Is That Email Really From "The Boss?"

The Explosion of Business Email Compromise (BEC) Scams

BBB International Investigations Initiative
BBB Chicago bbbinfo@chicago.bbb.org
BBB Dallas info@nctx.bbb.org
BBB Omaha info@bbbinc.org
BBB San Francisco info@bbbemail.org
BBB St. Louis bbb@stlouisbbb.org

BBB International Investigations Specialist
C. Steven Baker stbaker@bbbinc.org

Issued: September 2019

If your boss sends you an email, would you ignore it? Scammers know you probably won't, and that has helped them bilk businesses and other organizations out of $3 billion since 2016 through email scams and attempt another $23 billion.

Business email compromise (BEC) scams target specific individuals with emails that direct them to send money to "new" bank accounts for trusted business leaders, partners, customers, employees, or home buyers. BEC fraud has resulted in more losses than any other type of fraud in the U.S, according to the Federal Bureau of Investigations (FBI). This serious and growing fraud has tripled over the last three years and jumped 50% in the first three months of 2019 compared to the same period in 2017. In 2018, 80% of businesses received at least one of these emails. To thwart scammers, businesses need to improve internet security, employee training and general awareness.

There have been significant efforts to prosecute those behind this fraud.

- On Aug. 22, 2019, 80 defendants were indicted in Los Angeles for BEC fraud in a major effort led by the FBI. Most of the defendants are Nigerian nationals, and this group is responsible for at least $6 million in losses.
- On Sept. 10, 2019, a worldwide law enforcement effort yielded 74 arrests for BEC-related fraud in United States, 167 in Nigeria and 40 in several other countries. The operation resulted in the seizure of nearly $3.7 million in assets from the fraudsters.

What are business email compromise scams?

Business email compromise fraud is an email phishing scam that typically targets people who pay bills in businesses, government and nonprofit organizations. The scammer poses as a reliable source, such as the chief executive officer (CEO), who sends an email from a spoofed or hacked account to an accountant or chief financial officer (CFO). The email asks them to wire money, buy gift cards or send personal information, often for a plausible reason. If money is sent, it goes into an account controlled by the con artist.

The FBI's Internet Crime Complaint Center (IC3) identifies at least six particular scam variations as BEC and email account compromise (EAC) frauds. This activity is also called "spear phishing" — a targeted phishing attack that directs bogus emails to a specific individual, such as a company's CFO. It also goes by "CEO fraud," "mandate fraud," "whaling" and, particularly among Nigerian fraudsters, "wire wire." For purposes of this study, we simply refer to it as BEC fraud.

The FBI recognizes at least six types of activity as BEC fraud. The types differ by who appears to be the email sender:

1. The CEO directing the CFO to wire money to someone.
2. Vendors or suppliers asking that invoice payment be made to a different bank account.
3. Executives requesting copies of employee tax information such as W-2 forms in the U.S.
4. Realtors, title companies or lawyers redirecting proceeds from sales of homes or other real estate into a new account.
5. Senior employees seeking to have their pay deposited into a new bank account.
6. An employer or clergyman appealing to the recipient to buy gift cards on their behalf.

Each scenario is discussed in this study.

Criminal groups, typically from Nigeria, often engage in all BEC fraud types and use similar tactics between the types. They identify key individuals by name and organization so they can direct emails to people they believe will send money to bank accounts the criminals control or purchase gift cards on their behalf.

"Over the last several years, business email compromise (BEC) has quickly become one of the most profitable forms of cybercrime in the world," says Ronnie Tokazowski, Senior Threat Researcher at Agari, an email security solutions provider. "As we continue to study and understand it, threat actors will continue to evolve, and we must adapt to their changes faster in order to be successful in combating this ever-evolving threat."

BEC fraud affects both big and small organizations. And unlike many other online frauds, these are made to look like they are sent from organizations in addition to individual consumers.

How often does this happen?

BEC fraud is the biggest source of losses reported to the FBI's Internet Crime Complaint Center (IC3) and has been for several years. The Financial Crimes Enforcement Network (FinCEN) has compiled Suspicious Activity Reports filed by banks and reports that the value of attempted BEC fraud has increased from $110 million per month in 2016 to $301 million per month in 2018.

In a July 2018 alert, IC3 estimated that between October 2013 and May 2018, domestic and international losses and attempts to get money totaled more than $12.5 billion.

