Courriel : La porte numérique est-elle grande ouverte pour les voleurs d'identité?

L'authentification multifactorielle contribue à repousser les cybercriminels

CHUBB® | Microsoft

L'Internet Crime Complaint Center (IC3) du FBI a reçu

467 361

plaintes en 2019

soit une moyenne de près de

1 300

chaque jour

et a enregistré plus de

3,5 G$

de pertes pour les particuliers et les entreprises qui en sont victimes.

Ce n' est pas pour rien que les cybercriminels mettent au point des escroqueries en ligne qui ciblent les particuliers et les entreprises: leur commerce illicite leur permet de subtiliser des milliards de dollars chaque année. En effet, l' Internet Crime Complaint Center (IC3) du FBI a reçu 467 361 plaintes en 2019 - soit une moyenne de près de 1 300 par jour - et a enregistré plus de 3,5 milliards de dollars de pertes pour les particuliers et les entreprises qui en sont victimes1.Ces cybercrimes financent souvent le style de vie somptueux de cybercriminels qui en sont à l' origine, comme le tristement célèbre Ramon « Hushpuppi » Abbas, qui exhibe depuis des années sa collection de vêtements de marque, de voitures de luxe et de jets privés[2].

Pour réussir, les cybercriminels doivent élaborer des stratégies en constante évolution afin de persuader les gens de leur remettre, à leur insu, de l' argent, des données et des renseignements personnels permettant de les identifier. Les escroqueries souvent employées, telles que les liens cliquables autonomes ou les pièces jointes à des courriels provenant d' inconnus, ne peuvent pas fonctionner éternellement, surtout lorsqu' il devient de notoriété publique qu' elles sont utilisées pour causer des ravages et commettre des vols.

Certains cybercriminels ont donc commencé à employer une méthode très ciblée : le détournement de comptes de messagerie professionnelle et l'usurpation d'identité, également connue sous le nom de compromission de courriels professionnels. Heureusement, il existe des moyens simples de bloquer ces attaques de plus en plus complexes.

---

1 *2019 Internet Crime Report Released*, 2020, [https://www.fi.gov/news/stories/2019-internet-crime-report-released-021120].
2 KARIMI, Faith, *He faunted private jets and luxury cars on Instagram. Feds used his posts to link him to alleged cyber crimes*, 2020 [https://www.cnn.com/2020/07/12/us/ray-hushpuppi-alleged-money-laundering-trnd/index.html].

Comment fonctionne **l'usurpation d'identité par courriel**

Une boîte de réception compromise est un trésor inouï de renseignements d'entreprise qui peut être exploité par un criminel rusé.

Lors d'une attaque de compromission de courriels professionnels, le pirate peut réussir à s'introduire dans un compte de messagerie d'entreprise et se faire passer pour le véritable titulaire de l'adresse (souvent un chef d'entreprise ou un cadre) afin d'escroquer l'entreprise en incitant ses clients, ses partenaires ou ses employés à lui envoyer de l'argent ou des données sensibles. Ces attaques peuvent toucher des entreprises de toutes tailles et des consommateurs.

Souvent, les malfaiteurs arrivent à s'introduire dans le courrier électronique de l'entreprise en ciblant au départ un employé de niveau inférieur. Cela peut se produire de plusieurs manières :

1. La **force brute** ou l'utilisation d'un outil de perçage de mot de passe qui essaie automatiquement de nombreux mots de passe courants.
2. La **collecte de données d'identification** ou l'exploitation du fait que de nombreuses personnes utilisent les mêmes combinaisons d'identifiants et de mots de passe sur plusieurs comptes.
3. L'**hameçonnage** ou l'**envoi d'un faux courriel** demandant la réinitialisation du mot de passe, ce qui permet d'obtenir les données de connexion à l'adresse professionnelle de l'employé.

Une fois qu'elles y ont accès, les personnes mal intentionnées peuvent lire les courriels d'entreprise qui ont été envoyés à ce compte de messagerie ou qui en proviennent, ce qui leur permet d'obtenir des données précieuses sur les personnes qui, au sein de l'organisation, peuvent transférer de l'argent et sur la manière dont ces personnes communiquent habituellement. Une boîte de réception compromise est un trésor inouï de renseignements d'entreprise qui peut être exploité par un criminel rusé.

