proofpoint.

EBOOK

# 5 Real-World Cyberattacks and How to Stop Them

## Vol. 1: Social engineering attacks

# Introduction

Cybercriminals are crafty and highly motivated. And why wouldn't they be? They're in a growth industry where the risks are low and the returns are so high that by 2027 cybercrime is expected to cost the world a staggering $23.8 trillion per year.[1]

With so much money to be made, the creativity behind today's cyberattacks is seemingly endless. New and ingenious malware, phishing, and social engineering schemes pop up daily as defenders play a whack-a-mole game to stop them. Yet although these new threats may seem infinitely varied, they all have a few basic things in common, namely: they use email, and they target people.

In this e-book series, we've collected some of the most insidious email attacks out there right now. What's notable is that many of them have got past multiple security tools before we've caught them. To help you understand why, we take you through each attack step by step to show you how each one worked and how cybercriminals tried to take advantage of human vulnerabilities. Then we tell you how they were stopped.

This volume covers attacks that rely on social engineering. In volume 2, we'll cover more technical attacks.

1 World Economic Forum. "2023 Was a Big Year for Cybercrime—Here's How We Can Make Our Systems Safer." January 2024.

# Table of Contents

1 BEC and Supply Chain Attacks ..... 4

2 E-Signature Phishing ..... 7

3 Toad Threats ..... 11

4 Payroll Diversion ..... 15

5 Supply Chain Compromise ..... 19

6 Conclusion ..... 24

SECTION 1

# BEC and Supply Chain Attacks

In business email compromise (BEC) attacks, a threat actor pretends to be a person or entity that a recipient trusts, like a colleague, vendor, or partner. Many of today's BEC schemes are highly sophisticated, well-funded, and backed by careful planning and research.

In the past few years, these attacks have been a cash cow for cybercriminals. The *2023 FBI Internet Crime Report* notes that they cost U.S. businesses $17 billion. Globally, businesses lost an eye-watering $50 billion.[2] In contrast, ransomware victims lost $1.1 billion.[3]

2 FBI. "Business Email Compromise: The $50 Billion Scam." June 2023.

3 Wired. "Ransomware Payments Hit a Record $1.1 Billion in 2023." February 2024.

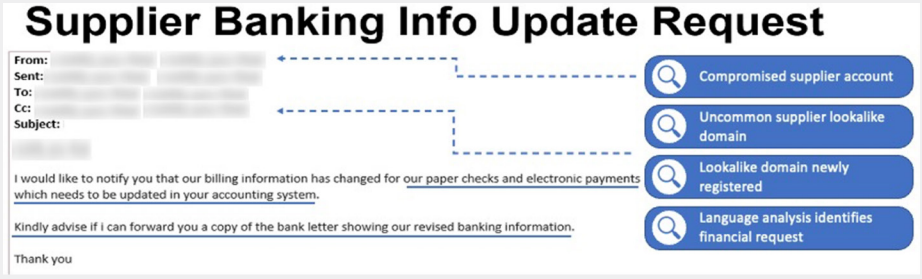
# The scenario

Proofpoint detected this BEC incident at a global retailer that has more than 40,000 users. The threat came from the retailer's supply chain, and its existing security tool failed to detect it. This example is helpful because it highlights how quickly the cybersecurity landscape evolves.

# How the attack played out

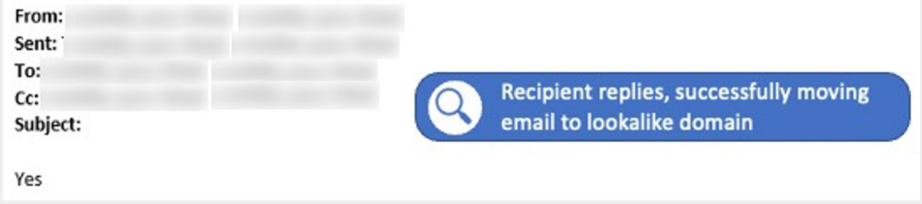
Here's a closer look at how the attack unfolded.

1. **The deceptive message.** The global retailer received an email from a sender within its supply chain who wanted their payment information updated. But what seemed like a routine request was malicious, as the sender's account had been compromised.




*An attacker's initial email, shown with forensic observations by Proofpoint.*

2. **The malicious lookalike domain.** The attacker wanted to redirect response emails to a newly registered lookalike domain. Their goal was to intercept sensitive data and divert funds.




*The customer's response, which was sent to a lookalike domain.*

## Why these threats are hard to catch

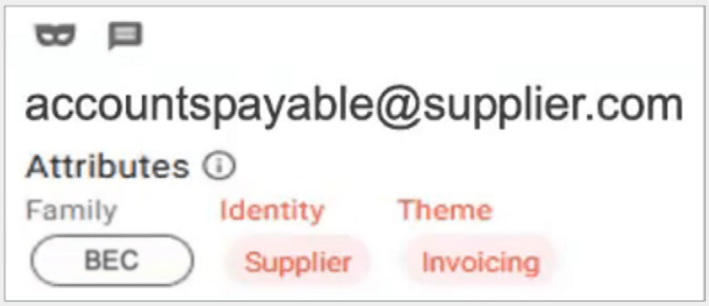
BEC attacks are very difficult to detect because they don't include the usual payloads like malicious URLs or file attachments. Instead, threat actors rely on impersonation and other social engineering techniques to trick people.

This retailer's existing security tool missed this threat for a variety of reasons. For starters, it relied too heavily on domain age as a detection factor. It also wasn't able to identify lookalike domains. And it didn't analyse the "reply-to" address in order to detect the pivot to a new domain.

## How Proofpoint detected it

The trick to identifying many types of threats – from BEC to credential phishing – is combining domain age with other identifiers of malicious intent. That's why Proofpoint uses a multilayered approach. Our detection engine uses artificial intelligence (AI), machine learning (ML) and behavioural analysis to identify key indicators of compromise. It identifies email patterns that fall outside of "normal" behaviour.

In this example, Proofpoint analysed the email's language and saw that there was a financial request. On its own, the request did not seem unusual. However, when it was combined with the change in the reply-to address, it was suspicious. Also, the domain was registered on the same day that the email was sent.




*The Proofpoint Targeted Attack Protection (TAP) dashboard categorises every threat. For this example, it shows that we identified the threat as BEC, that the threat came from a supplier and that invoicing was involved.*

SECTION 2

# E-Signature Phishing

Email signature (e-signature) phishing is a threat where a recipient is tricked into handing over their credentials or other personal information by a message that requests their signature. The message may include an attachment to a contract or an invoice that needs to be signed.

