Guarding Against Email Social Engineering Fraud: Re-examining a Global Problem

CHUBB®

Written by:

Christopher Arehart
Senior Vice President, Chubb

Scott Schmookler
Partner, Gordon Rees Scully Mansukhani, LLP

Taylor Nemeth
Head of Payments, PaymentWorks, Inc.

An estimated

300B

email messages are exchanged every day by businesses and individuals[1]

Cyber security risks have increased for organizations,

as many employees have shifted to working from home over less-secure wi-fi networks

The FBI estimates that cyber criminals stole more than

$28B

through email fraud from 2016 - 2020, with an average loss per incident of more than

$150K[2]

In a late 2020 survey by the Association of Certified Fraud Examiners, more than

80%

of respondents across different organization types had observed an increase in cyber fraud since the coronavirus pandemic began

Each year, an estimated

30%

of suppliers change a piece of their supplier information,[11] which could include a new physical address, a changed bank account, or something more complex

Even with protections put in place by internal IT departments or outside partners, email remains an unsecured and unreliable technology capable of being hacked, altered and manipulated.

Email has become an indispensable tool for global businesses, improving efficiency by facilitating nearly instantaneous communication and expediting vital actions about sales, payments and other critical business activities. An estimated 300 *billion* email messages are exchanged every day by businesses and individuals.[1] While its speed and ease of access have made email routine and universally accepted, these benefits mask the inherent vulnerability of email and often lull well-intentioned employees into a false sense of security. In reality, even with protections put in place by internal IT departments or outside partners, email remains an unsecured and unreliable technology capable of being hacked, altered and manipulated.

The FBI estimates that cyber criminals stole more than $28 billion through email fraud from 2016-2020, with an average loss per incident of more than $150,000.[2] In addition, since the coronavirus pandemic began in early 2020, cyber security risks have increased for organizations, as many employees have shifted to working from home over less-secure wi-fi networks. At the same time, to maintain their revenue, many businesses have adopted or increased their use of e-commerce and electronic transactions with their partners and customers.

When combined, these factors have created an even busier environment for cyber criminals to exploit email for fraudulent activities.

In fact, in a late 2020 survey by the Association of Certified Fraud Examiners, more than 80 percent of respondents across different organization types had observed an increase in cyber fraud since the pandemic began; this included business email compromise and payment fraud. Schemes are constantly evolving, requiring businesses to adopt procedures that guard against intrusions. While email attacks in the past focused on delivering links and attachments with malicious code, today's cyber criminals are employing more sophisticated social engineering attacks that are designed to manipulate a sender's identity, intercept important messages and send messages that appear authentic to recipients. Without attachments or files that would be detected by malware-scanning systems, these emails can readily pass through basic security defenses.

With the heightened level of deception and manipulation involved in these attacks, email security requires a zero-trust approach.

For example, an email requesting payment or bank routing information should be considered suspicious until the information can be independently verified through another channel, such as a direct phone call. This report outlines common types of social engineering schemes, particularly involving payments and suppliers, as well as the technology tools and enhanced procedures that can help employees protect themselves and their companies against them.

Email Components Enable Fraud

Email technology makes it easy for cyber criminals to pose as legitimate business associates over email

Think of email as a physical letter in an envelope. An email contains "envelope headers" that dictate its routing and delivery through email software, just as an address on an envelope enables postal workers to deliver a letter. Email also has "message headers" in the message itself, similar to the address at the top of a letter inside an envelope. Since email software only uses the envelope header to deliver email, the message header can display a different, fraudulent sender – the same way the name on a letter may differ from the name on the envelope.[3]

Email Envelope Header

Email Message Header

Email Message Header
can display a different, fraudulent sender

When a recipient opens an email, the software displays the message – **but hides the envelope header.** This provides an opportunity for cyber criminals to assume the identity of anyone they think might facilitate a payment.

Understanding Social Engineering Schemes

The widespread use of email provides cyber criminals with cheap and efficient means of targeting victims for fraud. Whether by "spoofing" email accounts or breaching business partners' email systems, cyber criminals continue to successfully deploy social engineering schemes, catching even well-intentioned employees with deceitful emails. These schemes often succeed despite a high level of publicity because employees trust and accept unsecured email without taking the necessary steps to verify a message's source and content, even when it involves electronic payment instructions.