Lorsqu'ils se font passer pour un cadre, les cybercriminels peuvent utiliser – ou faire semblant d'utiliser – un téléphone intelligent (ce qui leur évite d'inclure le logo de l'entreprise dans la signature des courriels frauduleux) pour envoyer une demande urgente à un collègue ayant accès aux actifs de l'entreprise. Ils demandent à l'employé de virer une grosse somme d'argent vers un compte bancaire appartenant aux criminels, sous prétexte d'une transaction commerciale confidentielle ou d'un nouveau projet.

Pour s'assurer que leur combine fonctionne, les cybercriminels peuvent agir à un moment où ils savent que le cadre est en déplacement et absent du bureau. Ils peuvent également envoyer leur demande en fin de journée, un vendredi, lorsque la vérification de la source est difficile, en particulier parce que leur demande est « urgente ».

Ils peuvent même faire référence à une activité présentée sur le profil du dirigeant dans les médias sociaux. Par exemple, si les activités du cadre indiquent qu'il est actuellement en voyage à l'étranger, le criminel peut dire « J'éprouve des difficultés à me connecter à l'étranger et j'ai besoin que cela soit traité rapidement », décourageant ainsi l'employé d'appeler le cadre pour confirmer la demande parce que le cadre est vraisemblablement difficile à joindre.

L'usurpation de l'identité d'un cadre peut être complexe, mais il existe un moyen encore plus simple pour les criminels de soutirer des fonds d'une entreprise : cibler d'abord le compte de courriel d'un membre du service des comptes clients.

Lorsque ce compte est compromis, la personne malintentionnée peut rediriger les factures payables à l'entreprise. Un simple logiciel de retouche d'images permet aux criminels de modifier les données de paiement sur des factures existantes, ce qui redirige les paiements vers un ou plusieurs comptes contrôlés par l'usurpateur. Dans ce scénario, deux parties sont perdantes : l'organisation victime de la compromission ne reçoit pas le paiement et le client qui croyait suivre les instructions du véritable fournisseur perd également de l'argent.

Ce mécanisme est également souvent utilisé pour cibler des particuliers et des familles. Dans ce cas, les personnes malintentionnées se concentrent sur des transactions financières plus importantes auxquelles les particuliers s'attendent, par exemple lors de l'achat d'un bien immobilier ou d'un véhicule. Après avoir pris le contrôle du compte de courriel d'un vendeur, le criminel envoie à l'acheteur des instructions à première vue légitimes, lui demandant de transférer les fonds du règlement dans un compte contrôlé par le criminel. Lorsque la supercherie sera découverte, il est fort probable que les fonds volés auront déjà été transférés hors du compte, et du pays.

Les tentatives d'hameçonnage évoluent également selon les manchettes. Par exemple, l'Internal Revenue Service des États-Unis est régulièrement victime d'usurpation d'identité. En 2020, de nombreux contribuables ont reçu des chèques de relance économique du gouvernement par dépôt direct, mais certains contribuables qui n'avaient pas autorisé le dépôt direct ont attendu des semaines avant de recevoir un chèque par la poste. Les fraudeurs demeurent à l'affût de moyens de tirer partide ce type de circonstances inhabituelles pour tenter d'escroquer les gens et de s'emparer de leur argent. Dans les faits, ils auraient enregistré 150 000 faux sites Web de chèques de relance économique avant que la plupart des chèques ne soient distribués. De nombreux fauxsites de ce genre incitent les utilisateurs à fournir leurs renseignements personnels pour obtenir le statut d'un prétendu chèque. Une fois que les renseignements sont saisis, le fraudeur les utilise pour rediriger le chèque vers un autre compte bancaire ou pour voler l'identité de l'utilisateur3. N'oubliez pas que l'Internal Revenue Service ne demande jamais de renseignements bancaires personnels, comme des numéros de compte ou d'acheminement, par téléphone, message texte ou courriel.

