Techno habile

Scénario

Avec un financement du
Canada

Habilo Médias

YWCA CANADA
A TURNING POINT FOR WOMEN
UN POINT TOURNANT POUR LES FEMMES

1. Bienvenue à l'atelier *Découvrir la sécurité en ligne*.

Il y aura une période de questions à la fin, mais je vous invite tout de même à lever la main pour poser toute question qui surgirait en cours de route.

2. Avant de commencer, j'aimerais que vous preniez une minute pour penser à ce que vous aimeriez retirer de cet atelier.

Vous n'avez pas à répondre à voix haute. L'important est simplement d'y réfléchir. Quel genre d'activités aimez-vous faire?

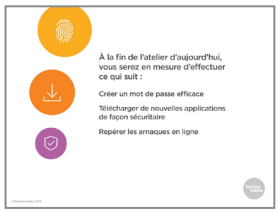
Quel genre d'activités aimeriez-vous être capable de faire?

À votre avis, comment Internet peut-il vous aider à réaliser ces activités?

3. Je ne vous apprends rien en vous disant que Internet peut nous faciliter la vie de nombreuses façons, en nous permettant notamment de regarder des séries et des films, de rester en contact avec les amis et la famille et de trouver des renseignements importants. De plus en plus, nous avons besoin d'Internet pour obtenir des services gouvernementaux ou pour postuler à un emploi.

Toutefois, nombreuses sont les personnes qui sont nerveuses à l'idée d'utiliser Internet. Il faut faire preuve de prudence pour éviter les vols d'identité, les virus informatiques, les arnaques et les autres problèmes.

La bonne nouvelle est que vous pouvez vous protéger de la plupart de ces risques en suivant quelques règles de base.

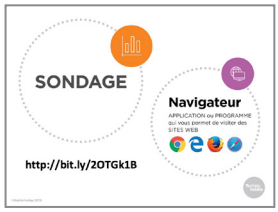


4. À la fin de l'atelier d'aujourd'hui, vous serez en mesure d'effectuer ce qui suit :

Créer un mot de passe difficile à deviner et dont vous pourrez vous souvenir

Télécharger de façon sécuritaire de nouveaux programmes et applications pour vos appareils

Apprendre à reconnaître les méthodes de fraude et d'escroquerie les plus courantes sur Internet



5. Avant de commencer, faisons un sondage rapide pour voir ce que vous savez déjà.

Vous pouvez répondre à la première question en levant votre main. – Combien d'entre vous avez apporté un appareil (comme un téléphone ou un ordinateur) que vous savez utiliser?

Combien d'entre vous avez apporté un appareil que vous n'avez encore jamais utilisé?

Si vous avez un appareil que vous savez déjà utiliser, allumez-le et utilisez votre navigateur pour vous rendre sur le site Web qui apparaît à l'écran. Un *navigateur* est une application ou un programme qui vous permet de visiter des pages Web.

Une fois que vous y êtes, vous pouvez remplir le sondage. Ça ne devrait prendre que quelques minutes.

Si vous n'avez encore jamais utilisé votre appareil, commencez par trouver l'un de ces symboles de navigateur à l'écran. Une fois que c'est fait, ouvrez le navigateur et entrez l'adresse du site Web pour accéder au sondage.

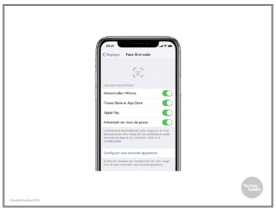
Je vais circuler dans la salle pour m'assurer que tout le monde est capable d'accéder au sondage. Si vous finissez avant les autres, vous pouvez aider vos voisins.

6. L'étape la plus importante pour vous protéger est de vous assurer que vous et seulement vous puissiez utiliser vos appareils et vos comptes.

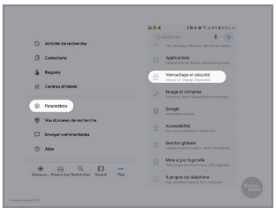
7. Les téléphones, les tablettes et certains ordinateurs sont généralement verrouillés à l'aide d'un NIP. Il s'agit d'un code – habituellement une suite de chiffres – que vous devez entrer pour pouvoir utiliser l'appareil.

Toutefois, la plupart des appareils ne sont pas, de base, verrouillés par un NIP; vous devez activer cette fonction. Ce devrait être l'une des premières choses que vous faites lorsque vous avez un nouvel appareil. Autrement, quiconque le trouve peut avoir accès à tout ce qu'il y a dessus.

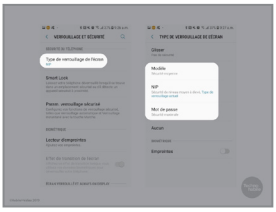
Combien d'entre vous utilisez déjà une forme de verrouillage par NIP sur votre appareil?



