proofpoint.

E-BOOK

Breaking Down BEC

The Modern CISO's Framework for Identifying, Classifying and Stopping Email Fraud

Introducing the Proofpoint Email Fraud Taxonomy Framework

Business email compromise (BEC), also known as email fraud, is one of cybersecurity's costliest and least understood threats. This fast-growing category of email fraud doesn't always garner as much attention as other high-profile cyber crimes. But in terms of direct financial costs, BEC easily overshadows other types.

In 2020 alone, BEC schemes cost organizations and individuals more than $1.8 billion.[1] That's up more than $100 million from 2019, and it represents 44% of total cyber crime losses.

As BEC schemes have evolved, industry nomenclature has outlived its usefulness. The terms used to explain BEC tactics and techniques have become ambiguous, conflated with other concepts and misused. Without a framework to describe BEC attacks—let alone conceptualize them—researching and managing the threat is difficult, if not impossible.

That's why we have created the Proofpoint Email Fraud Taxonomy. This framework is designed to help security professionals better identify, classify and ultimately block this costly threat.

Why words matter

The term "BEC" is often used in sweeping fashion to describe an entire subclassification of email threats. It's thrown around as a general term that could refer to any number of tactics and techniques linked to financially motivated, response-based, **socially engineered** email deception.

That's not just a mouthful. It's a clear sign that the term "BEC" has become far too inclusive. The threat has outgrown the words used to describe it, complicating researchers' efforts to study BEC and organizations' attempts to manage it.

1 FBI. "Internet Crime Report 2020." March 2021.

A new way of looking at BEC and email fraud

To simplify and highlight key aspects of BEC (and email fraud at large) we have created this taxonomy. Our goal: to help organizations better identify, understand and manage the many forms of email fraud they'll likely face.

Identity

We take a people-centric approach to email fraud. That's why our taxonomy map begins with *Identity*. In this tier, Identity refers to the person or entity that the threat actor (that is, the attacker) is pretending to be. We divide Identity into "employee," "supplier" and unknown." But you may want to make it even more granular, such as subdividing "employee" into "executives" and "general employees."

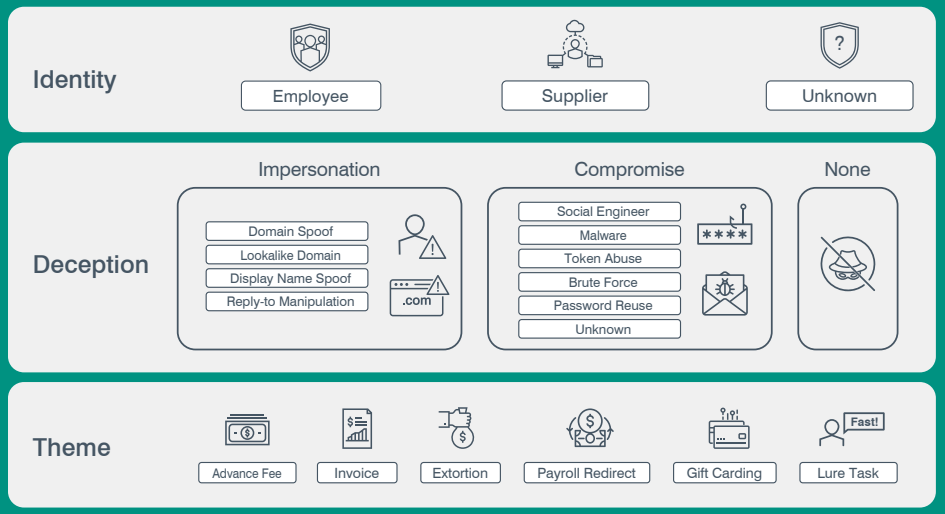


Figure 1: The Proofpoint Email Fraud Taxonomy

Deception

The next tier is *Deception*, which covers the techniques used by email fraudsters. This tier includes "impersonation," "compromise" and "none."

"Impersonation" refers to techniques that involve the threat actor manipulating one or more message headers to mask the origin of the message. This may include spoofed headers, lookalike domains and other techniques used to pose as someone else.

"Compromise" is when the threat actor gains access to a legitimate mailbox for email. The account may belong to a trusted supplier, a fellow employee or an authority figure. The recipient has no reason to question the email's legitimacy and lacks the usual clues to spot the attack.

When the deception technique is "none," the attacker is using a BEC tactic that doesn't rely on impersonation. The threat actor may send email from free email providers with no spoofing.

Theme

The final tier, *Theme*, contains the most relatable and actionable information. It is by far the most important part of this taxonomy. Themes include:

- Invoice fraud
- Payroll redirects
- Extortion
- Lures and tasks
- Gift carding
- Advance fee fraud

These themes cover the categories we found to be most relevant to the BEC threat landscape and useful to the widest range of organizations. While broad enough to account for nuance—because every attack is unique—the themes are also specific enough to help you quickly identify, classify and manage the full range of BEC threats.

Theme 1: Invoicing Fraud

At its core, invoicing fraud is an attempt to deceive someone into paying for products or services they did not purchase or redirecting a legitimate payment to the attacker's account. Among the email fraud themes in our taxonomy, invoicing fraud can arguably be the costliest. Business-to-business transactions tend to be large and numerous, giving fraudsters ample opportunity and incentive to cash in.

The subject lines of fraudulent invoice emails tend to be payment-oriented. The fake invoices may appear genuine, featuring company logos, professional formatting and the like. The email may also detail specific charges and include urgent language such as: "This invoice is 90 days past due and must be paid immediately." Often, the threat actor uses threatening language if the recipient doesn't act quickly.

At the *Identity* tier, a fraudulent invoice can appear to be sent from anyone—a fellow employee or someone outside the organization. But the most successful ones exploit existing supplier relationships. As prime examples of invoicing fraud, supplier attacks can end up costing anywhere from tens of thousands to multiple millions of dollars.

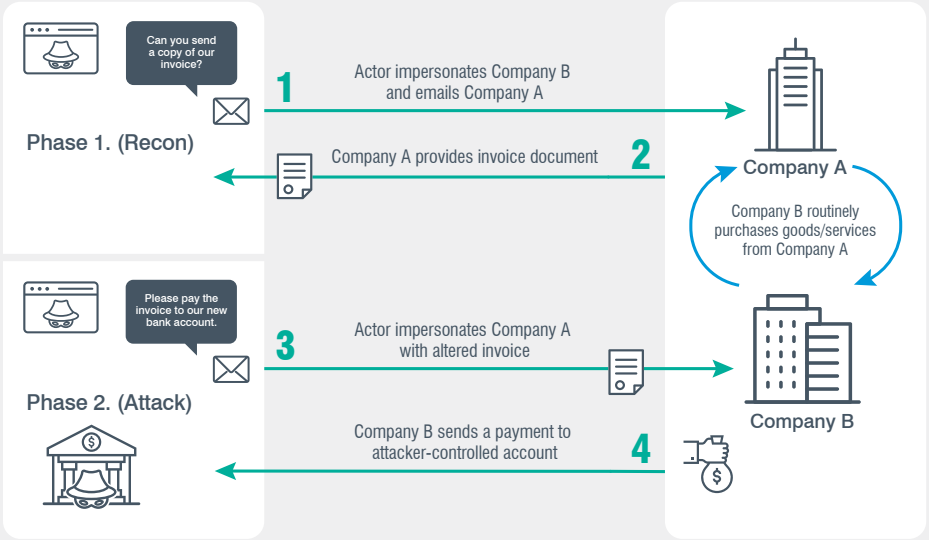


Figure 2: Anatomy of a supplier invoice fraud attack where attackers use multiple layers of impersonation

How it works

At the *Deception* tier, supplier invoice fraud schemes can occur through either impersonation or compromise.

