



Aide-mémoire

Les fraudes par textos



Les reconnaître et s'en protéger

C'est la plus un des genres de fraudes parmi les plus répandus actuellement, compte-tenu de l'omniprésence des téléphone intelligent. On parle ici de fraude « rapide », avec peu d'interaction avec votre malfaiteur qui n'ont qu'une idée en tête, vous dérober vos informations personnelles en utilisant tous les moyens possibles pour vous bernier.

Comment peut-on reconnaître un message texte frauduleux?

- La source est crédible. Pour attirer votre attention et tromper votre vigilance, les fraudeurs vont imiter les établissements bancaires, les société d'État et même les divers paliers de gouvernement. *Figure 1*
- On veut vous faire **peur**. Très souvent vous serez placé face à un ultimatum dont le délai de réponse doit être court. Tout est pensé pour vous désespérer et vous empêcher de réfléchir. *Figure 2*
- Le texte est en anglais ou est mal écrit (beaucoup de fautes). Soyons clairs, Desjardins ne vous écrira pas en anglais et jamais Vidéotron ne tolérerait un message rempli de fautes. *Figure 3*
- Pour qu'un hameçon soit efficace il faut un appât. Dans de très nombreux cas de fraude, on vous offre de l'argent en cadeau pour une pléthore de raisons (Bon client, trop perçu, impôts revus, ou pur inconnu généreux) mais pour l'obtenir, il vous faut suivre le lien inscrit au message. *Figure 4*
- Justement, un autre très bon indice est ce fameux hyperlien à suivre. Rappelez-vous que l'hyperlien n'est jamais au nom de l'institution qui vous écrit,

(www.Bell.xo.usager.monsieurX) par exemple n'est PAS l'adresse de Bell). Il est souvent aussi très long.

- Le transfert de numéro est la nouvelle fraude à la mode au Québec. Le texto en question vous annonce qu'à votre demande, votre numéro changera de fournisseur dans les prochains jours. Si ce n'est pas le cas, il faut contacter le numéro inscrit. Ce stratagème permet aux fraudeurs de s'emparer de votre numéro de cellulaire et d'en extraire plusieurs données de valeur. Il n'est en aucun cas recommandé de téléphoner au numéro inscrit, toutefois vous devez prendre contact avec votre fournisseur pour mettre fin aux démarches.

Que faire avec un texto frauduleux?

Rien. 

On ne clique sur aucun lien, on n'y répond pas, on l'ignore tout simplement. Un hameçon ne sert à rien tant que personne n'y mord. On supprime et c'est tout. Certaines institutions comme Desjardins ont un numéro pour leur transférer le texto suspect, mais ces mesures sont plutôt rares.

Vous avez un doute? C'est normal, mais si c'est le cas, passez par votre navigateur et allez vérifier via le site Web de l'institution qui vous a contacté. Le plus important est de ne **jamais cliquer sur le lien** inscrit dans le message.

Pourquoi ne **jamais cliquer sur le lien**? Cette simple opération peut mener à l'installation d'un virus ou d'un Cheval de Troie, ce qui peut mener aux fraudeurs à pouvoir :

- Lire nos notifications
- Voir la liste de nos contacts
- Connaître notre géolocalisation
- Intercepter et envoyer des SMS
- Renvoyer des appels téléphoniques
- Installer et démarrer des applications
- Regarder ce que l'on tape sur notre clavier

En résumé

- On ne clique jamais sur un lien provenant d'un message suspect
- Dans le doute, vérifiez! N'ayez jamais peur de téléphoner pour poser des questions.