IC3 receives complaints from all 50 states and 150 countries, but most come from U.S. victims. Canada's Competition Bureau has also warned about BEC fraud. The Canadian Anti-Fraud Centre collects complaints on this subject. The complaints received may be only the tip of the iceberg; much of this fraud is not reported.

U.S.	Complaints	Losses reported
2016	12,005	$360.5 million
2017	15,690	$676.2 million
2018	20,373	$1.3 billion
2019 (Jan-May)	10,603	$750.3 million
Total	**58,571**	**$3.1 billion**

Canada	Complaints	Losses reported
2016	515	$6.8 million
2017	381	$11.8 million
2018	250	$6 million
2019 (Jan-May)	58	$9 million
Total	**1204**	**$33.6 million**

BEC fraud operates beyond the U.S. and Canada. BEC losses in Australia in 2018 exceeded $60 million. This was a 170% increase over 2017, when losses were $22.1 million. In addition, a recent news program in South Africa covers the problem this fraud is causing there.

One study found that the average loss involving wire transfers is $35,000, while the average loss via gift cards is $1,000 to $2,000. Perhaps the largest known BEC fraud was perpetrated on Google and Facebook, which collectively lost more than $100 million before the fraudster was arrested in 2017.

Insurance usually does not cover these losses. There are recent reports that several businesses in Australia have declared bankruptcy due to BEC vendor fraud.

Why does BEC work?

It may be useful to think about another group that uses deception professionally – magicians. Although we know that they do not employ occult powers to perform their tricks, any good magician can do things that seem unbelievable. But when they explain their tricks, they seem obvious after the fact. We simply didn't know where to look or what the "catch" was. Magicians purposely move rapidly through their tricks to keep us from focusing on what is really happening.

The same may hold true with BEC fraud. Normally, there is no reason to closely examine an email received from a superior. If there is nothing that immediately causes suspicion, we tend to believe the email is from the person whose name is in the sender line and focus our attention on getting through the dozens of emails received daily.

While this fraud employs many clever techniques to identify key employees and send emails directly to them, what really makes it work is "social engineering," a euphemism for deception. The emails are carefully crafted to look believable, and they almost always claim a sense of urgency.

BEC attacks are 10 times more likely to produce a victim if the target answers an initial probe email, such as "Are you at your desk to make a payment?" One email security company has tried to identify the top subject lines used in BEC, with a breakdown by frequency:

- **"request"** 36%
- **"follow up"** 14%
- **"urgent/important"** 12%
- **"Are you available?" or "Are you at your desk?"** 10%

Internet Security company KnowB4, one of many companies that train employees about email fraud, finds that untrained employees will open and take some action with a bogus phishing email 30% of the time. After training and after sending some bogus emails to test and see if people respond, only 2% interact with a bogus email. It is like the aforementioned magic trick; once they know about and understand the danger, they rarely fall for these.

One problem with training is that many corporate leaders, who are often the targets of BEC fraud, mandate such training but don't take it themselves, perhaps believing that they are too busy or that they are too smart to fall for such schemes.

There may be other reasons this fraud is successful. Some BEC emails really do come from the CEO's email account. They may come when the sender is out of the office, and the emails commonly say that the CEO is busy and does not want to be disturbed. The request is commanding, and employees who are nervous about bothering a busy CEO may decide to just follow orders and move quickly.

The fraud gangs also seem to have determined the times when their fraud is most likely to be successful. Many BEC attacks are timed to hit organizations around major holidays, when there are more temporary employees, the senior executives are out of the office and people are reluctant to call them.

Not every attempt needs to succeed. Agari reports that success rates for each email are .37%, or about one time for every 300 attempts. The fraudsters know that most of the time these tactics will fail, but if they succeed even one time in 300, they can still bring in some serious money.

Anatomy of a Business Email Compromise Fraud

There are essentially three steps to operating a BEC fraud.

1. Fraud gangs need the names of people within an organization, their job function and their email username and password.
2. They must send emails directly to people, impersonating a trusted superior or partner and seeking money.
3. They need a way to obtain money sent by victims. Each of these are specialized functions, and fraud gangs may even hire third parties to help them with these efforts.

How do fraudsters know who is who in an organization?

In order for a BEC fraud to be effective, fraudsters need to know:

- Who is in charge of the organization so they can impersonate them
- Who controls the money and can pay vendors or do wire transfers.

There is a great deal of information about organizations readily available online. Open source tools help fraudsters find the information they need. Key information about individuals can sometimes be found on an organization's own website, Facebook page or on LinkedIn.