Impersonation

Supplier impersonation is a threat actor using common email spoofing techniques to pose as the supplier. Often, these fraudulent emails are sent from free webmail domains or unrelated compromised accounts the threat actor controls.

As shown in Figure 2, the impersonation isn't always straightforward. In some cases, an attacker may first impersonate the targeted company to get a real invoice from the supplier—then use that invoice to turn around and impersonate the supplier. (Because it involves a real invoice from an actual supplier, this two-way attack may at first appear to be a case of account compromise.)

Compromise

Supplier compromise involves a malicious actor gaining unauthorized access to a trusted supplier's email account, then using that account for BEC-style attacks against the supplier's customers. The attacker usually gains access to the account through a past phishing campaign or purchased credentials.

In some cases, attackers may even piggyback an existing email thread of a compromised account. (This technique is called "thread hijacking.") By observing, mimicking and responding to actual conversations within the email thread, they can craft believable messages with supporting documents.

Call it the ultimate impersonation tactic. The BEC emails become part of an active conversation. The recipient has no reason to suspect that the person they were communicating with has suddenly been replaced by an impostor. It's no wonder these emails are among the most convincing BEC attacks most users will ever face.

Why not both?

Often, threat actors use both impersonation and compromise as deception tactics. Some of these attacks are targeted. But many are opportunistic, springing from information attackers learn while compromising supply chains. (Our taxonomy accounts for this nuance by classifying such attacks as both compromise and impersonation in the *Deception* tier, as shown in Figure 3.)

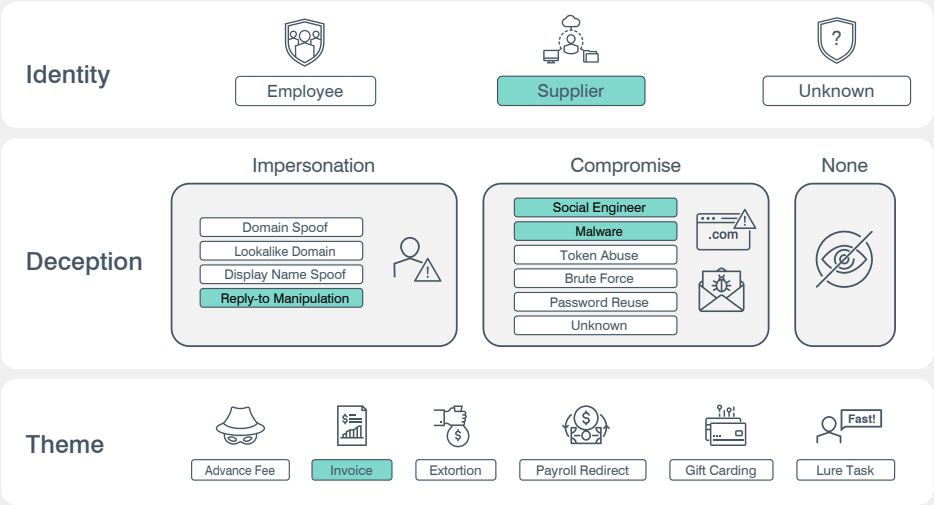


Figure 3: Supplier invoice fraud example with both impersonation and compromise deception tactics

A real-world example

In a supplier invoice fraud attack we recently observed, an attacker tried to steal more than $100,000 from a company by posing as its usual wine supplier.

The attacker replied to an existing email thread between the customer and the supplier, asking the customer to send payment directly to a specified bank account. (As seen in Figure 4, the message also said that all communication should take place over email.) Although the attacker had hijacked a real email thread and appeared to have inside knowledge of the supplier, the attack used spoofed emails rather than a compromised email account.

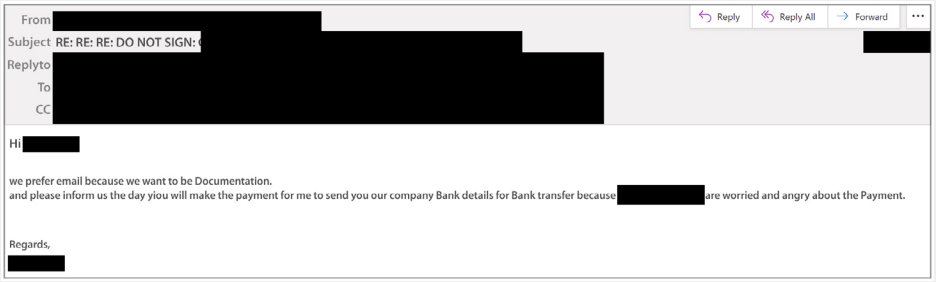


Figure 4: The initial invoice fraud attempt

After not getting the desired response, the threat actor followed up with more urgency, as shown in Figure 5. The email included a detailed invoice that featured the real supplier's logo and stamp to make it convincing (see Figure 6 on the next page).

