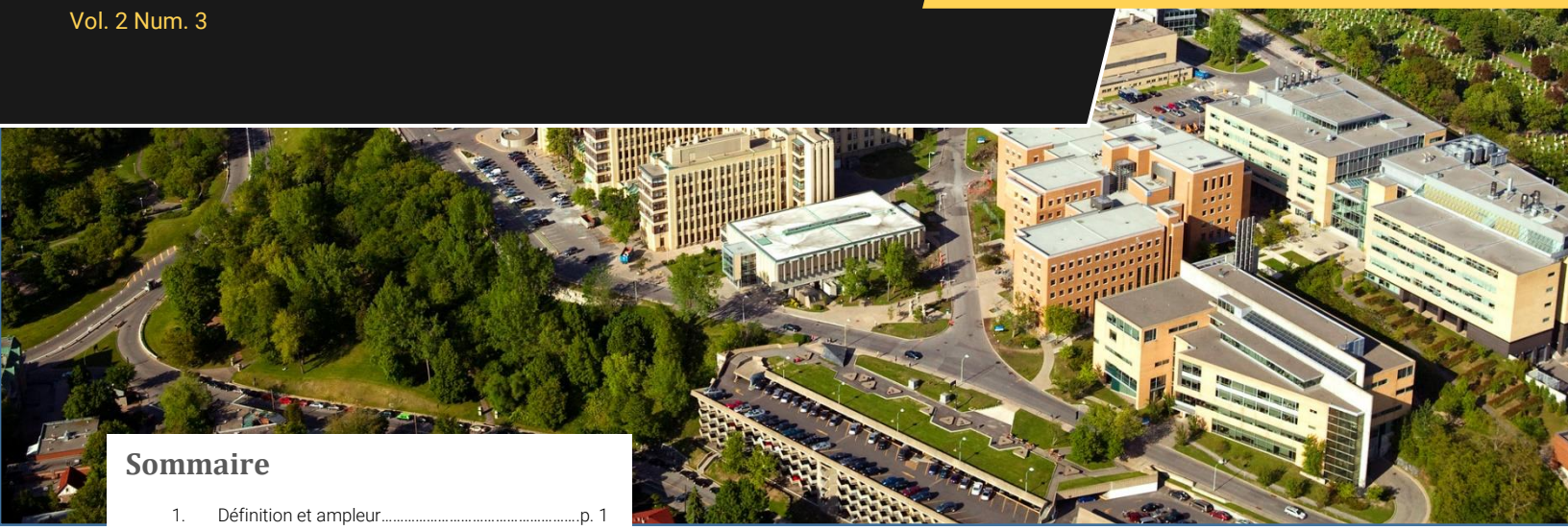
La fraude au président

Claire Gagnon, candidate à la maîtrise

Note de synthèse
Vol. 2 Num. 3

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

1. Définition et ampleur....p. 1
2. Profil des victimes....p. 1
3. Facteurs de risque....p. 2
   a. Facteurs de risque organisationnels....p. 2
   b. Facteurs de risque individuels....p. 2
4. Recommandations....p. 2
   a. Prévention technologique....p. 2
   b. Responsabilité de l'entreprise....p. 2
   c. Autres types de recommandations....p. 2
5. Références....p. 3

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Définition et ampleur

Apparue vers 2005, **la fraude au président consistait à ses débuts à usurper l'identité du président ou du responsable financier d'une organisation afin de tromper un employé et pousser ce dernier à effectuer un ou plusieurs transferts de fond non autorisés au profit des fraudeurs** [1,2]. Cette fraude s'étend aujourd'hui aux demandes de renseignements confidentiels, à l'achat de carte-cadeaux ou encore à l'usurpation d'identité de fournisseurs [3,4]. Pour donner l'impression que la demande est légitime, les fraudeurs initient l'échange à partir d'une adresse courriel piratée de l'organisation ou une adresse courriel quasi-identique[5].