Another common source is a lead generation service. Some fraudsters have signed up for consecutive seven-day free trials of such services, while some Nigerian gangs use Rocketreach, Crunchbase and Guidestar to find victims.

This fraud affects both large and small organizations. Internet security firm Agari has even tracked one Nigerian gang doing BEC fraud and found that they were collecting information on 30,000 individuals in 13,000 organizations and 12 countries. These included charities and nonprofits such as Boy Scouts of America, a Midwestern archdiocese of the Roman Catholic Church, YMCA chapters and, in the UK, the Salvation Army and a leading children's charity. In addition, this group targeted educational institutions, and they had information on 1,800 individuals at 660 organizations, ranging from K-12 schools to universities.

How do scammers impersonate people with email?

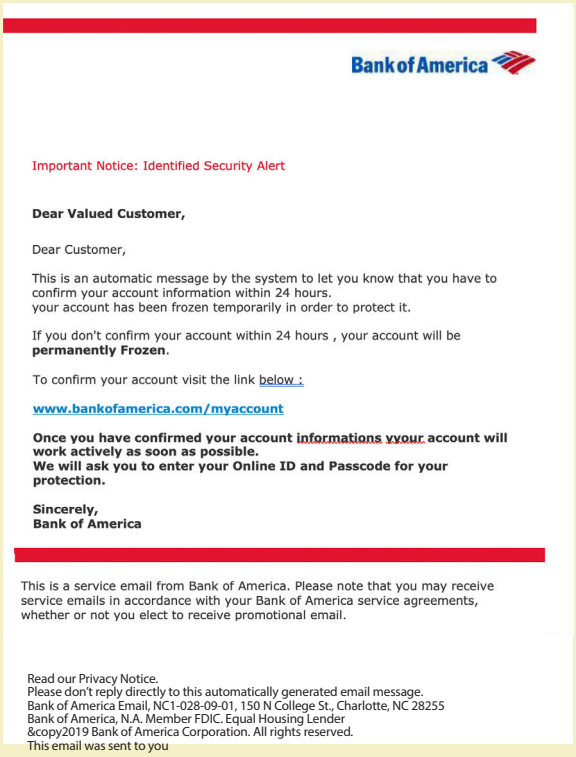
There are three basic ways that fraudsters can send direct email to people pretending to be from someone else:

1. They can just send an email from any email address,

Phishing Email

Major illicit enterprises try to obtain our online login information or trick us into opening a document that contains links to malicious software. Millions of these emails go to all of us. Spam filters at most email services capture many of these, but we are all likely to see them at some point.

Many of us have dozens of different online accounts that each requires a username and password. These range from online newspaper subscriptions to accounts at online retailers like Amazon or eBay, online personnel or retirement accounts and banking and bill paying. Often people use the same usernames of passwords for many of their accounts. And once those "credentials" are stolen, they can be tried at many different sites and used for a variety of frauds, including but not limited to BEC.



Bank of America

Important Notice: Identified Security Alert

Dear Valued Customer,

Dear Customer,

This is an automatic message by the system to let you know that you have to confirm your account information within 24 hours.
your account has been frozen temporarily in order to protect it.

If you don't confirm your account within 24 hours , your account will be **permanently Frozen.**

To confirm your account visit the link below :

www.bankofamerica.com/myaccount

Once you have confirmed your account informations yvour account will work actively as soon as possible.
We will ask you to enter your Online ID and Passcode for your protection.

Sincerely,
Bank of America

This is a service email from Bank of America. Please note that you may receive service emails in accordance with your Bank of America service agreements, whether or not you elect to receive promotional email.

Read our Privacy Notice.
Please don't reply directly to this automatically generated email message.
Bank of America Email, NC1-028-09-01, 150 N College St., Charlotte, NC 28255
Bank of America, N.A. Member FDIC. Equal Housing Lender
&copy2019 Bank of America Corporation. All rights reserved.
This email was sent to you

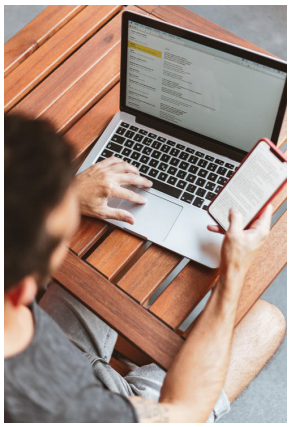
Besides grammatical errors, there are other red flags in this email. A closer look at the "from" line of this email showed that it was really from a German email address, abi-abendrothe@t-online.de. In addition, hovering the cursor over the link provided shows that this is not really a Bank of America link.

