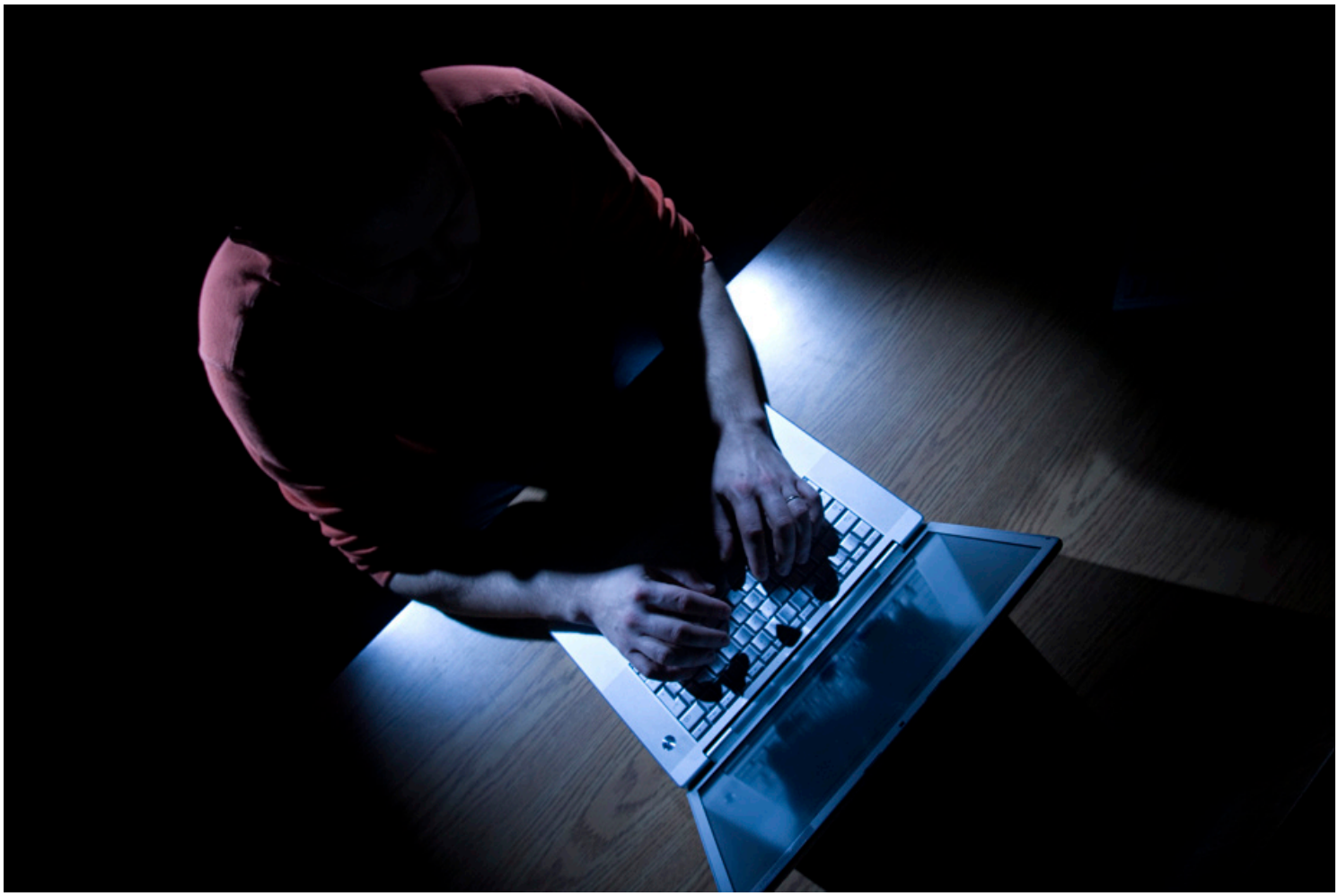
Fraude et réfléchir un peu avant de cliquer
Sécurité informatique

Emilie Laperrière :



Vol d’identité, hameçonnage, faux sites web : les fraudeurs informatiques rivalisent d’imagination pour attraper leur prochaine victime, et leurs techniques deviennent de plus en plus sophistiquées.
Pour éviter de tomber dans le panneau, il faut adopter les bons réflexes, user de prudence et, surtout, prendre du recul avant de cliquer.

« Depuis quelques mois, les fraudes les plus répandues au pays sont liées aux investissements », constate Benoît Dupont, professeur à l’École de criminologie de l’Université de Montréal.
« On parle de tout ce qui concerne les cryptoactifs.
Ce n’est pas le plus grand volume de fraudes, mais en matière d’impacts, de montants et de préjudices financiers, c’est la fraude numéro un », dit-il.

