PARLONS PRÉVENTION

QUELQUES TYPES D'ARNAQUES À SURVEILLER

QU'EST-CE QU'UNE ARNAQUE?

Une arnaque est une fraude commise par un criminel qui soutire de l'argent ou des renseignements personnels de valeur à une victime. Les arnaques sont omniprésentes. Vu la dépendance du monde moderne à l'égard de la technologie, entre autres des téléphones intelligents et d'Internet, si vous n'avez pas encore été victime d'une arnaque, vous avez probablement à tout le moins déjà été ciblé par un fraudeur.

Quelques termes reliés aux arnaques

Il y a quatre termes clés qu'il faut comprendre lorsqu'on parle d'arnaques :

- **Arnaque :** opération frauduleuse dont le but est de voler de l'argent ou encore des renseignements financiers ou personnels de valeur.
- **Piratage psychologique :** technique utilisée pour manipuler une victime afin de l'amener à divulguer des renseignements ou à faire quelque chose en particulier.
- **Hameçonnage en ligne :** un fraudeur se fait passer pour une autre personne ou une entreprise légitime en ligne dans le but de voler de l'argent ou des renseignements personnels.
- **Hameçonnage vocal :** un fraudeur se fait passer pour une autre personne ou une entreprise légitime lors d'un appel téléphonique dans le but de voler de l'argent ou des renseignements personnels.

De nos jours, nombreux sont les fraudeurs qui tentent de pousser leurs victimes au pied du mur et de les forcer à agir immédiatement (par exemple à fournir une somme d'argent ou des renseignements personnels) en leur faisant croire qu'autrement, elles pourraient subir des conséquences. Les fraudeurs peuvent faire référence à l'actualité ou se faire passer pour un détaillant local que vous connaissez bien ou encore un membre de votre famille dans le besoin dans l'espoir de vous soutirer de l'argent ou des renseignements d'identification personnels (RIP).

Analyse de termes reliés aux arnaques

Piratage psychologique

Les fraudeurs continuent de raffiner leurs techniques de piratage psychologique et de trouver de nouvelles façons de vous convaincre de leur donner de l'argent et des RIP. Voici quelques-unes de leurs astuces :

- **Miser sur la familiarité :** vous croirez plus facilement à la légitimité d'une personne si vous connaissez son nom ou si vous l'avez déjà rencontrée. (Par exemple, on pourrait vous faire parvenir un courriel qui semble provenir d'une grande entreprise ou de votre institution financière).
- **Faire preuve d'hostilité :** c'est dans la nature humaine de céder aux demandes d'une personne agressive pour éviter le conflit. Donc, si vous considérez quelqu'un comme une menace, vous pourriez être plus susceptible de faire ce qu'il vous demande. (Par exemple, vous pourriez recevoir un appel d'une personne se faisant passer pour un policier et exigeant que vous lui payiez une amende pour annuler un mandat d'arrêt).
- **Jouer au détective :** il est plus facile que jamais de recueillir des renseignements sur vous. Il suffit d'accéder à vos comptes de médias sociaux pour savoir où vous habitez et connaître vos centres d'intérêt. Certains malfaiteurs pourraient aussi fouiller dans vos poubelles, à la recherche de formulaires de carte de crédit ou de relevés bancaires. Bref, il existe de nombreux endroits où les fraudeurs peuvent puiser des renseignements personnels utiles pour commettre leurs actes malveillants.

Hameçonnage en ligne, vocal ou par texto

- Les fraudeurs ont souvent recours aux techniques de piratage psychologique pour arnaquer les gens en ligne (hameçonnage en ligne), par téléphone (hameçonnage vocal) ou par messagerie texte (hameçonnage par texto). Selon Statistique Canada, environ un cinquième des entreprises canadiennes ont subi un incident de cybersécurité en 2021.[1]
- Qu'il soit effectué en ligne (par courriel ou sur des sites Web trompeurs), par texto ou vocalement, l'hameçonnage est la méthode de cyberattaque la plus courante mondialement.

Hameçonnage en ligne

- Les fraudeurs vous envoient des courriels qui semblent légitimes et vous incitent à cliquer sur le lien fourni. Ces courriels ont l'air officiels et visent souvent à créer un sentiment d'urgence pour que vous agissiez vite et que vous cliquiez sur le lien sans réfléchir. Généralement, ces liens renvoient vers une page frauduleuse, sur laquelle sont affichés le logo ou la marque d'une entreprise légitime pour mieux vous convaincre de l'authenticité de l'opération. Les courriels d'hameçonnage peuvent aussi contenir des liens qui lancent des logiciels malveillants ou espions et qui peuvent être activés lorsque vous cliquez dessus ou encore à votre insu.
- Les sites Web frauduleux sont conçus pour ressembler à des sites légitimes afin de tromper les visiteurs et de les inciter à saisir des renseignements tels que leur numéro de carte de crédit, leur adresse de courriel, leur numéro de téléphone et leur numéro d'assurance sociale. Si vous êtes convaincu de la légitimité d'un site, vous serez plus susceptible de divulguer des renseignements personnels aux fraudeurs.

