A Closer Look at Cyberattacks and Payment Fraud

COMMON CYBERTHEFT SCAMS TARGETING BUSINESS TODAY

Fall 2020

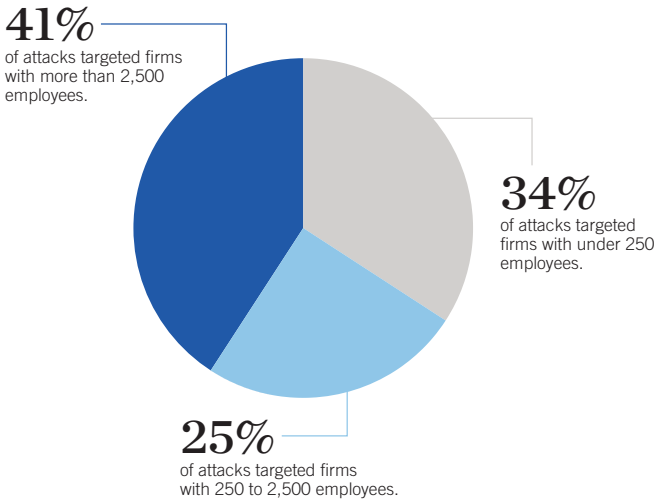
B2B Payment Fraud Is Increasing—Are You Ready?

Unfortunately, cybercrime is a reality for businesses today. Payment fraud activity is unlikely to abate any time soon. Scammers are becoming increasingly innovative with their repeated success in circumventing controls and their ability to infiltrate organizations' payments systems. Unfortunately, payments fraud attacks are the "new normal," and advancements in technology have opened the doors for fraudsters.[1]

Small and Midsized Businesses Are Targets

Over 80% of organizations were targets of actual or attempted payments fraud last year.[1] Unfortunately, small and midsized businesses remain attractive targets for cybercriminals.

Myth: Only Large Firms Area at Risk



Source:
Symantec: Internet Security Threat Report[2]

Many businesses have a lack of awareness about what cyberthreats actually are. In one study, researchers asked business owners if they'd experienced any form of cybercrime. Only 13% said they had. Yet when those same business owners were shown a list of different types of cyberattacks, the percentage who reported being victimized rose to 58%.[3]

It's not the well-publicized data breaches that are the biggest risks. Business are attacked with ordinary scams like spear phishing and account takeover fraud.

Phishing Attacks Expedite Cybercrime Risk

The Phishing Scam: All phishing is based on deception

92%	of malware comes through email, and it's the largest hole for organizational data loss
68%	of malware originates from Microsoft Office
30%	of all phishing emails are opened by users
12%	click on the infected attachment or link

Two Methods:

1: **Spear Phishing –** Targets a specific person to take action

2: **Social Engineering –** A wayward click triggers malware

Source:
2019 Report – Strategies for Minimizing Phishing Attack Risks, Sponsored by Reversinglabs

Increase Awareness of Cyberfraud Risk

Email fraud or spear phishing attacks are already one of today's biggest cyberthreats and show no signs of letting up. Fraud risk is growing—attackers are sending more fraudulent emails, they're impersonating more people and they're targeting more recipients. Some schemes directly steal money, while others go after employee credentials (usernames, passwords, etc.) and sensitive company data.[4]

However, a cyberthief's tools can only work when someone on your staff takes the bait and clicks on the wrong email, the wrong link or the wrong attachment. Today's cybercrime is designed to take advantage of the elements of human nature—trust, the desire to please superiors and the pressure to complete tasks quickly.

Key takeaway:
A cyberthief only succeeds if you click.

A Cyberthief's Toolbox

A cyberthief's treacherous toolbox exploits email to facilitate fraud. The three most popular attack tools are:[5]

- **Spear Phishing –** Email designed to trick you into performing a task for the thief (like sending a wire or ACH payment).
- **Social Engineering –** Features online schemes that lull victims into divulging sensitive information, login credentials or data.
- **Malware Software –** Malicious software like ransomware is used to deny victims access to their computers or networks until they pay the cyberthief.

Today, cybersecurity isn't just the IT or operations department's issue; it's every employee's issue.

Key takeaway: All people-focused attacks have one thing in common—they rely on identity deception.