In one single month in 2023, Proofpoint detected more than 75,000 different threats just like the one below.

# The scenario

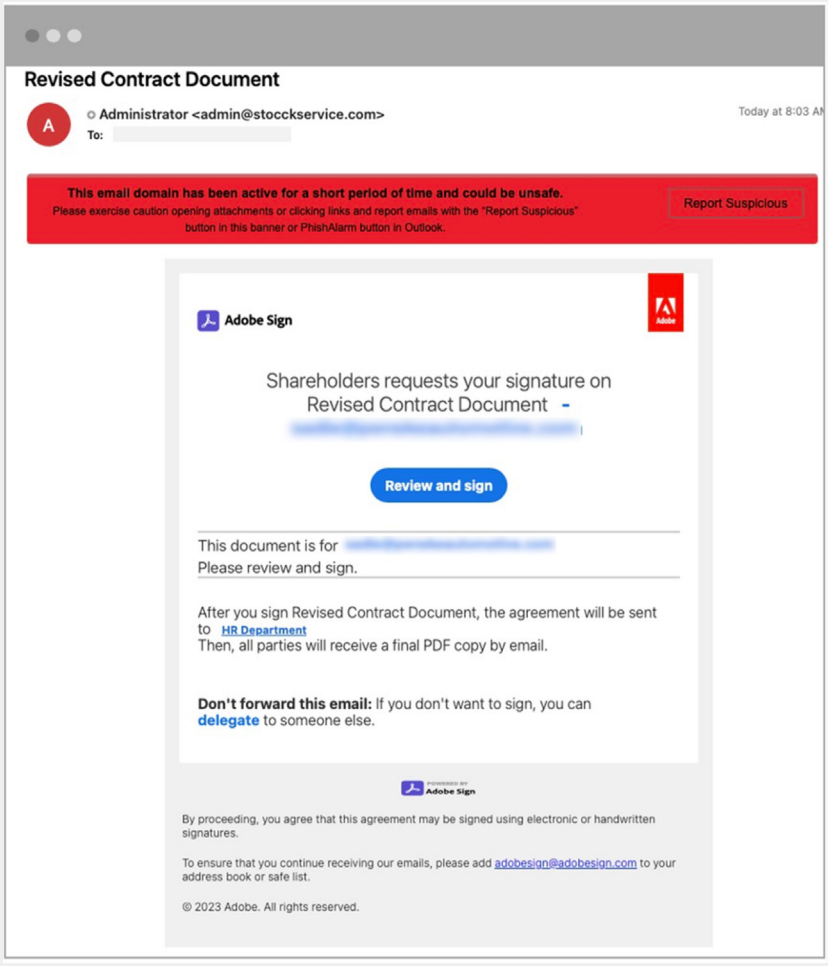
Proofpoint detected a credential harvesting threat that was hosted on the Amazon Web Services (AWS) Amplify SaaS application. The application was being used by our customer, an automotive company with 2,000 employees.

A bad actor had crafted a phishing lure that looked like a link to a sensitive document – an updated contract that needed to be reviewed and countersigned. The target was an employee who works with contracts and has other fiduciary responsibilities. They often communicate with board members, customers and suppliers in the course of their work. So they would expect to receive this type of request.

# How the attack played out

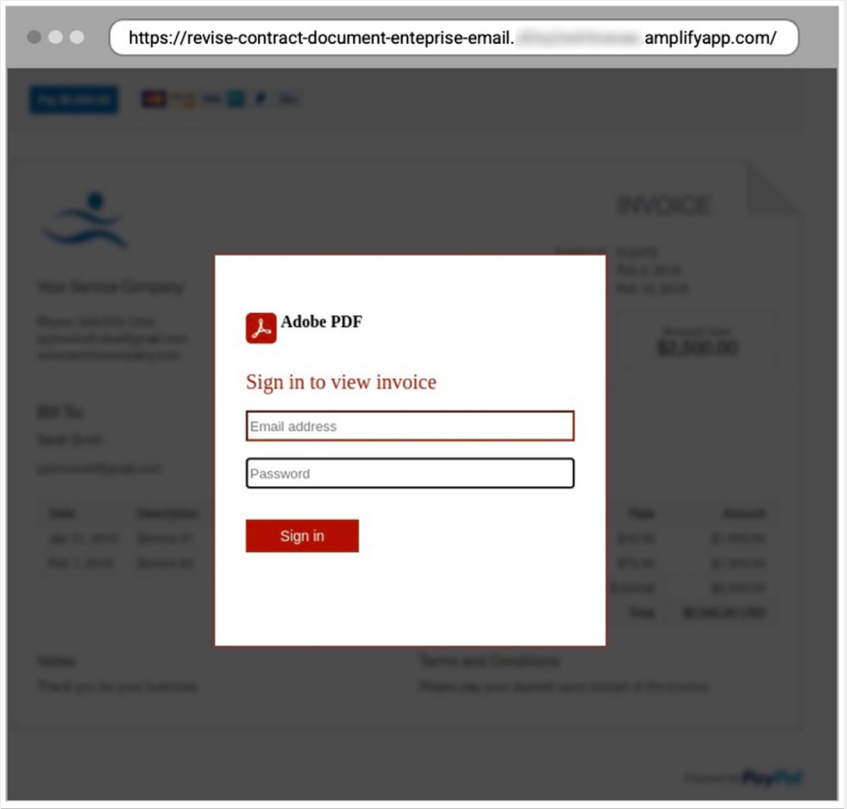
Here's a closer look at how the attack unfolded.

1. **The deceptive message.** Our customer received an email inviting the employee to view and sign an updated contract.




*The malicious email.*

2. **The malicious URL.** If the employee clicked the malicious URL, they would then see a login screen that was designed to look like other legitimate login screens. The attacker's goal was to trick the employee into handing over their credentials.




*The fake login page hosted on amplifyapp.com.*

## Why these threats are hard to catch

Applications like AWS Amplify and other SaaS services such as DocuSign, Adobe Sign and OneSpan Sign are often used in these attacks. They provide bad actors with an easy way to distribute malicious content while appearing legitimate.

In this scenario, the URL domain was over five years old. And the IP address belonged to Amazon, which would likely result in a clean verdict. Most email security vendors can detect a standard credential phishing attack. However, the SaaS provider's trusted domain adds a layer of complexity to most detection engines. Notably, 19 other email security vendors – many of which claim to use advanced AI and ML to stop these attacks – did not catch this threat.