Efforts like those of the Anti-Phishing Working Group track the volume and trends of such email. Over 80% of these attacks are aimed at the U.S. One study found that 25% of such emails evaded spam filters and were tagged as clean by Office 365 Exchange Online Protection.

Some types of fraud send emails that contains harmful malware. That tactic appears to happen infrequently with BEC fraud. However, it is always important to avoid clicking on the links in suspicious emails.

but have the name of a real person appear in the "from" line.

2. They can set up a domain name similar to that of a real company and create an email address that looks like it is from the person impersonated.
3. They can get access to a real person's email account. Those who are in someone's email account also can have access to all the other email traffic to that person, so for fraudsters it is more difficult but may be more effective in committing fraud.



1. The email isn't coming from the person listed in the "from" line.

Standard internet settings allow those sending emails to have any name they wish appear in the "from" line. Thus, fraudsters may simply send an email that says it is from Eddie Alias in the inbox, but if one looks closely, or hits reply, they can see that it is really from IMAfraud@yahoo.com. One study of BEC gangs found that 82% of the time BEC gangs simply use display name deception. These tactics may be more effective when people are reading emails on their phones or on other devices, where the screen is small and the actual email is hard to read.

So when an email comes "from" a superior or a trusted partner, there is a risk that people will not look closely, especially if it is marked urgent and the employee is anxious to please the supposed sender.

2. Fraudsters can set up an email domain that is similar to the real one.

All email addresses go to, or "@," a domain name, like "example.com," and BEC fraudsters often impersonate those domains. These efforts do not provide real access to anyone else's email, but they are likely very effective in fooling the recipient of the email into believing it is real. Then fraudsters might register the domain name "exarnple.com." Note, that unless you look closely, the eye reads the "r" and the "n" as an "m." These emails may come from CEO@exarnple.com, and those getting the email may not recognize it is not from the CEO of "example.com."

It is cheap and easy to set up such domains, and Proofpoint notes that millions of domains have been registered that are similar to those of real company domains. A large part of these are used to sell counterfeit goods, but they are also a staple of BEC fraud.

Many of the fraudulent BEC domains are attached to servers that can send email but have low volumes of mail coming from them. Because many of the programs that try to detect spam email (such as phishing attempts) try to identify the computers sending large volumes of bogus spam email, they may not recognize and block BEC attempts coming from different domains with smaller email volumes.

3. Fraudsters can log into someone else's email account.

BEC emails may actually come from the email account of the CEO. Fraudsters can simply log in to someone else's email account if they already have their username and password. Usernames and password combinations are frequently obtained through phishing attacks and are readily available for sale on the internet, often on the dark web. Armed with this combination, fraudsters may try to log in at dozens of different websites, a process known as "credential stuffing," and get into email systems.

If fraudsters do not already have login information for an email account, there are other ways to try and get it. For most people, logging into email accounts is a pretty simple process with a username and password. Often the username is simply your email address, which usually consists of some variation on first and last name and the domain name used by the organization. For example, an email to Eddie Alias at example.com would likely be ealias, e.alias, or eddiealias @example.com. If someone already has an email address from someone else at that organization, they can probably guess the correct email address and thus the username.

The second step is to have the password. One way to get access is to use a computer program that just keeps entering password combinations until one works, a process known as a "brute force attack." Some email systems will detect failed login attempts and lock the system, but many don't. Also, many people use the same easy-to-remember passwords, like "password1234," that are easily guessed. One study found that the five most common passwords are: "123456", "123456789", "qwerty", "password" and "111111."

Actually getting access to someone else's email seems to occur in only a small percentage of BEC cases, but the advantages are very large. It allows fraudsters to read all of the email and learn about ongoing transactions, such as real estate closings.

Fraudsters can reset email system "tools" so that they get copies of all incoming and outgoing email and make sure that the real owner of the email account does not recognize that there is someone else in their account. And if they are in the email account, they probably also have access to the person's calendar and may know when top executives are due to be out on travel and can't be reached by phone to confirm a transaction.

How do fraudsters obtain the money?