Nécessitant peu d'efforts et d'outils technologiques, cette fraude présente des avantages importants comparativement aux autres types de fraude en ligne[6]. En effet, les gains financiers pour les fraudeurs sont élevés, le taux de réponses de la part des victimes est supérieur aux autres attaques et bien que des recherches sur l'entreprise soient nécessaires, la durée de l'attaque à partir de la prise de contact avec la victime jusqu'à sa fin est de trois jours en moyenne[6].

Si, en terme de nombre de victimes, ce type de fraude n'est pas le plus significatif, il engendre des pertes financières importantes. Selon l'Internet Crime Complaint Center (IC3), les pertes engendrées par la fraude au président en 2019 ont été 3,7 fois plus importantes que pour tout autre type

de fraude[3]. Au total, les pertes mondiales déclarées entre juin 2016 et juillet 2019 ont été évaluées à plus de 26 milliards de dollars américains pour plus de 166 000 incidents déclarés[4].

Profil des victimes

Les pertes financières, souvent importantes, peuvent s'élever à plusieurs millions de dollars pour une seule entreprise[7]. Sur les trois derniers mois de 2019, les montants moyens exigés sous forme de virement bancaire par les fraudeurs s'élevaient à environ $55 000 par demande, allant de $2 500 à $680 000[8]. Lorsqu'il s'agissait de cartes cadeaux, les montants demandés étaient beaucoup plus modestes, allant de $250 à $10 000 avec une moyenne de $1 600[8].

De juillet 2018 à juin 2019, **les pays les plus touchés par la fraude au président étaient les pays anglophones**, soit les États-Unis (39%), le Royaume-Uni (26%) et l'Australie (11%)[9]. Viennent ensuite la Belgique (3%), l'Allemagne (3%) et enfin le Canada (2%)[9]. Au total, plus de 177 pays ont été ciblés[4]. La grande majorité des attaques provient du Nigéria, mais des organisations frauduleuses ont été également localisées en Russie, au Ghana, au Kenya et en Israël[6,10].

Les montants frauduleux ont été transférés vers pas moins de 140 pays, **les destinations principales se trouvant être Hong-Kong et la Chine**. Le Royaume-Uni, le Mexique et la Turquie sont des destinations de plus en plus souvent évoquées[4]. Certains de ces pays servent d'intermédiaires pour blanchir l'argent avant de l'envoyer aux fraudeurs. De plus, selon le FinCEN, 73% des incidents rapportés aux États-Unis impliqueraient également des virements locaux, rendu possible grâce aux réseaux de mules[11]. Les mules sont des intermédiaires de la fraude dont le rôle consiste à « prêter » leur compte bancaire aux organisations criminelles. L'argent des organisations victimes y est déposé puis transféré vers un compte bancaire localisé à l'étranger[6]. La demande de virement est moins susceptible d'éveiller les soupçons des victimes et des services anti-fraude des institutions financières si elle provient des organisations victimes. Ces mules n'ont parfois pas conscience que ces transactions servent à des fins illégales et peuvent être elles-mêmes victimes d'une fraude à l'emploi ou de fraude sentimentale[6].

La fraude au président cible les entreprises et organisations et **peut toucher n'importe quel secteur d'activité**. Ainsi, les institutions scolaires et universitaires, les entreprises manufacturières ou de services, les institutions financières et même les organisations à but non lucratif peuvent en être la cible[4,5,6,12]. Une église de l'Ohio a par exemple perdu près de 1,8 millions de dollars américains après avoir été victime d'une telle fraude[13]. Même si tous les secteurs peuvent être ciblés, certains d'entre eux sont cependant plus à risque que d'autres : parmi eux, figurent en tête le secteur manufacturier et de la construction, qui a été victime de 25% de toutes les tentatives pour un montant moyen de $54 000, celui du commerce de détail (18%) et enfin le secteur de l'immobilier (16%)[11]. Ce dernier inclut une variante de la fraude au président dans laquelle le fraudeur usurpe l'identité de l'agent immobilier, change ses coordonnées bancaires auprès du client et lui réclame le paiement du bien acheté[14]. Le montant moyen demandé est de $179 001[11], ce qui est supérieur aux sommes réclamées dans le cas des autres usurpations d'identité. Étant donné l'importance des gains potentiels, les tentatives dans le secteur immobilier ont augmenté drastiquement au cours des trois dernières années[11].