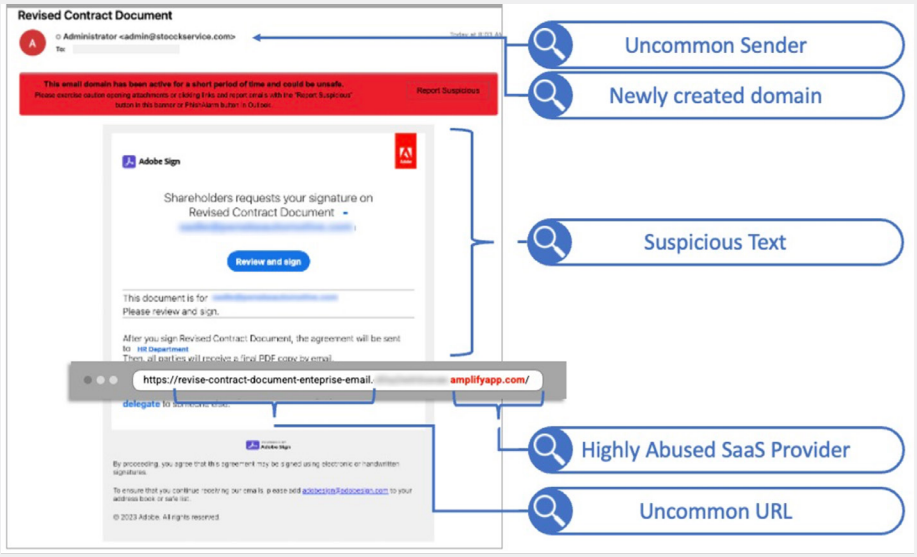
# How Proofpoint detected it

Proofpoint's behavioural AI engine uses multiple message-level signals to detect and block a range of threats. This means we can detect phishing threats that haven't been seen before and do it earlier in the attack chain so that threats can be blocked before they're delivered.

Proofpoint conducted a multilayered, deep analysis of the user's profile and found an uncommon sender/recipient based on historical communication patterns. We found that the sender rarely communicated with the recipient or anyone else at the automotive company.

Using behavioural AI and ML, Proofpoint conducted an in-depth analysis of the URL. That analysis included the URL's relevance based on previous historical data points and other anomalous activity. Across the entire company's sending patterns, the URL had never been used by the recipient or anyone else within the company.

Proofpoint also detected the use of a legitimate and well-known SaaS provider's domain. At other companies we help to protect, we have detected attackers abusing this same domain and using it to distribute malicious content.




*A summary of observations by Proofpoint about the e-signature email, which led to condemnation of the email.*

SECTION 3

# Toad Threats

Social engineering tactics continue to evolve as bad actors look for new and creative ways to gain initial access to sensitive systems. Telephone-oriented attack delivery (TOAD) attacks are proof of that. Attackers send emails to recipients and try to trick them into calling an attacker at a bogus “call centre”.

Users aren’t typically protected from malicious phone calls. That’s why blocking these emails is crucial. These attacks are very difficult to detect because they often don’t contain URLs or attachments.

Across all threat assessments in a single month in 2023, Proofpoint detected over 19,000 TOAD threats behind 14 different email security tools.

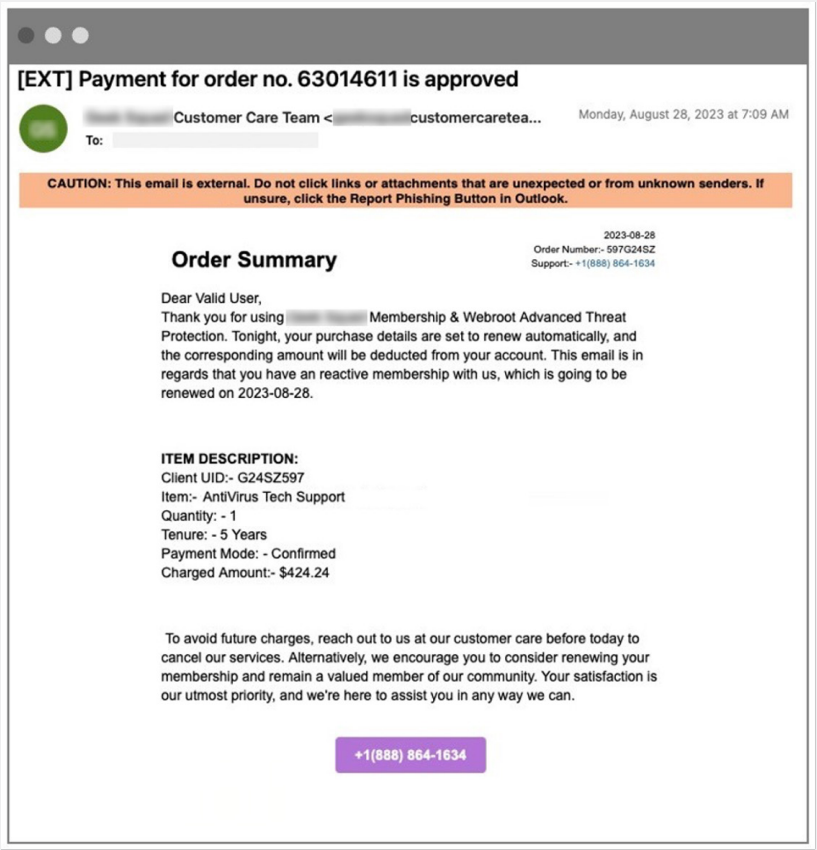
# The scenario

Proofpoint detected a TOAD threat at a manufacturing company with more than 45,000 employees. A bad actor who was pretending to work at a well-known antivirus company sent a fraudulent message to one of its employees. The attacker included a phone number instead of adding URLs or attachments to the message.

# How the attack played out

Here's a closer look at how the attack unfolded.

1. **The deceptive message.** An email claimed to be an alert about an upcoming purchase from a well-known technology company.



[EXT] Payment for order no. 63014611 is approved

[redacted] Customer Care Team <[redacted]customercaretea...  Monday, August 28, 2023 at 7:09 AM

To: [redacted]

CAUTION: This email is external. Do not click links or attachments that are unexpected or from unknown senders. If unsure, click the Report Phishing Button in Outlook.