The following scenarios represent the more common social engineering fraud schemes and the best ways to prevent them:

Spoofing: The Fake CEO and Band of Accomplices

Knowing that email envelope and message headers can differ, cyber criminals will often assume the identity of the CEO of an organization or someone in a law firm that has been purportedly hired to facilitate a transaction, and the target of the email is a person authorized to initiate and approve wire transfers.

These types of emails are shockingly easy to produce, and there are even websites specifically for this purpose.[4] This social engineering scheme is both simple and low-touch for cyber criminals, as they do not need to gain access to or actually use any computer owned or operated by a business, nor do they need to load, insert, implant or enter any destructive program, virus, malware or operable code into a computer. They only rely on the inherent human tendencies to trust email and overlook any red flags of fraud.

Despite the brazenness of such attempts, impersonation of executives, vendors and suppliers continues to be a common means of attack. The imposter sets the trap by describing a transaction or merger that requires an immediate transfer of payment. Such ploys succeed even when a business requires segregation of duties, so that one individual is unable to complete a transaction on their own. Unfortunately, segregation of duties assumes that those entrusted with the authority to process wire transfers are also willing and empowered to *question* requests, even those that are supposedly made by their superior. Criminals understand this hesitation, and prey on those with authority who are not second-guessed by colleagues.

How can an organization prevent such attacks?

Corporate email systems should be reconfigured to better screen for spoofed emails, since the protocols that underpin them are 40 years old.[5] Businesses should establish a strong policy for wire transfer authority, where multiple people are required to release funds, after a separate person has initiated the transfer.

Tech Fixes to Keep Email Secure

These updated technologies can be enabled to support more secure messaging:[6]

Sender Policy Framework (SPF):

An email-authentication technique used to prevent spammers from sending messages on behalf of your domain.

With SPF, an organization that hosts an Internet domain can publish authorized mail servers approved to send email from this domain, giving the receiving system information it can use to verify the origin of the email.

Domain-Keys Identified Mail (DKIM):

An email-authentication technique allows the receiver to check that an email was indeed sent from the owner of the domain.

Encrypted DKIM signatures are added to legitimate email to confirm that certain parts of the message, including its contents and attachments, have not been altered.

Domain-based Message Authentication, Reporting & Conformance (DMARC):

DMARC leverages the technologies of SPF and DKIM and also adds reporting capabilities, enabling the owner to automatically reject or quarantine specific messages based on a policy established by the email administrator.

Multi-Factor Authentication (MFA):

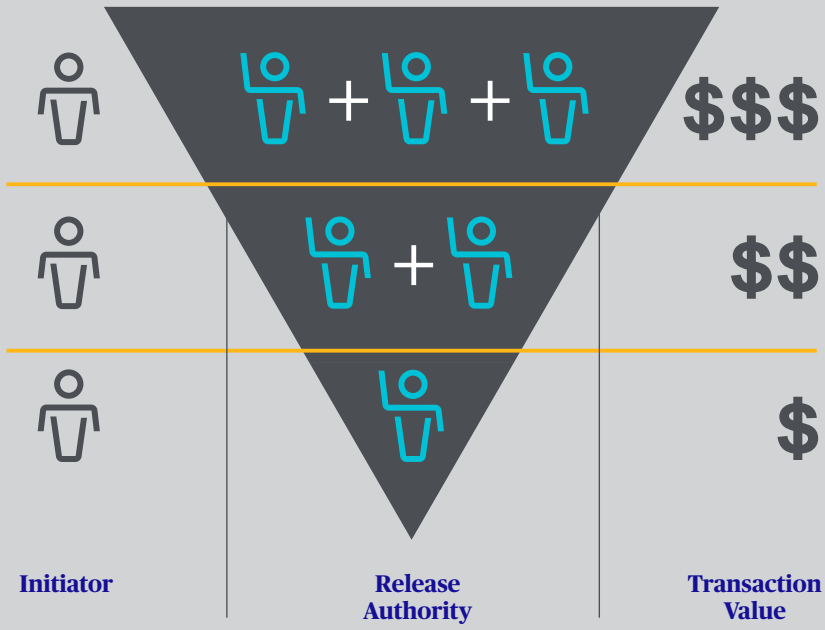
A system that adds an additional layer of authentication to a log-in process by requiring the user to provide an additional piece of information that regularly changes (such as a token, key or code delivered to a cell phone or other device), in addition to their known user credentials (i.e., username and password).