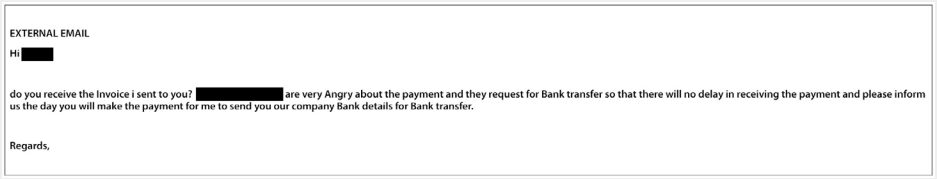
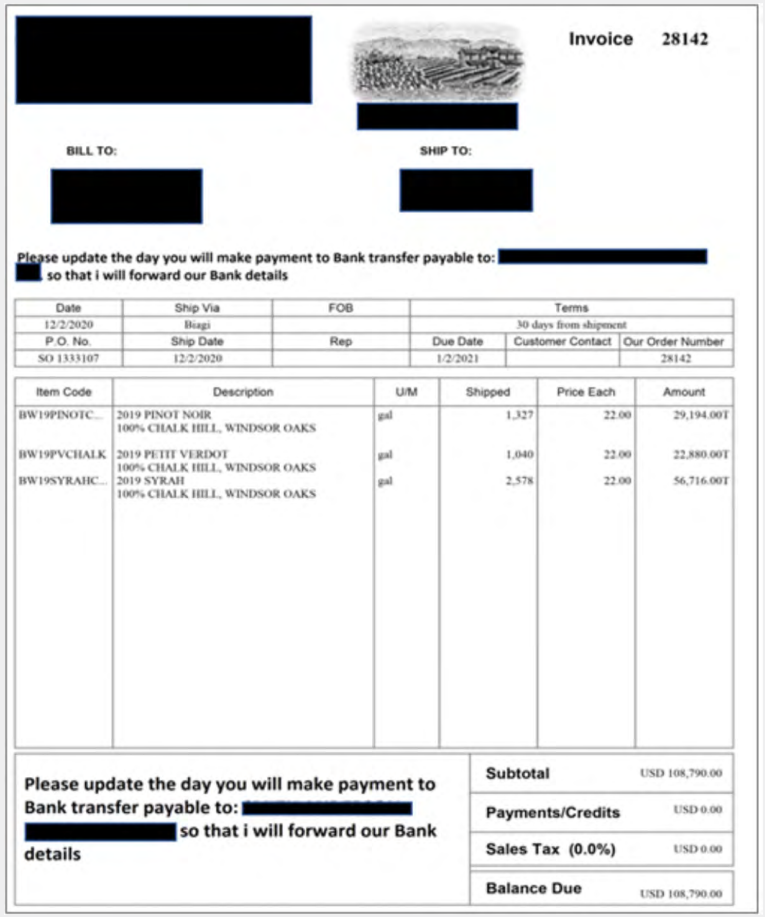


Figure 5: A follow-on attempt by the same attacker



[redacted]

Invoice 28142

BILL TO:

[redacted]

SHIP TO:

[redacted]

Please update the day you will make payment to Bank transfer payable to: [redacted]
[redacted] so that i will forward our Bank details

Date	Ship Via	FOB	Terms		
12/2/2020	Bagi		30 days from shipment		
P.O. No.	Ship Date	Rep	Due Date	Customer Contact	Our Order Number
SO 1333107	12/2/2020		1/2/2021		28142

Item Code	Description	U/M	Shipped	Price Each	Amount
BW19PINOTC...	2019 PINOT NOIR 100% CHALK HILL, WINDSOR OAKS	gal	1,327	22.00	29,194.00T
BW19PVCHALK	2019 PETIT VERDOT 100% CHALK HILL, WINDSOR OAKS	gal	1,040	22.00	22,880.00T
BW19SYRAHC...	2019 SYRAH 100% CHALK HILL, WINDSOR OAKS	gal	2,578	22.00	56,716.00T

Please update the day you will make payment to Bank transfer payable to: [redacted] so that i will forward our Bank details

Subtotal	USD 108,790.00
Payments/Credits	USD 0.00
Sales Tax (0.0%)	USD 0.00
Balance Due	USD 108,790.00

Figure 6: Invoice PDF

Because the emails revealed knowledge that only the real wine supplier would know, we suspect that the supplier had been compromised before the BEC attempt. The attacker likely used details gleaned from the compromise along with display name spoofing and reply-to manipulation to impersonate the vendor. (Figure 7 shows how we mapped this attack.)

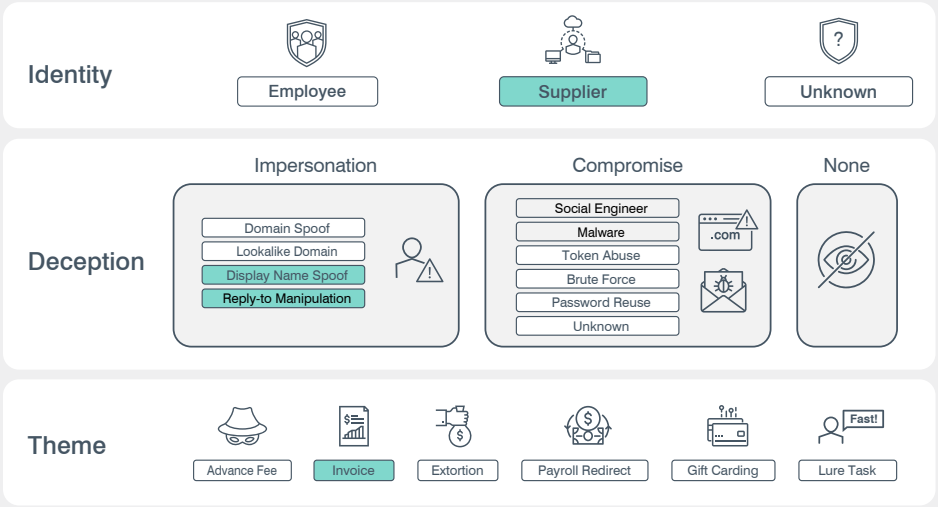


Figure 7: Real-world example of supplier invoice fraud

Theme 2: Payroll Redirects

Payroll redirects, also called payroll diversions, are among the simplest BEC attacks we see. Whether they target finance, tax, payroll or human resources (HR) departments, the goal is simple: trick the recipient into rerouting employees' hard-earned wages—or even tax refunds—to the attacker.

We detect an average of about 2,000 payroll redirect attempts per day (see Figure 8) and consider these attacks a medium risk to employers.

According to the FBI, the average loss from such attacks is $7,904 per reported incident.[2] The IRS included payroll redirects on its "Dirty Dozen" list of tax schemes for 2020.[3] The agency says attackers use IRS documents in payroll redirect schemes to convince recipients that fraudulent bank change requests are legitimate.

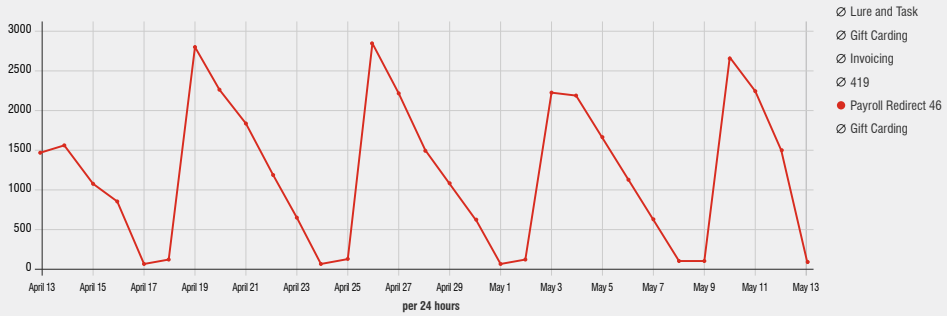


Figure 8: Payroll redirect attempts (total attempts within 24-hour period, April 13 through May 13, 2021)

How it works

Payroll redirect schemes can use compromise as the *Deception* technique, but usually involve impersonation. (Threat actors with access to a compromised account tend to focus their efforts on higher-dollar forms of BEC, such as invoice fraud.)

