ACCÉSSS
Alliance des Communautés Culturelles pour l'Égalité dans la Santé et les Services Sociaux

AUTORITÉ DES MARCHÉS FINANCIERS

Que signifie la fraude sur le Web ou le hameçonnage ?

Vous recevez un courriel d'une société avec laquelle vous faites affaire. On vous demande de mettre à jour immédiatement vos renseignements personnels. Le courriel vous informe généralement que :

- La société a été victime de fraude ;
- Quelqu'un essaie d'avoir accès à votre compte ;
- Une nouvelle loi oblige l'institution à vous demander de mettre à jour vos renseignements
- Etcétéra

On appelle également ce crime « usurpation de marque » (exemple : un courriel qui provient soi-disant des Caisses Desjardins).

Comment reconnaître un tel message et le différencier d'un message authentique ?

- Le contenu d'un courriel ou d'un message texte hameçon vise à déclencher une réaction impulsive de votre part. Ces courriels vous annoncent une nouvelle bouleversante ou excitante et vous demandent une réponse immédiate sous un faux prétexte. Les courriels hameçon ne sont habituellement pas personnalisés et comportent des fautes d'orthographe.
- En règle générale, les messages de ce genre vous demanderont de mettre à jour, de valider ou de confirmer les renseignements de votre compte, à défaut de quoi, les conséquences pourraient être fâcheuses. On pourrait également vous demander de faire un appel téléphonique.

Attention ! Bien souvent, le message ou le site Web comporte des logos qui semblent authentiques de même que d'autres renseignements d'identification tirés de sites Web légitimes. Les organismes gouvernementaux, les institutions financières et les services de paiement électronique constituent des cibles courantes pour l'usurpation de marque.

Que recherchent les fraudeurs ?

Votre numéro d'assurance sociale, votre nom complet, votre date de naissance, votre adresse complète, le nom de jeune fille de votre mère, vos noms d'utilisateur et mots de passe de services en ligne, votre numéro de permis de conduire, vos numéros d'identification personnels (NIP), des renseignements sur vos cartes de crédit (numéros, dates d'expiration et les trois derniers chiffres inscrits à l'endos de votre carte) et vos numéros de comptes bancaires.

À quoi vos renseignements pourraient servir ?

Grâce à vos renseignements, les fraudeurs peuvent accéder à vos comptes bancaires, ouvrir de nouveaux comptes, virer le solde de vos comptes, demander des prêts, des cartes de crédit et d'autres biens ou services, effectuer des achats, accéder à votre compte de courriel personnel, dissimuler des activités criminelles, recevoir des prestations du gouvernement ou obtenir un passeport.

J'ai reçu un courriel suspect; que puis-je faire ?

Signalez-le en envoyant un courriel à info@centreantifraude.ca ou en communiquant avec l'institution financière de laquelle il semble provenir.

Si vous avez reçu l'un de ces courriels suspects et que vous avez fourni sans le savoir des renseignements personnels ou financiers, faites ce qui suit :

- **Étape 1.** Communiquez avec votre banque ou votre institution bancaire ou la compagnie émettrice de votre carte de crédit.
- **Étape 2.** Communiquez avec les agences d'évaluation du crédit et demandez à ce que des alertes à la fraude soient inscrites à vos rapports de solvabilité.
    - Equifax Canada
      Numéro sans frais : 1 800 465-7166
    - TransUnion Canada
      Numéro sans frais : 1 877 525-3823
- **Étape 3.** Communiquez avec votre service de police local.
- **Étape 4.** Signalez toujours l'hameçonnage. Si vous avez répondu à un courriel suspect, signalez-le en envoyant un courriel à **info@centreantifraude.ca**

الاحتيال عبر النت

ما معنى الاحتيال عبر النت أو التصيّد؟

تتلقى بريدا الكترونيا من طرف شركة تتعامل معها. تطلب منك الشركة تحديث بياناتك الشخصية. يحتوي هذا البريد الالكتروني عادة على المعلومات التالية:

- تعرّض الشركة الى الاحتيال
- هنالك من يحاول الدخول الى حسابك
- يوجد قانون جديد يُلزم الشركة ان تحييّن بياناتك
- الى آخره...

