Email: Is the Digital Door Propped Open for Identity Hijackers?

Multi-Factor Authentication Helps Shut Cyber Criminals Out

CHUBB® | Microsoft

The FBI's Internet Crime Complaint Center (IC3) received

467,361

complaints in 2019

an average of nearly

1,300

every day

and recorded more than

$3.5 billion

in losses to individual and business victims.

There's a good reason why cyber criminals expertly develop online scams that target individuals and businesses: their trade nets billions of stolen dollars each year. In fact, the FBI's Internet Crime Complaint Center (IC3) received 467,361 complaints in 2019 – an average of nearly 1,300 every day – and recorded more than $3.5 billion in losses to individual and business victims.[1] These cyber crimes often fund lavish lifestyles of the cyber criminals behind them, such as the infamous Ramon "Hushpuppi" Abbas, who has flaunted his collection of designer clothes, luxury cars, and private jets for years.[2]

To succeed at this level, cyber criminals must develop ever-changing strategies to persuade people to unwittingly hand over money, data, and personally identifying information. Often-employed scams such as standalone clickable links or email attachments from unknown parties don't work forever, especially once it becomes common knowledge that they are vehicles used to wreak havoc and enable theft.

Some cyber criminals have, as a result, begun employing a highly targeted method: business email account hijacking and impersonation, also known as Business Email Compromise (BEC). Thankfully, there are simple ways to block these increasingly complex attacks.

[1] 2019 Internet Crime Report Released (2020). Retrieved from https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

[2] Karimi, Faith (2020). He flaunted private jets and luxury cars on Instagram. Feds used his posts to link him to alleged cyber crimes. Retrieved from https://www.cnn.com/2020/07/12/us/ray-hushpuppi-alleged-money-laundering-trnd/index.html.

How Email **Impersonation Works**

A compromised inbox is a treasure trove of corporate information that can then be exploited by a cunning criminal.

In a BEC attack, the attacker may hack into a corporate email account and impersonate the real owner (often a business owner or executive) to defraud the company by tricking its customers, partners, and/or employees into sending money or sensitive data to the attacker. It affects companies of all sizes and consumers alike.

Often, the bad actors hack into the company's email by initially targeting a lower-level employee at the company. This can happen in several ways:

1 **Brute force** or using a password cracking tool to automatically try many common passwords.

2 **Credential harvesting** or exploiting the fact that many people use the same ID and password combinations across multiple accounts.

3 **Phishing** or **sending a fake email** request for password reset, thereby harvesting that employee's business email information.

Once they have access, bad actors can read company emails that have been sent to or from that email account, giving them valuable information about who within the organization can transfer money and how those individuals tend to communicate. A compromised inbox is a treasure trove of corporate information that can then be exploited by a cunning criminal.

When impersonating an executive, the cyber criminals may use – or pretend to use – a smartphone (thus bypassing any need for a company logo at the bottom of scam emails) to send an urgent request to a colleague with access to company assets. They'll tell the employee to wire transfer a large amount of money to a bank account owned by the criminals, under the auspice of a confidential business transaction or new venture.

To further ensure their success, cyber criminals may launch their scam when they know the executive is traveling and out of the office. They may also send their request at day's end on a Friday, when authenticating the source will be difficult, particularly because a quick turnaround will be part of their request.

They may even reference an activity tied to the executive's social media profile. For example, if the executive's activity feed shows that he or she is currently traveling abroad, the criminal may say, "I'm having difficulty connecting while overseas and need this handled promptly," thereby discouraging the employee from calling back to verify the request because the executive presumably can't be reached.

Executive impersonation can be complicated, but there is an even simpler way for criminals to scam a company out of its money: initially targeting the email account of a member of the accounts receivable department. When that email is compromised, the bad actor can redirect invoices that the company is due. Simple image editing software enables criminals to alter the payment information on existing invoices, redirecting the payments to one or more accounts controlled by the imposter. In this scenario, two parties lose: the breached organization doesn't get paid, and the customer who believed they were following instructions sent by the real supplier is out their money as well.