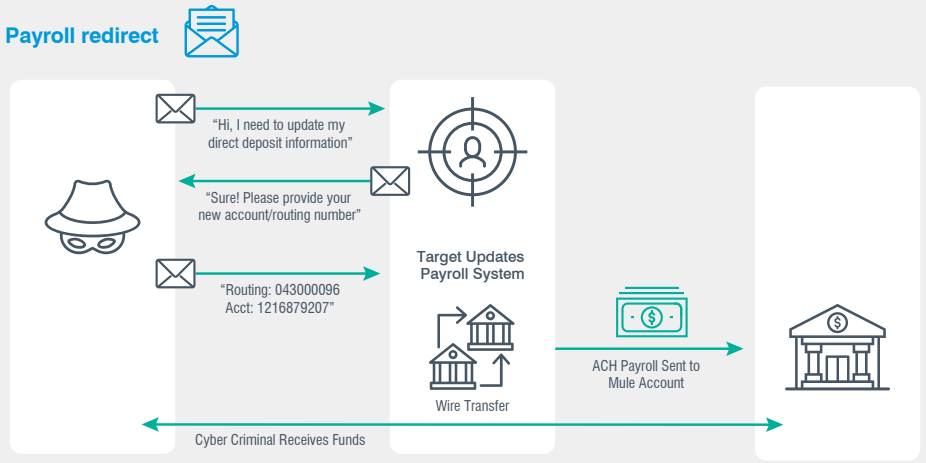


Figure 9: Anatomy of a payroll redirect attack that uses impersonation

Most impersonation-based payroll attacks use free email services such as Gmail. Typically, the threat actor uses display name spoofing so that the email appears to be from an employee (see Figure 9 above).

Some payroll redirects target C-level executives and upper management for the chance to score a bigger paycheck. In these attempts, threat actors may use email addresses with executive themes to lend credibility—and for recipients eager to please the boss, a sense of urgency. (See Figure 10 on the next page. Other recent examples include "ceo@companywebaxccs.com" and "ceo_task2@icloud.com.")

1. FBI. "2020 Internet Crime Report." March 2021.
2. IRS. "Dirty Dozen." September 2021.

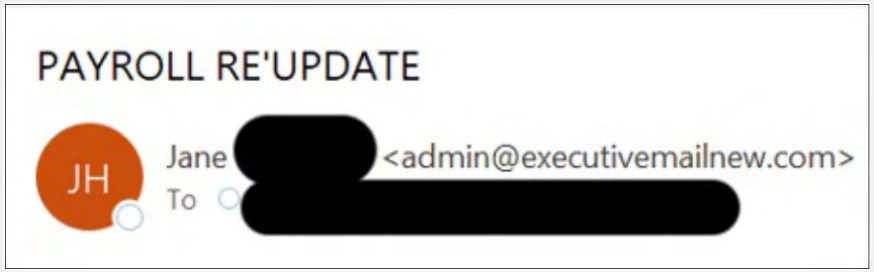


Figure 10: An email domain designed to convey executive authority

Figure 11 shows how our taxonomy would classify the two attacks we just described.

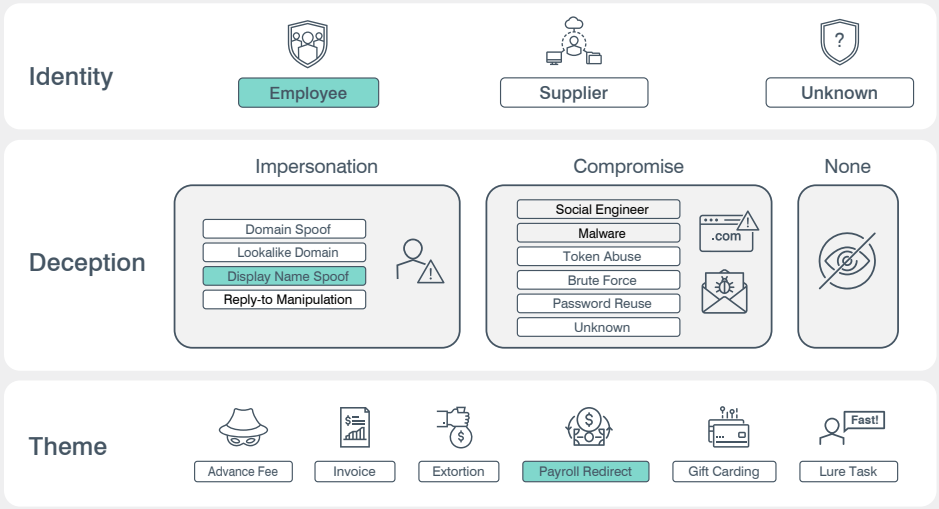


Figure 11: Payroll redirect scheme using a spoofed email display name

Real-world examples

One hallmark of payroll redirect schemes is their simplicity. In an attack we recently observed, the threat actor impersonated several employees in emails sent to a large company's payroll department. As seen in Figure 12, each of the emails used the same approach, differing only in:

- Who the email was sent to
- Who was being impersonated
- The language used (English, German or Spanish)

Figure 12: Sample of emails impersonating employees in payroll redirect attempts

Some attempts are even simpler and more brazen. In Figure 13, the attacker tries to impersonate the CEO of a company.

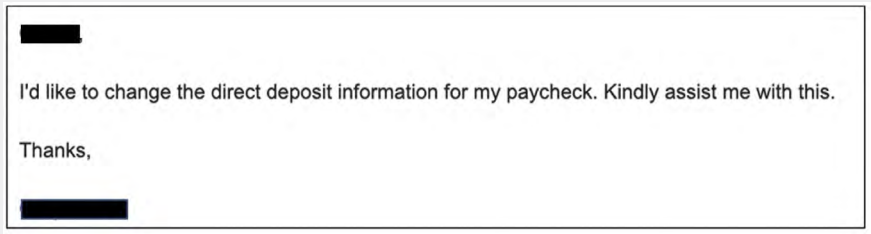


Figure 13: Payroll redirect email impersonating a CEO

Despite the low-tech nature of these attacks, they can be surprisingly effective. That's because they exploit a normal business process. Payroll, finance, tax and HR employees receive these kinds of requests by email every day, most of them legitimate.

Theme 3: Extortion

Extortion-themed email fraud works like other forms of extortion. The attacker threatens to destroy property, commit violence or release confidential, embarrassing or compromising information unless the recipient provides payment (typically through cryptocurrency) or something else of value. Extortion has several subtypes, including:

- **Data release.** The threat actor threatens to release sensitive, embarrassing or compromising information; customer data or trade secrets; or evidence of criminal activity (whether real or not).
- **Distributed denial of service (DDoS).** The attacker threatens to overwhelm the recipient's online operations with bogus traffic, making it inaccessible to legitimate users.
- **Physical harm.** This attacker threatens physical harm to the recipient or the organization. Common tactics include bomb threats, murder-for-hire plots and other warnings of looming violence.
- **Sextortion.** The attacker threatens to release sexually related photographs or videos of the victim. Sextortion is probably the most common of these extortion subtypes.

How it works

Unlike the other themes outlined in this e-book, extortion email fraud uses just one deception tactic—impersonation—if it uses any at all. When impersonation is the approach, the attacker will usually make the email look as if it originated from the victim's email account.