2023-08-28
Order Number:- 597G24SZ
Support:- +1(888) 864-1634

**Order Summary**

Dear Valid User,
Thank you for using [redacted] Membership & Webroot Advanced Threat Protection. Tonight, your purchase details are set to renew automatically, and the corresponding amount will be deducted from your account. This email is in regards that you have an reactive membership with us, which is going to be renewed on 2023-08-28.

**ITEM DESCRIPTION:**
Client UID:- G24SZ597
Item:- AntiVirus Tech Support
Quantity: - 1
Tenure: - 5 Years
Payment Mode: - Confirmed
Charged Amount:- $424.24

To avoid future charges, reach out to us at our customer care before today to cancel our services. Alternatively, we encourage you to consider renewing your membership and remain a valued member of our community. Your satisfaction is our utmost priority, and we're here to assist you in any way we can.

+1(888) 864-1634

*The original malicious email delivered to the recipient's inbox.*

2. **TOAD attack sequence.** If the employee had called that number, the attacker could have directed them to their computer and guided them to click on a malicious URL. That could, in turn, could have led to various threats, including remote access, theft of sensitive data or a ransomware infection.


*Overview of a typical TOAD attack sequence.*

## Why these threats are hard to catch

TOAD threats can be challenging to detect because they rarely include malicious payloads. Plus, attackers often use well-known domains that belong to Google, Microsoft or other legitimate email services.

Since this particular TOAD threat was sent from a Google-owned domain, the message passed email authentication checks like SPF (Sender Policy Framework) and DMARC. This message also didn't have a malicious payload. This might explain why the manufacturing company's existing security tool delivered the threat.

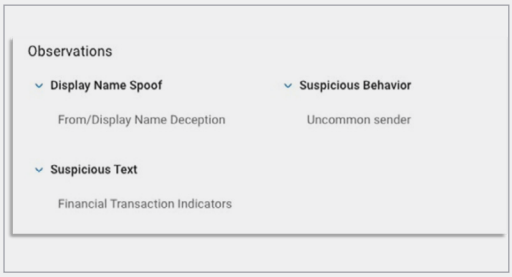
# How Proofpoint detected it

Proofpoint uses advanced AI and ML to analyse and combine various behavioural indicators and detect TOAD threats. This approach is more reliable than just tracking and maintaining a database of previously identified malicious phone numbers associated with TOAD attacks.

When the Proofpoint behavioural AI engine analysed this message, it found language about a financial transaction as well as a need for urgency, indicating a potentially malicious email. An additional tell is that TOAD threats always include a phone number and urge the recipient to call it. That's why Proofpoint scans messages for a phone number.

We conducted a multilayered analysis, which also found that the recipient hadn't received an email from the sender in the past, based on historical communication patterns. In fact, no one in the company had received an email from this sender before.

As is typical with TOAD attacks, bad actors will send messages that look like they are being sent by a legitimate brand to try and build implicit trust. Our analysis also detected this tactic.




*Summary of Proofpoint's observations that lead to condemnation.*

SECTION 4

# Payroll Diversion

Payroll diversion is a form of BEC. The prime targets of these attacks are typically employees who fulfil payroll-related requests. Typically, a bad actor pretends to be an employee who needs to update their direct deposit information. The new information is for an account that the bad actor owns. Once the fraudulent request is complete, the lost funds cannot be retrieved by the business.

Payroll diversion fraud isn't a new form of BEC, but the frequency of this type of attack is on the rise. Proofpoint continues to see this type of threat getting through the defences of other email security tools. Across all of our recent threat assessments, we found that more than 400 got past 12 other email security tools.

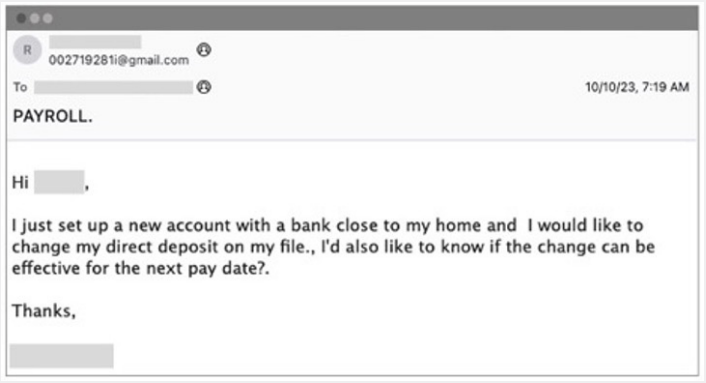
## The scenario

Proofpoint detected one of these threats at an energy and utilities firm with 300 employees. In this case, an attacker pretended to be a non-executive employee and sent an email to the firm's director of human resources (HR). Not only did the firm's existing email security tool deliver the message, but its API-based post-delivery remediation tool also failed to detect and retract it.

## How the attack played out

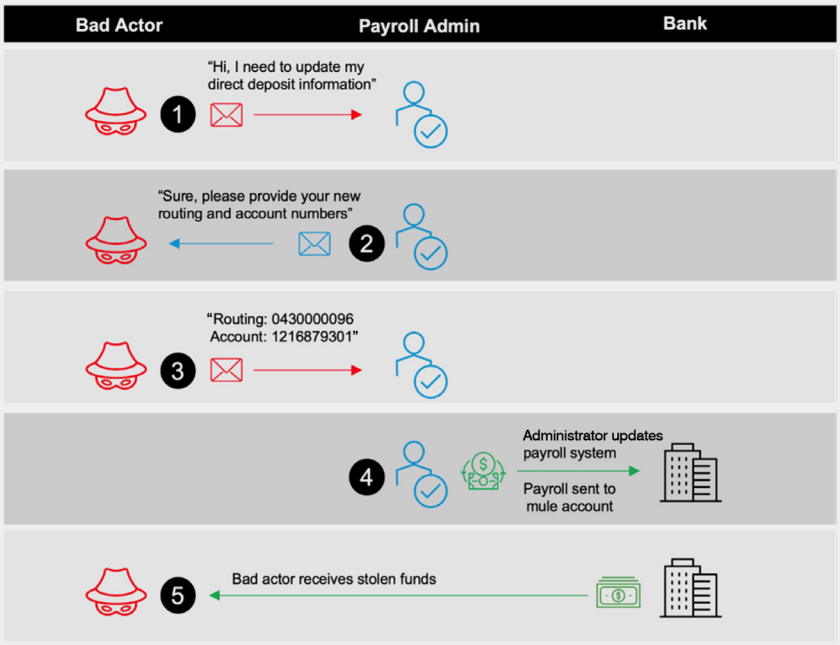
Here's a closer look at how the attack unfolded.

