BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Qu'ont les fraudeurs dans leurs boîtes à outils? Et qu'y a-t-il dans la vôtre?

LA FRAUDE : IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA 2023-03-02

Le Mois de la prévention de la fraude portera cette année sur le thème « Les ficelles du métier : Qu'y a-t-il dans la boîte à outils d'un fraudeur? ». Nous vous présentons les principales astuces et tactiques utilisées par les fraudeurs pour faire des victimes au Canada. Nous vous aidons aussi à constituer votre propre boîte à outils pour vous protéger.

Qu'ont les fraudeurs dans leurs boîtes à outils?

Même si les fraudeurs changent constamment de tactique et exploitent les avancées technologiques pour voler des renseignements personnels et de l'argent, voici quelques-uns des outils qu'ils utilisent couramment :

- **Mystification** : Les fraudeurs s'en servent pour vous tromper et vous convaincre que vous communiquez avec des personnes que vous connaissez ou avec des entreprises et organisations légitimes. Ils peuvent modifier le numéro de téléphone apparaissant sur votre afficheur et l'adresse de l'expéditeur dans un courriel et créent souvent des sites Web qui ressemblent à des sites légitimes.
- **Urgence** : Les fraudeurs prétextent une urgence pour vous inciter à envoyer de l'argent, à fournir des renseignements personnels ou à cliquer sur des liens malveillants. En invoquant un motif d'urgence, ils veulent vous laisser moins de temps pour déterminer si la demande est suspecte.
- **Manipulation émotionnelle** : Les fraudeurs jouent avec vos émotions pour vous amener à croire leur histoire et à leur envoyer de l'argent. Ils utilisent cette tactique dans les stratagèmes de rencontre, les arnaques des grands-parents/besoin urgent d'argent, les fraudes liées aux organismes de bienfaisance, etc.
- **Menaces** : Les menaces sont souvent utilisées conjointement avec les prétextes d'urgence et la manipulation émotionnelle. Les fraudeurs peuvent menacer de vous arrêter, de vous causer des préjudices physiques ou financiers, ou de divulguer des renseignements ou des photos de nature délicate, ou proférer des menaces contre des membres de votre famille si vous n'envoyez pas d'argent. Ils peuvent aussi vous faire peur pour garantir que vous ne parliez pas de la transaction afin de vous isoler davantage.
- **Fenêtres contextuelles** : Il s'agit de boîtes qui apparaissent à l'écran de votre ordinateur ou de votre appareil. Elles peuvent indiquer que vous avez gagné un prix ou que votre

ordinateur est infecté et fournissent un numéro de téléphone sans frais à composer. Dans d'autres cas, il faut cliquer sur la boîte, ce qui permet aux fraudeurs d'installer un logiciel malveillant ou de vous mener vers un site frauduleux.

- **Référencement naturel** : Saviez-vous que les fraudeurs peuvent recourir au référencement naturel pour que leurs sites Web figurent dans les premiers résultats de votre recherche en ligne?

- **Liens** : En envoyant des centaines de milliers de messages contenant des liens malveillants, les fraudeurs sont assurés qu'une victime cliquera sur l'un d'eux. Les liens malveillants peuvent sembler suspects ou légitimes. Ne cliquez pas sur des liens dans des messages.

- **Usurpation d'identité** : Les fraudeurs peuvent se faire passer pour à peu près n'importe qui pour vous inciter à envoyer de l'argent ou des renseignements. Dans les cas de comptes de courriels d'entreprise compromis, les fraudeurs étudient les courriels et les échanges entre les employés afin de mieux se faire passer pour quelqu'un d'autre.

Qu'y a-t-il dans votre boîte à outils?

Soyez un détective chaque fois que vous recevez un message ou un appel. Vous attendiez-vous à cela? Communique-t-on généralement avec vous de cette façon? Y a-t-il des fautes d'orthographe ? Vous incite-t-on à cliquer sur un lien? Les fraudeurs essaient toujours de vous piéger, alors coupez-leur l'herbe sous le pied en vous méfiant de chaque message et appel et en vous rappelant les conseils ci-dessous.

- **Mystification** : Raccrochez et composez le numéro de téléphone officiel de l'entreprise ou de l'organisme en question. Si l'appelant prétend être une de vos connaissances, raccrochez et appelez vous-même le numéro qui figure dans vos contacts.

    - **Faux courriel** : Placez le pointeur de votre souris sur l'adresse de courriel de l'expéditeur ou cliquez sur répondre. Dans bien des cas, après avoir cliqué sur répondre, une adresse électronique différente apparaîtra.

- **Urgence** : Le temps joue en votre faveur. Vous n'avez pas à envoyer de l'argent, à cliquer sur un lien ou à répondre immédiatement. Prenez cinq minutes pour vous demander si l'appel ou le message vous semble suspect. Utilisez ce temps pour essayer les outils de votre boîte à outils.

- **Manipulation émotionnelle** : Méfiez-vous des interactions en ligne où une personne que vous venez de rencontrer vous déclare son amour ou son amitié, vous raconte une

histoire triste ou vous fait sentir en danger. Vous n'avez pas à vous sentir isolé(e); communiquez avec vos amis ou votre famille et parlez-leur de cette rencontre – voyez ce qu'ils en pensent. Consultez les différentes arnaques qui figurent dans l'index A-Z du CAFC pour voir si votre situation s'y trouve.

- **Menaces** : Si vous recevez un appel qui vous semble suspect, raccrochez! Mettez fin à l'appel si on vous menace, si on vous demande de l'argent ou des renseignements personnels ou si vous avez des doutes quant à la crédibilité de l'appel.
- **Fenêtres contextuelles** : Il existe bien des façons de protéger votre appareil. Installez un logiciel antivirus et des bloqueurs de fenêtres contextuelles. Videz votre mémoire cache et bloquez les témoins lorsque vous le pouvez. N'utilisez pas un réseau sans fil public ou des réseaux non protégés. Ne composez jamais un numéro de téléphone fourni dans une fenêtre contextuelle.
- **Référencement naturel** : Ne supposez pas que les premiers résultats sont synonymes de légitimité ou de qualité. Vérifiez le lien et les coordonnées. Les fraudeurs créent souvent des sites web d'apparence officielle, mais ils changent une lettre dans l'adresse ou utilisent un domaine différent.
- **Liens** : Si un lien vous est envoyé par courriel, par texto ou par message sur les médias sociaux, ne cliquez pas dessus. Vous pouvez consulter le site à l'aide de propre moteur de recherche ou trouver les coordonnées de l'entreprise dans votre moteur de recherche et communiquer directement avec celle-ci pour vérifier si le message que vous avez reçu était légitime.
- **Usurpation d'identité** : Ne présumez jamais qu'un message provient de la personne que l'expéditeur prétend être, surtout lorsqu'on vous demander d'envoyer quelque chose. Vérifiez l'identité de la personne en recherchant ses renseignements en ligne, en lui parlant en personne si vous la connaissez ou en lui posant des questions auxquelles elle seule connaît les réponses.

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