www.lapresse.ca /affaires/portfolio/2024-02-29/securite-informatique/texto-la-fraude-au-bout-du-doigt.php

Sécurité informatique et Texto, la fraude au bout du doigt

Marie-France Létourneau :

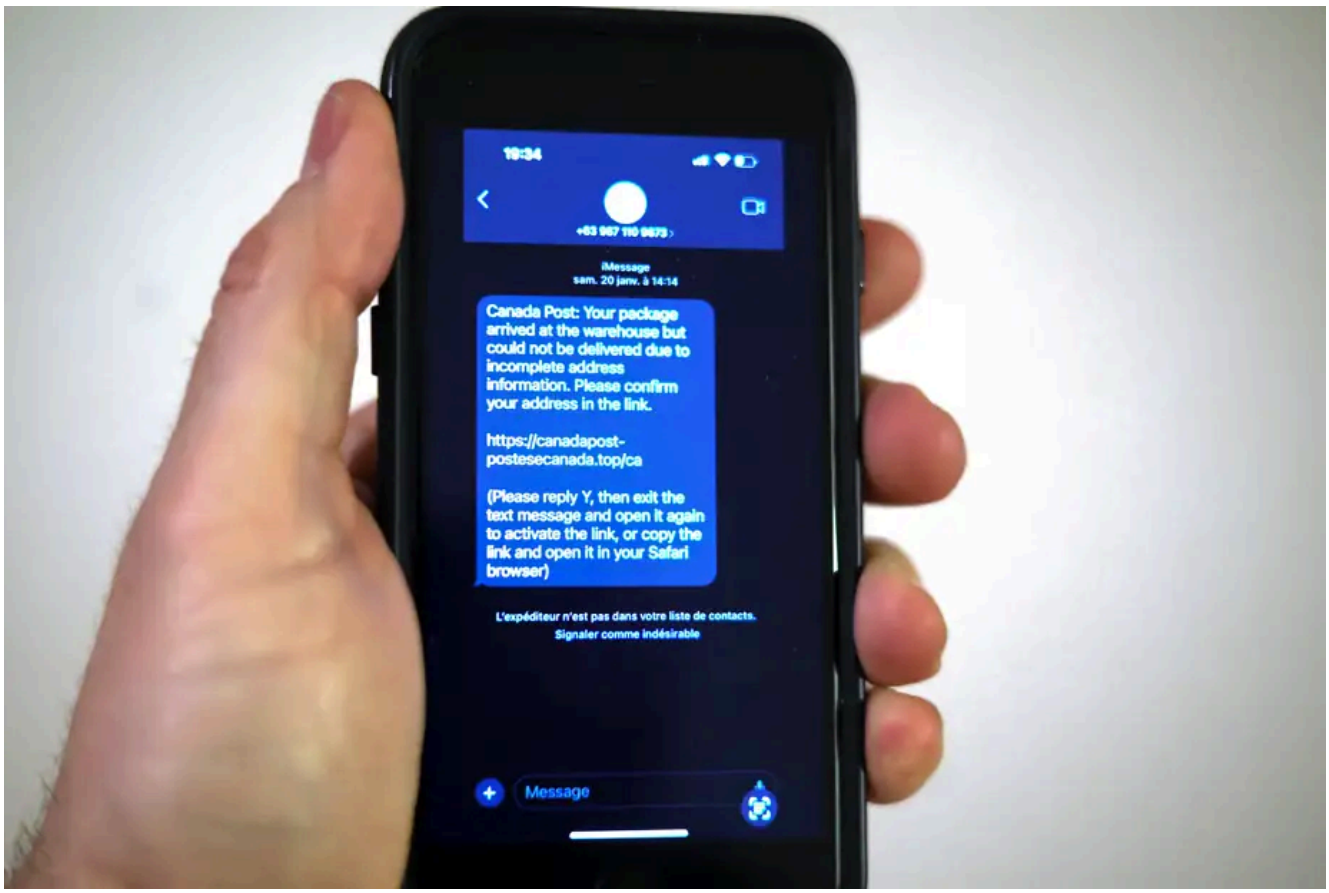

PHOTO MARTIN CHAMBERLAND, LA PRESSE

Les tentatives d’hameçonnage par message texte sont devenues monnaie courante.
Les fraudes impliquant Postes Canada sont fréquentes.