8. Sur les appareils Apple, comme les iPhone, appuyez sur « Réglages », puis sur « Face ID et code ». (Apple utilise le mot « code » pour parler d'un NIP.) Vous serez alors invité à régler un NIP de six chiffres, mais vous pouvez décider de créer un NIP plus court ou aussi de créer un NIP qui comprend des lettres.

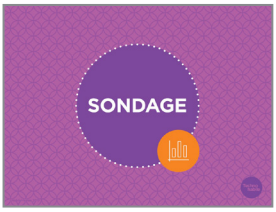


9. Sur les appareils Android, appuyez sur « Paramètres », faites défiler l'écran vers le bas et appuyez sur « Écran verrouillé et sécurité ».



10. Ensuite, appuyez sur « Type de verrouillage de l'écran » et choisissez le type qui vous convient : un NIP, un mot de passe ou un modèle que vous dessinerez à l'écran.

Le type de verrouillage n'importe pas vraiment; l'essentiel est de verrouiller votre appareil d'une façon ou d'une autre.



11. Parlons maintenant des mots de passe.

Qui parmi vous savez ce qui distingue un mot de passe fort ou faible?

Combien d'entre vous avez de la difficulté à créer plusieurs mots de passe pour des comptes différents? Combien d'entre vous avez de la difficulté à vous rappeler de vos mots de passe?

12. Contrairement aux appareils, il est OBLIGATOIRE d'établir un mot de passe pour la plupart des comptes en ligne, notamment pour utiliser la messagerie électronique, des services bancaires en ligne ou des réseaux sociaux comme Facebook. Si vous souhaitez utiliser un service de messagerie ou des réseaux sociaux comme Facebook, vous devrez créer un mot de passe.

Comme tout se passe assez vite à la création du compte, on n'a pas toujours beaucoup de temps pour réfléchir au mot de passe. C'est la raison pour laquelle beaucoup de gens utilisent des mots de passe qui ne sont pas sécuritaires.

Voici quelques-uns des mots de passe les plus souvent utilisés en 2018 : 123456

Motdepasse

QWERTY (il s'agit des six premières touches de la première rangée du clavier.) 11111

jetaime

Il arrive aussi que les gens utilisent des mots de passe que n'importe qui pourrait deviner, comme leur nom de famille ou leur date de naissance.

13. Mais même lorsque vous n'utilisez pas un mot de passe commun oui qui est facile à deviner, celui-ci peut tout de même être considéré comme « faible ». En effet, il y a trois règles à retenir pour créer un mot de passe dit « fort»:

D'abord, il ne doit pas être composé uniquement de lettres ou uniquement de chiffres. Ensuite, il ne doit pas être composé d'un seul mot.

Enfin, il ne doit pas être utilisé sur plus d'un site.

14. Après avoir tenté les mots de passe les plus communs, la plupart des pirates informatiques (c'est-à-dire des personnes qui infiltrent les systèmes ou les comptes d'autrui, communément appelées « hackers ») utilisent un programme qui essaie tous les mots de passe possibles. Comme il s'agit d'un programme informatique, tout se fait très rapidement. En mélangeant des lettres, des nombres et d'autres caractères, comme les signes de ponctuation, vous mettez des bâtons dans les roues au programme pirate.

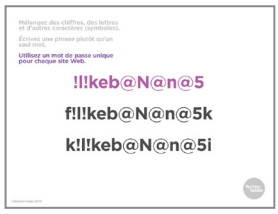
Vous pouvez commencer par choisir un mot normal, puis remplacer certaines lettres par des chiffres ou d'autres caractères, comme l'illustre l'écran.

Si possible, mélangez les majuscules et les minuscules. Évitez de toujours mettre une majuscule en début de mot!

15. Les programmes pirates essaient souvent tous les mots du dictionnaire lorsqu'ils tentent de trouver un mot de passe. Même si vous avez changé quelques lettres en chiffres ou caractères, ils peuvent arriver à deviner le mot de passe.

Pour éviter cette situation, créez une phrase avec votre mot. Par exemple, changez « bananes » pour « les bananes sont jaunes » ou « vive les bananes ». (Dans la plupart des mots de passe, les espaces ne sont pas autorisés, donc il vous faudra coller les mots.)

Ensuite, remplacez certaines lettres des mots ajoutés par des chiffres ou des caractères spéciaux.



