[Marque de TELUS Averti]

[Introduction à Internet avec TELUS Averti]

[11. Rester en sécurité : éviter les arnaques sur Internet]

[Voix d'une femme]

Nombreux sont ceux qui s'inquiètent de tomber victimes d'arnaques sur Internet.

Dans cette situation, les escrocs essayent d'inciter leurs victimes à leur donner d'argent ou de renseignements personnelles.

[Un ordinateur portable apparait sur l'écran. Un cafard passe par l'écran. Un homme portant des lunettes de soleil et un chapeau apparaît derrière l'écran de l'ordinateur portable et puis disparaît.]

Il existe de nombreuses arnaques dont vous devrez vous méfier. Et elles pourraient vous couter beaucoup d'argent si vous n'êtes pas prudents.

[Un verrou apparaît. Le cafard et le verrou disparaissent derrière l'écran.]

Heureusement, connaitre les pièges le plus courants, peut vous aider à reconnaitre et à éviter la plupart des arnaques en ligne.

[Des billets de banque et une carte d'identité apparaissent sur l'écran.]

Il y a deux choses principales que les escrocs cherchent à obtenir de vous : Soit qu'ils vous demandent de leur envoyer de l'argent ou ils sont après vos renseignements personnels.

[Renseignements de compte bancaire
Renseignements de carte de crédit
Mot de passe de courriel
Mot de passe de réseaux sociaux]

La plupart du temps ils essayent d'obtenir vos renseignements de compte bancaire ou de carte de crédit pour pouvoir vous extorquer de l'argent, ou ils tentent d'obtenir le mot de passe de votre compte courriel et de réseaux sociaux pour pouvoir se faire passer pour vous.

[Une page de courriel apparaît sur l'écran. Un doigt clique sur un courriel de Pierre avec le sujet « Une affaire incroyable! » Le courriel s'ouvre et puis le doigt ferme ce courriel de Pierre et ouvre un autre, de Club des testeurs.]

Les escrocs peuvent s'attaquer à vous de plusieurs façons. Beaucoup utilisent le courriel. Vous devez donc vous méfier de courriels que vous recevez de la parte de personnes que vous ne connaissez pas.

[Un téléphone cellulaire apparaît sur l'écran à côté de l'ordinateur.]

Ils envoient de même pour des messages-texte ou des messages reçus via les réseaux sociaux, comme twitter et Facebook.

[Le doigt tape sur un courriel de Louis, avec le sujet « Achetez des actions dans cette compagnie maintenant ». Dans la boite de réception apparaît un autre courriel de Elsa Guzman, sujet « Bonjour ».]

Cependant, les escrocs peuvent parfois se faire passer pour quelqu'un que vous connaissez. Un de vos contacts pourrait avoir téléchargé un program malveillant, forçant son ordinateur à envoyer des courriels qui ont l'air d'avoir être envoyées par ces soins mais qui sont faites pour vous duper.

[Le courriel de Elsa Guzman s'ouvre. Il comprend le texte « Bonjour, Peux-tu me répondre immédiatement? J'ai besoin d'aide. Elsa »]

Une arnaque répandue consiste à envoyer un message semblant venir de l'un de vos contacts et disant que ce dernier a des ennuis et qu'il a besoin d'argent immédiatement. Ne répondez pas à ces messages.

[Un téléphone cellulaire apparaît sur l'écran. Le groupe de contacts « Amis » se déroule sur l'écran du cellulaire et le doigt tape sur le nom de Elsa Guzman, puis sur l'option Message Texte.]

Si vous pensez que la personne qui vous connaissez pourrait réellement avoir des ennuis, utilisez des coordonnées sûres pour la contacter et vérifier si elle a vraiment besoin de votre aide.

[Message texte pour Elsa Guzman :
« Allo, je viens de recevoir un courriel de ta part – tour va bien? »
« Je ne t'ai pas envoyé de courriel. »]

En général, les courriels frauduleux vous demandent d'envoyer des renseignements ou de l'argent, de mettre à jour votre mot de passe ou de cliquer sur un lien.

[Un courriel de Desjardins apparaît dans la boite de réception. Le sujet est « Action immédiate requise ». Le doigt tape sur le courriel et il s'ouvre.]

