IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

AVIS DE L'OCRCVM

Avis relatif à la formation

Destinataires à l'interne :
Affaires juridiques et conformité
Audit interne
Comptabilité réglementaire
Crédit
Détail
Financement des sociétés
Formation
Haute direction
Inscription
Institutions
Opérations
Pupitre de négociation
Recherche

Personnes-ressources :
Suzanne Lasrado
Chef principale de la conformité
des finances et des opérations
416 943-5880
slasrado@iiroc.ca

Ryan Li
Directeur de la sécurité de l'information
416 943-5890
rli@iiroc.ca

Avis de l'OCRCVM 20-20-0083
Le 21 avril 2020

La COVID-19 et la cybersécurité – Conseils pour les conseillers et les autres employés des courtiers membres

Le 30 mars, nous avons publié un avis aux courtiers membres de l'OCRCVM, dans lequel nous les avertissions du risque accru de cyberattaques liées à la pandémie de COVID-19. Les cybercriminels ciblent également les personnes, particulièrement celles qui travaillent à distance.

Les conseillers et les autres employés des courtiers membres constituent la première ligne de défense contre les attaques et doivent demeurer vigilants en tout temps pour protéger leur employeur et les clients de celui-ci et pour se protéger eux-mêmes. Le présent avis leur offre quelques conseils sur la façon de prévenir les cyberattaques et d'y réagir, même lorsqu'ils travaillent de la maison.

Rappel des attaques courantes

- La cybermenace la plus répandue à l'heure actuelle est l'**hameçonnage** et l'envoi de liens malveillants au moyen de courriels et de messages textes ayant pour thème la COVID-19. Beaucoup de fournisseurs de services de cybersécurité ont constaté une hausse importante de telles attaques chez tous leurs clients, et nous aimerions insister de nouveau sur la vigilance dont tout le monde doit faire preuve pour contrer les cybermenaces.
    - Que faire?
        - Avant de cliquer sur un lien, passez votre curseur sur celui-ci pour vérifier son authenticité. Méfiez-vous des courriels qui vous incitent à cliquer sur un hyperlien ou à ouvrir une pièce jointe.
        - Si vous cliquez sur un lien ou une pièce jointe suspects ou ouvrez une pièce jointe suspecte, avisez tout de suite votre équipe des TI ou de la sécurité de l'information, débranchez votre câble de réseau et désactivez votre connexion Wi-Fi (n'éteignez pas votre ordinateur).
    - De manière générale, si vous avez des doutes quant à l'authenticité d'un message, communiquez avec votre équipe des TI ou de la sécurité de l'information.

Exemples d'hameçonnage lié à la pandémie de COVID-19

1. Courriels ou messages textes envoyés par des personnes qui prétendent agir au nom d'une organisation gouvernementale et qui vous demandent de leur fournir vos renseignements bancaires pour vous verser des fonds d'aide liée à la pandémie.

2. Courriels ou messages textes prétendument envoyés de la part d'un hôpital, d'un gouvernement ou d'un organisme de santé vous demandant de cliquer sur un lien ou d'appeler un numéro pour obtenir de l'information sur la COVID-19 ou les traitements disponibles.

Conseil

Si vous n'êtes pas certain de la validité d'un courriel ou d'un message texte que vous avez reçu, ne cliquez pas sur le lien contenu dans le courriel et n'appelez pas au numéro d'où on vous a appelé ou envoyé un message texte. Utilisez plutôt un moteur de recherche connu pour vérifier les coordonnées de l'organisation sur son site Web officiel.

- Le **piratage psychologique** est un type de fraude au moyen duquel une personne malveillante tente de convaincre un utilisateur de lui transmettre des renseignements sensibles ou de lui transférer des fonds en se faisant passer pour quelqu'un d'autre (un agent d'un service de dépannage, un représentant des services santé ou d'une institution financière, un employé de confiance, etc.). Les auteurs de ces attaques, qui sont parmi les plus courantes, tirent profit des événements actuels et utilisent divers types de communication (courriel, téléphone, messages textes, etc.). Veuillez demeurer extrêmement vigilants lorsque vous communiquez avec d'autres, même si vous croyez qu'il s'agit de sources de confiance.
    - Que faire?
        - Posez-vous les questions suivantes et communiquez avec votre équipe des TI ou de la sécurité de l'information si vous avez le moindre doute :
            - Ai-je pris l'initiative de cette demande?
            - Cette demande est-elle une pratique courante?
            - Cette demande ou communication a-t-elle été transmise par les canaux appropriés?
            - La communication est-elle suspecte de quelque manière que ce soit (coquilles, grammaire déficiente, mise en page inhabituelle, aspect étrange, menaces, texte énigmatique, etc.)?
    - Si vous croyez avoir fourni des renseignements, des fonds ou un accès à une personne malveillante, veuillez informer immédiatement votre équipe des TI ou de la sécurité de l'information.