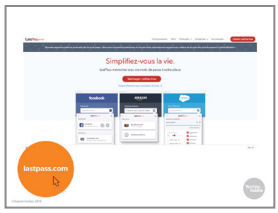
16. Enfin, n'ut ilisez pas le même mot de passe sur plus d'un site. Souvent, ce sont les sites qui se font pirater, et pas les comptes des individus, et lorsque c'est le cas, les pirates peuvent avoir accès à votre mot de passe, même s'il est fort.

Mais un problème se pose : comment arriver à se souvenir de plusieurs mots de passe pour différents sites? Une façon simple de procéder est d'ajouter la première et la dernière lettre du site au mot de passe. Par exemple, pour votre compte Facebook, vous pourriez mettre un « f » au début du mot de passe et un « k » à la fin. Pour votre compte Kijiji, vous mettriez un « k » au début du mot de passe et un « i » à la fin.

Vous n'avez pas à utiliser exactement cette méthode. Vous pouvez mettre les lettres au milieu, les inverser, ou les intégrer de la façon qui vous plaît, pourvu que vous vous rappeliez votre façon de faire.

17. Vous pouvez utiliser cette méthode pour tous vos mots de passe, à l'exception de celui de votre messagerie électronique. S'il vous arrivait d'oublier le mot de passe d'un autre compte, c'est à votre adresse électronique que vous serait envoyé un courriel pour réinitialiser le mot de passe oublié. Cela signifie que quiconque a accès à votre messagerie électronique peut réussir à avoir accès à vos autres comptes, d'où l'importance de bien la protéger. Vous pouvez utiliser la méthode que nous avons vue pour trouver un mot de passe pour votre messagerie, mais assurez-vous qu'il est complètement différent de celui de vos autres comptes.

En fin de compte, vous devez vous souvenir de deux mots de passe : celui de votre messagerie électronique et celui qui change légèrement pour chacun de vos autres comptes.



18. Une autre option qui s'offre à vous est d'utiliser un *gestionnaire de mots de passe*. Il s'agit d'un programme qui gère vos mots de passe pour différents comptes. Il crée un mot de passe différent, presque impossible à trouver, pour chacun de vos comptes, puis s'occupe de remplir les identifiants de connexion pour vous.

LastPass est l'un des gestionnaires de mots de passe populaires à offrir une version de base gratuite.

Les gestionnaires de mots de passe peuvent être utiles, mais ils servent uniquement à vous éviter d'avoir à vous rappeler plusieurs mots de passe pour différents sites Web. Vous devez tout de même vous assurer d'avoir un mot de passe fort auprès du gestionnaire de mots de passe, car quiconque réussit à se connecter à ce compte a accès à tous vos autres comptes.

19. Faisons un petit quiz pour vérifier que vous avez bien assimilé tout ce que nous avons vu jusqu'à présent.

On fonctionnera de la même façon que pour le sondage effectué au début de l'atelier.

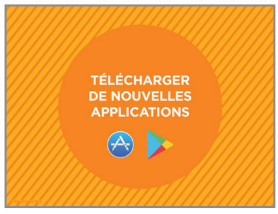
20. Essayons de créer de bons mots de passe.

Pensez à un mot et inscrivez-le sur la feuille « Outil de création de mot de passe ». Remplacez certaines lettres par des chiffres ou des caractères spéciaux.

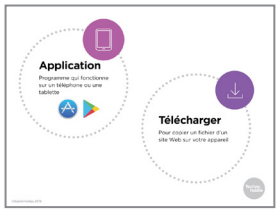
Ensuite, faites une phrase avec le mot choisi, et changez quelques-unes des nouvelles lettres par des chiffres ou des caractères spéciaux.

Je vais circuler dans la salle pour aider ceux qui éprouveraient des difficultés.

Maintenant, retournez la feuille. Nous allons y revenir plus tard pour vérifier si vous vous en souvenez!



21. Sur la plupart des ordinateurs, des téléphones intelligents et des tablettes, des applications sont déjà installées par défaut, mais il est probable que vous vouliez en avoir de nouvelles. Par exemple, un membre de votre famille utilise un nouveau réseau social comme Instagram et vous aimeriez vous aussi vous inscrire, ou encore un nouveau jeu est disponible auquel vos enfants aimeraient jouer.

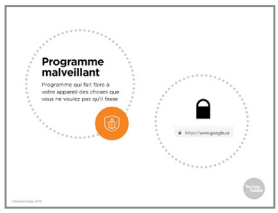


22. Une application est un programme que vous pouvez utiliser sur un téléphone ou une tablette. Tout ce que vous feriez normalement à partir d'un navigateur sur un ordinateur, tel que regarder Netflix et utiliser un réseau social comme Facebook, sera habituellement fait à partir d'une application sur un téléphone ou une tablette.

Pour utiliser une application qui n'est pas encore sur votre appareil, vous devez d'abord la *télécharger*. Cela signifie que

vous faites une copie de cette application sur votre appareil.