Les fraudeurs auraient enregistré 150 000 faux sites Web de chèques de relance économique avant que la plupart des chèques ne soient distribués.

3 CLIFORD, Lee, *Scammers have registered 150,000 fake stimulus check websites. Here's how to protect yourself*, 2020, [https://fortune.com/2020/04/28/irs-stimulus-check-portal-fake-websites-scammers-personal-information-how-to-avoid/].

Pourquoi l'usurpation d'identité par courriel fonctionne-t-elle?

Dans tous les cas de fraude par courriel, il faut d'abord et avant tout que les destinataires du message frauduleux croient en l'authenticité de la demande. Dans de nombreux cas, comme les arnaques de paiement des fournisseurs et de transactions immobilières personnelles, le vol est possible précisément parce que, à la base, les transactions sont réelles et prévues. Les circonstances entourant ces transactions sont modifiées pour confondre les parties légitimes participant à la transaction. C'est de là que vient le terme *ingénierie sociale*.

75 $

millions de dollars redirigés vers des comptes bancaires de cybercriminels avec une seule compromission de courriels professionnels

Les secteurs les plus touchés selon le Cyber Index^{SM} de Chubb

Au total, l'ingénierie sociale représente 21 % des cyberincidents signalés à Chubb au cours des trois dernières années. Ces graphiques montrent certains des secteurs les plus touchés :

Les spécialistes de la compromission de courriels professionnels savent que le courriel est devenu la méthode de communication de facto. Les entreprises ont encouragé les gens à opter pour des solutions sans papier, et la plupart d'entre eux pensent pouvoir repérer les courriels indésirables. Mais ils font également confiance à ceux avec qui ils travaillent et sont plus enclins à répondre aux demandes des dirigeants de leur entreprise ainsi que de leurs fournisseurs et partenaires commerciaux de confiance. Un compte réel, mais compromis à n'importe quelle étape du flux de communication peut entraîner des conséquences désastreuses.

Les cybercriminels misent littéralement sur ces habitudes humaines, renforcées par la société. Il n'est donc pas surprenant que les cybercriminels réussissent à mettre en place des combines qui semblent, du moins rétrospectivement, incroyablement primitives et transparentes. En fait, une escroquerie bien connue de compromission de courriels professionnels utilisait un logiciel malveillant d'enregistrement de frappe pour peaufiner l'accès au courriel. Cette astuce, qui a fonctionné sans être détectée pendant six mois en 2015, a permis de rediriger des paiements de factures d'un montant total de 75 millions de dollars vers des comptes bancaires de cybercriminels[4]. Rétrospectivement, on pourrait s'attendre à ce que quelqu'un s'en aperçoive, compte tenu des sommes importantes en jeu. Mais personne n'a rien vu.

Aussi graves que puissent être les conséquences des compromissions de courriels professionnels, ces arnaques sont malheureusement plutôt fréquentes. Depuis 2009, 17 % des cyberincidents signalés à Chubb sont attribuables à l'ingénierie sociale. Selon le Cyber IndexSM de Chubb, les secteurs les plus touchés sont les petites et moyennes entreprises (25 %), les fabricants (26 %) et le secteur de l'éducation (27 %)5.Et ce risque ne fait qu'augmenter – des récents rapports de sécurité de Microsoft6, de Verizon7 et de Cisco8 indiquent que l'ampleur et la menace des attaques par hameçonnage par courriel sont de plus en plus importantes.

---

4 FLORES, Ryan et Lord REMORIN, *Piercing the HawkEye: Nigerian Cybercriminals Use a Simple Keylogger to Prey on SMBs Worldwide*, Trend Micro, [https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-piercing-hawkeye.pdf].

