Vous avez gagné 100 000 000 de dollars américains!

Félicitations!!! Notre système informatique, financé par un riche magnat de la presse allemande, et situé à New Delhi, a choisi votre adresse de courriel parmi les milliards d'adresses de courriel que nous avons en banque.

Grâce à un programme hyper sophistiqué d'algorithmes binaires, votre courriel, rattaché au billet numéro 9520025263-5656 (numéro de série 6352-652), a généré les numéros chanceux 4-12-65-69-78-37. En conséquence, vous avez gagné la faramineuse somme de

100 000 000 de dollars US

FÉLICITATIONS!!! FÉLICITATIONS!!! FÉLICITATIONS!!!

Procédure de remise du gain

Afin de récupérer ce qui vous est dû, vous avez 72 heures pour contacter notre huissier officiel, Maître Jérôme Claveau, par courriel ou par téléphone, afin de lui donner les informations nécessaires pour confirmer votre identité. Passé ce délai, l'argent sera redistribué à un organisme qui assure la survie des moustiques en Abitibi.

Voici les informations que vous devez nous transmettre :

Nom : _____
Prénom : _____
Sexe : _____
Adresse : _____
Code postal : _____
Pays : _____
Téléphone (maison) : _____
Téléphone (travail) : _____
Profession : _____
Numéro d'assurance sociale : _____

De plus, vous devrez nous faire parvenir une copie de votre passeport.

Afin d'éviter des retards dans le dépôt de vos 100 000 000 de dollars US, veuillez aussi inclure votre numéro de compte et de transit, ainsi que tous vos numéros de carte de crédit.

Bien à vous,

Kabran Jonas
Fraudeur!

Les fraudes et arnaques par courriel...

Par Jérôme Claveau

Vous y avez cru? Oui? Alors, attention. En quelques secondes, vous vous seriez adroitement fait voler votre identité.

Les fraudes par Internet sont de plus en plus monnaie courante. Et malheureusement, lorsque nous en sommes victime... les recours légaux sont pour ainsi dire nuls. Le meilleur moyen est donc de ne pas se faire prendre! J'ai donc pris le temps de vous présenter trois exemples de fraudes communes, et de vous expliquer sur quels principes elles se basent. Vous serez ainsi en mesure de les détecter facilement. Soit dit en passant, j'ai écrit moi-même ces « courriels frauduleux ». Comme quoi c'est à la portée de n'importe qui!

Allons-y pour celle en première page. Comme ça, on vous annonce que vous avez gagné une somme faramineuse! Voilà qui est intéressant. Ce qui l'est moins, c'est qu'on vous demande des informations très personnelles. Si vous les envoyez à la personne mentionnée, ces informations pourront être utilisées pour diverses actions : faire un prêt bancaire, acheter une maison ou une voiture, faire un transfert de fonds... et cela, à VOTRE nom!

Méfiez-vous de ce genre de courriel qui vous garantit une somme immense. De toutes façons, ce genre de « concours » où on choisit une adresse au hasard n'existe tout simplement pas! Pour vous y faire croire, les fraudeurs vont utiliser divers moyens, le principal étant de vous faire croire que ça vient d'une personne milliardaire bien connue (par exemple, cette semaine, c'est Bill Gates lui-même qui voulait me donner 250 000 euros!).

Avec ce premier exemple, je vous invite à noter ces deux premières règles d'or :

RÈGLES D'OR DE LA SÉCURITÉ INTERNET

1- Si c'est trop beau pour être vrai, ce l'est sûrement!
2- N'envoyez jamais d'informations personnelles par Internet à une personne que vous ne connaissez pas, PRINCIPALEMENT si cette personne vous semble très gentille et absolument digne de confiance.

Exemple de fraude par courriel numéro 2 : La fraude « mon bon ami, aide-moi »

« Bonjou, mon ami. Je mapèl mamadou je sui un ami du nigéria.

Cé un ami à nous que j'ai recu ton courriel-adress. Il m'a donné, parce que il sais que tu as gran cœur. Voilà jai des enfant, treize enfants. J'ai le paludisme, et le hiv+, et jai perdu travail que j'aimai, à vendre et cuir des poulets pour les touristes du canada et d'europe. Comment je vai faire, pour faire nourri tou mes enfant. Je souffre beaucoup de la maldie, il faut que jachet tous les médicaments à la pharmcie. Je n,Ai plus l'argent pour vive. Alor, mon ami, j'en appel de ton grande générosité de ton cœur qui compren que je sui dans la souffranc du corps et de l,Esprit pour m'envoyé du bon argen canadien par la pitié de ton coeur. Envoi-le par la Western Union. Après, il faudra que tu m'envoi la copie de la transaction qui indique ton nom et mon nom et le montant (pour bien maidé, il faudfrais qi'il soit de 1863 de dollar du canada).