Vous pouvez également télécharger d'autres fichiers, comme des photos, des vidéos et de la musique. Ces fichiers peuvent provenir de sites Web, de textos, de courriels ou d'une autre forme de message reçu.



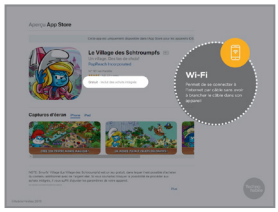
23. Comme le téléchargement vise à intégrer une nouveauté sur votre ordinateur, il peut se révéler risqué. Si vous téléchargez un fichier qui n'est pas ce que vous pensez, vous pourriez laisser un programme malveillant s'installer sur votre ordinateur.

Un programme malveillant, aussi appelé logiciel malveillant ou maliciel, est un programme qui fait faire à votre appareil des choses que vous ne voulez pas qu'il fasse. Il prend parfois la forme d'un virus informatique, qui utilise votre ordinateur pour envoyer des copies du virus à d'autres ordinateurs, ou d'un logiciel espion, qui surveille vos activités en ligne et envoie cette information aux pirates qui ont créé le logiciel. Ils peuvent ainsi avoir accès à votre compte bancaire ou à d'autres comptes en ligne.

Pour ne prendre aucun risque, ne téléchargez jamais rien provenant d'un courriel, texto ou autre forme de message que vous n'avez pas sollicité.

Lorsque vous utilisez un navigateur, téléchargez uniquement des fichiers à partir de sites Web de confiance.

Vous devriez également vous assurer que l'adresse Web commence par « h-t-t-p-s » (assurez-vous qu'il y a bien un « s » à la fin) et que le symbole du cadenas apparaît dans la barre d'adresse. Ce symbole signifie que personne d'autre ne peut voir ce que vous téléversez sur le site Web ou ce que le site vous envoie.



24. Lorsque vous utilisez un téléphone ou une tablette, assurez-vous de toujours télécharger vos applications à partir de la boutique d'applications officielle de votre appareil. Pour les appareils Apple, comme les iPhone, il s'agit de l'App Store. Pour les appareils Android, il s'agit du Google Play Store.

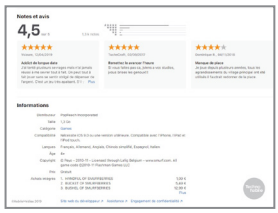
Normalement, l'application correspondante est déjà installée sur votre appareil.

Si vous entendez parler d'une application que vous souhaitez télécharger, cherchez- la dans l'App Store ou le Google Play Store.

N’oubliez pas qu’il y a beaucoup d’applications qui ne coûtent rien à télécharger, mais qui proposent une version payante. D’autres vous obligent à visionner des publicités pour continuer d’utiliser la version gratuite ou essaient de vous vendre des extras pendant que vous utilisez l’application. Assurez-vous de bien lire ce qui est dit au sujet des frais et des paiements sur la page de l’application en question dans la boutique.

Il se peut que vous deviez entrer votre numéro de carte de crédit à l’ouverture d’un compte App Store ou Google Play Store. Toutefois, rien ne devrait être facturé sur votre carte, à moins que vous n’achetiez une application ou un extra dans une application.

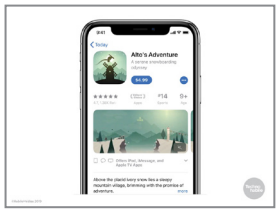
Pour ne courir aucun risque, évitez de télécharger des applications lorsque vous utilisez un réseau Wi-Fi public, comme celui d’une bibliothèque ou d’un café.



25. Les deux boutiques d’applications permettent aux utilisateurs de noter les applications; vous pouvez donc voir ce que les autres ont dit à propos de l’application que vous voulez obtenir.

26. Sur un iPhone ou un iPad, touchez d’abord l’icône de l’App Store sur votre écran.

Si vous n’avez encore jamais utilisé l’App Store, vous devrez commencer par créer un compte.



27. Une fois que c’est fait, vous pouvez lancer votre recherche. Une bonne façon de procéder est d’écrire la fonction souhaitée de l’application. (Par exemple, vous pourriez taper

« météo » pour trouver une application de météo.)

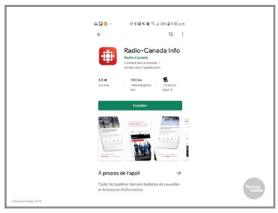
Si plusieurs choix s’offrent à vous, appuyez sur l’application qui vous intéresse.

Vous verrez alors des informations sur cette application. Si elle est gratuite, vous pouvez la télécharger en appuyant sur « Obtenir ». Si elle est payante, appuyez sur le prix affiché.

