Cofense Intelligence™ Strategic Analysis

Report date: 2022-06-23

BEC: Tactics and Trends of the Most Costly Email Threat

Business Email Compromise (BEC) describes a business-oriented social engineering attack carried out solely via email communication, largely without the use of malware and credential phishing mechanisms such as malicious attachments and links. To request funds from their intended victims, BEC threat actors conduct a variety of scams impersonating coworkers, vendors, or customers. Despite the relatively low technical sophistication of the attacks, they have led to billions of dollars in losses worldwide, making BEC the #1 cause of financial loss among threats reported by the FBI Internet Crime Complaint Center (IC3) in 2021. In this report, we bring the realities of BEC to life by interacting with real threat actors, becoming familiar with the stories they present, and examining trends in real-world BEC campaigns. We will also consider BEC impacts and the potential for recovery of assets, along with mitigation strategies.

Key takeaways:

- BEC emails commonly include language meant to ingratiate the victim to the threat actor and/or to create a sense of urgency.
- Rarely will a BEC campaign show its cards in its initial email. Threat actors almost always wait for at least the first reply from their victim before making their true request. Some may choose to build trust in several rounds of conversation before doing so.
- Payroll diversion and gift card scams are the most common forms of BEC reaching inboxes.
- BEC emails that reach inboxes are most often sent from well-known free webmail services, with Gmail constituting the majority.

Business Setting Provides Context for BEC Scams

BEC campaigns are similar to everyday consumer fraud campaigns, containing no attached malware or credential phishing links. However, while consumer fraud seeks to establish a relationship, BEC campaigns may capitalize on relationships that already exist in the context of the business. A business context offers threat actors several particular benefits that consumer fraud may not:

- There are ample opportunities for pretexting, such as impersonating a vendor, customer, or coworker.
- Open-source information is often available for reconnaissance, target selection, and crafting more convincing attacks.
- Payouts from successful scams are likely be higher from businesses than from consumers.

BEC campaigns use a wide variety of scams, attempting to steal money, sensitive information, or both:

- Gift Card Fraud
- Payroll Diversion / Direct-Deposit Scams
- Invoice Fraud
- Aging Reports
- W2 Scams
- Advance Fee Fraud (419 Scams)

Below is real-world example of a BEC email conversation illustrating the exploitation of the CEO-to-employee relationship, in order to acquire funds via gift card. Cofense researchers replied to each of the threat actor's emails, expressing a willingness to help and asking for further instructions.

BEC Email Text	Synopsis
Hello [name], I got a request for you to handle discreetly. Let me know if you are available for this I will be going into a meeting in a few minutes with no calls kindly respond back via email. Kind Regards, [Name of company CEO].	The threat actor impersonates the CEO of the intended victim's company. This initial email does not include a specific request. Instead, the threat actor waits for a reply, which will indicate that the victim is willing to cooperate. The threat actor also adds a story about being in a meeting to discourage the victim from trying to contact the real CEO directly via a phone call.
Here's what I want you to do for me because I'm a little busy right now. I have been working on incentives and I aim at surprising some of our diligent staff with gifts today. This should be confidential until they all have the gift as it's a surprise. Let me know if you can take care of this So I'll send the rest of the details	After receiving a positive reply, the threat actor tells a story that explains a need for secrecy. They continue to keep the specific details of their request secret until they get one more reply.
Great! I need you to help purchase 10 pieces of Google play Gift Cards in all $100 face value A total of $1000 for the set of staff I have in mind, I need you to keep this on the low till I reveal the beneficiaries. To make things easy, Scratch off the back of the gift cards, take a clear photo of each gift card showing the pins and email the images to me here with the receipts for reimbursement.	The threat actor finally reveals what they want: $1,000 in prepaid gift cards for the Google Play store. If the victim really paid for the cards and sent photos of the card PINs, the threat actor would be able to redeem them. The threat actor reinforces the desire for secrecy and speed, encouraging the victim to carry out the purchase before they recognize the fraud. They also repeat that the victim should reply to the email thread, so that they continue to email the threat actor rather than the real CEO.

I'll need this done as soon as possible. Let me know if this can be done,	
Did you get the cards? I'm still waiting for your email	This email arrived several hours after the last reply. The threat actor keeps the pressure on, as they seemed so close to success.
This is a reminder of the cards you were suppose to get for me yesterday, I'm still waiting for your email.	This final email arrived the day after the initial conversation. After this point, the threat actor disengaged.