Au sein des organisations, **toute personne ayant le pouvoir d'effectuer ou ordonner un virement bancaire ou de révéler des informations confidentielles peut être une cible potentielle**[15]. Dans la plupart des cas, les fraudeurs étudient l'organigramme de l'organisation, notamment grâce aux informations disponibles en ligne, allant même jusqu'à pirater les comptes courriels. Cette incursion au cœur des communications internes de l'entreprise leur permet d'obtenir des signatures, de prendre connaissance des protocoles habituels pour effectuer les virements, d'identifier les failles dans les protocoles d'autorisations et d'authentification, et enfin d'envoyer le courriel

frauduleux sans crainte que celui-ci ne soit détecté comme suspect[5,16].

Les fraudeurs s'adaptent aux organisations qu'ils ciblent selon les heures d'ouverture afin que les envois de courriel frauduleux tiennent compte du décalage horaire et soient reçus durant les heures de bureau[14,17]. À ce propos, 91% des attaques sont effectuées durant les jours de semaine[17]. Enfin, les fraudeurs utiliseraient des outils de corrections grammaticales afin d'éviter les fautes d'orthographes ou de ponctuation dans les courriels en anglais[6].

Facteurs de risque

Considérant le caractère ciblé de cette fraude, celle-ci nécessite que les cybercriminels prennent connaissance de la structure organisationnelle des institutions victimes et identifient la relation hiérarchique entre la cible et la personne dont ils vont usurper l'identité[18]. La personnalisation de l'attaque est importante afin de conférer une apparence de légitimité à la requête[2,18]. Plusieurs facteurs de risque et de protection au niveau organisationnel et individuel sont associés à cette fraude.

Facteurs organisationnels

Les entreprises ayant un grand volume de facturation ou qui font affaire à l'international sont particulièrement ciblées par la fraude au président [11,18,19]. Une entreprise ayant pour habitude d'effectuer des virements importants sera également plus lucrative qu'une compagnie n'effectuant que des virements de montants moindres.

Selon le FinCEN, le secteur d'activité de l'organisation cible joue un rôle important. Par exemple, en 2017, les entreprises financières étaient davantage ciblées que les autres[11].

Les organisations dont **les informations sur la structure hiérarchique et les partenaires sont disponibles publiquement** sont particulièrement à risque. En effet, mieux les fraudeurs connaissent leur cible, meilleures sont leurs chances de réussite[20].

La période de l'année modifie les tendances de la fraude au président. Par exemple, **les tentatives d'achat de cartes-cadeaux sont en augmentation à l'approche des fêtes de fin d'année**[17]. Les institutions d'enseignement sont davantage ciblées au mois de septembre, pendant la rentrée scolaire. Il s'agit en effet d'une période chargée pour ces institutions pendant laquelle les achats sont nombreux et de nouveaux employés prennent leur fonction[17]. La saison des impôts est également une période attractive pour les fraudeurs[17]. Certaines périodes voient au contraire le nombre de tentatives de fraude au président baisser, tels les congés du week-end du 4 juillet (fête nationale des États-Unis) et de la Fête du travail[17].

Facteurs individuels

La surcharge de travail, l'urgence, ou le manque de sensibilisation aux fraudes sont des facteurs de risque[22,23]. Les fraudeurs peuvent également s'appuyer sur le zèle d'un nouvel employé qui, désirant bien paraître, ne remettra pas en question les requêtes du président et y répondra rapidement.

Certains facteurs psychologiques tels un **déficit de l'attention, le sentiment de fatigue et la sensibilité aux techniques de manipulation** peuvent également représenter des facteurs de risque[22,24]. En effet, cette fraude s'appuie sur des techniques d'ingénierie sociale notamment celles exerçant une pression psychologique sur la victime à travers l'urgence de la requête. Ce sentiment d'urgence se reflète dans les courriels envoyés à la victime par l'emploi de mots-clés comme « avoir un moment », « demande de transaction », « important » et « urgent »[9,17,25] et au fait que le courriel est volontairement envoyé à l'approche de la fermeture des bureaux[26].