Typically, the threat actor sends victims an email claiming to have accessed their computer and recorded them viewing adult content. The email includes sensitive content made to look like it came from the recipients' own email account. Unless the recipients pay up, the attacker warns, the embarrassing content will be sent to co-workers and family.

Figure 14 shows how such an attack maps to our BEC framework.

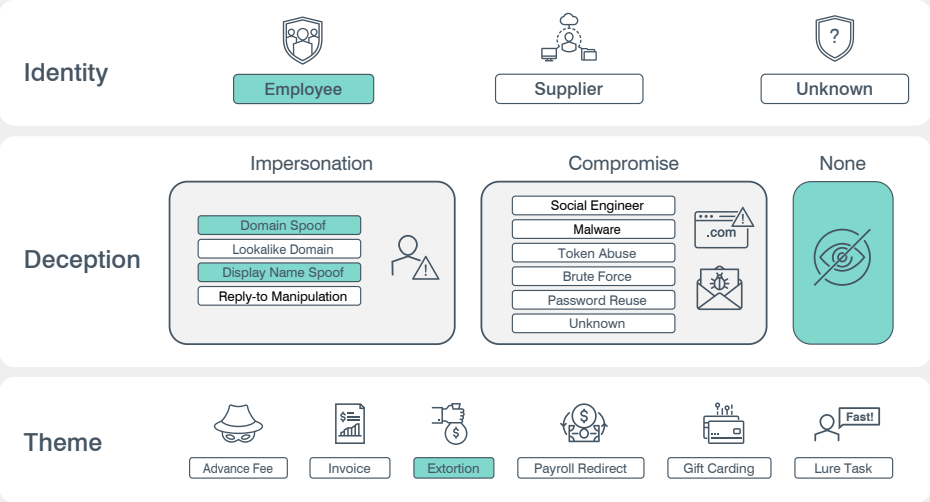


Figure 14

Unless attackers are trying to impersonate someone, they typically use free email providers and don't bother spoofing the address. Such a scenario would map to the framework as follows (Figure 15).

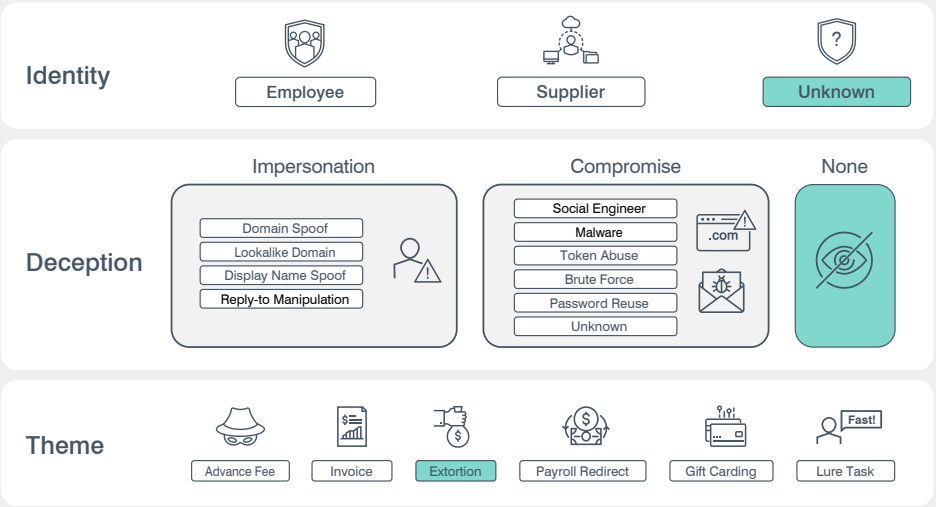
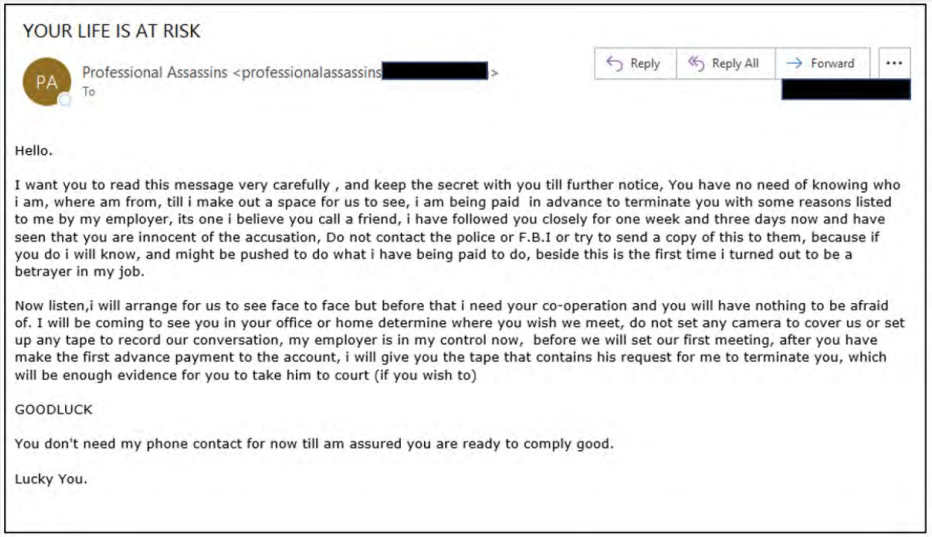


Figure 15: Some extortion schemes do not use identity deception tactics



YOUR LIFE IS AT RISK

PA Professional Assassins <professionalassassins[redacted]>
To

Reply | Reply All | Forward | ...

Hello.

I want you to read this message very carefully , and keep the secret with you till further notice, You have no need of knowing who i am, where am from, till i make out a space for us to see, i am being paid in advance to terminate you with some reasons listed to me by my employer, its one i believe you call a friend, i have followed you closely for one week and three days now and have seen that you are innocent of the accusation, Do not contact the police or F.B.I or try to send a copy of this to them, because if you do i will know, and might be pushed to do what i have being paid to do, beside this is the first time i turned out to be a betrayer in my job.

Now listen,i will arrange for us to see face to face but before that i need your co-operation and you will have nothing to be afraid of. I will be coming to see you in your office or home determine where you wish we meet, do not set any camera to cover us or set up any tape to record our conversation, my employer is in my control now, before we will set our first meeting, after you have make the first advance payment to the account, i will give you the tape that contains his request for me to terminate you, which will be enough evidence for you to take him to court (if you wish to)

GOODLUCK

You don't need my phone contact for now till am assured you are ready to comply good.

Lucky You.

Figure 16: An extortion attempt promising to call off a supposed murder-for-hire plot if the recipient pays the sender

Real-world examples

Sextortion is by far the most common form of extortion we see. These emails tend to be lengthy and detailed. But the goal is simple and pragmatic: convince victims that they are in a precarious position and must meet the threat actor's demands.

Threats of physical harm are less common, though understandably alarming to the people who receive them. As seen in Figure 16, these strong-arm tactics try to scare the victims into thinking their lives are in grave danger unless they pay.