Only having all three pieces of information (the username, password and one-time code) allows the user into the system. Chubb's Multi-Factor Authentication[7] whitepaper focuses on the ways an organization can block business email account hijacking and impersonation attacks.

These tools are supported by all email providers, and in most cases, may be included at low or no additional cost, but it is up to the company's IT administrator, or those in charge of maintaining email systems, to activate these services to harden their email security.

While these technology tools can be effective, organizations should also consider updating their business practices, such as adding more layers of authority as a transaction rises in value and urgency. Rather than trusting one person to approve the release of a large wire transfer of funds, organizations should institute policies that require a second person to review the supporting materials and authenticate the request. This **"four eyes" principle** is regularly employed in other mission critical systems where redundancy is a must,[8] from rocket launches to safe deposit box opening. Wire transfers should be treated with similar caution.

Wire Transfer Authority Matrix



The Compromised Vendor's Online Email Account

Cyber criminals also take advantage of email security vulnerabilities to hack into vendors' email accounts. Because email can be globally accessed with a username and password, it is insecure by design and the weakest link in any payment process.[9] In early 2020, the FBI warned private industry partners about hackers exploiting both Microsoft Office 365 and Gmail, citing more than $2 billion in reported losses, using stolen credentials to directly access and hijack real business email accounts.[10]

This type of scam begins with a cyber criminal searching for businesses that externally broadcast their web-based email access (mail.organization.com, for example) and infiltrating a supplier's email account. They then target the supplier's employees with fake administrator emails, attempting to trick them into disclosing their username and password.

Over time, the criminal methodically gathers confidential information about payments. Once they understand the organization's processes, they can alter real invoices using simple PDF editing software to direct payment to a bank account they control. Then, they simply wait for the client's Accounts Payable department to pay the bill. These schemes succeed because the bill is expected by the client and comes from a supplier's actual email account. As a result, the request does not set off alerts within the Accounting department, and the email does not trigger technology designed to screen it.

How can an organization prevent such attacks?

To combat this, organizations can re-evaluate and rebuild vendor management processes to account for changes to vendor data, rather than address them ad hoc during the payment process. Each year, an estimated 30 percent of suppliers change a piece of their supplier information,[11] which could include a new physical address, a changed bank account or something more complex, such as accounting for a merger of companies under one taxpayer identification number. Few vendors proactively supply this information; most simply adjust their invoices to request payment to a different bank. Companies that can manage these supplier changes internally should establish a verification protocol that requires a phone call to a known vendor contact to verify the changes requested on the invoice. If the number of suppliers is too many to manage this process in-house, companies should hire a vendor management partner that can verify ownership of bank accounts, not just whether the account exists.[12]

The Compromised Vendor Management Account

To address a high volume of requests to change vendor payment information, businesses often implement an online "vendor portal" to push the updating of account information back to their suppliers. These web-based self-service platforms allow suppliers to input or change payment information efficiently and cost effectively. However, these systems can actually assist hackers, who troll the web for portals that either do not require users to authenticate themselves or only require weak credentials that can easily be obtained from a compromised email account. After the criminal enters the portal, they request changes to payment details and wait for the company to process payments.

While many popular enterprise management systems include supplier portals, they often require very little, if any, validation to vet information provided by users. For example, if a user enters the correct credentials, they can input bank routing information without any verification of the legitimacy of the routing information or their authority to alter a business partner's information.

How can an organization prevent such attacks?

The best way to prevent this type of fraud is to work with solution providers that understand the core problem that needs solving – to *authenticate* the information being provided, rather than collect the information in a different way. For example, PaymentWorks'[13] platform allows users to onboard vendors, or payees, in a networked environment for identity proofing and verification.