This scheme is also often targeted against individuals and families. In this space, bad actors focus on larger financial transactions that individuals are expecting, such as real estate or automobile purchases. Having taken over a seller's email account, the criminal sends legitimate-sounding instructions to the buyer, instructing them to transfer settlement funds to an account controlled by the criminal. By the time the breach is discovered, the criminal may have moved the stolen funds out of the account — and out of the country.

These scams even evolve based on the latest headlines. For example, the Internal Revenue Service is regularly impersonated. In 2020, many taxpayers received stimulus checks from the government as a direct deposit, but some taxpayers who hadn't authorized a direct deposit waited weeks for a check to come by mail. Fraudsters are often on the lookout for ways to take advantage of these kinds of unusual circumstances to attempt to defraud individuals and access their money. In fact, scammers reportedly registered 150,000 fake stimulus check websites before most checks were distributed. Many fake sites like these entice users to give up their personal information by falsely offering to provide the status of their check. Once they input their private information, the scammer uses that data to either redirect the check to another bank account or steal the user's identity.[3] *Remember: the Internal Revenue Service will never call, text, or email consumers requesting personal banking information such as routing or account numbers.*

Scammers reportedly registered **150,000** fake stimulus check websites before most checks were distributed.

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

Why Email **Impersonation Succeeds**

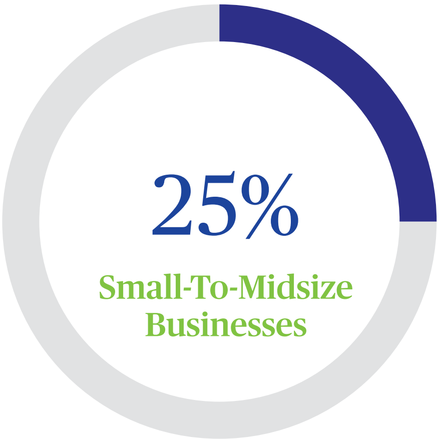
In every case of email-related fraud, the critical factor is whether the recipients of scam email believe in the authenticity of the request. In many cases, such as with vendor payment scams and scams where personal real estate transactions are misdirected, theft is possible precisely because, at their core, the transactions are real and expected. It is the circumstances around those transactions that have been altered to confuse the legitimate parties involved. This is where the term *social engineering* is derived.

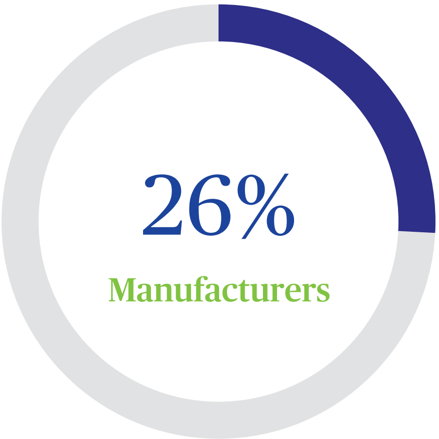
$75

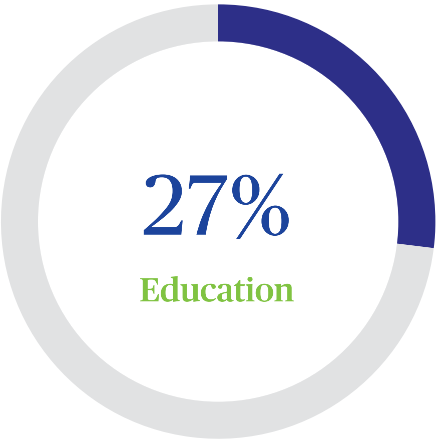
million redirected to cyber criminal bank accounts in one BEC scam

The most affected sectors according to the Chubb Cyber Index^{SM}

In total, social engineering represents 21% of the cyber incidents reported to Chubb in the past three years. These charts show some of the most impacted segments:







BEC criminals know that email is today's *de facto* method of communication. People have been encouraged to "go paperless" by companies, and most feel confident they can spot spam email. But they also inherently trust those they work with and are more likely to respond to requests from their company's executives as well as their trusted suppliers and business partners. A real but compromised account anywhere in the communication stream can lead to disastrous results.