Certains fraudeurs vont tenter d'établir un contact avec la victime avant de lui donner toutes les

informations nécessaires pour répondre à la requête. Il s'agit par exemple de lui demander si elle est à son bureau ou si elle est disponible pour opérer une transaction urgente. Une personne qui répond à un tel courriel est dix fois plus susceptible de devenir victime[6].

Des informations sensibles peuvent également être rendues disponibles par les employés. Par exemple, le profil LinkedIn d'un employé peut révéler des informations sur ses propres responsabilités par rapport aux finances de l'entreprise[20].

Recommandations

Les conséquences de la victimisation à la fraude au président peuvent être nombreuses et particulièrement importantes. La **perte financière** est la conséquence la plus directe. Une chute des titres boursiers et une **atteinte à la réputation** peuvent également survenir lorsque la victimisation est révélée au public[24,27]. L'impact de ces conséquences négatives explique que certaines entreprises ne signalent pas leur victimisation[28]. Dans des cas plus graves, certaines entreprises doivent congédier leurs employés ou déclarer faillite[24,27]. Au niveau individuel, l'employé responsable de la transaction frauduleuse peut souffrir de séquelles psychologiques, subir une perte de la confiance de l'entreprise et se voir retirée ses responsabilités, voire être congédiée[22,24,27,29].

Prévention technologique

Plusieurs caractéristiques de cette fraude rendent la détection technologique complexe. En effet, le caractère ciblé du courriel et l'utilisation de services de courriel possédant un score élevé de réputation sont des limites à la prévention technologique[17,18]. Étant donné que ces courriels frauduleux sont rarement envoyés avec des liens ou fichiers malveillants, **ils ne sont pas considérés comme dangereux par les logiciels anti-virus**[30]. De plus, le courriel frauduleux n'est envoyé qu'à un maximum de six personnes au sein d'une entreprise et ne peut donc pas être considéré comme un pourriel[17]. Enfin, si le courriel provient d'un compte courriel piraté, la probabilité que la tentative de fraude soit détectée est faible.

Afin d'éviter le piratage des comptes courriels, il est important de connaître les gestes de protection de base, comme **l'utilisation de mots de passe uniques et complexes**[31]. Il est également recommandé d'adopter des technologies d'identification multifacteur (MFA) qui évitent les compromissions de comptes en exigeant plusieurs formes d'identification lors de chaque connexion. De nombreuses solutions facile d'usage et à bas coût existent et protègent contre le piratage des comptes courriels. Un système de détection des intrusions peut être ajouté pour compléter les protections de base[24]. L'organisation doit également soumettre ses contrôles de sécurité interne à des réévaluations régulières, voire embaucher un consultant en cybersécurité ou développer une unité interne dédiée à cet effet, tout dépendant de la taille de l'entreprise[21,24].

Le protocole d'authentification de courriel DMARC détecte et limite l'exposition des consommateurs aux emails frauduleux tels que les pourriels et les courriels d'hameçonnage. Les observations tirées de l'étude du groupe criminel Cosmic Lynx ont permis de montrer qu'ils sélectionnent spécifiquement les entreprises n'ayant pas mis en place de normes DMARC[10].

Responsabilité de l'entreprise

Les demandes de virement doivent faire l'objet d'une **double confirmation**, soit vérifier la légitimité de la requête par deux moyens différents. Par exemple, répondre au courriel à partir d'une nouvelle chaîne de message puis en téléphonant à la personne concernée en utilisant le numéro de téléphone fourni par l'organisation[18,24]. La meilleure solution reste néanmoins une confirmation en face-à-face ou le cas échéant, en vidéoconférence. En effet, des cas de fraudes au président ayant utilisé l'intelligence artificielle ont été observés[35]. Pour confirmer l'identité usurpée ou envoyer une confirmation orale du président, ces fraudeurs ont

utilisé des vidéos existantes afin de reproduire la voix du président de l'entreprise[36]. La transmission d'informations sensibles et la modification des informations bancaires d'un employé ou partenaire doivent faire l'objet de contrôles similaires[18,24].