Reacting in the Wake of a Fraud

If you believe you are a victim of business email compromise, it is imperative that you act quickly:

1. Immediately contact the originating bank and request a recall of the wire transfer and confirm that recall in writing.
2. Immediately file a complaint with the FBI at www.ic3.gov. Reporting to the FBI triggers the Bureau's Recovery Asset Team and the FBI's assistance in seeking return of the wire transfer.
3. Preserve records of the incident, including emails sent and received in their original electronic state. Correspondence and forensic information contained in these electronic files helps investigators shed light on the perpetrator(s), and parties responsible for the incident.
4. Once the above steps are complete, contact your insurance carrier per the reporting instructions in your policy.

While neither recalling the wire transfer nor reporting to the FBI guarantees the return of your funds, these steps maximize the opportunity to mitigate your loss, assist the FBI in tracing the funds and help establish any insurance claim.

Re-evaluating the Role of Email in the Payment Process

Given the motivation and ingenuity of cyber criminals, organizations should keep in mind that these frauds continue to rise as criminals adapt to countermeasures deployed to thwart them.

Curbing social engineering online payment fraud not only requires organizations to protect themselves with updated technology defenses, but also to re-evaluate their policies and procedures for verifying information received electronically, authenticating the identity of those that provide it and authorizing payments to their business partners. Cyber criminals will continue to find opportunities for payment fraud until businesses – both suppliers and customers – adapt their processes and fundamentally change their procedures to fill the gaps made possible by email.

About the Authors

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.

Chubb
carehart@chubb.com | 312.529.6712
www.chubb.com/us/socialengineeringfraud

Scott Schmookler is a Partner in the Chicago office of Gordon Rees Scully Mansukhani, LLP. Scott counsels clients on insurance issues relating to technology, cybercrime, cyber security, and data breaches. Representing insurers in claims under commercial crime policies, computer crime policies, cyber security policies, and data breach insurance policies, he provides advice on insurance claims arising from data breaches and cyber-attacks, coordinates remediation and regulatory responses, and litigates disputes.

Gordon Rees Scully Mansukhani, LLP
sschmookler@grsm.com | 312.980.6779 | www.grsm.com

Taylor Nemeth is Head of Payments at PaymentWorks – a Business Identity Platform. Taylor has been at the company since its infancy and has spent much of his time responsible for corporate strategy and Go-to-Market execution. Taylor led company efforts to transform PaymentWorks' B2B Payment Security solution from concept to reality. Taylor is currently responsible for the strategy, successful operation, and growth of the Payments business at the company. Taylor is also co-host of the PaymentWorks Presents: Risky Business podcast with his co-host and colleague Angela Sarno. Prior to PaymentWorks, Taylor worked for 10+ years in payments-related Product Management and Operations roles at CBORD.

PaymentWorks
partners@paymentworks.com | 781.916.8855
www.paymentworks.com

Sources

1. www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf accessed March 30, 2021
2. www.ic3.gov/Media/Y2019/PSA190910 accessed February 1, 2021 and www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf accessed March 30, 2021
3. www.techlicious.com/how-to/how-to-tell-if-email-has-been-spoofed/ accessed February 1, 2021
4. www.makeuseof.com/tag/deadfake-send-fake-anonimous-email-messages/ accessed February 1, 2021
5. https://tools.ietf.org/html/rfc788 accessed February 1, 2021
6. www.dmarcanalyzer.com/spf/
7. https://dmarcly.com/blog/how-to-set-up-dmarc-dkim-and-spf-in-office-365-o365-the-complete-implementation-guide
8. www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/cyber-insights/documents/pdf/2020-12.10%2017-01-0279%20MFA%20Helps%20Shut%20Cyber%20Criminals%20Out.pdf
9. www.unido.org/overview/member-states/change-management/faq/what-four-eyes-principle
10. www.viget.com/articles/email-is-completely-insecure-by-default/
11. www.bleepingcomputer.com/news/security/fbi-warns-of-bec-attacks-abusing-microsoft-office-365-google-g-suite/
12. www.paymentworks.com/?utm_campaign=Q3%2021%20Fraud&utm_source=Chubb%20Whitepaper&utm_medium=PDF&utm_content=Chubb%20Whitepaper%20link
13. www.fbi.gov/news/stories/money-mule-sentenced-for-role-in-bec-scheme-071620
14. www.paymentworks.com

Chubb. Insured.℠