Table 1: Messages from a BEC threat actor.

Trends in Real-World BEC Campaigns

While the specific conversation above illustrates some common tactics and techniques, it is helpful to understand just how common these tactics and techniques are. To help our customers better understand BEC threats, Cofense analyzed hundreds of BEC emails that reached corporate inboxes in March and April of 2022, identifying noteworthy trends in the campaigns. We recorded key details about each campaign, including the BEC method, the sending email address, and whether the initial email included the details of the threat actors' request. For about half the campaigns, we engaged with the senders to find out how much interaction it would take to arrive at their request. We found several key takeaways in our analysis.

BEC Emails Commonly Include Language of Ingratiation, Urgency

As our BEC example illustrated, threat actors often try to inspire both trust and urgency in their intended victims. We analyzed the BEC threat actors' initial emails to find the most common trigraphs (three-word phrases).

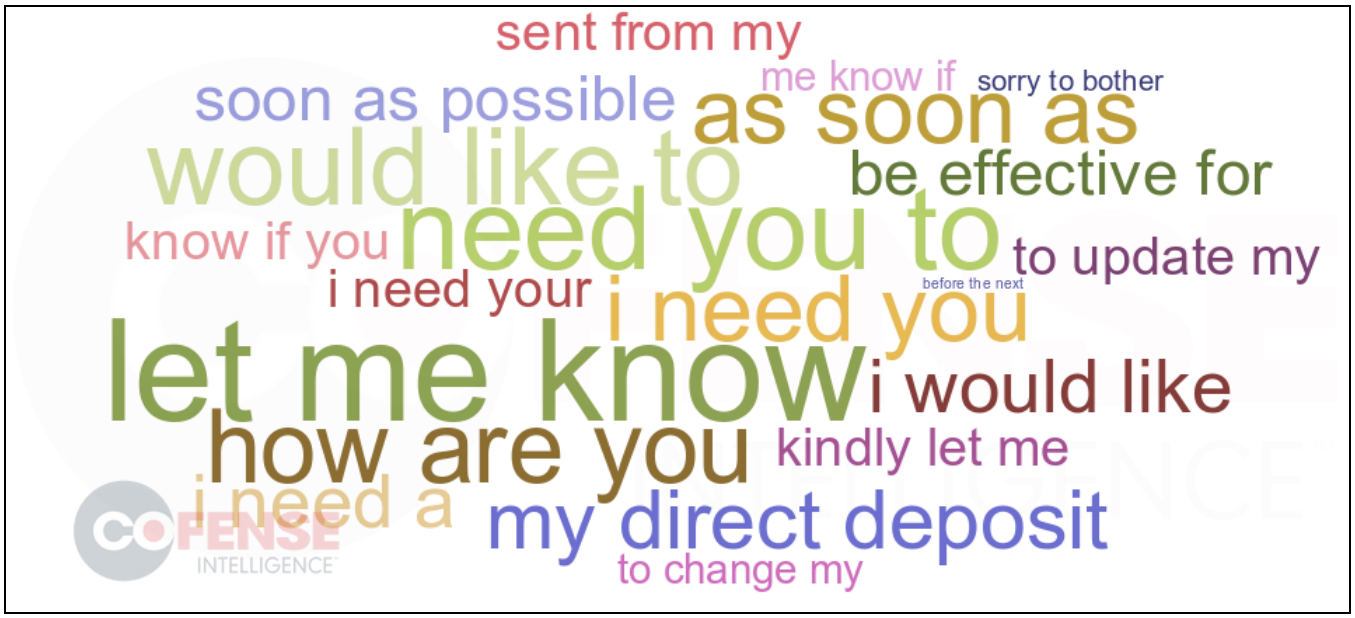

Figure 1: Word cloud of the most common trigraphs in initial BEC emails.

A few common themes stand out:

- Ingratiating phrases like “sorry to bother” make the threat actor seem friendly. Asking for a favor (“kindly let me”) adds to the impression that they are nonthreatening.
- Threat actors use language that creates a sense of urgency (“I need you”, “soon as possible”) to complete the attack before the victim realizes anything is wrong. They use it even when they’re only asking for a reply—before they reveal the details of their scam.
- Direct-deposit scams were the only BEC method that commonly included the narrative in the initial email, making phrases like “to update my” and “my direct deposit” to appear among the most common trigraphs.