Vous devrez ensuite confirmer que vous souhaitez l’acheter.

Une fois l’application téléchargée, elle apparaîtra sur votre écran d’accueil sous la forme d’une icône unique.

28. Dans le Google Play Store, vous pouvez chercher une application en particulier ou parcourir les choix d'applications par sujet.



29. Appuyez sur n'importe quelle application qui vous intéresse. Si vous décidez de la télécharger, vous pouvez appuyer sur « Installer » si elle est gratuite, ou sur le prix si elle est payante.

Une icône correspondante apparaîtra sur la dernière page de votre téléphone.

30. Certaines applications ont l'air fiables, mais vous demandent de fournir des renseignements personnels dont elles n'ont pas besoin. N'entrez jamais de renseignements personnels qui ne sont pas nécessaires au fonctionnement de l'application, et désinstallez (retirez) toute application qui vous demande une telle chose.

Certaines applications ont réellement besoin de connaître un renseignement précis, comme votre emplacement, ou d'avoir accès à certaines fonctionnalités de votre téléphone, comme la caméra, mais si une application vous demande de la laisser faire quelque chose d'étrange sur votre téléphone sans raison valable, dites « non » et désinstallez-la.

31. Pour désinstaller une application sur un appareil Android, appuyez sur l'icône de l'application en question et maintenez votre doigt enfoncé jusqu'à ce que l'option « Désinstaller » apparaisse. Appuyez sur cette option pour désinstaller l'application.

Sur un iPhone, appuyez sur l'icône de l'application concernée et maintenez votre doigt enfoncé jusqu'à ce qu'un «X » apparaisse dans le coin supérieur gauche de l'icône.

Appuyez sur le « X », puis sur « Supprimer » dans la fenêtre qui s'ouvre.

(Sur les iPhones les plus récents, l'option permettant d'effacer une application apparaîtra à chaque fois que vous touchez et maintenez enfoncée l'icône d'une application.)

32. Un autre élément à surveiller est la quantité de données utilisées par l'application. Les données vous permettent d'utiliser Internet sur votre téléphone intelligent et leur utilisation coûte de l'argent.

Si vous utilisez toujours le Wi-Fi, la quantité de données requises n'est pas un problème (quoique si vos activités consomment beaucoup de données, comme regarder des vidéos, vous pourriez dépasser la limite de données de votre forfait Internet).

Si vous utilisez des données mobiles, vous en écoulerez lorsque vous téléchargerez une application et chaque fois que cette application se mettra à jour, ce qui pourrait ultimement se traduire par des coûts additionnels. Beaucoup d'applications consomment des données lorsqu'elles sont ouvertes, en envoyant par exemple des vidéos, des photos, de la musique, etc. Même une application météo enverra et recevra des données, pour reconnaître votre emplacement et envoyer la météo correspondante à votre appareil.

Pour connaître la quantité de données que vous utilisez sur un appareil Apple ou Android, commencez par appuyer sur « Réglages » ou « Paramètres ». Sur un iPhone ou un iPad, cliquez ensuite sur « Réseau cellulaire ». À partir de cette page, vous pouvez régler certaines applications de sorte qu'elles n'utilisent pas de données sans d'abord obtenir votre utilisation. Pour ce faire, faites glisser la case de défilement correspondante vers la gauche.

Sur un appareil Android, appuyez sur « Consommation des données ». À partir de là, vous pouvez activer ou désactiver les données pour chacune de vos applications et définir un avertissement chaque fois qu'une application veut consommer des données.

33. Exerçons-nous à trouver des applications qui pourraient vous être utiles.

Si vous utilisez un téléphone ou une tablette, commencez par ouvrir le Google Play Store ou l'App Store. Si vous utilisez un ordinateur avec Windows, rendez-vous sur le site Web de la boutique de Microsoft (la première adresse Web sur la diapo). Si vous utilisez un Chromebook, rendez-vous sur le site Web de Chrome.

Maintenant, essayez de trouver une application qui pourrait vous intéresser pour chacun des sujets suivants :

Une application pour votre bibliothèque municipale

Une application qui vous indique les conditions météorologiques

Une application qui vous aide à planifier vos repas ou ceux de votre famille

Je vais circuler dans la salle pour aider ceux qui éprouveraient des difficultés.

Maintenant, discutez de votre expérience avec votre voisin immédiat. La fonction de recherche a-t-elle été facile à utiliser? Pour chaque recherche effectuée, combien de choix d'application se sont offerts à vous? Quels renseignements fournis ont pu vous aider à déterminer si l'application vous convenait?

