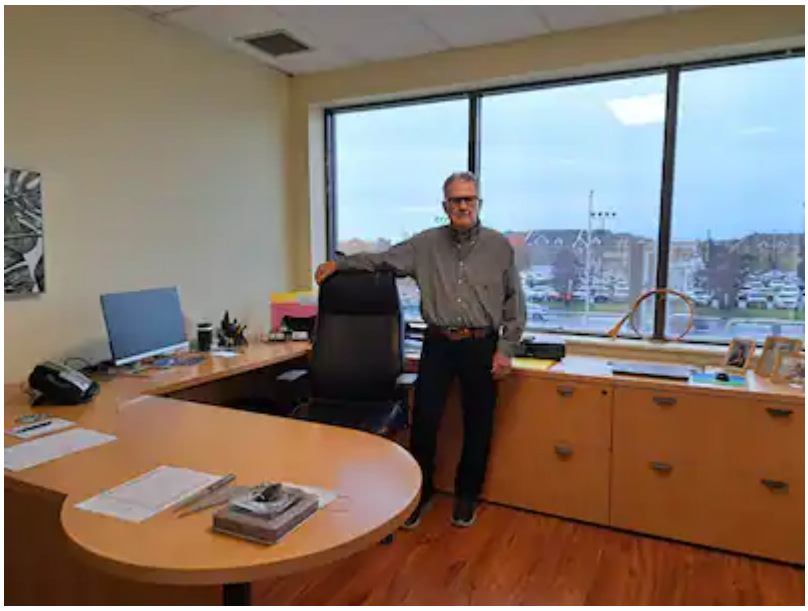
www.journaldemontreal.com /2023/10/28/comment-perdre-350-000--en-5-minutes

«Ça va couper ma retraite» et des hackers lui dérobent 350 000 $ à 77 ans

Julien McEvoy :



La Banque Nationale n'est pas la seule à ne pas lever le petit doigt quand des clients se font vider leur compte par des *hackers*.
Toutes les institutions financières font la même chose et laissent à elles-mêmes des victimes humiliées et désespérées.

• À lire aussi: La banque n'appelle jamais

• À lire aussi: Zéro protection contre les fraudes bancaires

• À lire aussi: D'autres PME arnaquées à la Banque Nationale

«Je n'ai pas besoin de mon 350 000$ pour vivre, mais ça va couper ma retraite court», dit Guy Fortin, 77 ans, en affaires depuis 50 ans.

Le 25 juillet, le propriétaire du Groupe Pador, une entreprise de Montréal, s'est fait dérober 350 000$ dans son compte entreprise de la Caisse Desjardins.

À 77 ans, soyons francs, c'était une proie facile.
Son erreur?
Avoir lui-même téléphoné au numéro indiqué dans un courriel frauduleux pour le renouvellement d'une licence McAfee.

Il pensait parler à une entreprise sérieuse en appelant pour annuler le paiement de 529,99$ qu'on lui demandait.

Il a plutôt téléphoné dans un centre d'appels qui ne fait que ça, des fraudes.

Les *hackers* lui ont envoyé une invitation TeamViewer afin de prendre le contrôle de son ordinateur.
Il a accepté.
Puis tout a déboulé.

«Mon écran est devenu noir.
J'ai perdu le contrôle de mon ordinateur pendant trois jours.
Quand je l'ai repris, le mal était fait», raconte le septuagénaire.

Les fraudeurs ont fait trois virements vers Hong Kong, pour un total de 350 000$.
Le premier a eu lieu le 25 juillet, le deuxième le 27 et le troisième le 28.

Même si Guy Fortin n'a jamais viré d'argent ailleurs qu'au Canada et aux États-Unis, les transactions vers l'Asie sont passées comme dans du beurre.

Jamais la Caisse n'a levé un drapeau avant qu'il ne soit trop tard.
Elle n'a pas non plus appelé son client pour lui demander si c'était bien lui qui venait de virer 350 000$.

Pas de remboursement

Desjardins utilise pourtant la biométrie vocale, une technologie qui permet d'identifier un individu grâce à sa voix au téléphone, indique Simon Marchand, expert en fraude.

Mais la Caisse n'a appelé M. Fortin que le 1er août, et non au moment du crime.
De son côté, l'entrepreneur pensait parler à la banque tout ce temps, mais il s'adressait aux fraudeurs.

- **Écoutez le segment judiciaire avec Nicole Gibeault via QUB radio :**

Il existe aussi une autre technologie, la biométrie comportementale, qui permet de cibler les habitudes des clients et de détecter des anomalies quand un étranger manipule un compte ou une session AccèsD.

«Un Indien de 22 ans ne manipule pas une souris comme un Québécois de 77 ans», illustre Simon Marchand, qui ajoute que Desjardins n'utilise pas la biométrie comportementale.

Hors de lui, Guy Fortin a signifié le crime à la police et demande à Desjardins de le rembourser.
La Caisse refuse.
Dans une lettre datée du 16 août, celle-ci indique à son client que «l'ensemble des circonstances» l'oblige à refuser sa réclamation.

«J'ai travaillé fort toute ma vie, je suis en affaires depuis longtemps et je pense que je suis un pas pire administrateur.
Je n'ai jamais mangé une claque sur la gueule de même», dit celui qui est client de Desjardins depuis 30 ans.

Il accuse Desjardins d'avoir manqué à ses obligations en ne réagissant pas assez vite lors du crime.

La Caisse, elle, répond que ses équipes de prévention de la fraude sont entrées en communication téléphonique avec M. Fortin dès la première transaction.
«Puisqu'il avait été dument authentifié et qu'il avait autorisé le transfert, nous ne pouvons pas procéder à un remboursement des sommes», indique un porte-parole.

