CYREBRO

2022 Fraud and Email Compromise Investigation Analysis

Zero-days capture headlines but fraud is far more likely to impact modern businesses.

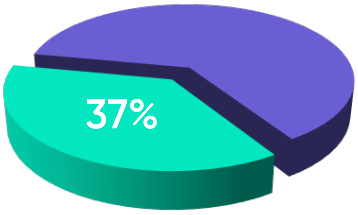
TABLE OF CONTENTS

Executive Summary

Ransomware incidents, supply chain disruption, and the theft of funds or data are constantly featured in the news cycle. While cyberattacks can be catastrophic and extremely costly for businesses, they are frequently caused by simple scams and basic security mistakes.

Fraud existed long before access to the internet became an essential tool for our personal and work lives. Fraud is an age-old concept; however, businesses now face far more dangerous threats than mass spam campaigns claiming you've won the lottery or owe government taxes.

Scam artists have moved with the times and have evolved their methods to suit. Phishing emails, malicious social media links, fake monetary scams, and Business Email Compromise (BEC) schemes are widespread. While they might not seem as interesting as zero-day vulnerabilities or exploit kits, they are far more likely to impact today's companies.



BEC-related fraud caused 37% of all security-related losses last year in the US

$4.2 billion estimated losses in 2020

BEC-related fraud caused 37% of all security-related losses last year in the US, costing billions of dollars in the country alone. The FBI estimates that 2020 losses exceeded $4.2 billion.

CYREBRO has investigated many fraud cases involving BECs and illegitimate transactions between vendors. For example, when an employee's account is compromised ahead of a planned transaction, it can be used to spy on company dealings.

At the right moment, attackers will interfere.

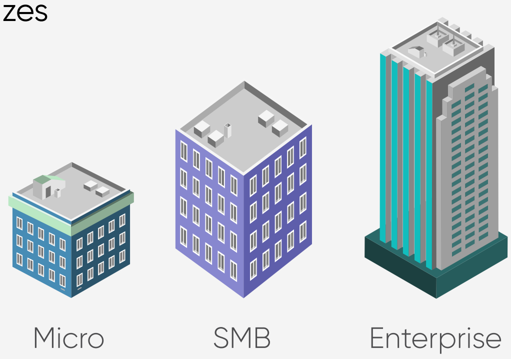
This can include changing financial account details, impersonating an executive, communicating with payroll or suppliers, and more. Transactional fraud cases are usually complex and take several days to several weeks for a heist to be successful. By tracking them, however, CYREBRO can provide you with valuable insight into the modern fraudster's playbook.

Research Methodology

One of CYREBRO's digital forensics and incident response (DFIR) capabilities is fraud investigation, in which we have analyzed countless forms of fraud impacting organizations today.

For this research, we analyzed two dozen fraud cases that CYREBRO investigated, to establish the most common fraud attacker actions, their underlying intentions, and who is at most risk. The clients had very little in common both in size and industry. We included enterprise firms with upward of 5,000 employees, SMBs, and Micro businesses while considering clients operating different network architectures, contrasting network sizes, and those with varying software and network management solutions.

Organization sample sizes



Now armed with this information, we can tell you how best to protect against modern scams and attempts at fraud.

Many types of fraud appear the same on the surface. However, by diving into our clients' mail systems, we can extract every message relating to a fraud case, creating an attack timeline, and explaining each step in the attack chain in our incident response reports.

We also verify IP addresses, collect audit and account access activity logs, timestamps, User-Agent details, and more. This helps us determine which accounts have been compromised, and when.

To best prepare for and build the proper security processes and measures, CYREBRO has detailed the most common recurring recommendations that would have prevented a fraud incident. You will find insights and details that can help build a secure network and safer employee transactions.

Key Findings

100%

of cases could have been prevented by implementing multi-factor authentication (MFA) for users' mailboxes.

92%

of cases showed that a security awareness education program could have prevented a fraud incident.

71%

of cases revealed that enforcing a routine password change policy could have prevented a fraud incident

84%

of cases revealed that a fraud incident occurred due to lacking geolocation locks or IP whitelists

Key Fraud Prevention Analysis Findings

Our investigations have shown that currently, a large majority of online fraudsters originate from African and Asian countries.

However, attackers can 'be located' anywhere through virtual private networks (VPNs), which can make them appear to come from whatever country they wish in the world. It is not just external threats that businesses have to be on the lookout for – they can come in the form of insiders, too.

Insider incidents, whether malicious or accidental, have risen by 44% over the past two years and are estimated to cost enterprise organizations up to $15.4 million per incident.

Based on our years of fraud investigation, we recommend the following steps to limit exposure to common forms of business scams and fraud.