34. Un autre phénomène qui inquiète de nombreuses personnes lorsqu'elles vont sur Internet est de se faire avoir par des escrocs. Par « escrocs», j'entends les personnes qui vous incitent par la tromperie à leur envoyer de l'argent ou vos renseignements personnels.

Les arnaques ou escroqueries en ligne sont nombreuses, et elles peuvent vous coûter très cher si vous vous laissez embobiner.

Heureusement, en connaissant les menaces qui planent sur vous, vous arriverez à reconnaître presque toutes les arnaques en ligne.

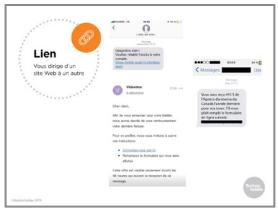
35. Les escrocs essaient principalement de vous soutirer l'une ou l'autre de ces deux choses : de l'argent ou des renseignements personnels. Très souvent, ils vous demanderont de leur fournir des renseignements sur votre compte bancaire ou votre numéro de carte de crédit, de façon à vous extirper de l'argent, ou encore de leur divulguer le mot de passe de votre messagerie électronique ou de votre compte de réseau social, pour se faire passer pour vous.

36. Les arnaques peuvent se présenter à vous sous plusieurs formes.

Nombreuses sont celles qui arriveront par courriel. Il est donc important de faire preuve de méfiance à l'égard des courriels provenant d'expéditeurs que vous ne connaissez pas. La même logique s'applique pour les textos et les messages reçus sur des réseaux sociaux, comme Twitter.

Mais même lorsque vous connaissez l'expéditeur, la prudence est de mise; il arrive que les escrocs essaient de se faire passer pour quelqu'un que vous connaissez. Il est également possible qu'une connaissance ait téléchargé un programme malveillant par erreur, qui fait que son ordinateur envoie de faux messages.

Une des arnaques les plus courantes de ce type consiste à vous envoyer un message de la part d'une connaissance, dans lequel elle dit être dans le pétrin et avoir besoin d'argent immédiatement. Ne répondez pas à de tels messages. Si vous pensez que la personne qui vous écrit puisse réellement avoir besoin d'aide, communiquez avec elle d'une autre façon pour vous en assurer.



37. Il arrive également que les escrocs prétendent être des établissements ou des sites où vous avez un compte, comme votre banque ou votre fournisseur Internet.

Restez à l'affût des signes d'arnaque : l'expéditeur vous demande de lui envoyer des renseignements personnels, vous invite à cliquer sur un lien (qui vous dirige d'un site Web à un autre) plutôt que de vous rendre par vous-même sur le site Web officiel, ou essaie de vous faire peur en suggérant que vous lui devez de l'argent ou qu'un de vos comptes est sur le point d'être fermé.

Autre signe : l'adresse courriel ne correspond pas à celle de l'entreprise que l'escroc prétend être.

Ne cliquez jamais sur un lien qui se trouve dans un message venant d'une banque, de Revenu Canada, de votre fournisseur Internet ou de tout autre expéditeur du genre.

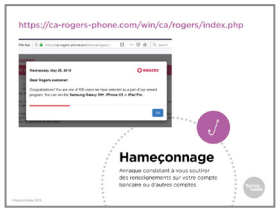
Allez plutôt sur le vrai site Web de l'expéditeur ou communiquez avec lui par téléphone pour vé

38. Parfois, les escrocs essaient de vous duper en vous faisant croire qu'ils *vous* donneront de l'argent. Vous pourriez par exemple recevoir un message vous disant que vous avez reçu un retour d'impôt, que vous avez gagné à la loterie ou que vous pourriez profiter d'une occasion d'affaires alléchante.

Parfois encore, les escrocs veulent simplement vous amener à cliquer sur le lien, de façon à obtenir vos renseignements personnels ou à installer un programme malveillant sur votre ordinateur, comme dans l'exemple à l'écran.

Dans tous les cas, rappelez-vous que rien n'est gratuit. Si vous recevez un message du genre, supprimez-le.

Si vous pensez qu'il s'agit peut-être d'un vrai message, rendez-vous sur le site Web de l'expéditeur ou communiquez avec lui par téléphone pour vérifier. (N'utilisez pas le numéro de téléphone ou l'adresse Web fournis dans le message suspect – effectuez une recherche.)



39. L'une des arnaques les pus courantes est l'« hameçonnage ». Les escrocs essaient alors de vous amener à leur envoyer des renseignements au sujet de votre compte bancaire ou d'autres comptes.