Threat Actors Wait for First Reply Before Making Their Move

Only 36% of BEC campaigns included the entire request in the first email. The rest required some engagement from the victim before the threat actor would give the full details. Our study included responding to those emails to find out how much effort the threat actors were willing to put into the conversation before they revealed the request.

For the emails we replied to, the response rate from threat actors was 58%. The overwhelming majority of the threat actors who responded made their request in the first reply. Very few of them took more than two replies.

Replies Until Request	Share
1	89.1%
2	5.4%
3	2.7%
4+	2.7%

Table 2: Number of replies for threat actors to make their request (among campaigns requiring engagement).

For BEC threat actors, there are some benefits to hiding the details of their scheme at first. Getting replies from an intended victim may help the threat actor build rapport, identify other targets, and assess how much they can steal. Furthermore, one-off BEC emails are more likely to be detected and reported immediately, which would “burn” the threat actor’s email accounts and bank accounts. Keeping the details out of the first email makes them less likely to be reported. However, extended conversations may also give the intended victim time to recognize the fraud, so threat actors have to strike a balance between too little conversation and too much. Based on our data, most of them deem one reply to be effective.

Payroll Diversion and Gift Card Scams Are Most Common

Two BEC methods stood out as particularly common in the analyzed set of emails that reached inboxes. Payroll diversion was the top method by far, followed by gift card scams. Several factors may contribute to their high rank:

- Threat actors can use public information like company websites or social networks to identify targets and create their pretext. For example, they might locate a member of a company’s human resources staff, then find a different employee to impersonate for a payroll diversion scam.
- Most other BEC methods require extra steps before a payout can occur, such as the two-step process of an aging report scam followed by invoice fraud. Payouts from gift card scams and payroll diversion scams are more direct.

- The top BEC methods may simply represent blind spots in most organizations' awareness of threats.
- In the case of gift card scams, payouts can be substantial while remaining difficult to trace or reverse. The amounts that threat actors requested in our research ranged from $200 to $3000, averaging almost $900.

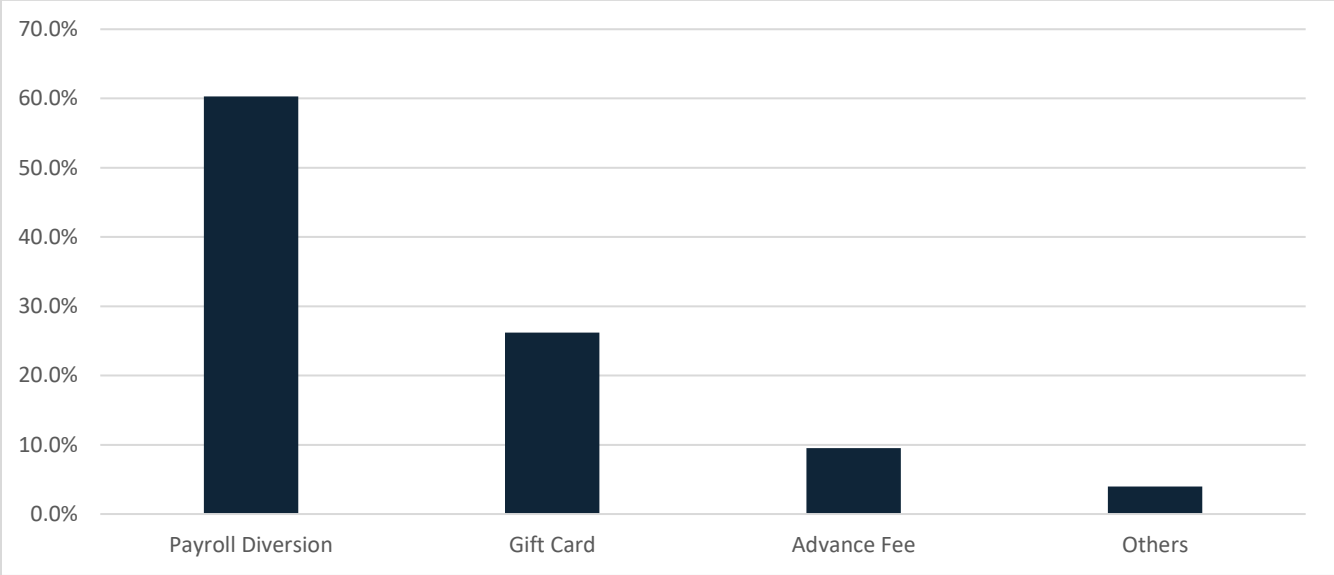

Figure 2: Share of BEC methods in our study.