5 Cyber Index$_{SM}$ de Chubb, octobre 2020, [https://chubbcyberindex.com/index.html#/splash].

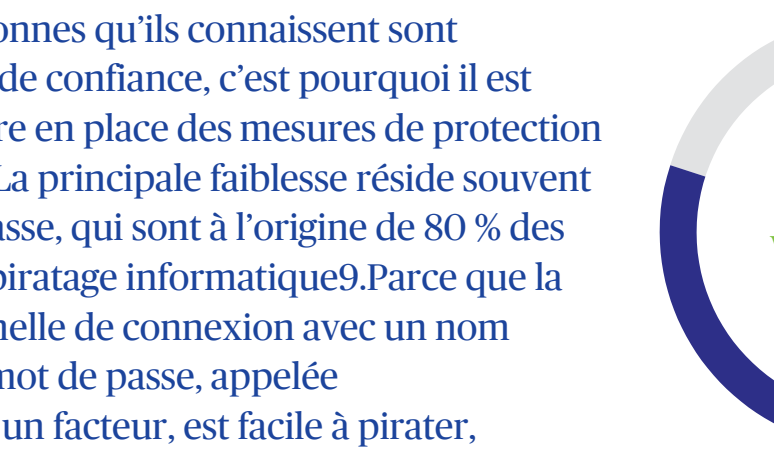
6 Archives des rapports sur la défense numérique de Microsoft, 2020, [https://www.microsoft.com/fr-fr/security/business/security-intelligence-report].

7 VERIZON, Rapport d'enquête sur les violations de données, 2020, [https://www.verizon.com/business/fr-fr/resources/reports/dbir/].

8 CISCO, Rapports sur la cybersécurité, 2020, [https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html].

Comment l'authentification multifactorielle déjoue la fraude

Les gens ont tendance à penser que les courriels provenant de personnes qu'ils connaissent sont légitimes et dignes de confiance, c'est pourquoi il est nécessaire de mettre en place des mesures de protection pour les courriels. La principale faiblesse réside souvent dans les mots de passe, qui sont à l'origine de 80 % des violations liées au piratage informatique9.Parce que la méthode traditionnelle de connexion avec un nom d'utilisateur et un mot de passe, appelée l'authentification à un facteur, est facile à pirater, d'autres couches de protection sont nécessaires pour prévenir les pertes dues à la cybercriminalité.



La principale faiblesse réside souvent dans les mots de passe, qui sont à l'origine de 80 % des violations liées au piratage informatique.

La méthode la plus efficace est sans doute l'authentification multifactorielle, qui offre essentiellement une deuxième ligne de défense contre le détournement de comptes de courriels et la compromission de courriels professionnels. L'authentification multifactorielle exige au moins deux facteurs d'authentification, ou preuves d'identité, afin de confirmer que les personnes qui tentent d'accéder au compte de courriel et à d'autres actifs clés de l'entreprise sont bien celles qu'elles prétendent être. La compromission de deux facteurs d'authentification ou plus représente un défi de taille pour les pirates informatiques et réduit ainsi considérablement le risque de compromission[10].

La stratégie qui sous-tend l'authentification multifactorielle comporte jusqu'à trois couches de protection[11] :

1

Quelque chose que vous connaissez (généralement un mot de passe ou un code de vérification)

2

Quelque chose que vous possédez (un dispositif de confiance qui n'est pas facilement reproduit, comme un téléphone ou un jeton de sécurité)

3

Quelque chose que vous êtes (biométrie)

Les banques, par exemple, utilisent une variante courante de l'authentification multifactorielle aux guichets automatiques, en exigeant une carte bancaire (qu'une personne possède) *et un NIP* (qu'une personne connaît) pour distribuer des fonds. Une autre forme courante d'authentification multifactorielle est un mot de passe unique, comportant une durée de vie limitée, envoyé par messagerie texte à un téléphone intelligent ou par courriel. Les facteurs biométriques, tels que les empreintes digitales et rétiniennes et l'authentification vocale, sont moins répandus.

La protection la plus simple contre la prise de contrôle d'un compte de courriel demeure néanmoins l'authentification multifactorielle. Ainsi, les employés ou les consommateurs doivent prouver leur identité d'au moins deux manières pour accéder à leur compte de courriel. Cela comprend, sans s'y limiter, la saisie d'un nom d'utilisateur et d'un mot de passe, suivie de la saisie d'un code généré par un jeton sur le téléphone ou l'ordinateur de l'utilisateur. Ce code demeure généralement valide durant une courte période.