نطلق على هذه الجريمة اسم "انتحال العلامة التجارية". مثال: بريد الكتروني يزعم انه مُرسل من قبل بنك ديجاردان Caisses Desjardins.

كيف التعرّف على هذا النوع من الرسالات و تفريقه عن الرسالات الحقيقية؟

- يرمي مضمون البريد الكتروني او الرسالة المكتوبة الطعم الى اطلاق ردّة فعل انفعالية منك. يعلمك هذا البريد بخبر مثير و مزعج و يطلب منك اجابة حينيّة تحت اعذار وهمية.يفتقر البريد الطعم عادة الى الطابع الشخصي و يحتوي على أخطاء لغوية.
- بصفة عامة، يطلب منك هذا النوع من الرسائل أن تُحييّن البيانات الموجودة في حسابك و أن تثبّتها و تؤكدها و ان لم تفعل فان العواقب ستكون وخيمة. ايضا، يمكن ان يطلب منك ان تتصل هاتفيا.

انتبه! في الغالب، تحتوي الرسالة او الموقع الالكتروني على علامات مميزة للدعاية متشابهة و بيانات كشف هوية تعادل تلك التي توجد على مواقع شرعية. تمثل المنظمات الحكومية و المؤسسات المالية و

خدمات الدفع الالكتروني المستهدفين السائدين لانتحال العلامة التجارية.

عن ماذا يبحث المحتالون؟

رقم التامين الاجتماعي، اسمك الكامل، تاريخ ميلادك، عنواك الكامل، اسم الام قبل الزواج، اسماء المستخدم و كلمات السر التي تستعملها في الخدمات الالكترونية، رقم رخصة السياقة، ارقام الكشف عن الهوية (NIP)، بيانات بطاقات الائتمان (الارقام، تاريخ انتهاء الصلوحية، الارقام الثلاث الاخيرة المسجلة في ظهر البطاقة) و ارقام حسابك البنكي.

فيم تُستخدم بياناتك؟

بفضل بياناتك، يمكن للمحتالين الدخول الى حساباتك البنكية و فتح حسابات جديدة ثم تحويل رصيدك و طلب قروض، بطاقات تأمين و غيرها من الخدمات، القيام بعمليات شراء و الدخول الى بريدك الالكتروني، التستر على نشاطات اجرامية، تسلّم استحقاقات حكومية أو التحصل على جواز سفر.

تلقّيت بريدا الكترونيا مشبوها فيه، ماذا يمكن ان افعل؟

بلّغ عن طريق بريد الكتروني ترسله الى info@centreantifraude.ca أو بالاتصال بالمؤسسة المالية التي يبدو متأتيا منها.

اذا تلقّيت بريدا الكترونيا مشبوها فيه و كنت قد مددت ببياناتك الشخصية أو المالية دون دراية ، قم بالآلي:

- **خطوة 1.** اتصل ببنكك او بمؤسستك البنكية او بالشركة التي اصدرت بطاقة التأمين.
- **خطوة 2.** اتصل بوكالات تقييم الائتمان و اطلب منها ان تسجّل انذارات ضدّ النصب في تقارير الملاءة الخاصة بك.

- **اكيفاكس كندا** **Equifax Canada**
رقم مجاني 1 800 465-7166

- **ترونس اونيون كندا** **TransUnion Canada**
رقم مجاني 1 877 525-3823

- **خطوة 3.** اتصل باقرب فرع شرطة في جهتك
- **خطوة 4.** بلّغ دائما عن التصيّد. اذا اجبت بريدا الكترونيا مشبوها فيه، ارسل بريدا الكترونيا الى info@centreantifraude.ca