100%

CYREBRO's fraud investigations analysis showed that 100% of the cases could have been prevented if multi-factor authentication (MFA) had been enforced for users' mailboxes.

1. ENFORCE MULTI-FACTOR AUTHENTICATION (MFA)

CYREBRO's fraud investigations analysis showed that 100% of the case's initial intrusion could have been prevented if multi-factor authentication (MFA) had been enforced for users' mailboxes. We found that in every case of fraud we examined involving a compromised account, the initial intrusion could have been prevented if MFA had been enabled.

As phishing is so successful against humans, applying another layer of authentication can prevent fraud and other types of cyberattacks in their tracks as they alert victims to suspicious activity.

However, MFA is not foolproof and should consistently be implemented together with training in how these mechanisms work to ensure mailbox security.

MFA is divided into two main processes:

A. DEDICATED AUTHENTICATION APPS

Pressing "Allow" in an Authenticator application will permit account access attempts. While employees then have a second chance to recognize an intrusion attempt, without training, however, they may also not think and grant permission to their account reflexively.

B. SIX-DIGIT AUTHENTICATION CODES SENT VIA EMAIL, SMS MESSAGES, AUTOMATED PHONE CALLS

This form of MFA requires users to enter their credentials alongside a one-time six-digit code sent to a device or email account they own.

These codes are only valid for a short amount of time. So, it is more difficult for fraudsters to access a victim's account – unless they can convince users to provide them with the code, which should fail if the victim has a good level of cybersecurity awareness. However, MFA codes can be intercepted and stolen through mobile malware.

MFA isn't perfect, but it is quickly becoming a basic security standard in the industry. Another alternative is MFA keys, such as YubiKey, which require users to possess a physical device as a form of verification.

2. GEOLOCATION LOCKS OR IP WHITELISTING

Businesses should apply a geolocation lock or an IP whitelist. Based on CYREBRO research analysis, in 84% of cases, we recommended clients to implement a geolocation lock or an IP whitelist for logging in to the company's mail system (externally to the network).

Geolocation locks, or geo-blocking, restrict user activity based on their geographical location. So, for example, we may recommend that a company based in the United States only permits login attempts to their mail system from an IP address in the same country or even state.

While you may think this could cause problems for remote workers or employees abroad, it is also possible to accept their location – either via temporary additions to geolocation settings or by IP safelisting.

84%

CYREBRO's research analysis revealed that 84% of fraud incidents occurred due to lacking geolocation locks or IP whitelisting.

Controlling access point locations can reduce the chance of mailbox breaches.

IP safelisting is the setting of network permissions based on IP addresses. However, this can be more difficult to manage, as employees could be trying to access corporate resources and their mail through several devices, including PCs and mobile devices – and so their IP addresses are constantly changing.

If a company has strict mail login rules, they could help achieve a state where users have static IPs in their houses and can only log in through them.

3. PASSWORD CHANGE ENFORCEMENT

CYREBRO's research analysis showed that 71% of fraud incidents could have been prevented if the business enforced a routine password change policy for all users.

Everyone knows they should change the passwords of their online services and accounts frequently, but in practice, we often fall short.

Technology vendors now often ban simple and easy-to-guess combinations – such as "QWERTY" or "ADMIN," but this isn't across the board.

A recent study found that while 92% of us realize re-using passwords is poor security practice, 45% of respondents admitted they had not recycled their online account credentials in the past year. Furthermore, 51% of those surveyed rely on their memory to manage passwords rather than using strong combinations or password vaults.

****71%**

CYREBRO's research showed 71% of fraud incidents could have been prevented if the business enforced a routine password change policy.

As data leaks and brute-force attacks are commonplace, businesses must force employees to change their credentials through frequent rotations.

We recommend enforced password changes to happen at least every three months. While this is enough time for a breach to occur, we acknowledge that a balance needs to be maintained between security and user experience – and so this, at least, will mitigate the risk of a leaked password becoming an attacker's key to performing successful BEC fraud.

4. INITIATE CYBERSECURITY AWARENESS PROGRAMS

Through our own research, CYREBRO identified that in 92% of cases a security awareness education program could have prevented a fraud incident from occurring.

Maintaining a solid security posture means investing in suitable monitoring solutions for network visibility, threat response, patching, and endpoint protection. However, as the popularity of phishing as an initial attack vector shows, humans are often the weakest link in a corporate chain.

Cyber-attackers know this. Compromising an employee account via phishing or brute-force attacks can be far easier than finding a zero-day vulnerability in software. So, organizations must train their staff to recognize security threats.

92%

CYREBRO identified that in 92% of cases a security awareness education program could have prevented a fraud incident.

A past IBM study suggested that human error was a "major contributing cause" in 95% of all breaches.