Les tentatives d’hameçonnage par message texte sont devenues monnaie courante.
Et l’imagination des fraudeurs ne semble pas avoir de limites.
Si certains stratagèmes sont plus difficiles à repérer, il est néanmoins possible, en portant attention à certains éléments, de ne pas tomber dans le panneau, selon Olivier Bilodeau, directeur recherche en cybersécurité chez GoSecure, à Montréal.

Le message est-il pertinent ?

C’est la première question à se poser.
Est-il normal que la personne ou l’institution à l’origine du texto (*Short Message Service*) souhaite nous contacter de cette façon ? relève Olivier Bilodeau.
Détail important, selon lui : la source de l’émetteur d’un texto est très facile à modifier. Même si le message

semble provenir, par exemple, de « Revenu Québec – 1 800 267-6299 » (une information exacte), il peut avoir été émis par un tiers qui falsifie sa provenance, affirme l'expert en cybersécurité.
Celui-ci recommande ainsi de ne pas hésiter à joindre l'individu ou l'organisme à un numéro de téléphone « de confiance » pour valider l'authenticité du message.

PHOTO CHARLES WILLIAM PELLETIER, COLLABORATION SPÉCIALE

Il est possible de déjouer les fraudeurs en adoptant certaines pratiques, estime Olivier Bilodeau, directeur recherche en cybersécurité chez GoSecure et président de NorthSec.

Gare aux liens dans les messages textes

L'analyse des liens inclus dans les messages textes peut aider à valider ou pas la légitimité des envois.
Olivier Bilodeau, qui préside NorthSec, une conférence doublée d'une compétition de cybersécurité annuelle à Montréal, cite en exemple un texto reçu de Postes Canada, accompagné du lien : https://hope-tq.top/.
Ce dernier n'étant pas relié à l'organisme, il vaut mieux s'abstenir de donner suite au message.

Il faut par ailleurs y regarder par deux fois, car la différence entre le lien officiel et le lien frauduleux est parfois ténue.
Tout peut se jouer sur l'ordre de quelques lettres.
La vigilance est de mise.

Méfiez-vous du sentiment d'urgence

Que ceux qui n'ont jamais reçu un texto les avisant que des frais supplémentaires sont nécessaires pour assurer la livraison imminente d'un colis (qu'ils n'ont pas commandé) lèvent la main.

Ce type de message texte, populaire par les temps qui courent, illustre bien une des techniques utilisées par les fraudeurs, celle de miser sur le sentiment d'urgence, note Olivier Bilodeau.

Les services de livraison étant plus sollicités que jamais, certains arnaqueurs y voient une occasion à exploiter.

Dans cet esprit, souligne le directeur chez GoSecure, si vous recevez un texto d'une personne que vous connaissez et qui semble en détresse, lâchez-lui un coup de fil pour valider la situation.

Des frais à payer, vraiment ?

Les gouvernements, les institutions financières ou toutes les autres sociétés d'État ne communiquent pas avec les citoyens pour les inviter à laisser une enveloppe avec de l'argent en espèces ou en cartes-cadeaux, fait valoir Olivier Bilodeau.

Selon lui, il faut également se méfier des demandes de virements en ligne ou en bitcoins. Ce type de message devrait automatiquement être jugé suspect.

Le directeur recherche en cybersécurité cite cet exemple.

« Pourquoi le FBI me demanderait 500 $ en cartes-cadeaux Walmart, alors qu'il dit me suspecter d'un crime ? »

Si plusieurs flairent rapidement l'arnaque, certains tombent, malgré tout, dans le panneau, déplore Olivier Bilodeau.

Fautes d'orthographe et outils pour repérer les types de fraude

La présence d'erreurs d'orthographe dans les textos peut être un indice de tentatives d'arnaque.

Mais la donne tend à changer. L'utilisation de l'intelligence artificielle pour la traduction ou la rédaction des messages contribue à atténuer cette faille, estime Olivier Bilodeau.

Des outils sont par ailleurs offerts pour distinguer le vrai du faux.

La Clinique de cyber-criminologie de l'Université de Montréal a créé Fraude-alerte.ca, une plateforme communautaire sur laquelle sont référencées les fraudes relevées sur l'internet et par texto.

Le Centre antifraude du Canada répertorie également les différents types de fraude.

Il est possible d'y signaler les tentatives d'arnaque et d'obtenir des informations, si vous croyez avoir été victime d'une fraude.

Consultez le site Fraude-alerte.ca Consultez le site du Centre antifraude du Canada

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240229
"C'est ensemble qu'on avance"