"All it takes is one spoofed, socially engineered email that plays on human nature to respond quickly and act. It's far easier to manipulate one person to click on an email, provide their login credentials, download a PDF from a cloud application or wire funds to a fraudulent bank account. Email is a lucrative and effective approach."[6]

– Sherrod DeGrippo
Senior Director of Threat Research and Detection
at security firm, Proofpoint

Spear Phishing Attacks

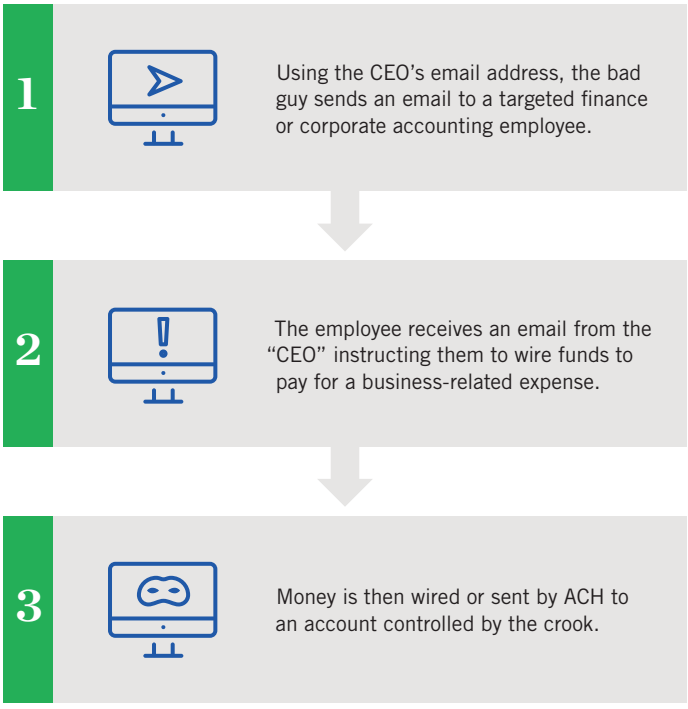
The complex nature of these threats makes it imperative to have a good basic understanding of what they look like and how they work.

BUSINESS EMAIL COMPROMISE (BEC)

In BEC or CEO/CFO email fraud schemes, a key employee (often in the accounting department) is targeted for an email that attempts to trick them into sending money to the crook.

Spear Phishing—The #1 Attack Method Targeting Businesses

HOW BUSINESS EMAIL COMPROMISE WORKS:



These emails are often scheduled to coincide with an executive's travel plans, making it more difficult to quickly confirm the veracity of the request with the exec in question. Cleverly, they're often crafted to look like previous requests, statements or invoices so as not to arouse suspicion.

Watch out for variations on BEC scams:

- **Bogus Invoice Scheme:** Attackers call or email a business that has a longstanding relationship with a supplier, pretending to be the supplier. They try to trick you into wiring funds for invoices to the crook's account, or they request invoice payments be sent to them at a new address. Unless you verify all changes, you won't see the fraud until your real vendor contacts you to request payment.
- **Payroll Diversion:** The bad actors snare login credentials from executives or employees and request an update to the direct deposit information. The crook's goal is to divert payroll into their account.
- **Data Theft:** Attackers use personally identifiable information—including Social Security numbers—or employees' tax statements in what's known as W-2 attacks. The data is used for filing fake tax returns and identity theft.

Phishing & Malware

Certain phishing emails are used in conjunction with other techniques to fulfill a cybercriminal's scheme. Malware is designed to exploit vulnerabilities in software, operating systems, web browsers, etc. The attacker sends malicious email to an unsuspecting person. The email looks legitimate but contains malware hidden in an attachment or link. When the user clicks on it, it takes them to a malicious site.

WHAT HAPPENS WHEN YOU CLICK?

Danger #1:
Email attachment with embedded malware

- User downloads attachment
- File executes, malware checks machine for vulnerabilities

Danger #2:
Malicious link to spoofed login

- User clicks link in email
- Link opens spoofed web login page
- User enters their credentials and hits submit

Danger #3:
Malicious link launches an exploit kit

- User clicks link in email
- Link opens malicious site
- Site launches an exploit kit and checks machine for vulnerabilities

Now the cybercrook is in your system—what happens next? For Dangers #1 and #2, the attacker gains unauthorized access to all assets that the user/victim has rights to until the malware is detected. For Danger #3, the credentials are sent to the attacker, who can now access personal or work data as if they were the actual authorized user.[7]

Some of the ways cybercrooks use malware to steal from you are shown below:

CORPORATE ACCOUNT TAKEOVER

Using malware that is installed on your computer, the cybercrook takes control of the target's bank account. To accomplish this form of identity theft, the cyberthief uses malware called spyware, which allows them to monitor and record your online activity, log your keystrokes and more. Then thieves log into your bank account and initiate fraudulent ACH or wire transfers to their own accounts.

MAN IN THE MIDDLE

Cybercriminals may install malware that hijacks the victim's web browser during online banking sessions in what's known as man-in-the-middle (or man-in-the-browser) attacks. After disconnecting the legitimate user, cybercriminals take control of the online banking session and begin initiating fraudulent payments. This form of cybertheft is now being used in conjunction with smartphones too.

RANSOMWARE

One of the most frightening types of malware is ransomware, which you have seen lock down computer systems in cities, hospitals and businesses. In the simplest terms, it's an online extortion scheme. Ransomware encrypts all the data on your computer or systems, rendering it useless until the victim has paid the cybercriminal.