Ils peuvent aussi essayer de vous faire peur en vous disant qu'un de vos comptes et sur point d'être annulé.

[Les courriels frauduleux vous demandent :
- Information
- Argent
- Mettre à jour votre mot de passe
- Actions concernant votre compte]

Ce type du courriel s'appelle de courriel d'hameçonnage, où les escrocs essayent de vous inciter à leur donner des renseignements sur vos comptes bancaires ou vous activités en ligne.

[Un courriel d'Agence du revenu du Canada apparaît dans la boite de réception. Sujet :
« Confirmez vos renseignements pour un… » ]

Soyez prudents si vous recevez un message qui semble venir de votre banque, de votre fournisseur d'accès à Internet ou de l'Agence du revenu du Canada vous demandant de fournir ou de vérifier vos renseignements personnels.

[Le courriel d'Agence du revenu du Canada contient ce message :

« Sujet : Confirmez vos renseignements pour un remboursement d'impôt.
Cher contribuable,
Vous avez reçu 476 $ de l'Agence du revenu du Canada.
Confirmer votre identité. »
« Confirmer votre identité » est un lien.]
Au lieu de cliquer sur le lien de ce type de courriel, rendez vous directement sur le site web du l'organisme.

[Le site web du gouvernement du Canada apparaît. L'écran se déroule et le doigt tape sur le lien « Contactez-nous »]

Trouvez ces coordonnées et téléphonez pour vérifier s'ils ont réellement besoin des informations de votre part.

[Un courriel de Loto-Québec apparaît dans la boite de réception. Le sujet est « Vous avez gagné – obtenez votre prix ». Le doigt tape sur le courriel et il s'ouvre.
Le courriel contient ce message :
« Lisez le document ci-joint pour savoir comment obtenir votre prix.
Félicitations & bien joué
Signé
Loto-Québec »]

Parfois les escrocs peuvent essayer de vous duper en vous faisant croire qu'ils vous donneront de l'argent ou même un voyage gratuit. Vous pouviez recevoir un message vous disant que vous avez droit à un remboursement d'impôt, que vous avez gagné à la loterie ou que vous pourriez tirer profit d'une opportunité commerciale.

[Un courriel de Carte des Fêtes apparaît dans la boite de réception. Le sujet est « Une chance de magasiner gratuitement! »
Le doigt tape sur le courriel et il s'ouvre.
Le courriel contient ce message :
« Cher client,
Nous offrons des cartes cadeaux gratuites pour vos magasins préfères pour Noel. Pour en apprendre davantage, cliquez ici. »
« Cliquez ici » est un lien.]
Parfois, ils veulent simplement que vous cliquiez sur un lien qui leur permet de voler vos renseignements personnels ou d'installer un program malveillant sur votre ordinateur.

[Le doigt tape sur tous ces messages et ils sont effacés.]

Quoi qu'il en soit, souvenez-vous que si quelque chose a l'air trop beau pour être vrais, c'est probablement le cas.

Si vous recevez un message comme celui-ci, effacez-le.

[siteinternetofficiel.com apparaît sur l'écran. Le doigt tape sur « Contactez-nous » et la page de contact apparaît, affichant l'adresse, le courriel et le téléphone.]

Si vous pensez qu'il est possible que ce soit vrai, allez sur le site web officiel du l'expéditeur présumé, pour vérifier ce que le message affirme ou demande, ou appelez-le au téléphone. N'utilisez pas un numéro ou une adresse contenu dans le message. Faites une recherche.

Comment savoir si un courriel que vous recevez est une arnaque?

[Un courriel de Netflix apparaît dans la boite de réception. Le sujet est « Avertissement : compte suspendu ». Le doigt tape sur le courriel et il s'ouvre.
Le courriel contient ce message :
Votre compte a été suspendu.
Reprendre votre Abonnement »
« Reprendre votre Abonnement » est un lien.]

Imaginez que vous recevez un courriel. Il est fait d'une manière à vous laisser croire que votre abonnement à Netflix est sur le point d'être désactivé. Dès qu'il soit possible de recevoir un courriel que celui-ci de la part d'une compagne avec qui vous faites affaires, vous devez quand-même être prudents, en particulier s'il n'y a aucune raison pour que votre compte Netflix soit désactivé.

