Comprendre la cybersécurité et la fraude liée aux paiements

La sécurité de vos renseignements et de vos transactions bancaires vous préoccupe? Vous n'êtes pas seul. Les progrès rapides de la technologie et la complexité croissante des tentatives de fraude font de chaque organisation une cible pour les opérations frauduleuses. Même s'il existe des systèmes de cybersécurité de grande qualité, vous devez prendre des mesures pour vous protéger et pour protéger vos renseignements.

62 % **des organisations américaines** ont signalé avoir été exposées à des fraudes ou à des tentatives de fraude[1].

30 % **En 2014, 30 % des entreprises** qui ont fait l'objet d'une fraude liée aux paiements ont subi des pertes financières à la suite de l'attaque[1].

445 milliards de dollars **Coût annuel estimé** de la cybercriminalité et de l'espionnage économique pour l'économie mondiale[2].

Conseil : Ne mordez pas à l'hameçon.

L'hameçonnage par courriel vise à vous faire croire que les courriels proviennent d'un site légitime, comme celui de votre banque. En réalité, l'objectif consiste à recueillir vos renseignements personnels ou à vous faire télécharger un logiciel malveillant.

450 000 attaques par hameçonnage ont été recensées dans le monde en 2013[3].

On évalue à **5,9 milliards de dollars** les pertes financières liées ces attaques en 2013[3].

1 Au cours des 12 derniers mois, le nombre d'attaques est passé de **19,9 millions à 37,3 millions, soit une augmentation de 87 %**[2].

À faire : Mettre régulièrement à jour ses programmes antivirus et anti-logiciels malveillants.

À faire : Télécharger le logiciel IBM[MD]* Trusteer Rapport[MC]*[5], gratuitement offert aux clients de BMO[MD]. Il est conçu pour vous protéger contre les maliciels qui représentent une menace pour vos finances et fonctionne avec les pare-feu et logiciels antivirus existants, pour une sécurité accrue. Pour le télécharger, consultez le site suivant : **trusteer.com/landing-page/fr/bmo-fr.**

À ne pas faire : Cliquer sur des liens ou télécharger des renseignements à partir de courriels ou d'Internet, sauf si la source est légitime.

Conseil : Ne partagez pas n'importe quel renseignement personnel.

23 % des destinataires ouvrent les messages d'hameçonnage et **11 %** d'entre eux cliquent sur les pièces jointes[4].

50 % des personnes testées ont ouvert les courriels et cliqué sur les liens au cours de la première heure[4].

À faire : S'assurer de partager ses renseignements personnels ou financiers que sur des sites sécurisés. En cas de doute, inscrire l'adresse URL exacte.

À faire : Se méfier des demandes de renseignements sur une carte. Ne jamais communiquer les renseignements sur sa carte à moins de pouvoir déterminer que la demande est légitime.

À faire : Protéger sa carte de débit ou d'entreprise et son NIP. Ne noter son NIP nulle part et s'assurer que personne ne peut le voir lorsqu'on est à un terminal de paiement.

À ne pas faire : Communiquer ses données d'identification ou ses renseignements financiers (nos de compte, noms d'utilisateur, mots de passe, NIP, jeton de sécurité et mot de passe du jeton).

Conseil : Élaborez un processus de paiement qui limite votre exposition à la fraude

Dans **60 %** des cas, les fraudeurs peuvent nuire à une organisation en seulement quelques minutes[4].

À faire : Séparer la fonction d'exécution du paiement et celle de l'approbation aux fins de double validation.

À faire : Établir des limites de virement de fonds qui ne dépassent pas le maximum prévu des besoins de son entreprise.

À faire : Mettre en place des mesures de contrôle des dépenses et de blocage pour certains titulaires de carte et catégories de transaction.

À ne pas faire : Permettre un paiement sans vérifier la source de la demande de transfert de fonds. Il faut toujours obtenir une confirmation verbale du demandeur, en personne ou en utilisant un numéro de téléphone connu.

Connectez-vous

Pour obtenir de plus amples renseignements, communiquez avec votre représentant de BMO ou consultez le site :

bmo.com/securite bmo.tps@bmo.com

BMO[MD] Banque de Montréal

Ici, pour vous.[MC]

[1] 2015 AFP Payments Fraud and Control Survey, Association for Financial Professionals. [2] Economic Impact of Cybercrime II, Center for Strategic and International Studies, juin 2014. [3] Rapport de RSA sur la fraude 2014. [4] Rapport d'enquête 2015 sur les compromissions de données de Verizon Enterprise Solutions. [5] Le téléchargement et l'utilisation du logiciel sont assujettis aux conditions de la convention de droits d'utilisation qui accompagne le logiciel Trusteer Rapport. En téléchargeant et en installant le logiciel Rapport de Trusteer, vous consentez à respecter les modalités dudit logiciel. La Banque de Montréal n'est pas responsable de ce logiciel ni des autres produits ou services d'IBM, et elle ne peut s'en porter garante. Elle n'est pas non plus responsable des difficultés, des conséquences, des coûts, des demandes d'indemnisation, des dommages ou des pertes pouvant découler de quelque façon que ce soit du téléchargement ou de l'utilisation du logiciel. Les problèmes, questions et préoccupations concernant le logiciel Trusteer Rapport doivent être soumis à IBM.

02/16-0268