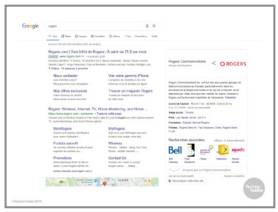
Voici un exemple d'une tentative d'hameçonnage récente. Une page Web s'ouvre sans que nous n'ayez cliqué sur quoi que ce soit. Comme vous pouvez le voir, il s'agit du type d'arnaque où vous recevez de l'argent sans raison, car on vous indique que vous pouvez participer à un tirage pour gagner une tablette ou un téléphone intelligent.

Si vous n'êtes pas un client de Rogers, alors vous pouvez être sûr qu'il s'agit d'une arnaque. Mais si vous l'êtes, comment faire pour savoir?

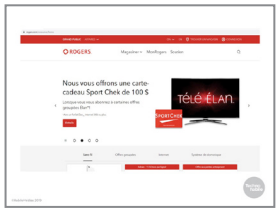
D'abord, regardez l'adresse Web de la page.

Elle est un peu étrange, n'est-ce pas? Ce n'est pas écrit rogers.com ou rogers.ca, comme on pourrait s'y attendre, mais ca-rogers-phone.com.

40. Si vous voulez en avoir le cœur net, vous pouvez aller sur Google et faire une recherche pour trouver le site de Rogers (ou vérifier l'adresse Web qui apparaît sur l'une de vos factures).

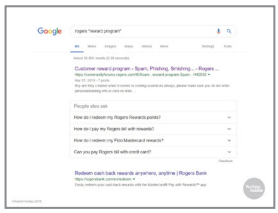


41. Vous constaterez alors que la véritable adresse est Rogers.com, et pas celle qui apparaît en haut de la page.



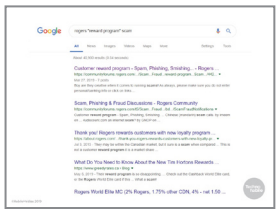
42. Si vous vous rendez sur le vrai site de Rogers, vous verrez qu'il n'y a aucune mention d'un concours.

Rappelez-vous que sur Internet, il est assez facile de créer un faux site Web qui ressemble au vrai, mais qu'il est beaucoup plus difficile de falsifier une adresse Web.

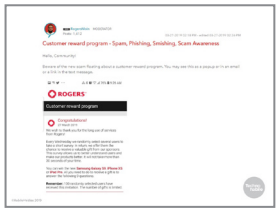


43. Une autre méthode pour vérifier l'authenticité du message est de faire une recherche à propos de ce qui vous est promis.

Ainsi, si on fait une recherche sur Google au sujet de Rogers et d'un programme de récompense (en anglais, « reward program »), le premier résultat qui apparaît est un article nous indiquant qu'il s'agit d'une arnaque.



44. Si on fait la même recherche en ajoutant le mot « scam » (arnaque), il sera encore plus clair qu'il s'agit bel et bien d'une arnaque.



45. Si on clique sur l'un des liens qui apparaissent, on verra un message de Rogers nous mettant en garde contre l'arnaque.

46. Un autre type d'arnaque n'ayant pas directement trait à l'argent est le *vol d'identité*. On parle de vol d'identité lorsqu'une personne prétend être vous pour ouvrir des comptes en ligne et prendre une carte de crédit à votre nom.

Généralement, si vous êtes victime d'un vol d'identité, c'est parce que vous avez communiqué suffisamment de renseignements à votre sujet pour permettre aux escrocs qui recueillent ce genre d'information de se faire passer pour vous.

Pour éviter que cela se produise, ne communiquez jamais les renseignements suivants dans des espaces publics en ligne, comme dans une publication sur un réseau social :

Votre nom complet (y compris votre deuxième prénom) Votre date de naissance complète (y compris l'année) Votre numéro d'assurance sociale

Le nom de jeune fille de votre mère (il arrive souvent que cette information serve de question de sécurité)

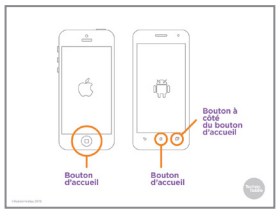
47. Faisons un autre quiz pour voir si vous avez tout retenu.

48. Vous avez créé un mot de passe un peu plus tôt aujourd'hui. Prenez un moment pour voir si vous êtes *capable* de le retrouver.

Maintenant, tournez la feuille pour vérifier si vous avez la bonne réponse.

49. L'une des raisons les plus souvent évoquées pour justifier le refus d'utiliser Internet, c'est la peur que quelque chose tourne mal.

La bonne nouvelle est qu'il est assez facile de corriger ses erreurs la plupart du temps.



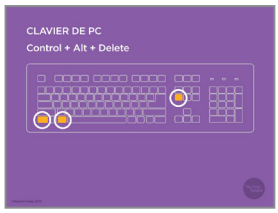
50. Sur les téléphones et les tablettes, vous pouvez généralement quitter une application sans avoir à la fermer, simplement en appuyant sur le bouton d'accueil.