Merci de me répondre vit, ma vie et celles des enfants en dépend

De tout mon amitié,
Mamadou, arnaqueur! »

Explication :

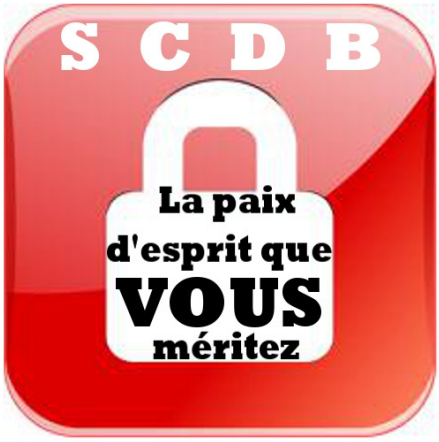
Comme c'est touchant! On a envie de pleurer en lisant ce genre de courriel. Et c'est le but recherché! Malheureusement, notre cher « Mamadou » n'est ni malade, ni au Nigéria! Il est assis bien au chaud, devant son ordinateur du MIELS (je le sais, puisque c'est moi!). « Comment s'opère la fraude, alors? Si j'envoie de l'argent au Nigéria, il faut que la personne soit au Nigéria pour la récupérer, non? » me direz-vous. Et c'est ce que le gros bon sens porte à croire, et voilà où on se fait avoir. Pour comprendre, voyons un petit résumé du fonctionnement de la « Western Union (WU)» : quand vous allez dans une succursale de la WU, vous déposez un certain montant, à l'intention d'une personne donnée, dans un pays donné. L'autre personne se rend alors dans sa succursale locale de la WU et récupère l'argent. Ainsi, **la Western Union est un système fiable et efficace pour envoyer de l'argent à l'étranger, à une personne de confiance!** Seulement, pour diverses raisons légales, dans certains pays, tout ce qu'il faut pour « intercepter la transaction », c'est le nom de l'expéditeur, le nom de la personne qui doit recevoir l'argent, le montant, et le pays où cet argent devrait aller. Même pas besoin de montrer de preuve d'identité! Voilà pourquoi l'expéditeur insiste pour que vous lui envoyiez le reçu de la transaction. C'est ce qu'il lui faut pour récupérer votre argent. Après ça... allez savoir où est rendu cet argent?

RÈGLES D'OR DE LA SÉCURITÉ INTERNET

3- N'envoyez pas d'argent à un inconnu par la Western Union (ou tout autre système de transfert d'argent). Ces services sont sécuritaires dans la mesure où vous êtes certains à 100% de la personne qui doit le recevoir (par exemple, un parent ou un enfant en voyage).

Allez, hop. Allons dans le plus sophistiqué en matière de fraude par courriel.

Système central de données bancaires



Cher client, chère cliente.

Comme vous le savez, le « Système central de données bancaires » (SCDB) est une base de données transcanadienne qui gère de façon sécuritaire et confidentielle les informations de tous les clients des diverses banques établies au Canada.

Suite à une défectuosité majeure de notre système informatique de bases de données, nous avons perdu des informations capitales sur des centaines de nos clients. La défectuosité a été réparée, mais les informations restent perdues. Heureusement, nous pouvons vous assurer qu'aucune personne malintentionnée n'a pu avoir accès à ces données durant la défaillance.

Afin de nous aider à vous assurer que vous ne serez pas affecté par ce problème dont nous sommes totalement désolés, nous aimerions que vous nous confirmiez certaines informations en cliquant sur ce lien : http://www.scdb.com/securite .html

Ayez en main les informations que vous devrez fournir (votre nom complet, votre adresse, votre numéro de téléphone, votre date de naissance, le nom de votre banque, votre numéro de compte, votre numéro de transit, ainsi que le montant de votre plus récente transaction bancaire). Ainsi, nous serons en mesure de valider votre identité, et de faire en sorte que votre dossier sécurisé soit mis à jour.

Merci de nous aider à protéger vos informations personnelles et à vous procurer la paix d'esprit.

Avec nos excuses pour les désagréments causés par cette situation,

Jérôme Claveau
Président directeur général et concierge du SCDB (et, aussi, arnaqueur à temps perdu!)

Explication :

POUAHAHA!!! J'en ris encore! C'est fou ce qu'on peut inventer avec un tant soit peu d'imagination! Et encore, j'ai mieux à faire que de frauder les gens, parce qu'avoir voulu, je vous aurais monté une page du « SCDB » des plus crédibles!