Advance fee fraud followed as the third most common BEC method in our research. Since they do not involve other members of an intended victim's organization, they tended to be more randomly targeted. Other methods, such as cryptocurrency scams and invoice scams accounted for about 4% of the campaigns.

BEC Emails Are Commonly Sent from Free Webmail Accounts

As we discussed above, most BEC threat actors prefer conversations over one-off emails. Unlike the threat actors behind credential phishing and malware campaigns, BEC threat actors cannot simply send an email and hope that the targeted user opens it. Since they desire two-way communication with the user, they need email accounts that can send and receive reliably, rather than send-only tools like web-based mass-mailing scripts. In the analyzed set of emails reaching inboxes, the threat actors used a few different types of email accounts.

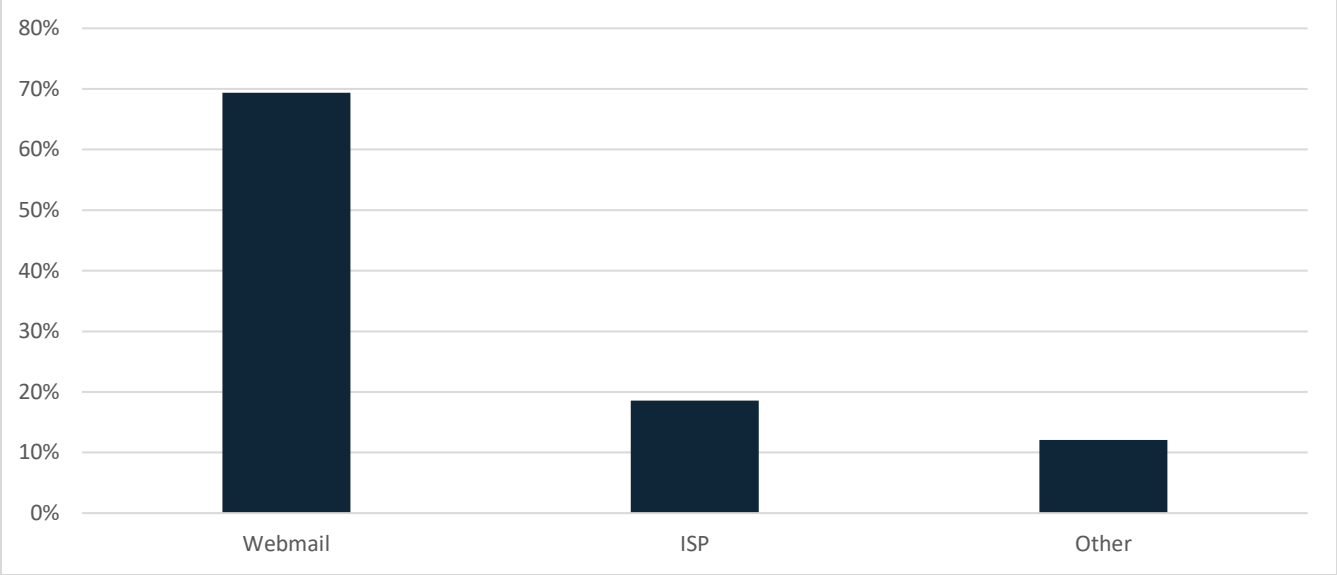

Figure 3: Share of email sender types in our study.

The majority of the emails came from free webmail services—nearly 90% from Gmail accounts. Microsoft, Yahoo, and an assortment of other free services represented the rest of the webmail group.