1. **The deceptive message.** The attacker sent a request to HR asking that their direct deposit information be updated. This message was sent from an account that looked like a legitimate employee's personal email account.




*The original malicious message delivered to the recipient's inbox.*

2. **Payroll diversion attack sequence.** If the recipient had engaged, the attacker's goal would have been to convince them to transfer funds into another bank account that was not owned by the impersonated employee.




*The typical attack sequence of a payroll diversion attack.*

## Why these threats are hard to catch

These threats don't often carry malicious payloads like attachments or URLs. They also tend to be sent from personal email services like Google, Yahoo and iCloud. And they target specific users.

Notably, API-based email security tools that scan for threats post-delivery are the most susceptible to missing this type of threat. This partly comes down to how these tools work. For them to be effective, security and IT teams need to manually populate them with a dictionary of possible display names of all employees, which is very time-consuming and hard to scale.

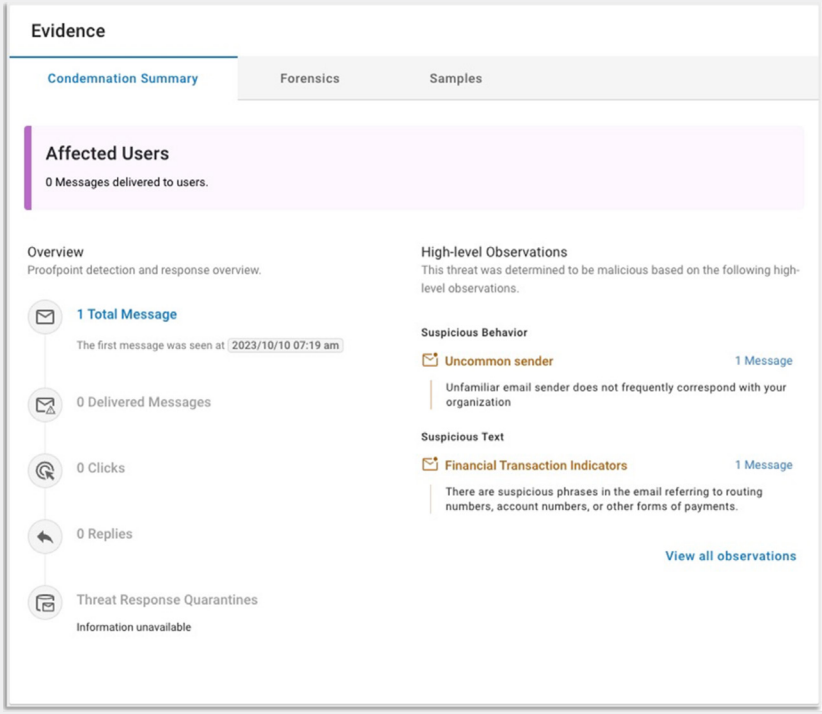
To avoid this, many companies simply choose to enable display name prevention for their senior executives only. But bad actors behind payroll diversion don't just impersonate executives, they target anyone in the company who can access corporate funds. In our example above, an attacker took advantage of this exact weakness.

# How Proofpoint detected it

To understand the true purpose of an email, an email security tool must interpret a message's tone and intent. Proofpoint uses multiple detection signals, analytic engines and behavioural AI to figure this out. Our AI and ML detection engines are continuously trained with millions of daily email messages from our worldwide threat intelligence ecosystem.

One signal we use for detecting malicious emails is by analysing how common it is for a sender to communicate with a recipient and how frequent their messages are. In the example above, it was rare for the director of HR to get emails from that particular employee from their personal email address.

Most email security tools use stand-alone, uncommon or unusual sender signals. That's why they create a high number of false positives. However, Proofpoint is different. We combine many signals to ensure that we don't rely too much on one or two signals. By combining the uncommon sender signal with an analysis of the language in the body of the message, Proofpoint extracts the tone and interprets the intent of an email.




*Proofpoint Condemnation Summary outlines the signals that led us to condemn this threat.*

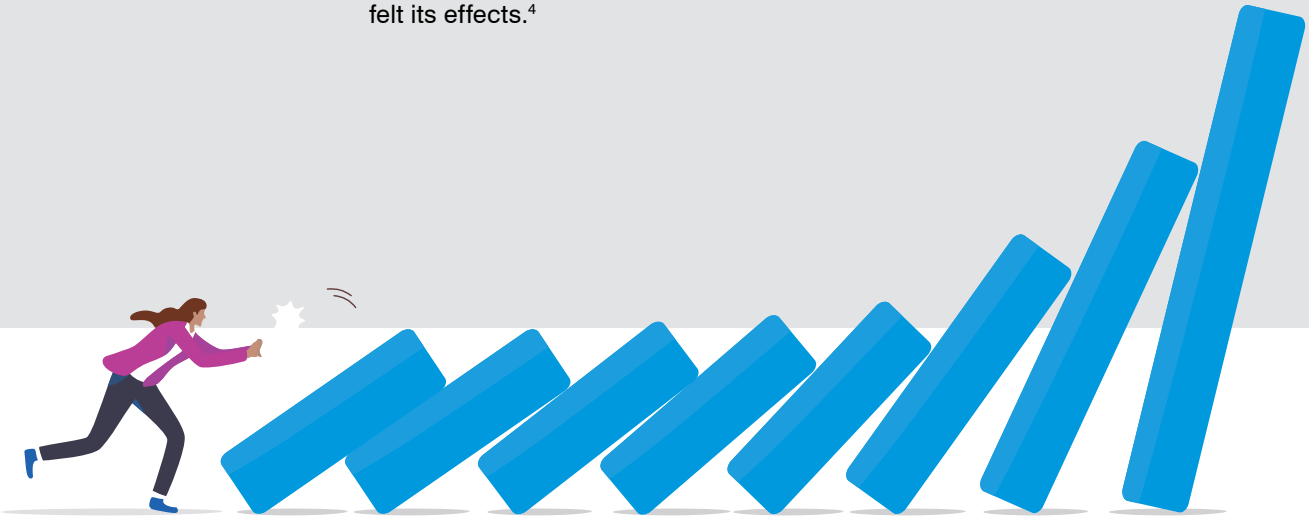
SECTION 5

# Supply Chain Compromise

Supply chain compromise is another form of BEC that's on the rise. In these attacks, a bad actor targets a company by compromising the security of its suppliers, vendors and other third parties in its supply chain. That's because attackers know that enterprises with mature supply chains tend to have stronger cybersecurity defences, which makes them challenging targets.

