'une tentative d'hameçonnage par courriel. Trouvez les erreurs :



Exemples d'hameçonnage - SUITE

Par courriel

michmoly, You'veeee been Chosen!

Mauvaise adresse courriel n'appartenant pas à Amazon

A Alisa <no-reply-auto@bewakoof.com>
Sam 2022-03-19 14:56
À : Vous

Faute d'orthographe

michmoly, Gongratulations

Pseudonyme?!

Claim now

Incitation à passer à l'action

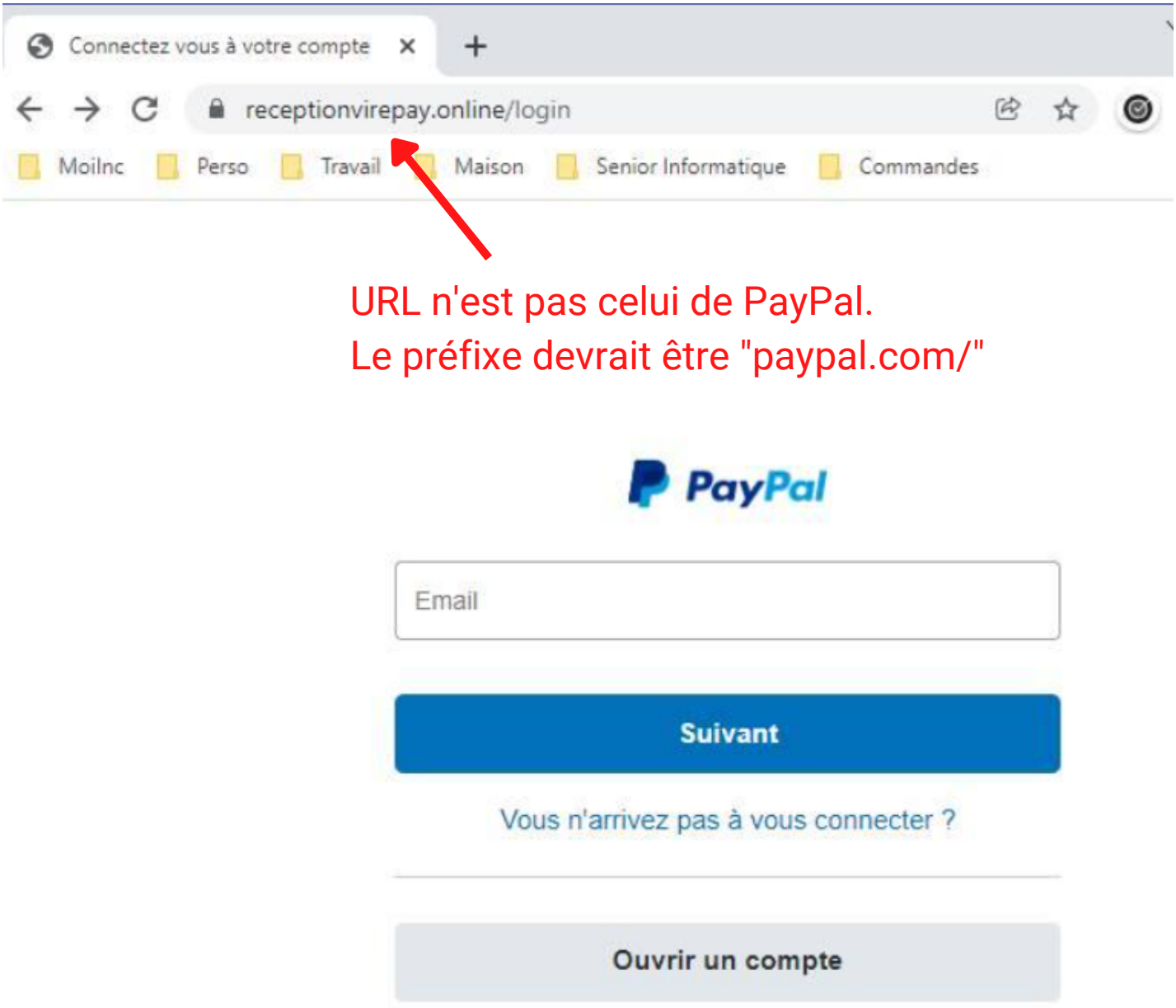
lyli.fi/afc

En survolant le bouton "LEARN MORE" avec la souris, un lien douteux apparaît en bas à gauche de l'écran.

Exemples d'hameçonnage

Par page web

Ceci est une copie de la page de connexion du très populaire système de service de paiement en ligne PayPal. Elle permet de voler les informations de connexion.



Félicitations! En passant à l'action, vous venez de renforcer votre sécurité sur Internet. Continuez à rester à l'affût des tendances sur la fraude et protéger les autres en partageant vos nouvelles connaissances.

Et n'oubliez pas, la meilleure protection en ligne demeure votre vigilance et votre esprit critique. Au moindre doute, écoutez votre instinct ☺

Au plaisir!

Michael & Richard Molloy
Senior Informatique