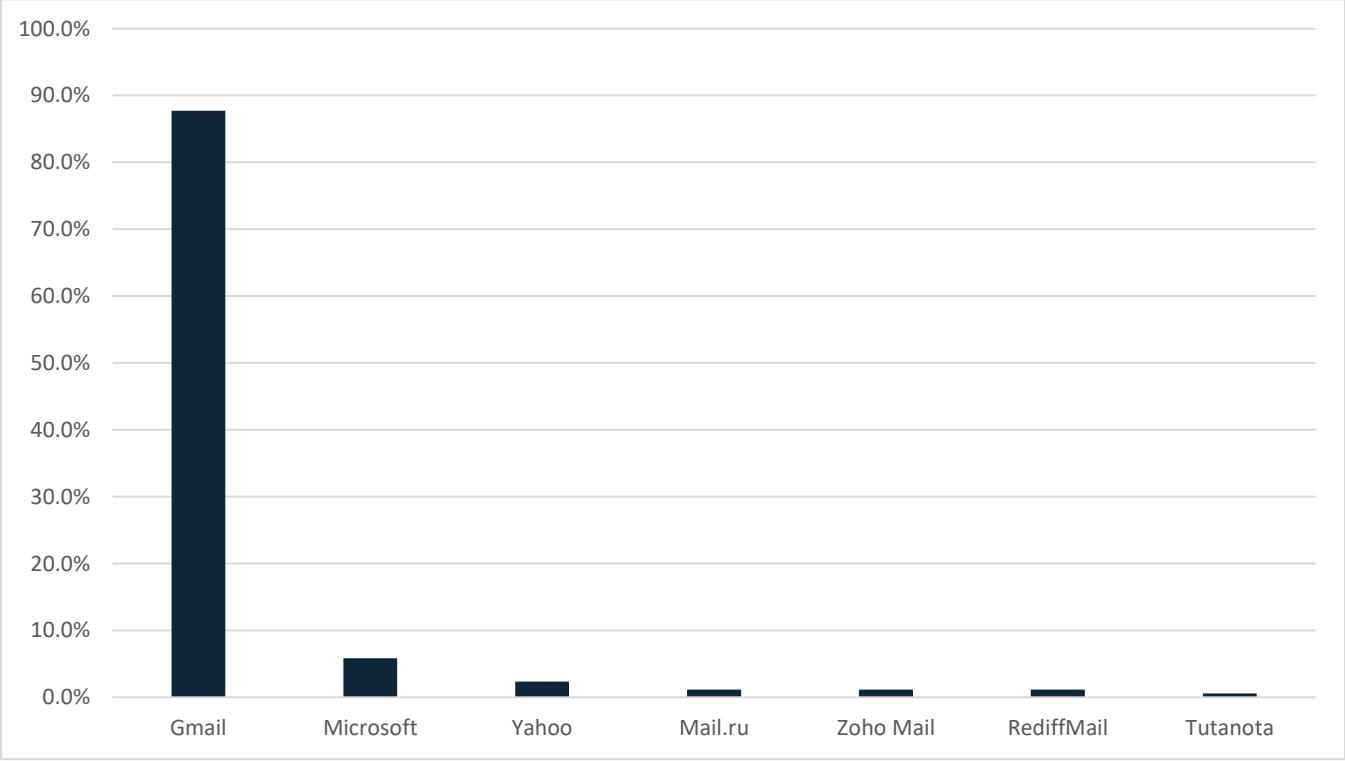

Figure 4: Free webmail providers sending BEC emails.

Email accounts hosted by internet service providers (ISPs) were the next most common group. Few if any ISPs offer free email, so the threat actors are likely using hacked customer accounts. The remaining senders consisted

of addresses at educational institutions, legitimate websites, and domains that no longer resolve. The latter may represent domains registered by threat actors for the sole purpose of BEC campaigns, or they may be legitimate domains that were hijacked. In any case, the most popular tactics are to abuse free webmail services or use stolen email accounts.

Impact and Recoverability

According to the IC3, reported losses from BEC scams exceeded $43 billion between 2016 and 2021, with reports from all 50 states as well as 177 countries. The period included a 56% increase from mid-2019 to late 2021. However, even these figures likely underestimate total damages from BEC. Smaller-scale incidents may go unreported as companies choose to simply write off the loss. In addition, successful attacks can lead to related crimes that may not be counted in BEC statistics, such as identity theft committed after a W2 scam.

The possibility of recovery from BEC attacks depends on the type of scam and the amount of time before it is detected. Most of the scams ultimately lead to a transfer of funds from the victim's bank account to an intermediate account. The funds are steadily removed from the intermediate account, in amounts small enough to avoid financial reporting requirements. If law enforcement authorities are notified quickly enough, they may be able to freeze the intermediate account so that remaining funds can be returned to the victim.

Scams that use a victim's personal payment card, like gift card scams, are more complicated. In the United States, if a threat actor uses a payment card, the card provider is responsible for the losses. But if the threat actor convinces the victim to use the card willingly, then the victim bears the responsibility.