Cyber criminals bank, quite literally, on these human, socially reinforced patterns. And it's not surprising that cyber criminals succeed with schemes that appear, at least in retrospect, unbelievably primitive and transparent. In fact, one quite well-known BEC scam that used keylogger malware to fine-tune email access — and operated without detection for six months in 2015 — redirected invoice payments totaling $75 million to cyber criminal bank accounts.[4] In hindsight, one might expect that someone would notice, given the vast amount of money involved. But no one did.

As severe as the consequences of BEC can be, they are unfortunately also quite frequent. Since 2009, 17 percent of the cyber incidents reported to Chubb have stemmed from social engineering. According to the **Chubb Cyber Index^{SM}**, the sectors most affected include **small-to-midsize businesses** (25 percent), **manufacturers** (26 percent), and **the education industry** (27 percent).[5] And this risk is only increasing — recent security reports from Microsoft,[6] Verizon,[7] and Cisco[8] all indicate the scale and threat of email phishing attacks is growing.

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

[5] Chubb Cyber Index^{SM} (October 2020). Retrieved from https://chubbcyberindex.com/index.html#/splash.

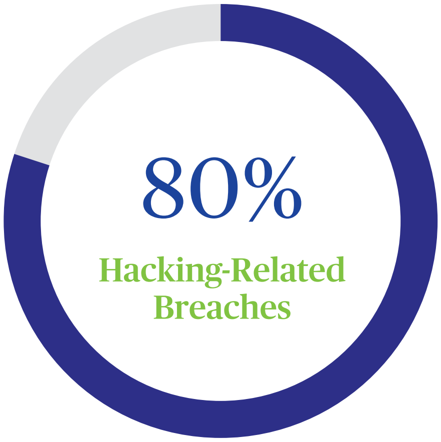
[6] Microsoft Security Intelligence Report Archive (2020). Retrieved from https://www.microsoft.com/en-us/security/business/security-intelligence-report.

[7] Verizon Data Breach Investigations Report (2020). Retrieved from https://enterprise.verizon.com/resources/reports/dbir/.

[8] Cisco Cybersecurity Reports (2020). Retrieved from https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html.

How Multi-Factor Authentication **Foils Fraud**

The human tendency to assume emails from people we know are legitimate and trustworthy underscores the need for email safeguards. The major weakness point is often passwords, which are accountable for 80 percent of hacking-related breaches.[9] Because traditional user login and password access, known as Single-Factor Authentication (SFA), is so easy for criminals to hack into, other layers of protection are needed to prevent cyber crime losses.



The major weakness point is often passwords, which are accountable for 80 percent of hacking-related breaches.

Perhaps the most effective method is Multi-Factor Authentication (MFA), which essentially offers a second line of defense against email account hijacking and related BEC cyber crime. MFA requires two or more authenticating factors, or proofs of identity, to ensure that those seeking access to company email and other key company assets are actually who they say they are. Compromising two or more authentication factors presents a significant challenge for attackers — substantially reducing the risk of compromise.[10]

The authenticating strategy behind MFA involves up to three layers of protection:[11]

1

Something you know
(typically a password or verification code)

2

Something you have
(a trusted device that is not easily duplicated, like a phone or security key)

3

Something you are
(biometrics)

Banks, for instance, use a familiar variant of MFA at ATM machines, requiring a bank card (something someone has) *and a PIN* (something someone knows) before dispensing funds. Another common form of MFA is a time-limited, one-time password texted to a smartphone or sent via email. Less common are the biometric safeguards like fingerprints, retinal scanners, and voice authentication.

The simplest protection against an email account takeover, however, is email MFA. This means that employees or consumers must prove their identity in at least two ways before receiving access to their email. This includes but is not limited to inputting a login and password, followed by inputting a code generated by a soft token on the user's phone or PC. This code is usually only valid for a short period of time.

The idea behind MFA is that, although cyber criminals may steal what legitimate users know, it is much less likely that they'll also have what those users possess. In the case of an email account, what users possess is the soft token or device that generates or receives a unique, short-lived code.