Key attributes include a sense of urgency, short deadlines for complying and dire warnings not to contact police.

Theme 4: Lures and Tasks

Because of their basic nature, lure and task emails are easy to overlook. They start with a request for a simple, even routine, favor. While some attacks open with a specific ask, many are vaguely worded, reeling the victim in over the course of multiple emails. In these cases, the initial messages might make a general request in the vein of:

- "Are you available?"
- "I need a quick favor"
- "Do you have a moment?"
- "Are you there? I need you to buy me gift cards."

Lures and tasks are often a gateway, the first step in multistage attacks that encompass other email fraud themes. A lure/task email gets the recipient's attention, and the threat actor's ultimate goal—such as payment redirects or invoice fraud—unfolds over time.

These multi-category attacks can make classification tricky. Often, the difference between lure/task emails and others in our taxonomy is whether we see what the threat actor does next. If we see only a single lure/task-oriented email, we classify it as such. But if follow-up emails reveal an underlying aim beyond the initial lure and task, we classify it as both lure and task and another theme.

How it works

Lure and task emails use just one form of *Deception* in our taxonomy, impersonation. Attackers commonly pose as someone the intended victim knows or trusts, including:

- Authority figures, both personal and professional
- Close friends
- Family members

Posing as someone familiar disarms any suspicions the recipient might have about an unexpected or unusual request and almost compels a response.

A simple reply achieves the threat actor's first aim: identifying an active email account and potentially receptive audience.

Most lure/task emails use display name spoofing to deceive the recipient, as shown in Figure 17. Some use other impersonation tactics, such as spoofing the domain or reply-to addresses. After receiving a response, the threat actor may change deception tactics if it helps make the scheme seem more credible.

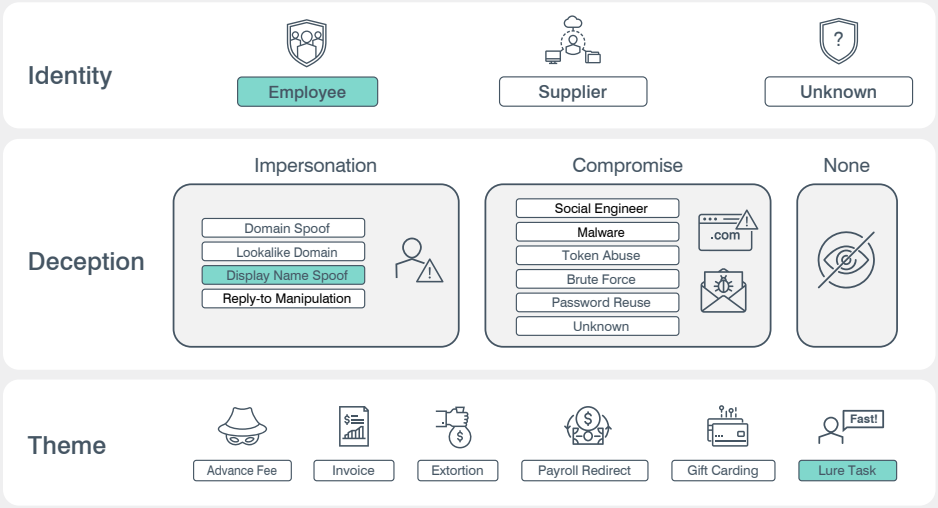


Figure 17

Real-world examples

Many of the lure/task fraudulent emails we see begin with a brief email that gauges how receptive the target might be. As shown in Figure 18, these early emails may not even try to create a sense of urgency.

Figure 18: Initial lure/task-themed email

Lure/task-themed email fraud is prolific, accounting for more than half the email fraud threats that we saw in 2021. (We stop about 30,000 of these emails per day from being delivered.)

These emails seem benign at first. But if the recipient falls for one, it can lead to more serious forms of email fraud with potentially costly outcomes—gift carding, invoice fraud, and payroll redirect fraud and the like.

Theme 5: Gift Carding

In gift carding schemes, threat actors obtain payouts in the form of retail gift cards. Recipients are tricked into buying the cards and sending the numbers and PINs to the attacker, who then redeems or resells the cards.

These attacks work because companies often reward employees and partners with gift cards. To the recipient, the request might seem routine. If the email sounds urgent and offers a reasonable-sounding explanation, the recipient might act without giving it a second thought.

How it works

In the *Deception* tier, threat actors typically spoof a person in leadership or a position of authority to give the request a sheen of legitimacy. As is the case with other forms of email fraud, posing as someone familiar, including close friends and family members, makes the recipient more likely to fall for the scheme.

Most gift carding email fraud uses display name spoofing to deceive recipients (see Figure 19). Sometimes, threat actors use other impersonation tactics, such as spoofing the domain or altering the reply-to field.

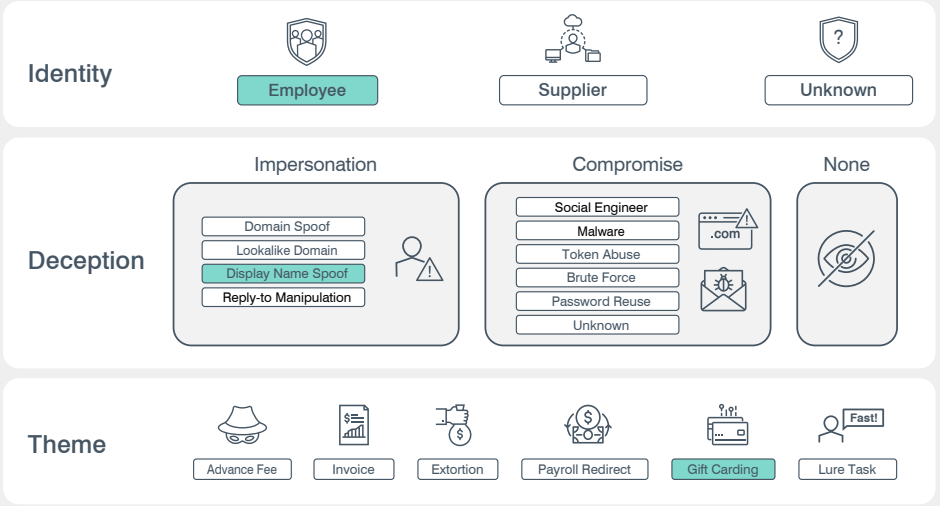


Figure 19: Gift carding taxonomy

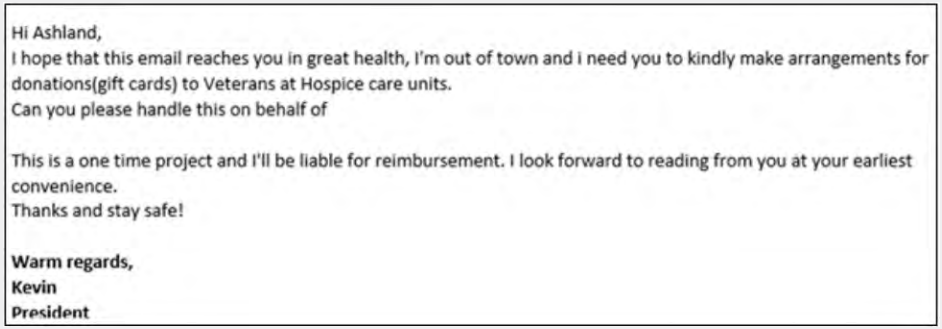
Real-world examples

Gift carding emails use all kinds of lures to make the request seem valid to the recipient (see Figure 20, Figure 21 and Figure 22 on the next page). Threat actors may enlist everything from current events, such as the pandemic, to national holidays. Whatever the lure, the goal is to provide a plausible reason for the request and to elicit sympathy for the best chance of success.