Le principe qui sous-tend l'authentification multifactorielle est que, bien que les cybercriminels peuvent voler ce que les utilisateurs légitimes savent, il est beaucoup moins probable qu'ils réussissent à s'emparer de ce que ces utilisateurs possèdent. Dans le cas d'un compte de courriel, l'utilisateur possède un jeton ou un dispositif qui génère ou reçoit un code unique ayant une courte durée de vie.

---

[9] *Why MFA is a top priority in 2020,* 2020, [https://techcommunity.microsoft.com/t5/azure-active- directory-identity/fash-whitepaper-why-mfa-is-a-top-priority-in-2020/ba-p/1194467].
[10] *Why MFA is a top priority in 2020,* 2020, [https://techcommunity.microsoft.com/t5/azure-active-directory-identity/fash-whitepaper-why-mfa-is-a-top-priority-in-2020/ba-p/1194467].
[11] Ibid.

Implantation de l'authentification multifactorielle

L'implantation de l'authentification multifactorielle peut être l'un des moyens les plus rapides et efficaces pour protéger l'identité des utilisateurs. Cette fonctionnalité est offerte à tous les utilisateurs d'Office 365 depuis 2014, mais de nombreux administrateurs de systèmes de petites et moyennes entreprises ne l'ont pas encore activée pour leurs utilisateurs. Pour justifier cette omission, ils ont invoqué, notamment, que l'authentification multifactorielle rend l'accès aux comptes plus difficile pour les utilisateurs, qu'elle est trop complexe et que les utilisateurs doivent être formés. Certains doutent même de son efficacité[12].

Lorsqu'elle est correctement implantée, l'authentification multifactorielle s'avère à peine perceptible pour les utilisateurs. Évidemment, personne ne souhaite se soumettre à une authentification multifactorielle chaque fois qu'il ou elle consulte son courriel sur un téléphone intelligent ou se connecte à partir d'un appareil appartenant à l'entreprise. Mais il est logique de demander aux utilisateurs de s'y soumettre dans certains cas précis, par exemple lorsqu'ils se connectent à Office 365 à partir d'un appareil personnel comme une tablette ou un ordinateur personnel dans le cadre d'un programme de type « apportez votre appareil ». L'administrateur système ou l'équipe de sécurité d'une organisation ne peut pas connaître l'état de ces appareils personnels ni savoir s'ils sont infectés par des logiciels malveillants, d'où la nécessité de renforcer la protection de l'identité.

L'objectif consiste à protéger les données et l'identité de l'utilisateur sur les appareils fiables et non fiables, et l'implantation de l'authentification multifactorielle est l'un des meilleurs moyens d'y parvenir.

Les grandes entreprises utilisent l'authentification multifactorielle pour limiter l'accès aux systèmes critiques. Quant à eux, les systèmes de soins de santé utilisent l'authentification multifactorielle pour garantir la sécurité des renseignements médicaux. Les consommateurs utilisent quotidiennement l'authentification multifactorielle lorsqu'ils accèdent à leurs comptes bancaires en ligne, aux médias sociaux et à de nombreux autres sites. De plus, de nombreuses petites entreprises utilisent l'authentification multifactorielle pour les courriels, car elle permet d'empêcher les hameçonneurs de s'infiltrer dans les systèmes de l'entreprise.

Grâce à la technologie actuelle, l'authentification multifactorielle constitue désormais une solution facilement accessible et pratique pour toute entreprise et tout particulier. De nombreux services Web populaires, si ce n'est la plupart, proposent l'authentification multifactorielle – bien qu'elle soit souvent désactivée par défaut.

Le site « Turn on 2FA » de Telesign (www.telesign. com/turnon2fa) offre un outil utile que les consommateurs peuvent utiliser pour activer l'authentification multifactorielle dans leurs comptes personnels.