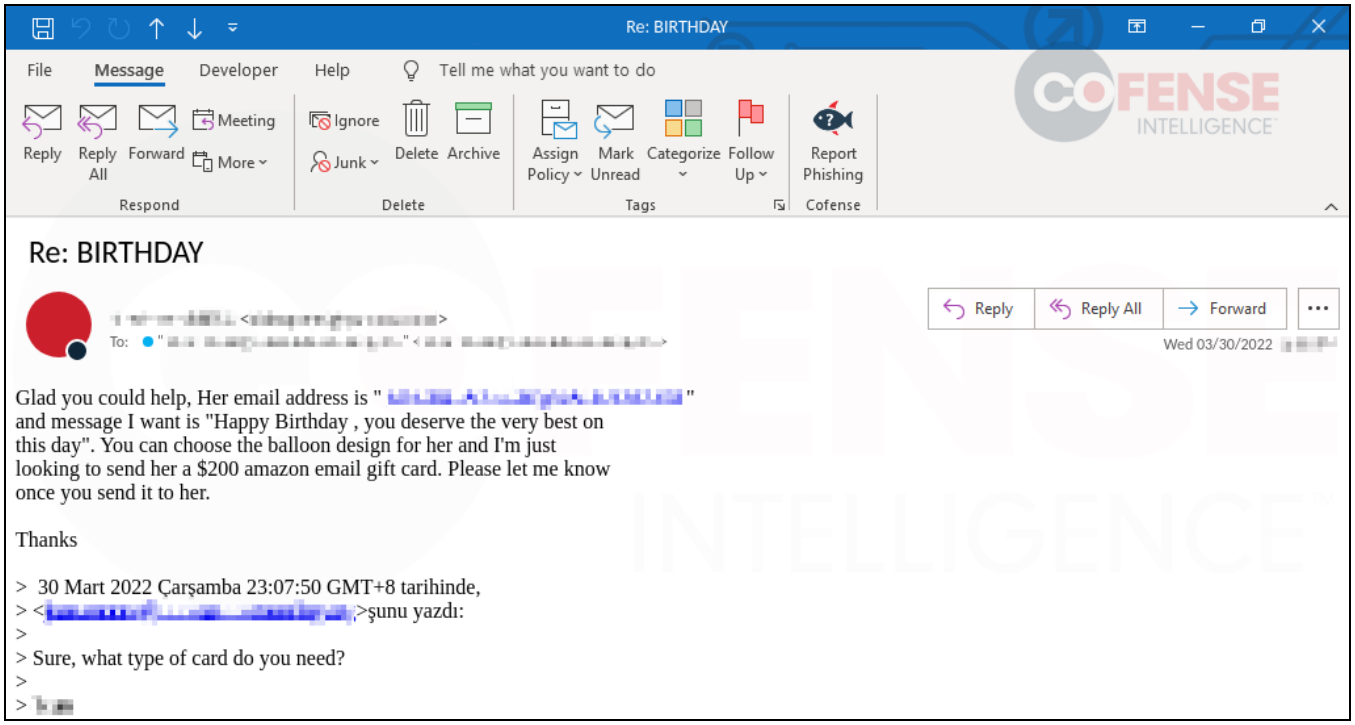

Figure 5: A BEC email attempting to get the victim to purchase a birthday gift card for a coworker. Note the Turkish language in the date and time information in the reply chain.

In cases of information theft or cryptocurrency payments, virtually no recovery or limitation of damage is possible.

Mitigations

BEC threat activity causes an enormous amount of damage, and requires significant skills on the part of the threat actor in several areas, including social engineering, financial crimes, and maintaining criminal networks. Even so, BEC emails themselves are technologically unsophisticated compared to other phishing threats. They don't involve malware or credential phishing pages, making it harder for automated defenses to detect and block them. Since they exploit a victim's trust, the best mitigations are user education and clearly-defined processes for verification of financial requests. For example:

- Maintain a set of verified contact information to use with wire transfers.
- Only allow payroll updates to be performed using a human resources portal, never via email or phone.
- If gift card purchases are ever required, establish a clear process to do so. If not, warn employees that they will never be asked to do it.
- Work with banks, customers, and vendors to verify accounts and establish a multi-party confirmation process for updating account details.

In case of a successful BEC compromise, always report details to law enforcement authorities such as the IC3. Even if a loss cannot be recovered, the information can help authorities direct their resources and advise the public on current threats.