Sympathy for the scammer

Figure 23 and Figure 24 are vivid examples of threat actors trying to tug on the recipient's heartstrings.

In Figure 20, the sender claims the request is for a hospice situation—for military veterans, no less. In Figure 21, the sender claims they are out of town and in isolation, likely a nod to the pandemic, and therefore unable to get a gift for a niece's upcoming birthday



Hi Ashland,
I hope that this email reaches you in great health, I'm out of town and i need you to kindly make arrangements for donations(gift cards) to Veterans at Hospice care units.
Can you please handle this on behalf of

This is a one time project and I'll be liable for reimbursement. I look forward to reading from you at your earliest convenience.
Thanks and stay safe!

Warm regards,
Kevin
President

Figure 20: Email asking recipient to buy gift cards for a purported hospice donation

Greetings,

I hope you and your family are in good health! I need a quick and urgent favor from you. I need to get a Target gift card for my Niece, it's her birthday but i can't do this now because i am currently out of town and isolated till 27th of this month as advised by my doc. Pls can you get the card from any nearby Grocery store around you or CVS, I'll pay back as soon as i get back and okay. Please let me know if you can handle this.

Thanks and stay safe,
I owe you a lot

Best Regards,

Ruben

Subject: RE: Greetings!

Hi Ruben, how are you doing?

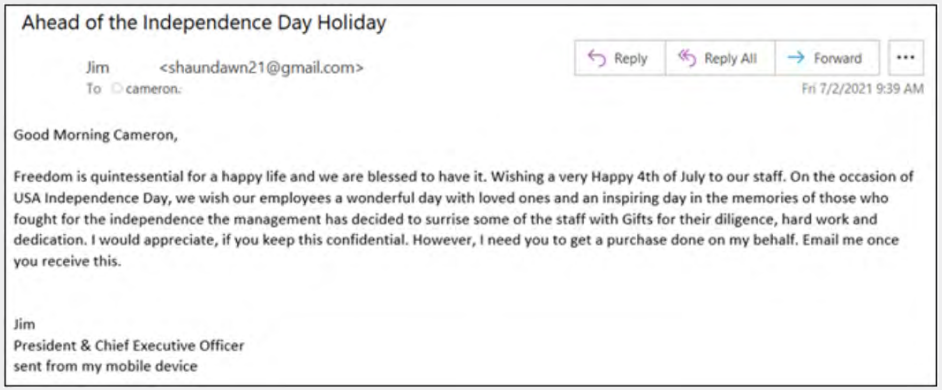
Richard

Figure 21: Email asking recipient to buy gift cards on the premise that the sender is in isolation

Figure 22 also shows that that some gift carding fraud starts with a brief lure and task email to test the receptivity of the potential victim (for more on this lure, see the previous section, "**Theme 4: Lures and Tasks**"). In this case, the threat actor first sought to see whether the intended victim was available. The gift card request came only after the person responded.

Corporate gift card fraud

In our final example (Figure 22), the threat actor spins a tale of wanting to get gift cards to distribute an employee thank-you, a common corporate practice. In this case, the request is tied to the U.S. Independence Day holiday.



Ahead of the Independence Day Holiday

Jim <shaundawn21@gmail.com>
To cameron.

Reply | Reply All | Forward | ...
Fri 7/2/2021 9:39 AM

Good Morning Cameron,

Freedom is quintessential for a happy life and we are blessed to have it. Wishing a very Happy 4th of July to our staff. On the occasion of USA Independence Day, we wish our employees a wonderful day with loved ones and an inspiring day in the memories of those who fought for the independence the management has decided to surrise some of the staff with Gifts for their diligence, hard work and dedication. I would appreciate, if you keep this confidential. However, I need you to get a purchase done on my behalf. Email me once you receive this.

Jim
President & Chief Executive Officer
sent from my mobile device

Figure 22: An email from someone posing as the company CEO asking the recipient to buy gift cards as an employee perk; the attacker tells the recipient to keep the request secret, supposedly to avoid spoiling the surprise

The gift that keeps on taking

Gift carding is a common form of email fraud. At an average $840 per incident, this crime has swindled people out of almost $245 million since 2018. We stop anywhere between 7,000 and 10,000 of these emails per day.

Theme 6: Advance Fee Fraud

Advance fee fraud is an old con that is sometimes, and somewhat misleadingly, called "419," "Nigerian 419" or "Nigerian prince" email fraud. It occurs when a threat actor asks the potential victim for a small amount of money in advance of a larger payout later. The requested funds are usually depicted as seed money to unlock or transfer the promised reward.

Threat actors have dreamed up countless variations of advance fee fraud. They often weave elaborate tales of why a large sum of money is available and why they need a small upfront fee to get it to the email recipient. The fraudsters often bait victims with subject lines that include:

- Inheritance
- Lottery winnings
- Awards
- Government payouts
- International business

Once the victim provides the advance fee, the fraudster may string the victim along for more money (citing unforeseen complications) or simply cut all contact and disappear.

How it works

In the *Deception* tier of our taxonomy, advance fee fraud uses impersonation techniques. Threat actors will commonly pose as a government official, legal representative or person in a dire situation. Most advance fee fraud emails use display name spoofing (see Figure 23), though some use other impersonation tactics such as domain spoofing or lookalike domains.