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

Implementing **MFA**

Enabling MFA can be one of the quickest and most impactful ways to protect user identities. This feature has been available for all Office 365 users since 2014, yet many small- to mid-sized business system administrators have not enabled it for their users. Reasons vary from "MFA makes accessing accounts difficult for users," to "it is too complicated," "there is user training involved," or even questions regarding its effectiveness.[12]

When set up properly, MFA is hardly noticeable to users. Certainly, no one wants to complete an MFA prompt every time they check their email on a smartphone or log in from a company-owned device. But it does make sense to prompt users for MFA in some instances, such as logging into Office 365 services from a personal device like a tablet or a home computer through a Bring Your Own Device program. An organization's system administrator or security team has no idea what condition these personal devices are in or whether they may be infected with malware, requiring the need for an increase in identity protection. The goal is to protect the data and user identity on both trusted and untrusted devices alike, and implementing MFA is one of the best ways to accomplish that.

Large companies use MFA to limit access to mission-critical systems. Healthcare systems use MFA to ensure Protected Health Information stays secure. Consumers interact with MFA daily when accessing their online bank accounts, social media, and many other sites. And many smaller businesses use MFA for email because it helps keep phishers out.

With today's technology, MFA is now an easily accessible and practical solution for any business or individual. Many, if not most, popular web services offer MFA — although it is often deactivated by default. Telesign's "Turn on 2FA" site (www.telesign.com/turnon2fa) is a helpful tool that consumers can use to enable MFA for their personal accounts.

Another tool is the Microsoft Authenticator app,[13] which helps users sign into accounts in several ways:

- **MFA:** The standard verification method, where one of the factors is a password. After signing in using a username and password, users can either approve a notification or enter a provided verification code.
- **Phone sign-in:** A version of MFA that lets users sign in without requiring a password, using a username and their mobile device with a fingerprint, face, or PIN verification.
- **Code generation:** As a code generator for any other accounts that support authenticator apps.

Ensuring Your **Security Posture**

Chubb and Microsoft collectively view MFA as one of the most critical and cost-effective cyber security controls that all businesses and individuals should adopt. In fact, it's the most heavily weighted aspect of Microsoft Secure Score.

Microsoft Secure Score is a measurement of an organization's overall security posture, with a higher number indicating more improvement actions have been taken. Following the Security Score recommendations can help protect organizations from threats. From a centralized dashboard in the Microsoft 365 security center, organizations can monitor and work on the security of their Microsoft 365 identities, data, apps, devices, and infrastructure.

Secure Score helps organizations:

- Report on the current state of the organization's security posture
- Improve their security posture by providing discoverability, visibility, guidance, and control
- Compare with benchmarks and establish Key Performance Indicators (KPIs)

Organizations gain access to robust visualizations of metrics and trends, integration with other Microsoft products, score comparison with similar organizations, and much more. The score can also reflect when third-party solutions have addressed recommended actions.

To learn more about Secure Score — including how to locate a current score, how the score is calculated, and how to improve a score — visit https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls.

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

[13] To learn more about the Microsoft Authenticator app, visit https://techcommunity.microsoft.com/t5/azure-active-directory-identity/what-s-new-in-azure-active-directory-at-microsoft-ignite-2019/ba-p/827831.

Closing the Digital Door **to Email Cyber Crime**

Even after MFA is enabled, it’s important to still recognize that cyber security shouldn’t stop at the organization’s digital doorstep. Organizations should ensure that any vendors, suppliers, business partners, and customers interacting with their computer network also enable MFA, because an authentication “open door” in any of their systems could serve as a gateway for cyber criminals.

In today’s world of rapidly escalating cyber crime, it’s critical to have a strong line of defense against highly sophisticated and often networked criminals who are bent on stealing from individuals and businesses alike. Installing MFA tells cyber criminals to move on – there are no easy victims here.

About the **Authors:**

Joram Borenstein is the General Manager of Microsoft's Cybersecurity Solutions Group. Joram also recently served as a Member of the U.S. Federal Reserve's Secure Payments Task Force and the Conference of State Bank Supervisors (CSBS) Fintech Advisory Panel. He has instructed financial regulators from the FDIC, OCC, OTS, Federal Reserve, and NCUA and has spoken at dozens of industry events including Gartner's IAM Conference, RSA Conference, the CSA/ENISA Conference, NACHA Payments, the Association for Finance Professionals, Money 20/20, the American Bankers Association, and more. He holds CISSP and CISA certifications, is currently a Board Advisor to a biometric identity start-up called Element, and was previously Board Advisor to Conjur (a DevOps Security start-up acquired by CyberArk in 2017).