Microsoft offre également l'application Authenticator[13] qui permet aux utilisateurs de se connecter à des comptes de différentes manières :

- **Authentification multifactorielle :** La méthode de vérification standard, où l'un des facteurs est un mot de passe. Après s'être connectés à l'aide d'un nom d'utilisateur et d'un mot de passe, les utilisateurs peuvent approuver une notification ou saisir un code de vérification fourni.
- **Connexion par téléphone :** Cette version de l'authentification multifactorielle permet aux utilisateurs de se connecter sans mot de passe, en utilisant un nom d'utilisateur et leur appareil mobile avec une vérification par empreinte digitale, reconnaissance faciale ou NIP.
- **Génération de codes :** On peut utiliser un générateur de code pour tout autre compte qui prend en charge les applications d'authentification.

Garantir votre posture en matière de cybersécurité

Chubb et Microsoft considèrent que l'authentification multifactorielle constitue l'un des contrôles de cybersécurité les plus cruciaux et rentables et que toutes les entreprises et tous les particuliers devraient l'adopter. En fait, cet aspect pèse le plus dans la notation Microsoft Secure Score.

Le Microsoft Secure Score offre une mesure de la posture globale de sécurité d'une organisation, où un chiffre plus élevé indique que davantage de mesures d'amélioration ont été prises. Suivre les recommandations de Microsoft Secure Score peut aider les organisations à se protéger contre les menaces. À partir d'un tableau de bord centralisé dans le centre de sécurité Microsoft 365, les entreprises peuvent surveiller et améliorer la sécurité de leurs identités, données, applications, appareils et infrastructures sur Microsoft 365.

Microsoft Secure Score aide les organisations :

- à faire rapport sur l'état actuel de la posture en matière de cybersécurité de l'organisation;
- à améliorer leur posture en matière de cybersécurité grâce à de la détectabilité, à de la visibilité, à des directives et à un contrôle;
- à se comparer à des références et à fixer des indicateurs clés de performance (ICP).

Les organisations ont accès à des visualisations rigoureuses des mesures et des tendances, à l'intégration avec d'autres produits Microsoft, à la comparaison des résultats avec des organisations similaires, etc. Le score peut également refléter lorsque les mesures recommandées ont été prises à l'aide de solutions tierces.

Pour en savoir plus sur Microsoft Secure Score – y compris sur la manière d'obtenir et d'améliorer un score et sur la manière dont les scores sont calculés – visitez le site https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls.

---

[12] SIMONS, Alex, *Announcing password-less login, identity governance, and more for Azure Active Directory*, 2018, [https://techcommunity.microsoft.com/t5/azure-active-directory-identity/announcing-password-less-login-identity-governance-and-more-for/ba-p/262472].

[13] Pour en savoir plus sur l'application Microsoft Authenticator, visitez le site https://techcommunity.microsoft.com/t5/azure-active-directory-identity/what-s-new-in-azure-active-directory-at-microsoft-ignite-2019/ba-p/827831.

Fermer la porte numérique à la cybercriminalité par courriel

Même après l'implantation de l'authentification multifactorielle, il est important de demeurer conscients que la cybersécurité ne devrait pas s'arrêter à la porte numérique de l'organisation. En effet, les organisations doivent s'assurer que tous les fournisseurs, partenaires commerciaux et clients qui interagissent avec leur réseau informatique activent également l'authentification multifactorielle, car les cybercriminels pourraient s'infiltrer dans les systèmes de l'organisation par toute porte laissée ouverte en matière d'authentification.

Dans le monde actuel où la cybercriminalité s'intensifie rapidement, il est essentiel de disposer d'une ligne de défense solide contre des criminels très sophistiqués, qui travaillent souvent en réseau et s'efforcent de dérober des fonds autant aux particuliers qu'aux entreprises. L'implantation de l'authentification multifactorielle force les cybercriminels à passer leur chemin - ils ne trouveront pas de proies faciles ici.