So rather than launching a direct attack, the bad actor infiltrates one of the company's trusted entities and pretends to be them. Often, they use thread hijacking or conversation hijacking. This is where attackers target specific email accounts and compromise them so that they can spy on conversations. When the time is right, the attacker inserts themselves into the conversation. Sometimes, they're bold enough to start a new conversation.

These attacks are growing more popular and sophisticated by the day. The largest one in 2023 cost the businesses that were impacted more than $9.9 billion. And more than 1,000 businesses and 60 million people felt its effects.[4]



4 TechCrunch. "MOVEit, the Biggest Hack of the Year, by the Numbers." August 2023.

# The scenario

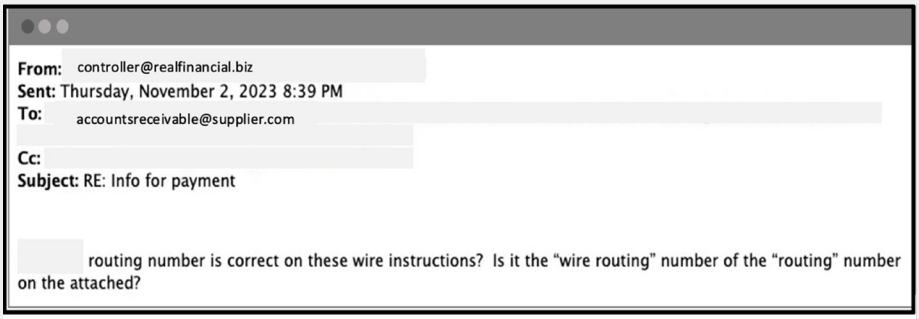
Proofpoint detected a fraudulent message that appeared to be sent from an employee working in the accounts receivable department at a small financial services company in Florida. However, it was actually a bad actor who was impersonating someone. Their goal was to launch a supply chain attack on a large law firm in Boston.

In an email to the law firm's controller, the attacker requested that a payment be stopped and that payment information be changed to another account.

# How the attack played out

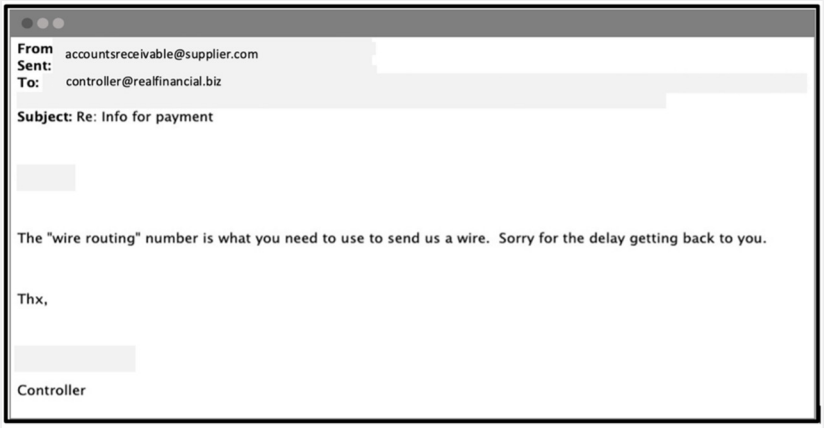
Here's a closer look at how the attack unfolded.

1. **Legitimate customer message.** The customer sent an email to the supplier to confirm the wire payment information was correct.

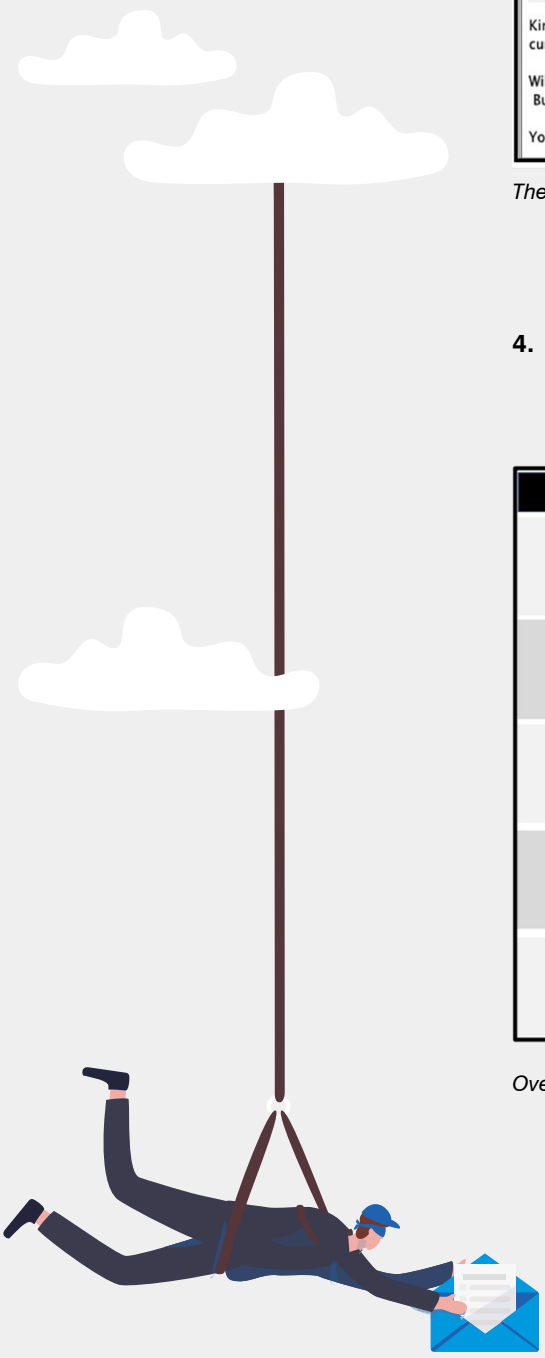



*The legitimate customer message confirming wire payment information.*

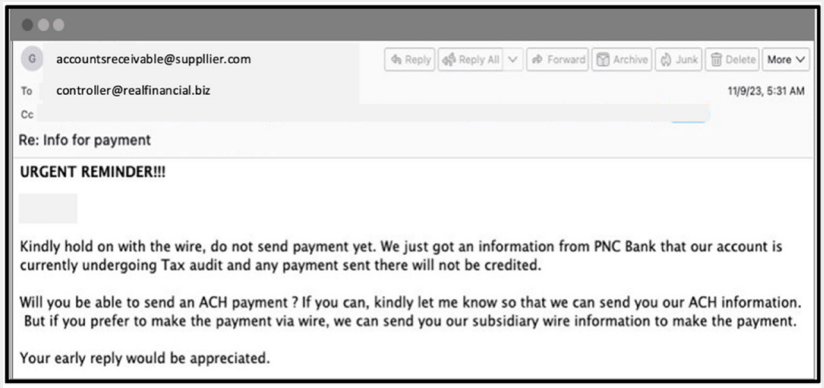
2. **Legitimate supplier email.** The supplier replied to verify the wire payment information.