Patrick Thielen is a Senior Vice President within Chubb's North America Financial Lines division, and is product lead for the Cyber and Technology Errors & Omissions lines of insurance for North America. He currently manages Chubb's efforts to enhance and expand cyber coverage and risk mitigation solutions for small- and mid-size businesses, as well as for successful individuals and their families. Patrick graduated with honors and distinction from the University of Minnesota's Carlson School of Management in 2003.

Christopher Arehart is Senior Vice President and Product Manager of Chubb's Crime, Financial Fidelity, Kidnap/Ransom and Extortion, Mail, and Workplace Violence Expense insurance solutions. Chris has been quoted in numerous articles that have appeared in industry publications, has appeared on NPR's *All Things Considered*, and is a frequent speaker on the topic of cyber crime. He has also been a speaker for the American Banking Association, the American Bar Association, the Casualty Actuarial Society, and PLUS University. He holds a Master's in Business Administration from the University of Colorado at Boulder, as well as Bachelor's degrees in Music and Business from Whittier College in Whittier, California.

Additional Research Sources:

Imam, Fakhar (2020). **Phishing technique: Message from the boss.** Retrieved from https://resources.infosecinstitute.com/phishing-technique-message-from-the-boss/#gref.

Protect Against Impersonation Attacks. Retrieved from https://www.mimecast.com/solutions/email-security/impersonation/.

Higgins, Kelly Jackson (2017). **Hacking the Business Email Compromise.** Retrieved from https://www.darkreading.com/threat-intelligence/hacking-the-business-email-compromise-/d/d-id/1328497.

Young, Ashton (2018). **Cybercriminals taking over email accounts and scamming contacts.** Retrieved from https://securitybrief.eu/story/cybercriminals-taking-over-email-accounts-and-scamming-contacts/.

Minimize Business Email Compromise Risk by Protecting Credentials (2017). Retrieved from https://www.secureworks.com/blog/minimize-business-email-compromise-risk-by-protecting-credentials.

Marshall, Emmanuel (2018). **CEO fraud attacks up 2,370% since 2015.** Retrieved from https://www.mailguard.com.au/blog/ceo-fraud-up-2370pc.

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

Young, Ashton (2018). **Cybercriminals taking over email accounts and scamming contacts.** Retrieved from https://securitybrief.eu/story/cybercriminals-taking-over-email-accounts-and-scamming-contacts/.

Why Don’t More Companies Use Multi-Factor Authentication? (2017). Retrieved from https://www.riskcontrolstrategies.com/2017/11/06/dont-companies-use-multi-factor-authentication/.

Bromiley, Matt (2019). **Bye Bye Passwords: New Ways to Authenticate.** Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ.

Chubb. Insured.$^{\text{SM}}$

To learn more about Chubb s industry-leading cyber risk management experience and expertise, visit www.chubb.com/cyber.

The information contained in this document is intended for general informational purposes only and is not intended to provide legal or other expert advice. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Neither Chubb nor its employees or agents shall be liable for the use of any information or statements made or contained in any information provided herein. This document may contain links to third-party websites solely for informational purposes and as a convenience to readers, but not as an endorsement by Chubb of the entities referenced or the contents on such third-party websites. Chubb is not responsible for the content of linked third-party websites and does not make any representations regarding the content or accuracy of materials on such linked websites. The opinions and positions expressed in this report are the authors' own and not necessarily those of Chubb.

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit www.chubb.com. Insurance is provided by ACE American Insurance Company and its U.S. based Chubb underwriting company affiliates. All products may not be available in all states. This communication contains product summaries only. Coverage is subject to the language of the policies as actually issued. Surplus lines insurance is sold only through licensed surplus lines producers.

Microsoft

Microsoft Corporation, all rights reserved. This document is provided “as-is.” Information and views expressed in this document, including URLs and other Internet website references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. This document does not provide you with any legal rights to any intellectual property in any Microsoft product.