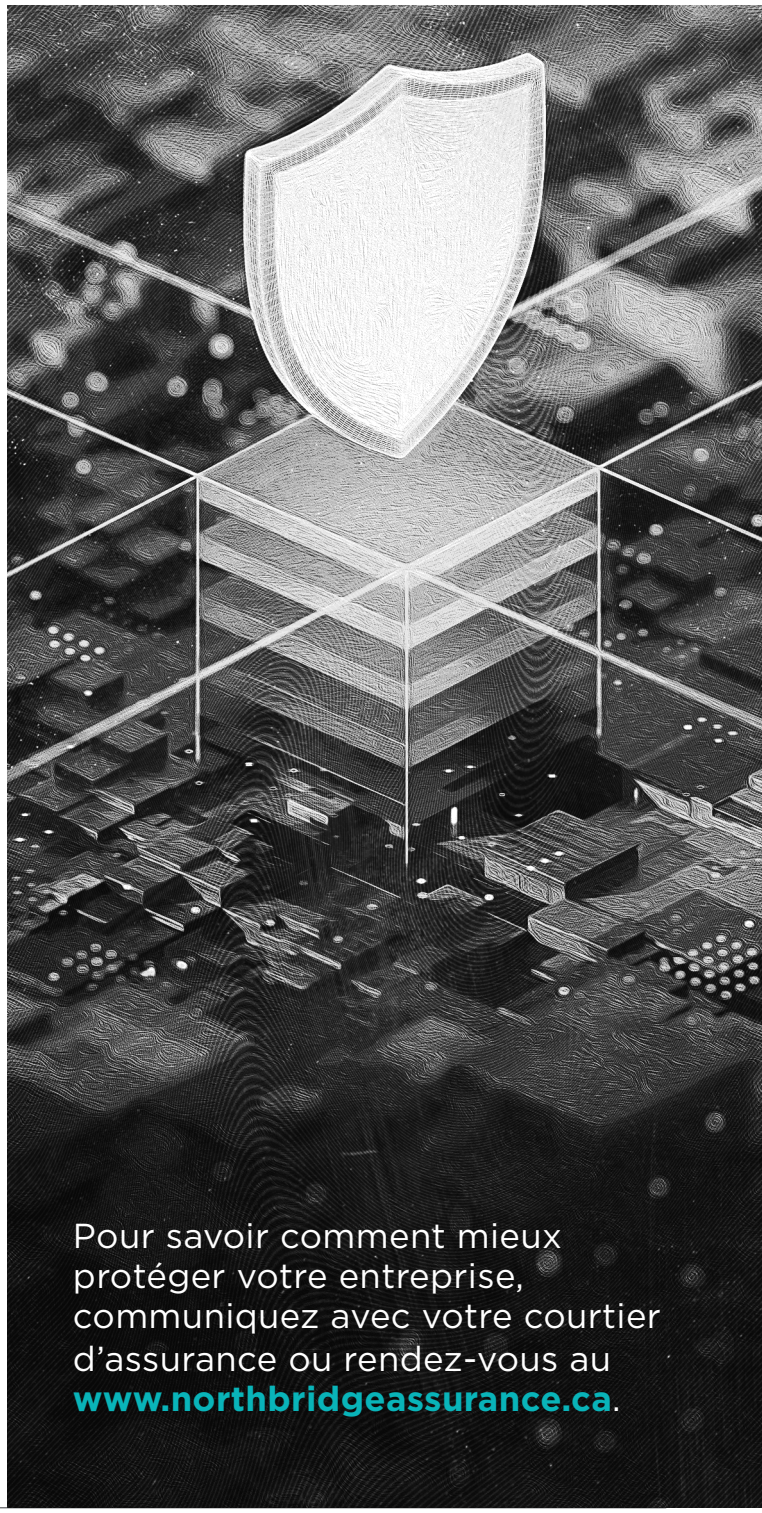
Hameçonnage vocal

- L'hameçonnage vocal s'effectue par téléphone. Les malfaiteurs peuvent se faire passer pour un représentant d'une banque, un ami d'un ami, un employé d'un restaurant ou toute autre personne de confiance dans le but de vous soutirer de l'argent ou des RIP. La différence entre ce type d'hameçonnage et l'hameçonnage en ligne réside dans le moyen utilisé pour commettre le méfait. De nos jours, les arnaques par téléphone sont un peu moins courantes que celles en ligne ou par messagerie texte, car il est maintenant très facile de filtrer les appels et de ne pas répondre à ceux qu'on n'attend pas.

Hameçonnage par texto

- On parle de ce type d'hameçonnage lorsqu'un fraudeur vous envoie un lien par messagerie texte, comme il le ferait par courriel, en faisant en sorte que vous ne vous doutiez de rien. Les messages textes étant généralement courts, les arnaqueurs peuvent essayer de vous convaincre de cliquer sur un lien en vous faisant croire que vous obtiendrez plus de détails sur un prix à gagner ou un remboursement quelconque.

Ils peuvent aussi avoir recours à d'autres types de messages pour tenter de créer un sentiment d'urgence et vous amener à agir.



Pour savoir comment mieux protéger votre entreprise, communiquez avec votre courtier d'assurance ou rendez-vous au **www.northbridgeassurance.ca**.

[4046-001-ed03F | 05.2023]

[1] Statistique Canada, *L'incidence du cybercrime sur les entreprises canadiennes*, 2021.

Northbridge Assurance | CYBERSCOUT A TransUnion® Brand