*The legitimate supplier email verifying wire payment.*

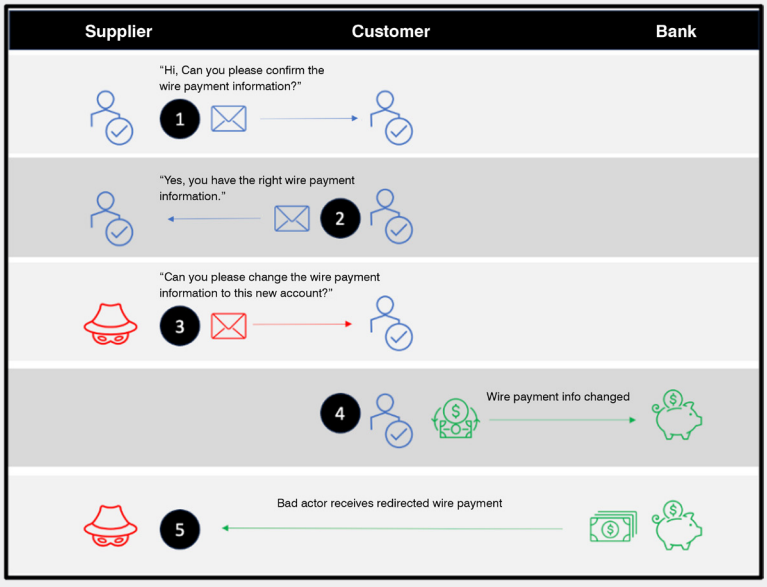


3. **Fraudulent supplier email.** The attacker entered the mix by sending an email to the customer from a different account that appeared very similar to the original one. Instead, it was sent from a lookalike domain, which had an additional letter in the sender's address. To make the email seem legitimate, the attacker copied the entire email conversation below.




*The attacker's fraudulent email.*

4. **Supply chain compromise attack sequence.** The bad actor requested that the wire payment be sent to another account through an automated clearing house (ACH). The attacker was the owner of that new account.




*Overview of the attack sequence.*

## Why these threats are hard to catch

Supply chain compromise attacks rarely have malicious payloads, which is one reason they're difficult to detect and stop. The bad actor uses social engineering to convince the recipient to assist them achieve their goal.

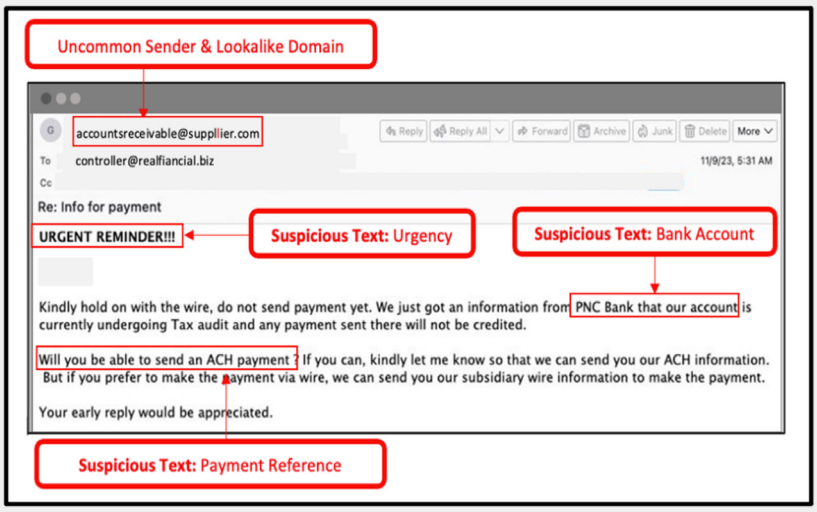
In this scenario, a supplier asked a vendor to change payment account information. Such a request is not uncommon, and that's why API-based email security tools struggle to detect these attacks. API-based tools depend on uncommon sender signals, and so they create a lot of false positives and alerts. This limited behavioural AI approach helps to explain why many businesses complain about the excessive noise that unusual sender patterns create.

To detect these types of malicious messages, an email security tool must interpret the contextual tone as well as the intent of a message. That's how to decipher the true objective of a message before it's delivered to a user's inbox.

## How Proofpoint detected it

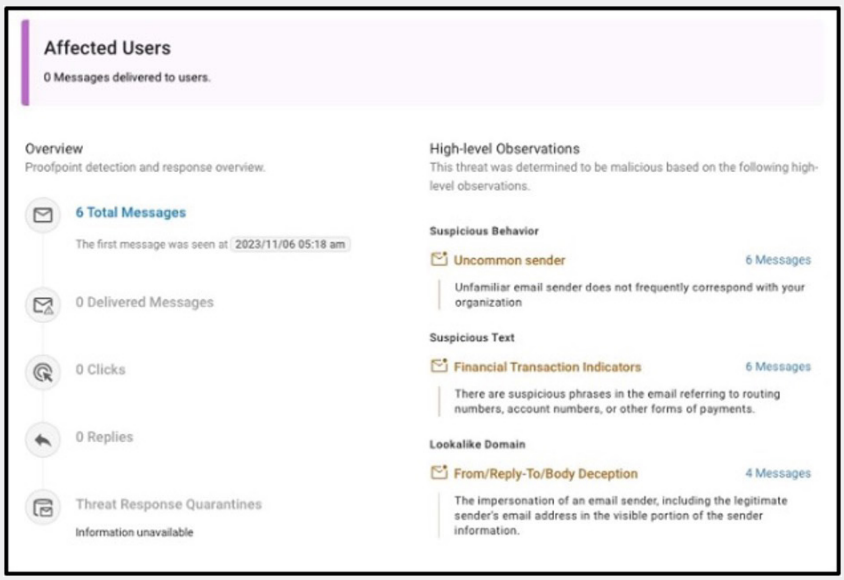
Proofpoint combines threat intelligence with behavioural AI and ML to determine whether business emails are legitimate or malicious. We continuously train our detection engines with millions of daily email messages from our worldwide threat intelligence ecosystem. This allows us to provide a higher level of confidence when we detect and block these types of messages.