Vous comprenez sûrement déjà que le « Système Central des Données Bancaires » n'existe absolument pas. C'est le fruit de mon imaginaire, tout simplement. Dans un vrai courriel frauduleux, en cliquant sur le lien, vous seriez arrivés sur un formulaire vous demandant les informations citées plus haut. Ensuite, vous cliquez sur « Valider », et hop! Je reçois dans ma boîte de courriel un splendide message qui me donne toutes ces informations sur vous. Et c'est tout ce dont j'aurais besoin pour passer un coup de fil à votre banque et faire transférer le contenu de votre compte dans un autre (le mien, si possible ☺ !).

Bien souvent, dans ce genre de fraude, les arnaqueurs vont insister beaucoup sur la présentation du message, en essayant de copier une page d'une grande banque (bien souvent, ils n'y arrivent pas vraiment. Il suffit de regarder la quantité incroyable de fautes de français!).

Voici donc nos deux dernières règles d'or :

RÈGLES D'OR DE LA SÉCURITÉ INTERNET

4- Souvenez-vous que votre banque (la vraie!) ne vous demandera JAMAIS de lui envoyer des informations concernant votre compte par Internet, ni même par téléphone.

5- N'envoyez jamais d'informations personnelles sur vous et votre compte par Internet. JAMAIS!

La grande question :

« Oui, mais... comment ont-ils fait pour avoir mon adresse de courriel? Si ils ont mon adresse, c'est qu'ils doivent être honnêtes, non? »

Non! Il est assez aisé, en faits, d'acheter des disques compacts remplis d'adresses de courriel diverses. Comment fait-on pour faire un tel disque? Les chaînes de lettre, vous connaissez? Vous savez, ces messages qui vous demandent d'envoyer le courriel à un nombre important de vos contacts (en échange de quoi, vous aurez de l'argent qui tombera du ciel, ou bien on fermera votre compte... ou encore, il y a de magnifiques blagues ou images drôles ou des pensées, que vous désirez partager avec vos amis). Et bien, sachez que chaque fois que vous transférez un de ces courriels à vos contacts, leurs adresses (et la vôtre) s'ajoutent au message. Ainsi, une personne voulant monter une liste d'adresses de courriel n'a ainsi qu'à copier les adresses

contenue-s sur ces messages (et dans les faits, c'est généralement ces personnes qui créent ce genre de message).

Heureusement, il est facile de se protéger et de protéger l'adresse de ses amis. Il suffit, lorsque vous transférez un message, de prendre 15 secondes pour effacer les adresses contenues dans le texte du message. Du coup, vos amis reçoivent bel et bien la blague « tordante », sans que personne ne puisse avoir accès aux adresses de qui que ce soit. (en passant, partagez ce petit truc avec vos amis, pour qu'ils vous protègent aussi!).

Faites toutefois TRÈS attention avec ce qu'on appelle le « PPS » (les présentations Power Point) envoyez par courriel. Bien que souvent très amusantes à regarder, ces présentations présentent un danger potentiel pour votre ordinateur. Je l'ignorais moi aussi jusqu'à tout récemment, et peu de gens semblent le savoir. Donc, je vous le partage. C'est que bien souvent, une partie des données électroniques de la présentation n'est pas contenue dans le message que vous recevez. Le PPS est en quelque sorte « programmé » pour aller chercher cette information sur un autre ordinateur. Durant cette opération, la porte est grande ouverte pour que l'utilisateur de l'autre ordinateur puisse insérer un virus dans votre ordinateur, ou même y installer un programme malveillant (qui pourrait par exemple vous voler des données confidentielles, telles que mots de passe, coordonnées, etc.). Soyez donc extrêmement prudents avec ces fameux PPS qui vous promettent de rire aux éclats... vous pourriez finir en riant jaune!

En finissant, je tiens à rajouter que je n'ai mis que trois exemples d'arnaques par courriel. Il en existe une très grande quantité ! J'ai trouvé pour vous deux sites Internet fort intéressants qui les répertorient pratiquement toutes :
http://www.sq.gouv.qc.ca/cybercriminalite/legendes-urbaines/legendes-urbaines.jsp
http://monidentite.isiq.ca/decouvrez_menaces/pourriels.html

Voilà! N'hésitez pas à me contacter si vous voulez plus d'information sur le sujet. Je me ferai un plaisir d'aller chercher les réponses à vos questions! Et en attendant, ayez l'œil ouvert!

Jérôme Claveau

Vous avez des questions ou des idées de dossiers à traiter dans le prochain Vis-ta-VIH ?

Faites-nous en part ! Pour toute question que vous vous posez concernant les divers aspects du VIH (social, médical, biologique, moral, éthique, physique, alimentaire, etc.), nous ferons tout ce qui est en notre pouvoir pour trouver des réponses claires et faciles à comprendre. Ce sera la même chose si vous avez des idées de sujets à traiter.

Notre objectif est (et restera) de vous donner un VIS-ta-VIH qui répond à vos questions et vos besoins en matière de VIH.

Écrivez à intviecomm@miels.org.