Your risk of payment fraud, data breach or ransomware is very real. Typically, it takes IT to find and neutralize the malware.

Key takeaway: Links, email attachments and fraudulent software downloads are all ways cybercriminals spread malware.

WHY DO SPEAR PHISHING ATTACKS SUCCEED?

- **Simplicity –** The request seems normal. The crook asks victims to perform tasks that fall under their normal duties. The request looks authentic; it contains wire details and amount.
- **Leverages Today's Corporate Culture –** Employees are available 24/7; they respond quickly to solve a problem.
- **Lack of Awareness –** Employees don't recognize the threat. Your employee unsuspectingly accommodates the request because it looks like it came from an executive or trusted source.

Companies that have trained on the BEC threat, urged employees to be cautious and established payment processing procedures tend to catch schemes before they succeed.

Fraudsters Have Adapted to Changing Landscapes

THE CORONAVIRUS PANDEMIC[8]

COVID-19 brings new cyberthreats that are targeting organizations that have remote workers and fewer IT and security staff ready to mitigate attacks. Cybercrooks took the opportunity both to weaponize the desire for information and target a new set of prospective victims. The FBI reports that fraudsters are using the coronavirus as an excuse to request fraudulent payments.

BEC scammers have adjusted their messages to incorporate more concerns over COVID-19 into their social engineering techniques. New topics have included:

- Fake COVID-19 tests or warnings
- Federal PPP or SBA loans
- Federal government stimulus checks
- Requests for donations to the WHO
- Fake warnings or stats from the CDC

NEW TARGET – TEXT/SMS MASSAGES

Cybercriminals send malicious text/SMS messages to your smartphone. They want to download malware or gain access to your banking credentials, like payment cards, usernames and passwords. These text/SMS messages lure you into clicking on links that open fake mobile banking login pages. Once there, the cybercrook sees everything you enter. Then they go to the legit banking site and log in as you.

Smartphone users are more susceptible to phishing attacks because the features, functionality and screen size of these devices make it difficult to discern if the message is fraudulent or a website link is fake.

CYBERCRIME CAN CATCH ANYONE— EVEN A SHARK!

"Shark Tank" star Barbara Corcoran was a victim of a work email phishing scam. According to public reports, she revealed that she had nearly $400,000 stolen after scammers tricked her bookkeeper by sending a bill that appeared to come from her assistant.[9] Fortunately, her bank acted in time to halt the transfer and returned the money.[10] Not everyone who is scammed is so lucky.

"Lesson learned: Be careful when you wire money!" Corcoran tweeted. She also confirmed that, "This morning I wired $388,000 into a false bank account in Asia."

So how did such a savvy businesswoman and entrepreneur get duped? Corcoran's bookkeeper received what appeared to be a routine invoice from Corcoran's assistant to approve a payment to a known project, but it was fake.

> "Be careful when you wire money!"
>
> **– Barbara Corcoran**

Corcoran does not blame her bookkeeper for getting conned by the sophisticated scam. "When she showed me the emails, I realized immediately it's something I would have fallen for if I had seen the emails," Corcoran said.

Cybersecurity Essentials: Take Steps to Prevent Cybercrime

You can protect your organization by establishing sound internal controls and procedures for payment processing. Consider these five steps to minimize cybercrime risk:

Guard your computers

- Use firewalls and anti-virus software
- Add protection with Trusteer Rapport (It's free for Treasury Services clients)

Use layered security controls

- Segregate duties
- Protect/encrypt sensitive data
- Use multifactor authentication

Reconcile bank accounts daily

Make training a priority

Add proactive fraud prevention to commercial checking accounts

Sources:

[1] AFP: 2020 Payments Fraud and Control Survey Report

[2] Symantec: Internet Security Threat Report

[3] PYMNTS website, October 12, 2017, "When Small Businesses Don't Realize They're Cyber-Attack Victims"

[4] 2019 Threat Report: "Email Fraud in Financial Services", ProofPoint, Inc.

[5] Perimeter 81: The 7 Top Security Tips While Working Remote, Blog, Perimeter 81.com

[6] FBI: BEC Losses Totaled $1.7 Billion in 2019, Apurva Venkat, February 13, 2020

[7] 2019 Report – Strategies for Minimizing Phishing Attack Risks, Sponsored by Reversinglabs

[8] "UK and US Security Agencies Sound COVID-19 Threat Alert," Bank Info Security, April 9, 2020

[9] Shark Tank's Barbara Corcoran fell for this very common phishing scam, Nicole Lyn Pesce, CNN Business, February 27, 2020

[10] Scammers return money after 'Shark Tank' star Barbara Corcoran lost almost $400,000 in phishing, USA Today, Feb. 28, 2020

10/20