CANADIAN ANTI-FRAUD CENTRE BULLETIN

Sensibilisation et prévention de l'hameçonnage : partie 1 2022-10-12

FRAUD: RECOGNIZE, REJECT, REPORT

Le présent bulletin a été préparé en vue d'informer le public dans le cadre de la campagne du Centre antifraude du Canada (CAFC) pour le Mois de la sensibilisation à la cybersécurité en octobre.

En date du 30 septembre, 2022, le CAFC a reçu 7051 signalements de messages hameçon qui ont fait 1722 victimes. L'hameçonnage est une activité qui prend la forme de courriels ou de messages textes trompeurs prétendument envoyés par une organisation légitime comme une institution financière, une entreprise ou un organisme du gouvernement dans lesquels on vous demande de cliquer sur un lien ou de télécharger une pièce jointe pour toutes sortes de raisons. Le but est de voler vos renseignements personnels et financiers.

Les victimes d'hameçonnage peuvent aussi être victimes de ce qui suit :

Fraude à l'identité

Après avoir volé vos renseignements personnels, les fraudeurs peuvent utiliser votre identité pour :

- accéder à vos comptes bancaires;
- ouvrir de nouveaux comptes bancaires;
- effectuer des transferts de solde;
- faire des demandes de prêts et de cartes de crédit;
- acheter des biens et des services;
- dissimuler leurs activités criminelles;
- obtenir un passeport ou toucher des prestations du gouvernement.

Rançongiciel

La plupart des incidents liés aux rançongiciels prennent naissance dans une campagne d'hameçonnage par courriel. Le courriel contient une pièce jointe, qui peut être un fichier exécutable, une archive, une image ou un lien. L'ouverture de la pièce jointe ou le fait de cliquer sur le lien lance le maliciel dans le système de l'utilisateur. Le maliciel peut être dormant pendant plusieurs jours, voire plusieurs mois avant que les fichiers ou les systèmes soient chiffrés ou verrouillés.

Harponnage

Dans les stratagèmes de harponnage, les fraudeurs prétendent faire partie d'une organisation légitime et tentent de convaincre des entreprises ou des particuliers de leur envoyer de l'argent. Ces stratagèmes exploitent les relations existantes entre le destinataire et l'expéditeur du message. L'adresse de courriel utilisée par le fraudeur semble être l'adresse réelle de l'expéditeur. Dans bien des cas, les suspects peuvent obtenir les renseignements nécessaires pour un stratagème de harponnage après avoir accédé au système de la victime à l'aide de l'hameçonnage.

Indices – Comment vous protéger

- Méfiez-vous des messages textes et des courriels non sollicités qui ont été envoyés par des personnes ou des organisations et où l'on vous demande de cliquer sur un lien ou d'ouvrir une pièce jointe.
- Vérifiez si le message renferme des fautes d'orthographe.
- Vérifiez l'hyperlien derrière le texte ou le bouton du lien en passant le curseur sur le texte avec votre souris.
- En cas de doute, ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes : ils peuvent contenir des virus et des logiciels espions.
- Le gouvernement du Canada n'enverra jamais de fonds par courriel ou par message texte.
- Les organismes d'application de la loi n'exigeront jamais un paiement et ne menaceront pas de vous arrêter par courriel ou par téléphone.
- Obtenez d'autres conseils pour vous protéger contre les fraudes.

Toute personne qui croit avoir été victime de cybercriminalité ou de fraude doit le signaler à la police et au CAFC, dans son système de signalement en ligne ou par téléphone au 1-888-495-8501. Si vous avez été la cible d'une fraude mais que vous avez su éviter d'en être victime, signalez tout de même l'incident au CAFC.

En ce mois de sensibilisation, passez à l'action :

- Suivez @cyber_securite et visitez son site Web : https://pensezcybersecurite.gc.ca/fr
- Suivez-nous @antifraudecan sur Twitter et Facebook et visitez notre site Web : http://centreantifraude.ca.
- Utilisez les mots-clics #MoisCyber2022, #PensezCybersécurité, #Cybersécurité et #Cyber.
- Apprenez-en davantage sur le nouveau système de signalement des incidents de cybercriminalité et de fraude qu'élabore le CAFC en partenariat avec le Groupe national de coordination de la lutte contre la cybercriminalité (GNC3).