[Le doigt tape sur le champ « De ». L'adresse d'expéditeur est NetflixAccounts@notice-access_273.com]

Vérifiez l'adresse dans le champ « De : ». Un courriel de Netflix devrait venir d'une adresse qui se termine par Netflix.com. Ce n'est pas le cas de celle-ci. Donc, l'expéditeur se présent sous un faux jour.

[« Reprendre votre Abonnement » est en focus]
Il y a également un gros buton « Reprendre votre Abonnement » sur lequel on vous demande de cliquer.
[Le doigt tape sur le lien et une site semblant à Netflix apparaît.
« Le buton Mettre à jour vos informations de facturation est en focus. »]

Cela ne vous emmènera surement pas sur le site du Netflix mais à la place, verront un site qui ressemble à celui du Netflix ou on vous demandera vos renseignements de carte de crédit.

[Le site du Netflix Canada apparaît]

Souvenez-vous qu'il est assez facile de créer un faux site internet et à l'air vrai. Mais, il est beaucoup difficile de créer une faux adresse web.

[La page du Google apparaît. Le mot « netflix » est tapé dans le champ de recherche.]

Si vous souhaitez confirmer l'adresse web, vous pouvez vous rendre sur Google et faire une recherche pour Netflix ou la chercher sur l'un de vos reçus ou factures.

[Le site du netflix.com apparaît
La page de compte apparaît]

Vous pouvez aussi vous rendre sur le site de Netflix et vous connecter à votre compte pour confirmer le statut de votre abonnement.

Vous pouvez également rechercher ce que le message vous promet.

[Un courriel d'Apple apparaît dans la boite de réception. Le sujet est « Félicitations! Vous avez gagné (1) un iPhone ». Le doigt tape sur le courriel et il s'ouvre.
Le courriel contient ce message :
« Félicitations! Vous avez gagné (1) un iPhone 256gb exclusivement pour vous!
Comment obtenir votre iPhone 256gb :
1- Entrez votre adresse de livraison
2 – Payez 4,95$ de frais d'envoi »
Un buton « Continuer » est présent.]

Imaginez que vous recevez un courriel, soi-disant de la part d'Apple, vous offrent de participer à un tirage pour gagner un iPhone gratuit, en cliquant sur un lien.

[Page de recherche Google, mettant en évidence les résultats pour la recherche de termes « apple concours iphone arnaque ».

La page se déroule et beaucoup d'articles apparaissent.

Gros plan d'un article intitulé « Arnaque : un faux sondage Amazon pour gagner un iPhone X »].

Si vous faites une recherche pour Apple et concours iPhone, ajoutez le mot « arnaque », par exemple. Les premiers résultats seront probablement de mise-en-garde contre cette escroquerie.

[visionnagedecontenuvideo.com apparaît sur l'écran.]

[Vol d'identité]

Un dernier tip d'arnaque qui n'implique pas d'argent est le vol d'identité. C'est-à-dire, lorsque quelqu'un se fait passer pour vous afin d'ouvrir des comptes en ligne ou de faire des demandes de cartes de crédit en votre nom.

[Un page d'inscription sur le site visionnagedecontenuvideo.com apparaît sur l'écran. Le nom d'utilisateur « Amateurdecinéma23 » et un mot de passe sont tapés.
Une autre page, avec des données identiques apparaît à côté de la première, dessous l'image d'un escroc.]

En générale, les vols d'identité ont lieu quand un escroc obtient des renseignements personnels sur une personne, en ligne ou par d'autres moyens, et les utilisent ensuite pour se faire passer pour elle.

[Ne partagez pas :
- Nom complet
- Date de naissance
- Numéro d'assurance sociale
- Nom de jeune fille de la mère

- Renseignements de carte de crédit
- Numéro de permis de conduire
- Numéro de passeport.

Afin d'éviter ça, ne partager aucun des renseignements suivants dans un espace publique en ligne, comme un profil, une publication sur un réseau sociale : 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 – est une donnée que des nombreuses personnes l'utilise comme question de sécurité -, vos renseignements de carte de crédit ou votre numéro de permis de conduire ou numéro de passeport.

[Marque de TELUS Averti]

Pour poursuivre votre introduction à Internet, consultez les autres vidéos de cette série. Visitez notre site, telus point com barre oblique techno cent un averti.

[telus.com/Techno101Averti]