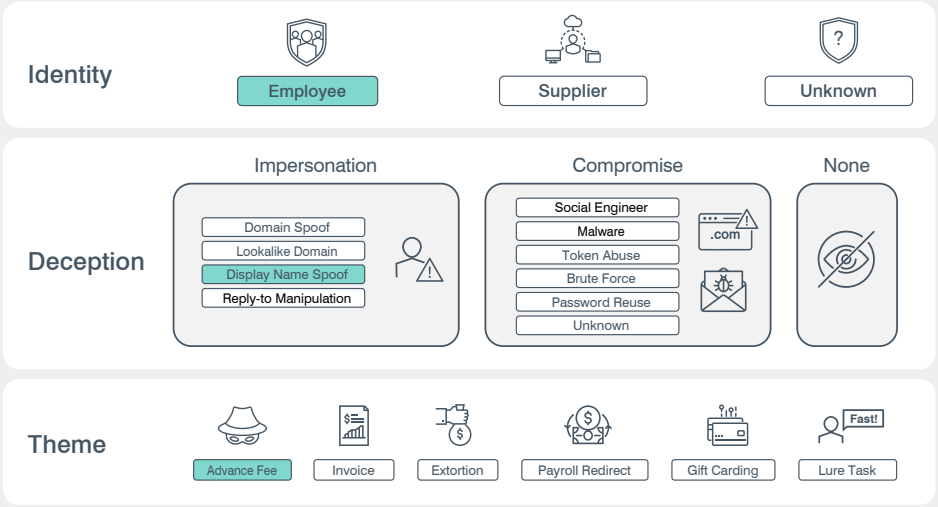


Figure 23: Advance-fee fraud taxonomy

Real-world examples

Advance fee fraud emails use various lures to reel in victims, maintain their trust and persuade them to act. As shown in the following examples, threat actors may latch on to anything that works—including current events such as the pandemic, business deals and beneficiary payouts.

In Figure 24 (see next page), the sender tries to capitalize on COVID-19. In Figure 25 (also on the next page), the sender urges the recipient to act quickly, giving the target little time to consider whether the email is fraudulent.

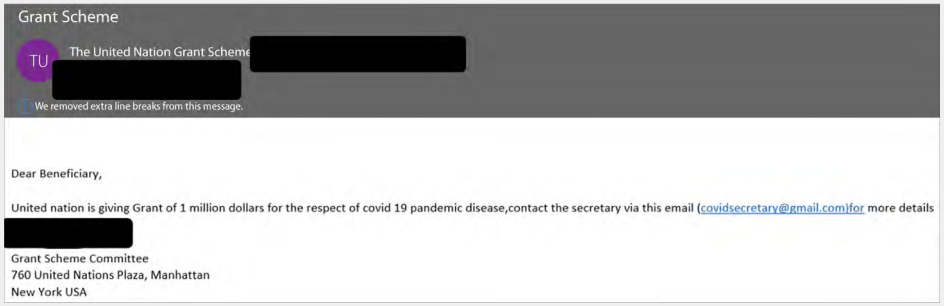


Figure 24: An advance fee fraud email promising a $1 million grant

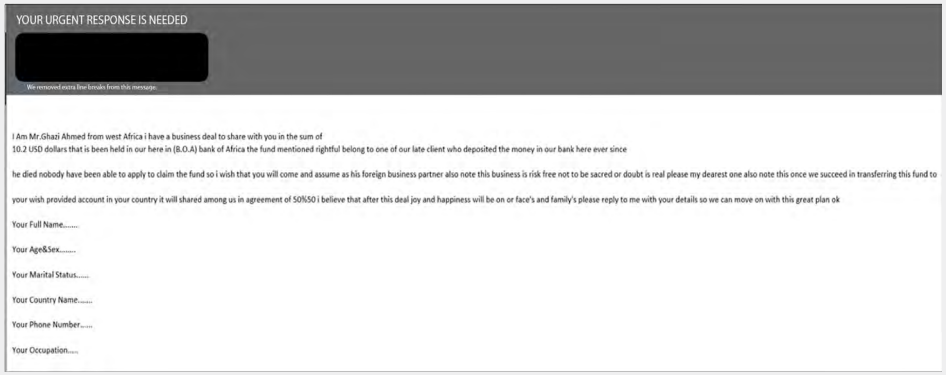


Figure 25: This email offers to split an unclaimed inheritance with the recipient

In Figure 26, the threat actor tries to tempt the victim with a large beneficiary payment, a common strategy in advance fee fraud that exploits human greed. Beyond tricking the recipient out of a $95 “security fee,” the email tries to get personally identifiable information.

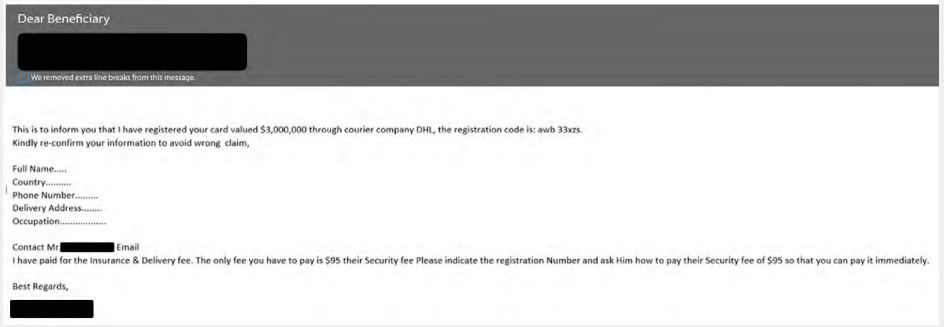


Figure 26: An email promising a $3 million payment after the recipient pays a $95 “security fee”

Most advance fee fraud emails are simple and easy to spot; few are well-crafted or more complex than the examples provided here.

Advance fee emails make up a small fraction of the fraud emails we see. Still, people do fall for them, with an average loss of about $5,100 per incident. Though the success rate is likely far lower than for other types of fraud such as gift carding, advance fee fraud can be lucrative for threat actors.

Conclusion and Recommendations

The types of email fraud outlined in our taxonomy are devious, unrelenting and hard to manage with traditional perimeter-focused security tools and gateways. Like most modern cyber attacks, they target people, not technology. That's why stopping these attacks requires a people-centric approach.

Financial controls—such as requiring two or more people to approve changes to payment accounts or payroll details—are a good start. But stopping BEC and email fraud also requires advanced email protection. To get more visibility into this human attack surface and stop BEC in all its various forms, you need a comprehensive platform with integrated controls across email, cloud accounts, users and suppliers.

Look for a solution that offers:

- Visibility into your human attack surface. You should know your most attacked users, the threat actors targeting your organization and the suppliers that might be compromised or impersonated.
- Advanced detection capabilities to stop BEC, email fraud and other threats that don't use malware. Email fraud uses social engineering and ever-evolving tactics that prey on human nature. That means static rule sets, even when regularly updated, aren't enough to identify and stop them. The best solutions also use machine learning that analyzes factors such as email headers, the sender/recipient relationship and the sender's reputation. But machine learning is only as good as the data that feeds it and the training models that shape it. So, look for vendors with large, diverse data sets and human threat expertise.
- The ability to prevent attackers from commandeering users' accounts and using them for email fraud attacks. As more businesses move to the cloud, protecting against email fraud also means protecting cloud accounts. Look for tools that prevent your users' accounts being commandeered for email fraud attacks.
- Security awareness training that augments technical controls. With the right education—especially when it's based on real-world threats—you can turn users into a strong last line of defense. Make it easy for users to report suspicious messages—and for your security team to verify them with automated analysis and remediation.

LEARN MORE

To learn more about how Proofpoint can help you manage BEC and email fraud, visit **www.proofpoint.com/us/solutions/bec-and-eac-protection**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' 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 organizations of all sizes, including more than half of the Fortune 1000, 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**.

proofpoint.

0501-010-01-01 04/22