When it comes to email-related breaches, users are always the weakest link. They often sign up to services – including corporate systems – using the same mail addresses and passwords, and all it takes is one breach, even if it occurred elsewhere, for attackers to access their accounts.

Furthermore, non-technical users may not even notice they are being targeted. They may fall for phishing attempts and end up entering their credentials into shady websites, which can have severe consequences for their employers. Users need to be aware of all the risks and specific guidelines and procedures to avoid potential mailbox breaches.

The global cyber security market size was estimated to be worth $167 billion in 2020 and a CAGR growth rate of 10.9% from 2021 to 2028 is expected.

The Initial Steps of a Fraud Attack

A successful phishing attack was the starting point in 92% of the cases CYREBRO analyzed in which an account was compromised and used for fraudulent purposes. It should come as no surprise that most business-related fraud today begins through a form of phishing attack. Phishing is generally split into two categories: the first being generic "spray and pray" mass emails or social media links sent en masse to snare a victim.

Phishing messages are sent to encourage individuals to click on malicious attachments that will execute malware or lead victims to phishing websites that mimic legitimate services and request account credentials.

Phishing websites may impersonate payment providers, email services, retailers, and more.

At least 1% of global internet traffic is malicious, with upward of three billion phishing emails sent daily. While the Domain-based Message Authentication, Reporting & Conformance (DMARC) protocol can help prevent domain spoofing, it is still a global problem.

The second form is known as "spear phishing." Spear phishing requires reconnaissance and an understanding of a target organization. For example, phishing emails may impersonate business leaders or employees and use social engineering to make communication appear legitimate and trustworthy.

Emails may also be spoofed with forged email addresses that appear to be from a trustworthy source. Another way to achieve this goal is the use of typo-squatting.

92%

A successful phishing attack was the starting point in 92% of the cases CYREBRO analyzed where a compromised account was used for fraud.

TYPO-SQUATTING: A POPULAR ATTACK METHOD FOR FRAUD TODAY

In 76% of fraud cases CYREBRO investigated, the attacker created one or more “typo-squatting” domain names during a fraud attack chain. Typo-squatted domains take advantage of our habit of skimming over recognizable words and brands. For example, a typo-squatting attacker could register a domain such as “wellsfarrgo.com” to impersonate “wellsfargo.com,” or “payypal.com” to mimic the legitimate “paypal.com” website.

These domains can also be used to register email addresses, such as “payroll@wellsfarrgo.com” as a means of impersonation.

76%

In 76% of fraud cases CYREBRO investigated, the attacker created one or more “typo-squatting” domain names during a fraud attack chain.

www.paypal.com	✓
Paypalprozess.com	☒
paypalinspection.com	☒
check-paypal com.	☒
paypal-support.website	☒

Phishing, spoofing, and typo-squatting are all threats that must be protected against. However, sometimes fraud also occurs indirectly through the supply chain.

We traced 41% of fraud-related incidents back to the compromise of a third-party service provider or application during our investigations.

The FBI IC3 has also observed an uptick in BEC scams involving virtual meeting platforms to instruct victims to send unauthorized transfers of funds to fraudulent accounts.

WHO IS MOST AT RISK?

From the fraud investigations CYREBRO conducted, we saw that no specific individual in an organization was targeted most of the time.

It is a numbers game during “spray and pray” attack chains. Thanks to automated tools, it takes little to no effort for attackers to send thousands of phishing emails to different users randomly, hoping that at least one person will fall for it.

Individuals at risk are usually non-technical employees who have difficulty determining phishing from genuine emails. They may also lack general cybersecurity training and awareness, so they are easy prey to modern fraudsters.

TARGETING THE GATEKEEPER

Our research also found, however, that breached accounts used in fraudulent activities belonged to employees in finance departments.

The most common business-related fraud emails contain the subject headers: "Urgent," "Request," "Important," "Payment," and "Attention," with an estimated 96% of all phishing attempts arriving over email.

As these staff members hold the financial keys to the kingdom, attackers will often try to compromise them rather than jump through hoops during BEC scams to reach them – if they can.

It is still possible to reel in someone involved in a target transaction by compromising an internal company mail account in another department, such as someone in HR. A phishing email could then be sent to a finance employee asking for their credentials.

Doing this is risky, though, because if the employee who owns the compromised account and the target communicate in any way, the attack could be discovered and stopped early.

Top 5 most common email-fraud subject line words:

- Urgent
- Request
- Important
- Payment
- Attention

MAILBOX RULES AND SUBTLE ATTACKS

The question remains: how can a fraudster manipulate communication between two organizations without being caught? The answer is mailbox rules.