Une protection supplémentaire consiste à proscrire les paiements en urgence au sein de l'entreprise[32].

Les employés responsables des finances doivent être **en nombre limité et leurs tâches différenciées**[33]. Par exemple, un employé s'occupe de la facture, un autre prépare le paiement et un troisième confirme le virement[32]. Il est primordial que tous les acteurs de la chaîne de paiement soient sensibilisés aux différentes fraudes et à leurs conséquences[5]. Il existe des formations de sensibilisation à la fraude en ligne, incluant la fraude au président, que les organisations peuvent utiliser gratuitement ou après achat[34]. La formation des employés doit être exhaustive afin d'englober les différentes méthodes utilisées par les fraudeurs et d'amener à une vigilance particulière durant les périodes à risque.

Considérant que les probabilités de réussir la fraude augmentent selon le niveau de connaissance des fraudeurs sur l'entreprise, il devient ainsi nécessaire de **contrôler l'information publique disponible** sur le fonctionnement interne et externe de l'organisation[12,20].

L'entreprise doit également se munir d'un **plan d'action** en cas de fraude afin de pouvoir réagir rapidement si cela se produit[32]. Malgré la grande proportion d'entreprises craignant une augmentation des fraudes et de la cybercriminalité, seulement la moitié aurait en place un plan d'urgence si une menace se concrétisait[32].

Autres types de recommandations

La littérature scientifique sur la fraude au président est limitée et s'attarde rarement sur les employés ciblés et les facteurs de risque spécifiques. Dans une optique de prévention et de sensibilisation, une attention spécifique sur cet aspect serait donc souhaitable.

Il est nécessaire que les institutions policières et les victimes continuent à agir de manière proactive notamment en encourageant les dénonciations, en gelant les comptes bancaires des mules, en supprimant les comptes utilisés frauduleusement et en effectuant des arrestations stratégiques grâce à une coopération internationale[6].

Il existe des liens étroits entre plusieurs types de fraude et celle au président, suggérant que cette dernière doit être analysée dans une perspective holistique. Par exemple, les mules peuvent être recrutée à la suite de fraude sentimentale ou à l'emploi[6]. En plus de celles-ci, la fraude au président est souvent menée conjointement avec la fraude de vente de véhicule en ligne, les fraude de location et les fraudes de loterie[19].

En dernier lieu, il existe aux États-Unis des programmes de prévention et recouvrement de l'argent tel la « Recovery Asset Team » du FBI créé spécialement pour les victimes de fraude au président[37]. Bien que celle-ci ne puisse recouvrer les fonds que dans le cas où l'argent est envoyé localement, 75% des 258 millions de dollars américains fraudés ont été rendus aux entreprises victimes[9]. Ce taux est bien supérieur par rapport à ce qui est autrement retrouvé. En effet, lorsque la fraude n'est pas repérée dans les 24 heures et si le paiement a été fait par usage de cartes-cadeaux ou envoyé à l'international, les chances de recouvrer l'argent sont minces[5]. Les résultats encourageants de ce programme suggèrent donc l'importance de son développement, voire son implantation dans les autres pays ciblés.

Références

[1] Bureau de la Concurrence .(2018). Faits sur la fraude — Détecter, contrer et signaler la fraude.

[2] Sûreté du Québec. (2017). Fraude du président, soyez vigilant.

[3] Federal Bureau of Investigation (FBI). (2019). Internet Crime Report.

[4] Internet Crime Complaint Center (IC3). (2019). Business Email Compromise The $26 Billion Scam.

[5] Financial Crimes Enforcement Network (FinCEN). (2019). Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business.

[6] Jakobsson, M., Wilson, J. et Linton, J .(2018). Behind the "From" Lines: Email Fraud on a Global Scale.

[7] Larouche, V.(2017). Comment un escroc a volé 5,5 millions à La Coop fédérée. *La Presse*.

