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 20-0061
Le 30 mars 2020

La COVID-19 et la cybersécurité

Le présent avis fournit de l'information aux courtiers membres de l'OCRCVM sur les cybermenaces liées à la pandémie de COVID-19 ainsi que des conseils pour aider les sociétés et leurs employés à se protéger et à protéger les renseignements sur leurs clients.

L'information et les nouvelles sur la pandémie de COVID-19 changent tous les jours. Dans ce contexte, il est naturel de vouloir chercher des nouvelles sur le Web ou de vouloir ouvrir des courriels externes offrant de l'information à ce sujet et les envoyer à ses collègues et amis.

Malheureusement, en temps de crise, il y a toujours des personnes malveillantes qui cherchent à en profiter. La pandémie de COVID-19 ne fait pas exception. Par exemple, l'Organisation mondiale de la santé (OMS) a récemment publié un avertissement (en anglais seulement) concernant des escroqueries en ligne et des courriels malveillants prétendant contenir de l'information sur la façon de se protéger de cette maladie.

Prenez garde à l'hameçonnage et aux logiciels malveillants

Les messages textes, courriels, pièces jointes, liens ou sites Web ayant pour sujet la COVID-19 devraient tous être traités avec prudence, car ils pourraient contenir un logiciel malveillant ou être de l'hameçonnage visant à obtenir un accès à votre réseau, à vos renseignements personnels et à vos actifs.

Faites preuve de prudence avant de cliquer sur un lien ou d'ouvrir une pièce jointe contenus dans un courriel, même si vous connaissez l'expéditeur. Voici des mesures de sécurité générales à prendre :

1) Avant de cliquer sur un lien, passez votre curseur sur celui-ci pour vérifier son authenticité;

2) Si vous cliquez sur un lien ou une pièce jointe suspects ou ouvrez une pièce jointe suspecte, avisez votre fournisseur de services informatiques et déconnectez-vous tout de suite d'Internet (n'éteignez pas votre ordinateur);

3) De manière générale, si vous avez des doutes sur l'authenticité d'un courriel, communiquez avec votre fournisseur de services informatiques.

Encore une fois, nous vous demandons d'être vigilants lorsque vous consultez de tels courriels, particulièrement si vous ne les attendiez pas et s'ils :

- vous demandent de cliquer sur un lien ou une pièce jointe ou de télécharger ou d'ouvrir une pièce jointe;
- vous demandent de fournir des renseignements personnels, vos données d'ouverture de session ou vos renseignements bancaires.

Ordinateurs et téléphones cellulaires

Si vous travaillez de la maison, veillez à la sécurité de votre ordinateur portable, de votre téléphone et de vos autres appareils mobiles et sécurisez l'accès à ces appareils. Évitez d'utiliser des appareils non autorisés ou d'accéder à des sites Web ou à des réseaux sans fil non sécurisés.

Votre fournisseur de services informatiques devrait également s'assurer que des correctifs logiciels de sécurité continuent d'être apportés à votre ordinateur pendant que vous travaillez de la maison.

Veuillez communiquer avec vos équipes de la cybersécurité ou votre fournisseur de services informatiques si vous avez des questions.

Tentatives d'accès frauduleux aux comptes

Nous avons remarqué une hausse des tentatives d'accès frauduleux aux comptes de clients et nous incitons les courtiers membres à faire preuve de vigilance. Les courtiers membres devraient s'assurer que les contrôles ou les processus mis en place pour prévenir ou détecter l'accès frauduleux à un compte sont fonctionnels. Voici quelques exemples de tels contrôles :

- des alertes en temps réel et des examens de conformité après les opérations pour détecter tout écart anormal par rapport aux habitudes de négociation d'un client;
- l'authentification à deux facteurs;
- le téléchargement gratuit de logiciels que les clients peuvent installer sur leur ordinateur pour accroître leur protection;
- des procédures décrivant les mesures correctrices à prendre une fois qu'il est établi que l'intégrité d'un compte est compromise, comme la suspension du compte et l'obligation pour le client de choisir un nouveau mot de passe ou de créer un nouveau compte;
- le blocage de l'accès ou l'imposition d'une authentification supplémentaire si une adresse IP non reconnue est utilisée pour accéder à un compte;
- le suivi des listes d'adresses IP frauduleuses connues et le blocage de l'accès aux systèmes du courtier à partir de ces adresses.

Nous rappelons aux courtiers membres que l'OCRCVM s'attend à ce qu'ils l'avisent de tout problème lié à des tentatives d'accès frauduleux aux comptes. Cela est important pour que nous puissions évaluer le préjudice qui pourrait être causé aux clients ou à l'intégrité des marchés.

Autres ressources

Vous trouverez de l'information supplémentaire sur la gestion des cybermenaces ainsi que des ressources telles que des guides et des webinaires sur le site Web de l'OCRCVM, à la page Cybersécurité.