À propos des auteurs:

Joram Borenstein est le directeur général du groupe des solutions de cybersécurité de Microsoft. Plus récemment, Joram a été membre du groupe de travail sur les paiements sécurisés de la Réserve fédérale américaine et du comité consultatif sur les technologies financières de la Conference of State Bank Supervisors (CSBS). Il a formé des régulateurs financiers de la FDIC, de l'OCC, de l'OTS, de la Réserve fédérale et de la NCUA. De plus, il s'est exprimé lors de dizaines d'événements dans le secteur, notamment la conférence IAM de Gartner, la RSA Conference, la CSA/ENISA Conference, Nacha Payments, Money 20/20 et les conférences de l'Association for Finance Professionals et de l'American Bankers Association. Il est titulaire des certifications CISSP et CISA, est actuellement conseiller auprès du conseil d'administration d'une entreprise en démarrage spécialisée dans l'identité biométrique appelée Element, et était auparavant conseiller auprès du conseil d'administration de Conjur (une entreprise en démarrage spécialisée dans la sécurité du développement et de l'exploitation, acquise par CyberArk en 2017).

Patrick Thielen est vice-président principal, Risques financiers, chez Chubb en Amérique du Nord et spécialiste des produits d'assurance erreurs et omissions pour les domaines des cyberrisques et de la technologie en Amérique du Nord. Il dirige actuellement les efforts de Chubb pour améliorer et étendre la couverture des cyberrisques et les solutions d'atténuation des risques pour les petites et moyennes entreprises, ainsi que pour les particuliers prospères et leurs familles. Il a obtenu un diplôme avec distinction de la Carlson School of Management de l'Université du Minnesota en 2003.

Christopher Arehart est vice-président principal et directeur des produits d'assurance contre les vols et les détournements (notamment financiers), les enlèvements, les demandes de rançon et les extorsions, la fraude postale et la violence au travail de Chubb. Chris a été cité dans de nombreux articles parus dans des publications spécialisées, est apparu à l'émission *All Things Considered* de NPR et est fréquemment invité comme conférencier sur la cybercriminalité. Il a également fait des présentations devant l'American Banking Association, l'American Bar Association, la Casualty Actuarial Society et la PLUS University. Il est titulaire d'une maîtrise en administration des affaires de l'Université du Colorado à Boulder, ainsi que de baccalauréats en musique et en commerce du Whittier College de Whittier, en Californie.

Autres sources de référence :

IMAM, Fakhar, **Phishing technique: Message from the boss**, 2020, [https://resources.infosecinstitute.com/phishing-technique-message-from-the-boss/#gref].

Protection contre l'usurpation d'e-mail, [https://www.mimecast.com/fr/solutions/email-security/impersonation/].

HIGGINS, Kelly Jackson, **Hacking the Business Email Compromise,** 2017, [https://www.darkreading.com/threat-intelligence/hacking-the-business-email-compromise].

YOUNG, Ashton, **Cybercriminals taking over email accounts and scamming contacts**, 2018, [https://securitybrief.eu/story/cybercriminals-taking-over-email-accounts-and-scamming-contacts/].

Minimize Business Email Compromise Risk by Protecting Credentials, 2017, [https://www.secureworks.com/blog/minimize-business-email-compromise-risk-by-protecting-credentials].

MARSHALL, Emmanuel, **CEO fraud attacks up 2,370% since 2015**, 2018, [https://www.mailguard.com.au/blog/ceo-fraud-up-2370pc].

Security 101: Business Email Compromise (BEC) Schemes, 2016, [https://www.trendmicro.com/vinfo/my/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes].

YOUNG, Ashton, **Cybercriminals taking over email accounts and scamming contacts**, 2018, [https://securitybrief.eu/story/cybercriminals-taking-over-email-accounts-and-scamming-contacts/].

Why Don't More Companies Use Multi-Factor Authentication?, 2017, [https://www.riskcontrolstrategies.com/2017/11/06/dont-companies-use-multi-factor-authentication/.

BROMILEY, Matt, **Bye Bye Passwords: New Ways to Authenticate,** 2019, [https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ].

Chubb. Insured.[SM]

Pour en savoir plus sur l'expérience et l'expertise de Chubb en matière de gestion des cyberrisques, visitez le site Web : www.chubb.com/ca-fr/.

Microsoft