Pour Simon Marchand, il s'agit d'une triste histoire qui mériterait un meilleur dénouement.

«Les fraudeurs ciblent délibérément les personnes âgées.
On ne peut pas les laisser se faire frauder comme ça, on a une responsabilité comme entreprise ou comme société», plaide l'expert.

Cinq types de fraudes à surveiller

Que ce soit votre grand-mère de 84 ans ou votre petit frère de 18 ans, tout le monde va se faire avoir par une fraude d'ici sa mort.
Voici les 5 exemples les plus fréquents à l'heure actuelle.

La fraude par texto

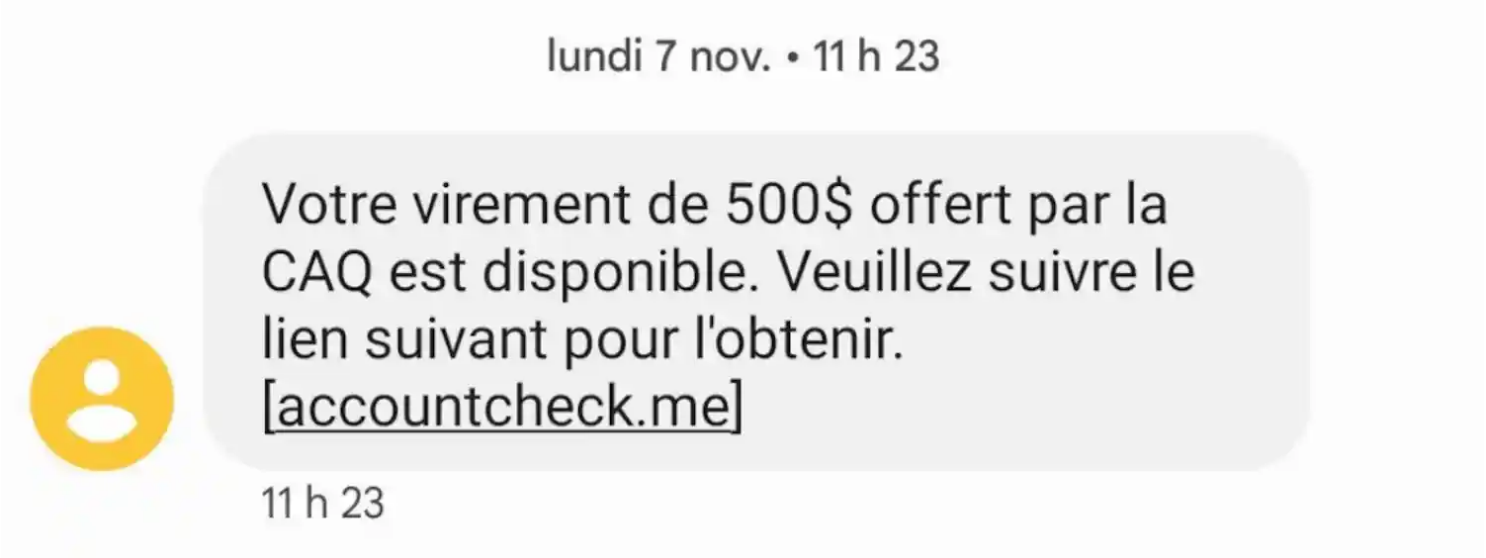


photo tirée du site web de HEC Montréal

Des groupes de *hackers* envoient le même message à 100 000 ou 1 000 000 numéros de téléphone.
L'envoi se fait en même temps et prend 1 minute.
Si trois personnes sur 100 000 tombent dans le panneau, le fraudeur peut faire des milliers de dollars en moins de 60 minutes.

Le retour des colis

Il existe une multitude de formations sur la fraude sur le *darkweb*, dit l'expert Simon Marchand.
«Le niveau de compétence requis pour frauder n'a jamais été aussi bas», dit-il.
Par exemple, il est facile de trouver un document de 60 pages qui explique en détail comment frauder en

retournant systématiquement tous les colis qu'on reçoit.
De quoi donner envie à n'importe qui de se lancer dans la fraude.

Le *spoofing* – usurpation d'identité

C'est ce qui est arrivé à David Trubiano (*voir autre texte*).
Les fraudeurs font semblant d'appeler de la banque.
Ils utilisent une technique très simple.
Ils volent votre mot de passe.
Ils vous parlent au téléphone et se connectent à votre compte en ligne.
Vous recevez un texto avec un code de sécurité.
Ils vous demandent de le leur donner pour confirmer votre identité.
Ils vous volent votre argent.
Et la banque refuse de rembourser.

L'argent facile sur internet

C'est probablement la fraude la plus ancienne de l'Internet.
On y a ajouté la cryptomonnaie, souvent utilisée pour soutirer des milliers de dollars à des gens avides de gains rapides.
Selon le Better Business Bureau, qui recense tous les types de fraudes, ceux qui se font avoir par une fraude liée à l'investissement perdent en moyenne 5500$.
C'est la plus dévastatrice des fraudes recensées par le BBB.

Ce que la Banque Nationale reproche à ses clients

Quand elle a remboursé ses clients entrepreneurs fraudés récemment, la BNC a tenu à souligner qu'ils étaient tous sans exception responsables de leur malheur.
Ils ont cliqué sur un lien, peut-être, a dit le chef de la sécurité de la banque.
Sont-ils responsables pour autant de voir 250 000$ disparaître du compte?
Non, dit l'expert Simon Marchand.
Si on obligeait les banques à rembourser, elles investiraient davantage dans la sécurité. Aussi simple que ça, lance-t-il.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231028
"C'est ensemble qu'on avance"