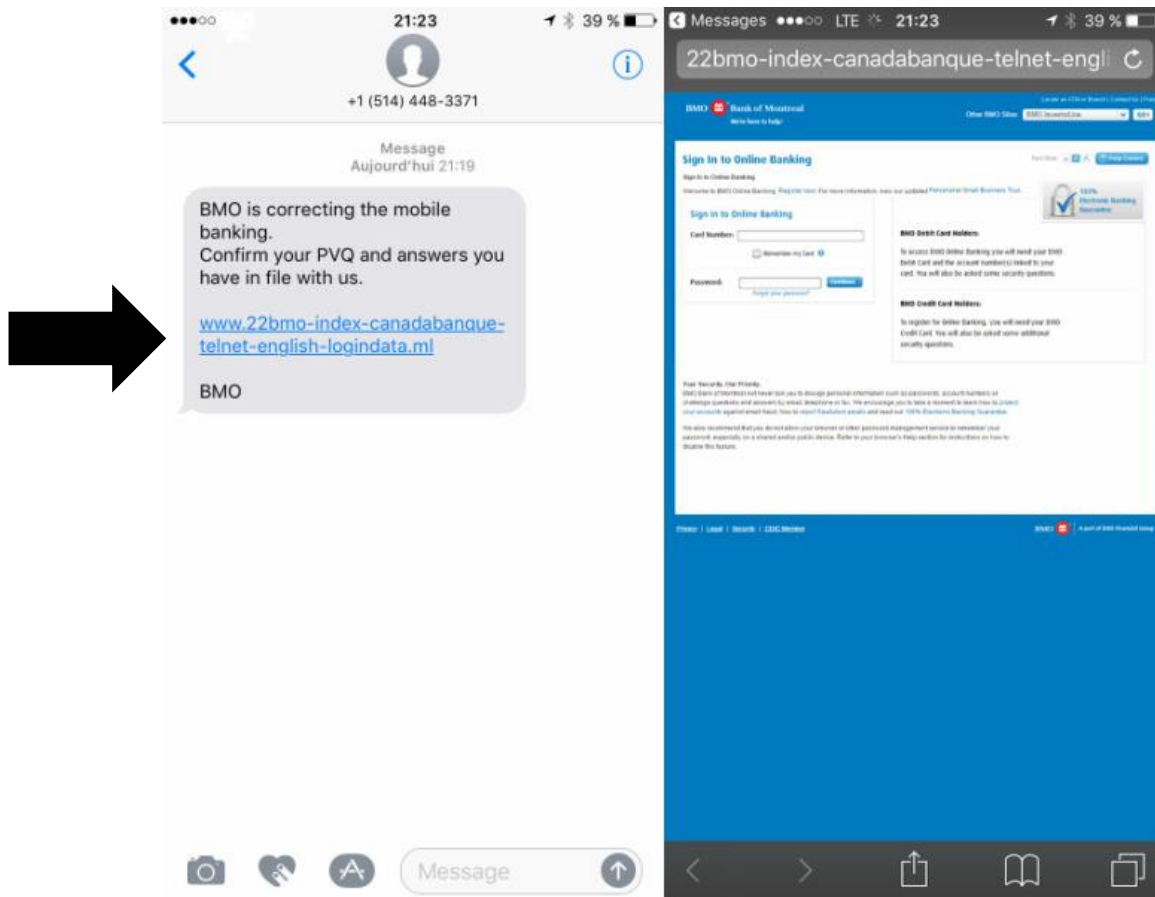


FIGURE 1

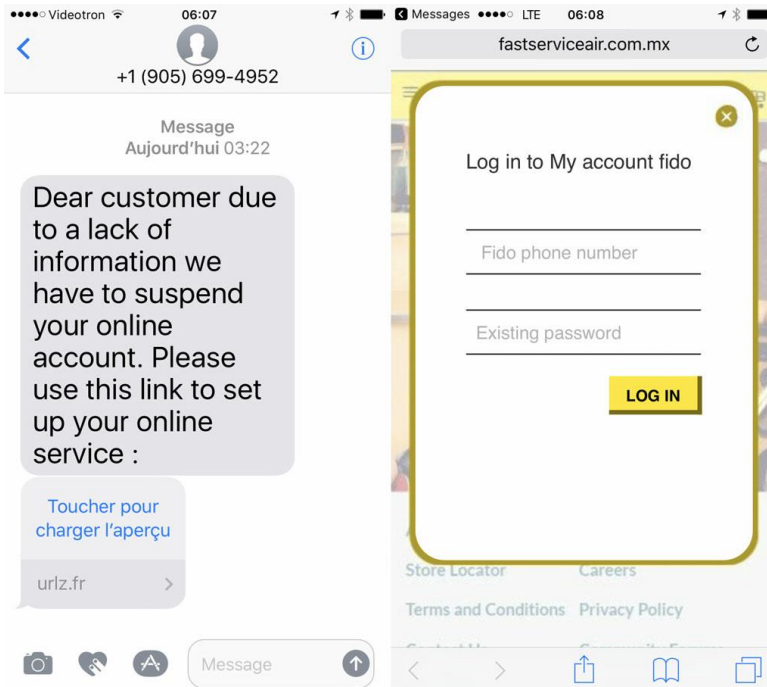


FIGURE 2



FIGURE 3

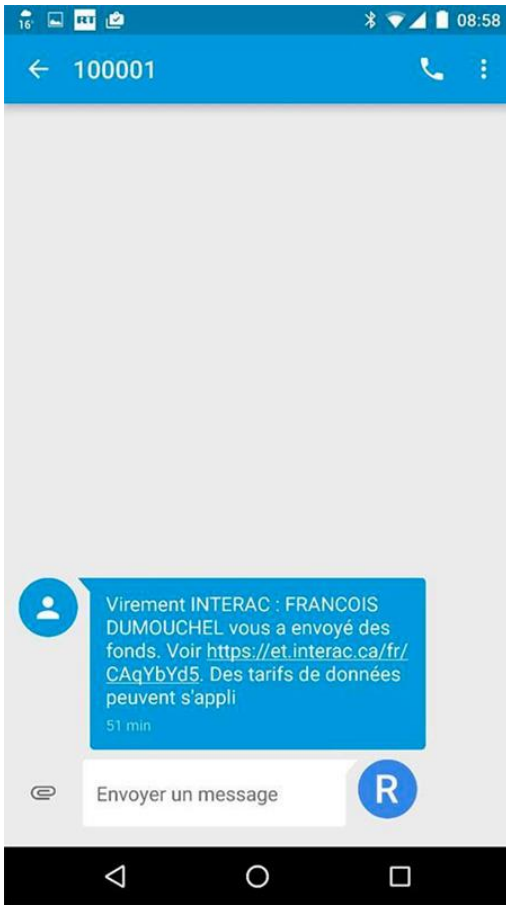


FIGURE 4