La boîte à outils du fraudeur

À l'aide de tactiques diverses qui tirent profit de l'évolution des technologies, les fraudeurs essaient continuellement de nouvelles façons de voler des renseignements personnels et de l'argent à leurs victimes canadiennes.

Voici donc une description de certaines des stratagèmes qui font souvent partie de leur boîte à outils, ainsi que des conseils pour vous aider à les reconnaître et à vous en protéger.

Mystification

Les fraudeurs recourent à la mystification, une forme d'hameçonnage, pour faire croire aux destinataires d'une communication que celle-ci vient d'une source légitime. Ils peuvent changer le numéro de téléphone qui apparaît sur l'afficheur, envoyer des messages convaincants et créer des courriels qui semblent venir d'une personne que vous connaissez pour vous amener à leur fournir des renseignements personnels.

Conseil : Si vous recevez un appel de solliciteur qui vous demande des renseignements personnels, recherchez et composez le numéro officiel de l'entreprise. Ne rappelez pas le prétendu dérangement. Ignorez le cas d'un courriel ou d'un autre message électronique, placez le pointeur de votre souris sur le nom de l'expéditeur et examinez-le soigneusement pour repérer toute anomalie.

Urgence

Les fraudeurs emploient souvent des tournures qui donnent un sens d'urgence, comme « agissez sans tarder » ou « cliquez maintenant », pour vous inciter à payer de l'argent, à fournir des renseignements personnels ou à cliquer sur un lien avant d'avoir le chance d'examiner s'il a demandé est suspects.

Conseil : Les vraies urgences ne se communiquent pas dans un message. Prenez le temps de réfléchir pour vérifier si la demande paraît légitime. Communiquez d'une autre façon avec la personne ou l'organisme dont elle semble provenir pour confirmer la situation.

Manipulation affective

Les fraudeurs jouent sur les émotions pour vous faire croire à leur histoire afin que vous leur envoyiez des renseignements personnels ou de l'argent. Ils peuvent simuler des sentiments amoureux à votre égard, se faire passer pour un membre de votre famille ou pour un représentant d'un organisme de bienfaisance, ou faire semblant d'être en situation d'urgence.

Conseil : Méfiez-vous de toute personne rencontrée en ligne qui prétendra son amour ou son amitié pour vous, qui vous demandera de l'argent ou qui vous met mal à l'aise. Peu importe depuis combien de temps vous entretenez la relation virtuelle, il est important de rester sur vos gardes et de ne pas divulguer de renseignements personnels ou de l'argent.

Menaces

Les fraudeurs recourent souvent aux menaces. Si vous ne faites pas ce qu'ils demandent, ils peuvent vous menacer, vous ou les membres de votre famille, d'arnaquage, de blessures physiques, de conséquences financières ou de la publication d'informations ou d'images compromettantes.

Conseil : Si vous recevez un appel ou un message menaçant, raccrochez ou supprimez-le. Si vous sentez le besoin d'en vérifier la légitimité, communiquez avec l'organisme chargé de mener à exécution la présumée menace.

Fenêtres contextuelles

Les fraudeurs utilisent des fenêtres contextuelles (ou pop-up) qui s'affichent à votre insu pendant que vous amencer que vous avez remporté un prix ou que votre appareil est infecté. Ils espèrent ainsi vous faire cliquer sur un lien ou composer un numéro de téléphone afin de vous soutirer des renseignements personnels ou d'installer un malicel sur votre appareil.

Conseil : Protégez votre appareil en activant le bloqueur de pop-up et d'un bloqueur de publicité pop-up. Videz souvent votre mémoire cache et refusez les cookies. Évitez avant tout de cliquer sur les pop-ups. Ils peuvent vous mettre en danger.

Optimisation pour les moteurs de recherche

Les fraudeurs peuvent optimiser leurs sites Web de façon qu'ils apparaissent parmi les premiers résultats d'une recherche en ligne. L'apparence légitime de ces sites malveillants peut vous amener à fournir des renseignements personnels ou à télécharger un malicel.

Conseil : Ne présumez pas que le fait que figurer parmi les premiers résultats de recherche signifie que le site est légitime ou de qualité. Les fraudeurs créent souvent des sites Web qui ressemblent à des sites officiels, mais l'adresse électronique ou le nom de domaine est légèrement différent. Vérifiez toujours le fait et les coordonnées.

Liens et pièces jointes

En faisant des envois massifs de messages d'hameçonnage contenant des liens et des fichiers malveillants, les fraudeurs sont presque assurés de voir quelqu'un cliquer dessus. Ces liens et fichiers peuvent télécharger un malicel à votre appareil ou vous diriger vers un site frauduleux.

Conseil : Ne cliquez sur aucun lien qui vous a été envoyé par courriel, par site de réseautage social. Utilisez votre propre navigateur pour vous rendre au site et utilisez les coordonnées sont officielles. Ne répondez pas aux courriels qui vous demandent de vérifier la légitimité du message avant de télécharger les pièces jointes.

Usurpation d'identité

Les fraudeurs se renseignent sur des personnes et se font entourage afin de mieux usurper leur identité pour exécuter des escroqueries diverses, notamment de harcèlement.

Conseil : Ne présumez pas qu'un message vient vraiment de la personne que l'expéditeur prétend être, surtout lorsqu'il vous demande de cliquer sur un lien ou de télécharger un fichier. Vérifiez auprès de la personne concernée par des communications qui lui donnent une apparence de légitimité, mais il faut toujours vérifier l'identité de l'expéditeur par un autre moyen.

Toute personne qui croit avoir été victime de cybercriminalité ou de fraude est priée de le signaler à la police et au Centre antifraude du Canada (CAFC), en mesure de son système de signalement en ligne ou par téléphone au **1-888-495-8501**. Si un incident c'est produit, mais que vous n'êtes pas sûrd dans la piège, signaler le tout de même au CAFC.

CAFC

DÉTERMEZ PLUS DE CONSEILS POUR VOUS PROTÉGER ET PROTÉGER VOS APPAREILS À

PENSEZCYBERSECURITE.CA

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Numéro de catalogue : D96-192/2018F-PDF | ISBN : 978-0-660-07422-9