Exemples de piratage psychologique lié à la pandémie de COVID-19

1. Appels téléphoniques de prétendus agents d'un « service de dépannage » qui demandent vos données d'accès, s'informent de la configuration de votre réseau à domicile ou demandent d'autres renseignements personnels.

2. Faux avis de santé provenant soi-disant d'hôpitaux, de gouvernements régionaux ou d'organismes de santé dans lesquels on prétend que quelqu'un du bureau ou vous-même avez été exposés au virus et devez subir un test.

Conseil

Assurez-vous d'obtenir les renseignements suivants auprès de votre employeur :

- qui communiquera avec vous pendant la période d'isolement, et comment?
- quels changements ont été apportés à vos fonctions habituelles (notamment aux processus d'approbation) par le plan de continuité des activités?
- quelles sont les coordonnées de votre équipe de soutien informatique?

Ordinateurs et appareils mobiles

- Lignes directrices générales :
  - Verrouillez votre écran ou fermez votre session avant de vous éloigner de votre ordinateur;
  - N'approuvez PAS une demande d'authentification si vous n'êtes pas à l'origine de cette demande;
  - NE branchez PAS de dispositifs de stockage USB non autorisés par votre employeur et qui proviennent d'une source inconnue ou que vous n'attendiez pas.
- Ordinateurs et appareils mobiles personnels :
  - N'oubliez pas de vérifier les mises à jour et les correctifs disponibles pour votre système d'exploitation et vos applications et de les installer en temps voulu;
  - Installez un logiciel antivirus et anti-maliciel et exécutez-le;
  - ÉVITEZ de sauvegarder, de télécharger ou de faire des saisies d'écran de renseignements personnels ou sensibles sur votre ordinateur ou appareil mobile;
  - Si d'autres personnes de votre ménage utilisent le même appareil, avant de le leur passer, assurez-vous de fermer votre session et de vous déconnecter de tous les portails et systèmes de votre employeur.
- Ordinateurs et appareils mobiles de votre employeur :
  - Consultez les politiques de votre employeur pour savoir si les autres personnes de votre ménage peuvent utiliser ces appareils et à quelles conditions;
  - Vérifiez si vous recevez régulièrement de votre équipe de soutien informatique des mises à jour pour vos logiciels et votre système d'exploitation;
  - Mettez à jour le système d'exploitation et les applications des appareils mobiles au besoin.

Réseaux utilisés pour le télétravail

- Utilisez un réseau sécurisé pour accéder à votre environnement de travail (p. ex. RPV, accès à distance, service infonuagique).
- Si vous utilisez le Wi-Fi à la maison :
  - assurez-vous qu'il est doté d'un protocole de sécurité strict (comme WPA2) et qu'il est protégé par un mot de passe fort;

- N’utilisez PAS de Wi-Fi public ou de connexion ouverte/non sécurisée pour accéder à votre environnement de travail ou aux renseignements personnels des clients ou des employés.
- Appliquez en temps voulu les mises à jour et les correctifs logiciels à votre routeur.
- Modifiez les noms d’utilisateur et les mots de passe par défaut de votre matériel de réseautage à la maison (routeurs, commutateurs, répéteurs multiport, etc.)

Traitement des documents et communications

- Continuez de suivre rigoureusement les procédures de traitement des documents (papier et électroniques) comme si vous étiez au bureau.
- NE sauvegardez PAS les documents dans des répertoires en ligne autres que ceux de votre employeur ou sur des lecteurs de disque dur locaux.
- Respectez le plus possible les consignes de mise en sécurité des documents pour ne pas perdre ou laisser traîner des documents importants.
- Communiquez à l’aide des canaux appropriés (p. ex. le courriel et l’application de messagerie instantanée fournie par votre employeur) lorsque vous exercez vos activités professionnelles.
- Assurez-vous que les applications de communication (vidéoconférence, conférence Web, etc.) que vous utilisez sont sécuritaires et que vous y accédez de façon sécurisée.

Intervention en cas d’incident

- Vous devez bien comprendre le rôle que vous jouez dans le plan d’intervention en cas d’incident de votre employeur et savoir avec qui communiquer en cas de cyberincident (violation de données, perte de renseignements des clients ou atteinte à leur sécurité, attaque par courriel réussie, activation d’un lien malveillant, attaque par rançongiciel, perte ou vol d’un appareil mobile, etc.).

Autres ressources

Vous pouvez trouver d’autres renseignements et ressources sur la gestion des cybermenaces (notamment la webémission Conseils de cybersécurité à l’intention des conseillers) sur le site Web de l’OCRCVM, à la page Cybersécurité.