Users set mailbox rules to perform particular actions automatically. In most business fraud cases CYREBRO observed, the attackers create mailbox rules for several reasons.

Among these reasons are disguising or deleting fraud-related emails sent to or from the compromised account so the victim account holder will not spot or query any messages they did not send. By removing the original phishing message, too, it can be harder to find the source of fraudulent or suspicious activity.

Relevant transaction emails from all parties can also be moved to specific mailbox folders. Keywords can be the trigger point to shift messages to folders such as an archive or RSS feed collections, and in addition, the scam artist can forward any emails they like to typo-squatted email accounts.

If rules like this are created, even if the attacker is locked out of an account due to a password change, they can still spy on business-to-business communication.

The Right Moment to Strike: a BEC Fraud Case, Explained

In an example BEC fraud incident, we can look at how invoice processing and formats can be abused.

When an individual or organization requests payment, they normally send an invoice in a PDF format for signing off. However, if an attacker has compromised an email chain coming up to the point of payment, they can copy the .PDF and edit its content with banking details for an account under their control.

CYREBRO found that the primary indicator for these frauds is that the cybercriminal will always send the hijacked PDF with an accompanying message, such as:

"Sorry for the inconvenience, but the previous bank account is under inspection, so please transfer the funds to our backup account."

Once the vendor due to make a payment agrees, the attacker will ask for proof of payment. The attacker will abandon the email chain when a receipt has been sent.

Research indicates that there was a huge leap in malicious documents sent via PDF and in Microsoft Office format during 2018 - 2020. This is likely to have continued as workers were forced to stay home during the pandemic.

We always recommend that clients who suspect a fraudulent transaction should immediately reset the passwords of all parties involved, enforce multi-factor authentication (MFA), and bind the mailboxes, legally if necessary, to stop any emails from being deleted. By doing so, forensics can ascertain what has taken place.

THROUGH CYREBRO'S ANALYSIS: AN ATTACKER'S TIMELINE IN BEC SCAMS, WIRE FRAUD

Cybercriminals are notorious for planning their attacks and sticking to successful fraudster Tactics, Techniques, and Procedures (TTP). CYREBRO has mapped out the patterns recognized by fraudsters and can be seen below as clear steps in a timeline of a fraud attack:

1

SPRAY AND PREY

Attackers send thousands of phishing emails to random users across the internet. These phishing emails usually encourage the user to click a link and enter their email credentials.

2

VICTIM GETS HOOKED

An employee who is part of a wire transfer chain, in which funds are sent or received, gets a phishing email. If they fall for the scam, their mailbox credentials are compromised.

3

KNOWING THE AUDIENCE

Once an employee from an organization has taken the bait, the attacker will get acquainted with all the personalities involved.

4

LOGIN TIMING (NOW OR LATER)

Attackers may save the credentials for later use or log in immediately to the compromised account. We've seen attackers logging in as short as a few hours after their phishing success.

5

SEARCHING FOR GOLD

The attackers sift through the user's emails, hunting for any outstanding invoices or pending wire transfers. If none are found, they will wait for an opportunity.

6

REROUTING YOUR MONEY

Once they find the right time, the attackers will use the compromised account to shift the wire transfer to another bank account tailored for this fraud. The details will imitate the authentic bank account details and at the very least use the same name as the victim organization.

A

PAYING SIDE

If the attacker compromised the paying side, they will create a "typo-squatted" domain and impersonate users from the receiving side to send the new bank account details and use the compromised account on the paying side to approve them.

B

CHARGING SIDE

If the attacker had compromised the charging side, they would simply take the original invoice, edit the details, and resend it, claiming the old invoice is invalid due to bank issues of some sort.

Simplifying the Fight Against BEC and Fraud

Fraud is an age-old concept, but your defenses don't have to be. At CYREBRO, we understand that the cybersecurity industry can be a daunting place, and it can be challenging to choose the right areas to invest in for your organization.

However, it is often the case that getting the basics right and protecting against the most common threats against businesses today – BEC scams, account compromise, and fraud – can do far more than throwing money at unproven or untested but exciting technologies.

Fraudsters have evolved from low-effort mass spam tactics to social engineering, spear phishing, and sophisticated, time-consuming scams that can result in fraudulent transactions right under your nose.

A balance has to be maintained between investment, user experience, and security. Just as cyber attackers are using new TTPs that move on with the times, we, too, need to up our game.

CYREBRO is dedicated to ensuring our existing and future clients are aware of how fraud can impact their business. Using the first interactive SOC Platform, organizations can maintain business continuity and receive alerts about suspicious and irregular emails or fraudulent activity within their network's infrastructure.

Want to learn more about how a SOC Platform can benefit your business?

Learn more about CYREBRO