[8] Agari Cyber Intelligence Division (ACID). (2020). Q1 2020: Email Fraud & Identity Deception Trends.

[9] Symantec Security Response. (2019). BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly.

[10] Agari Cyber Intelligence Division (ACID). (2020). Cosmic Lynx Threat Dossier: The Rise of Russian BEC.

[11] Financial Crimes Enforcement Network / FinCEN. (2019). Manufacturing and Construction Top Targets for Business Email Compromise.

[12] Federal Bureau of Investigation (FBI). (2017). Business E-mail Compromise E-mail Account Compromise The 5 Billion Dollar Scam.

[13] Muncaster, P. (2019). US Church Hit in $1.8m BEC Scam. Infosecurity Magazine.

[14] Remorin, Lord, Flores, R. & Matsukawa, B. (2018). Tracking Trends in Business Email Compromise (BEC) Schemes. Trend Micro 26.

[15] Federal Bureau of Investigation (FBI). (2017). Business E-Mail Compromise.

[16] Abbasi, F. Advanced Deception with BEC Fraud Attacks. (2018). Trustwave.

[17] Barracuda. (2019). Spear Phishing: Top Threats and Trends. Defending against business email compromise attacks.

[18] Centre canadien pour la cybersécurité. (2017). Campagnes de fraudes par nom de sosie de domaine et par virement bancaire.

[19] US Justice Department. (2019). 281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes.

[20] Mansfield-Devine, S.(2016). The imitation game: how business email compromise scams are robbing organisations. Computer Fraud Security, 5-10.

[21] Zweighaft, D. (2017). Business email compromise and executive impersonation: are financial institutions exposed? *J. Invest. Compliance*, *18*, 1–7.

[22] knowbe4. (2017). CEO FRAUD: Prevention Manual.

[23] Proofpoint. (2016). Qu'est-ce que le Business Email Compromise (BEC) ?

[24] Carlier, L. (2018). Fraude au président : vous êtes une cible, ne devenez pas une victime. *Richter*.

[25] Cidon, A., Gavish, L., Bleier, I., Korshun, N., Schweighauser, M. et Tsiking, A. (2019). High Precision Detection of Business Email Compromise. Proceedings of the 28th USENIX Security Symposium.

[26] Kikerpill, K. et Siibak, A. (2019). Living in a Spamster's Paradise: Deceit and Threats in Phishing Emails. *Masaryk Univ. J. Law Technol.*, *13*(45).

[27] Agazzi, A. E. (2020). Business Email Compromise (BEC) and Cyberpsychology. *ArXiv Cornell Univ.*

[28] Berthier, T. (2017). Attaques par HoaxCrash et par Faux Ordres de Virement : la puissance du leurre cognitif.

[29] Cross, C. et Gillett, R. (2020). Exploiting trust for financial gain: an overview of business email compromise (BEC) fraud. *J. Financ. Crime*, 1–14.

[30] Barracuda. (2019). Spear Phishing: Top Threats and Trends. Email account takeover: Defending against lateral phishing. *Barracuda*.
[31] AIG. (2019). Cyber Claims: GDPR and business email compromise drive greater frequencies.

[32] Boullier, C., Gicquel, F., Goy, O., Hager, S. et Chauffert-Yvart, V.(2019). 5e baromètre DFCG / Euler Hermes sur la fraude et la cybercriminalité.

[33] Bureau de la concurrence. (2018). Le petit livre noir de la fraude 2e édition.

[34] Association Internationale des Douaniers Francophones (AIDF). (2019). E-learning destiné à la prévention de la fraude au changement de coordonnées bancaires. Association Internationale des Douaniers Francophones.

[35] Radio-Canada. (2019). L'IA utilisée pour recréer la voix d'un PDG et voler 320 000 $ à une entreprise.

[36] Pindrop. (2018). Voice Intelligence Report.

[37] Halpern, M. et Gregory, D. (2019). FBI, This Week: Recovery Asset Team Helps Return Stolen Funds to Victims.