Les fraudes amoureuses, où le fraudeur établit une relation virtuelle avec la victime avant d’essayer de la convaincre de lui envoyer de l’argent, demeurent un grand classique, selon celui qui est également titulaire de la Chaire de recherche du Canada en cybersécurité.

« On trouve aussi les fraudes marchandes, liées au commerce en ligne, notamment sur Marketplace », ajoute-t-il.

Emeline Manson, formatrice en prévention des fraudes et en cybersécurité, remarque pour sa part une recrudescence des fraudes ciblant les personnes âgées.
« C'est un cas où le malfaiteur contacte un grand-parent en se faisant passer pour son petit-enfant.
Il prétend alors qu'il a un problème – qui va du bras cassé au passeport perdu jusqu'à la prison – pour obtenir de l'aide financière », explique-t-elle.

Prévenir plutôt que guérir

Comment peut-on s'assurer de ne pas devenir la prochaine victime ?
« C'est très difficile, admet Benoît Dupont.
Les fraudeurs sont des professionnels qui comprennent parfaitement les mécanismes de persuasion et le fonctionnement des plateformes en ligne. »

Selon lui, il vaut mieux être « extrêmement conservateur » dans ses pratiques sur l'internet.
L'expert conseille par exemple d'acheter seulement sur une poignée de sites marchands très réputés, de restreindre ses activités à des plateformes que tout le monde utilise et de limiter ses interactions aux personnes que l'on connaît déjà.

PHOTO DOMINICK GRAVEL, LA PRESSE

Emeline Manson, formatrice en prévention des fraudes et en cybersécurité

Emeline Manson mise de son côté sur les émotions.
« Ça peut sembler bizarre, mais je crois que c'est essentiel de savoir à quoi on est le plus sensible, ce qui nous fait réagir. »
En formation, elle aborde quatre émotions rattachées à la cybersécurité : la cupidité (ou la proposition attrayante), la curiosité, la peur et la serviabilité.

La première concerne toutes les offres trop belles pour être vraies, comme une offre d'emploi au salaire mirobolant.
Un proche qui nous envoie une vidéo en nous demandant si c'est nous s'en prend à notre curiosité.
Les situations où des conséquences graves peuvent survenir si on n'agit pas immédiatement – comme une fenêtre qui s'ouvre pour nous aviser qu'il y a un virus sur notre ordinateur – jouent plutôt sur la peur.
Et si un ami nous écrit sur Messenger parce qu'il a un problème avec son compte Interac, on aura évidemment envie de l'aider.

Généralement, toute tentative de fraude vient titiller l'une de ces émotions [cupidité, curiosité, peur ou serviabilité].
Il faut prendre un pas de recul pour analyser la situation, surtout si elle nous fait réagir.

Emeline Manson, formatrice en prévention des fraudes et en cybersécurité

On peut par exemple communiquer avec notre proche par un autre mode de communication pour vérifier l'information.

Des outils méconnus

L'information représente d'ailleurs la meilleure arme pour se protéger de la fraude.
Or, si des outils existent, le grand public n'en connaît généralement pas l'existence.

Benoît Dupont remarque que certains navigateurs offrent une extension pour vérifier la légitimité d'un site web.
« Les sites marchands, comme Amazon, permettent aussi d'évaluer la réputation de chacun des vendeurs », souligne-t-il.

Le professeur a en outre fondé à la Clinique de cyber-criminologie de l'Université de Montréal la première plateforme communautaire de signalement de cas de cyberfraude au Québec : Fraude-alerte.ca.
« On peut notamment entrer un numéro de téléphone, une adresse courriel ou le profil d'une personne pour vérifier si un historique de fraude y est associé. »

Consultez le site Fraude-alerte.ca

Et si on a mordu à l'hameçon ?

Les deux experts s'entendent pour dire que dans un monde idéal, toute fraude devrait être signalée à la police.
« On sait toutefois que ça demande du temps et que c'est décourageant de raconter son histoire pour une énième fois en sachant que ça ne débouchera pas sur grand-chose », convient Emeline Manson.

Selon Benoît Dupont, la fraude informatique devient un problème endémique au Canada. « Toutes les institutions qui font partie de la solution, des services de police aux banques, devraient essayer de se coordonner pour mieux y répondre. »
L'appel est lancé.

41 111

C'est le nombre de victimes de fraude d'un océan à l'autre en 2023, selon le Centre antifraude du Canada.
Ce chiffre représente uniquement la pointe de l'iceberg, selon les experts, puisqu'une faible proportion des fraudes sont signalées aux autorités.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240324
"C'est ensemble qu'on avance"