Si vous voulez fermer une application sur un iPhone ou un iPad, appuyez deux fois sur le bouton d'accueil. Puis, avec votre doigt, faites défiler l'application que vous voulez fermer vers le haut.

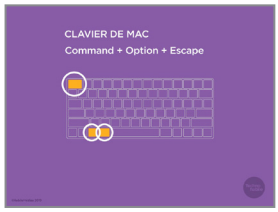
Sur un appareil Android, appuyez sur le symbole de carrés à droite du bouton d'accueil, puis faites défiler l'application vers le côté. (Il faut la faire défiler parfois vers la droite, parfois vers la gauche.)

Si vous ne faites pas ça, les applications ne se ferment pas totalement; elles continuent de fonctionner en arrière-plan.

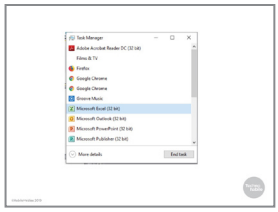
Prenez l'habitude de les fermer lorsque vous avez fini de les utiliser.



51. Si vous utilisez un ordinateur qui utilise le système d'exploitation Windows, appuyez sur les touches Ctrl, Alt et Suppr (ou Delete) en même temps. (L'emplacement de ces touches peut varier d'un clavier à l'autre.)



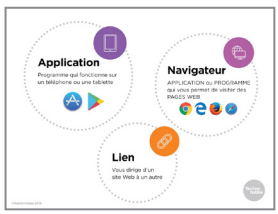
52. Si vous utilisez un ordinateur Mac, appuyez simultanément sur les trois touches suivantes : Option, Commande et Échap.



53. Cela ouvrira le gestionnaire de tâches. Cliquez sur le programme que vous souhaitez fermer, puis sur « Fin de tâche ».

54. Si vous avez un problème récurrent, vous pouvez communiquer avec le service de soutien de votre appareil.

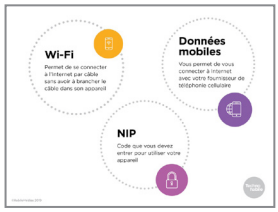
Voici les adresses Web pour les appareils les plus utilisés.



55. Avant de se laisser, revenons un peu sur les nouveaux termes appris au cours de l'atelier.

Une *application* est un programme sur un appareil mobile, comme un téléphone ou une tablette, qui vous permet d'effectuer une tâche en particulier. Par exemple, vous pourriez avoir une application pour jouer à des jeux, pour accéder à une boîte de messagerie électronique ou pour visionner des vidéos, comme YouTube ou Netflix.

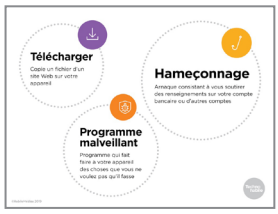
Un *navigateur* est l'application ou le programme qui permet à votre appareil de visiter des pages Web. Chrome, Firefox et Safari sont des exemples de navigateurs.



56. Les *données mobiles* captent le signal Internet du réseau cellulaire.

Le *Wi-Fi* envoie un signal Internet à votre ordinateur sans qu'aucun fil ou câble ne soit requis en utilisant un *routeur* sans fil connecté à l'Internet par câble.

Un NIP est un code que vous devez entrer pour utiliser votre appareil.



57. *Télécharger* signifie copier quelque chose d'un site Web ou d'un courriel sur votre ordinateur.

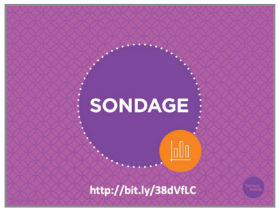
Un *programme malveillant* ressemble à un virus et apporte des modifications indésirables à votre ordinateur.

On parle de tentative d'*hameçonnage* lorsque quelqu'un essaie de vous soutirer des renseignements personnels, souvent au sujet de votre compte bancaire.

58. Cet atelier tire à sa fin. Si vous avez encore des questions au sujet des notions abordées aujourd'hui, c'est le moment de les poser.

Si vous préférez me les poser en privé, n'hésitez pas à venir me voir après l'atelier. Je resterai sur place un petit moment.

59. Assurez-vous d'apporter la fiche d'exercice pour cet atelier. Utilisez le lien vidéo qui s'y trouve pour revoir ce que nous avons couvert aujourd'hui.



60. Nous avons couvert beaucoup de matière au cours de l'atelier. J'aimerais maintenant vous entendre. Qu'avez-vous appris? Des questions sont-elles restées sans réponse? Avez-vous des suggestions pour améliorer l'atelier?