Appendix A: BEC Methods

BEC campaigns use a wide variety of scams, attempting to steal money, sensitive information, or both:

Gift Card Fraud

In gift card scams, the threat actor impersonates a high-ranking company executive. Citing an emergency or some other false pretext, they ask an employee to use their own personal money or credit to purchase gift cards or similar items, promising to reimburse them later.

Payroll Diversion / Direct-Deposit Scams

Threat actors contact human resources staff, impersonating another employee of the company. They ask to update the destination bank account for the direct deposit of their paychecks. If successful, weeks can go by before the attack is detected.

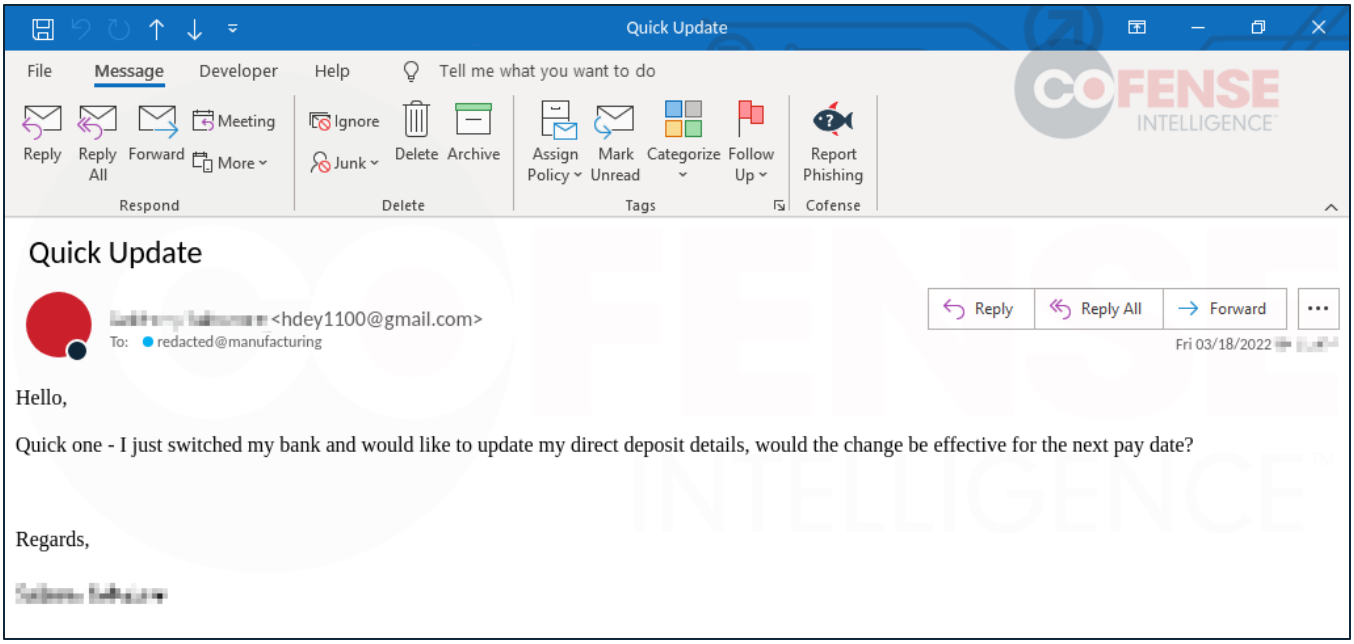

Figure 6: A payroll diversion BEC email.

Invoice Fraud

Threat actors forge an outstanding invoice to the victim company, often threatening legal action if payment is not made promptly. This type of scam can be made more convincing via the use of stolen email content or fraudulently obtained aging reports, described below.

Aging Reports

Threat actors request a list of customers with outstanding payments due to the victim company. If they obtain the list, they contact the customers and perform invoice fraud. Whatever payment was due to the victim company, they arrange to be paid to their own account instead.

W2 Scams

Using a pretext of accounting or tax preparation, the threat actor requests employees' W2 forms, which contain sensitive information. If successful, they can use the information to commit identity theft or other fraud against the employees.

Advance Fee Fraud (419 Scams)

The threat actor promises the victim a share of a large amount of money in return for an advance payment, which they claim is needed to obtain the money. Threat actors often claim to be foreign dignitaries or members of royal families as part of their pretext.