To reduce noise, we combine multiple signals instead of relying on one or two signals, which can create a high level of false positives. One signal is how common messages are between senders and how frequent those messages are. We also analyse the language in the body of the message for tone and to interpret its intent. And we look for lookalike domains and payment urgency.




*Multiple detection signals identified in a fraudulent supplier email.*

Based on the email's content, intent and language, Proofpoint deciphered that the message in our example was a fraudulent financial request. This campaign featured only a few impersonating messages and was targeted at one customer. No other Proofpoint customer had seen this attack before.

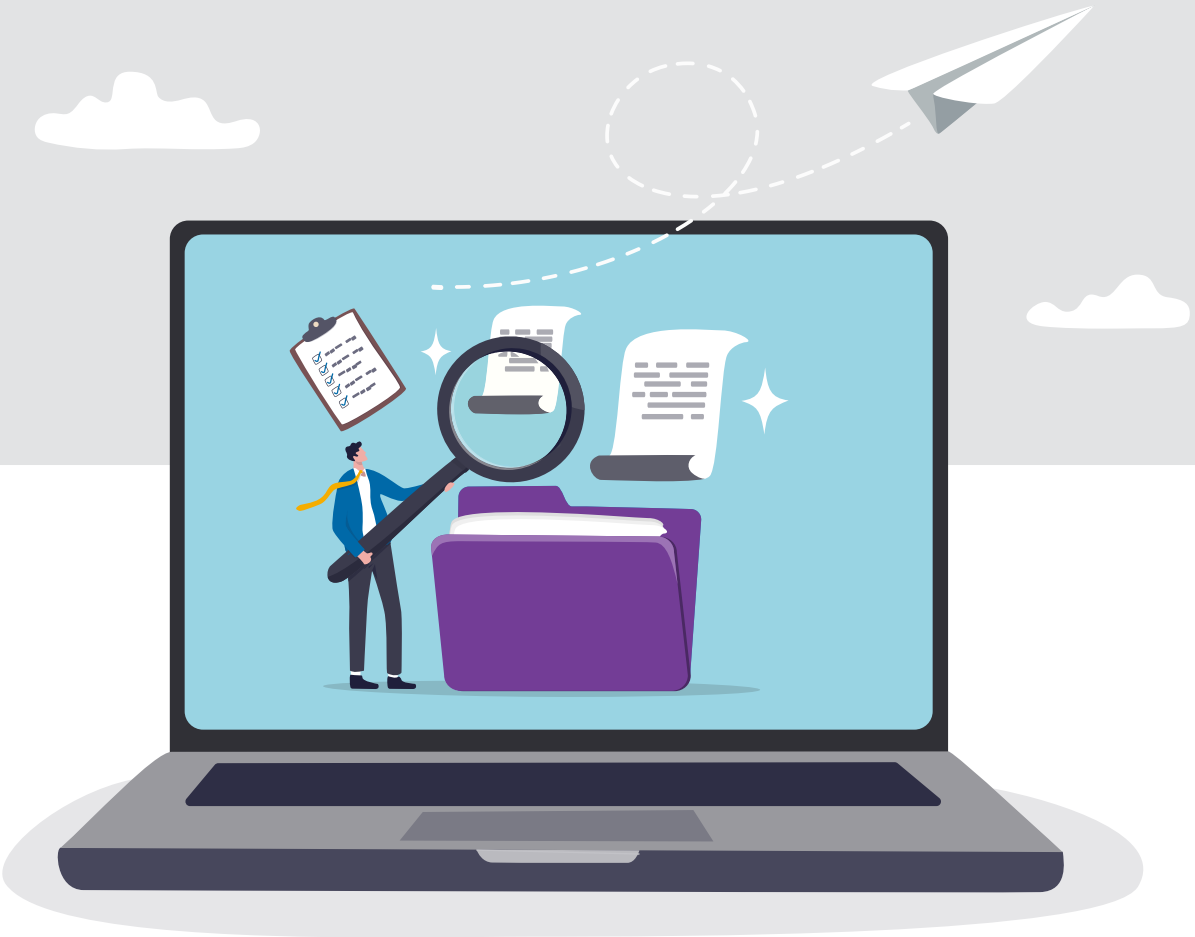



*Condemnation summary outlining the signals that Proofpoint detected to block this threat.*

SECTION 6

# Conclusion

All of these scams are just the latest reminder of the critical need for robust multilayered cybersecurity measures.



To stay ahead of evolving dangers, you need a comprehensive approach to protecting against threats targeting your people:

- **Detect threats pre-delivery.** The only way to keep users safe is to block malicious messages before they are delivered. Proofpoint research shows that 1 in 7 users will click on an email within one minute. Look for a tool that combines ML algorithms and advanced threat intelligence to identify and block advanced threats.
- **Educate your users.** Your employees, contractors and partners are your first line of defence. Make sure that they get security awareness training for all types of attacks. Remind them to move fast to report any unusual account behaviours.
- **Conduct regular security audits.** Audits can help you identify any potential vulnerabilities in your environment. As part of that work, be sure to look for irregularities in your configurations and access logs.
- **Set up your system to monitor for misconfigurations.** Besides checking for misconfigurations, don't forget to enable auto-remediation. This will ensure that you detect unauthorised changes and mitigate them promptly, which will stop attackers from establishing persistence.
- **Create an incident response plan.** Map out multiple attack scenarios. Then, define how you will investigate and mitigate them. Be sure to test how effective your plan really is by conducting regular simulated exercises.

# Next Steps

More than ever, it's important to protect your organisation from rising email threats. You need to take a proactive approach to keep your business, employees and customers safe from advanced attacks like ransomware, BEC and credential phishing.

The Proofpoint Email Rapid Risk Assessment provides you with comprehensive visibility and insights into your vulnerability to attacks. It helps you discover who is being targeted by email-based threats across your organisation.

Don't wait until it's too late to test your email security. Contact Proofpoint for a free **Email Risk Assessment.**

## LEARN MORE

For more information, visit **proofpoint.com**.

---

**ABOUT PROOFPOINT**

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.