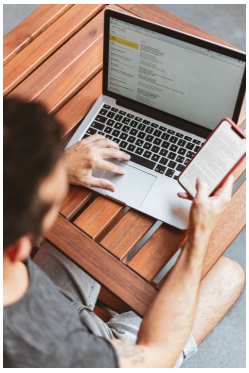
Romance fraud victims are key players in BEC fraud. Much of the time, money stolen in BEC fraud first goes into bank accounts opened by romance fraud victims, who then send the money out of the country. These victims are used as "money mules" to launder money or transport drugs for a variety of different frauds. Romance fraud victims believe they are helping out a "loved one" and most don't realize

that they are assisting with fraud. FinCEN reported recently that 73% of the time the money from BEC fraud first goes into domestic "money mule" accounts, and 27% of the time it goes to foreign banks in countries such as China, Malaysia or other locations in Asia.

Fraud gangs use romance fraud victims because they are likely to be reliable and unlikely to steal the money. In addition, romance fraud victims do not know the real names of the fraudsters, and so they cannot reveal that to law enforcers trying to follow the money. Another BBB study deals specifically with romance fraud victims used as money mules. Many prosecutions of BEC have led to romance fraud and included criminal charges for that fraud as well.

Keeping track of these mules, getting them to do the work and ensuring that the money is collected is a key to making BEC frauds successful.

Different kinds of BEC frauds



1. CEO – CFO

The classic BEC fraud involves an email that looks like it is from the CEO to the chief financial officer (CFO) or another person who can send wire transfers, asking them to send money right away.

These spear phishing emails also typically try to discourage the recipient from checking back with the CEO. They often claim that the matter is urgent and claim to be in a meeting, or out of the office. Anxious to please the boss, employees may proceed and send the money. There are employees who are new or reluctant to bother a busy boss. They may respond to the request without checking it out first.

From: Robert Smith [president.desk@wp.pl]
Sent: Thursday, May 16, 2019 11:00 AM
To: Chris XXXX
Subject: quick task
Hi Chris

Are you available to run an errand ? I need you to make provision for gift cards for me at any local store around.

Robert Smith

FinCEN reports that CEO email scams have declined somewhat. They say this accounted for 33% of BEC incidents in 2017 but that this figure dropped to 12% in 2018.

2. Vendors

Another way fraudsters use bogus emails to get money is to impersonate a vendor or contractor. FinCEN reports a large recent increase in vendor fraud from 30% in 2017 to 39% in 2018. They believe this is now the most common type of BEC fraud.

There are two main ways vendor fraud can occur.

1. A business may get an email they believe is from a customer placing an order and providing an address where the goods can be delivered. But the goods are actually sent to the fraudsters, or someone working on their behalf, who can receive the goods and then send them on outside the country. This has often occurred with emails that seem to come from colleges and universities placing an order for goods. Public institutions tend to send purchase orders, and these can be found online, altered and used to buy goods. For example, a computer company might receive an order for a batch of laptop computers from a state university, which asks that they be delivered to a satellite location or the address of a drop shipper. The computer company would ship the laptops to a fraudster's

A CEO's story

Steve, the CEO of a credit union in Omaha, was on a business trip when he received a text message from one of his vice presidents that said she received an email supposedly from him. The email read: "Dear Carol, I need you to perform a task for me. Let me know if you are available. Best regards, Steve." Steve told Carol that while the email had his name in the "from" line, he did not send it. A closer look showed that it was actually from m1staff@aol.com.

A month earlier, another senior employee, Tera, received an email that appeared to come from Joe, the credit union's board chairperson. "Hi Tera -- Let me know when you are available. There is something I need you to do. I am going into a meeting now, so just reply my (sic) email."

Tera read this on her phone and didn't detect that it was false, so she replied. A little later she received a response from "Joe": "Can you get this done ASAP? I need a couple of gift cards. There are some listed clients we are presenting the gift cards. How quickly can you arrange these gift cards because I need to send them out in less than an hour. I would provide you with the type of gift cards and amount of each."

Tera forwarded the email to Steve, saying, "I received this weird email from Joe which doesn't seem right? I responded initially to see how I could help and received this subsequent request. How do you want to proceed?"

Steve told her not to proceed. A closer look showed that the email was actually from alexio007@gmail.com.

Pleased that his employees did not send money or buy gift cards and reported the events right away, Steve says he suspects fraudsters found the information they needed to create the bogus emails on the credit union website. He still wonders how they knew he was out of town when one of the emails arrived.

location and then send the bill to the university, which might even pay it if they are not watching carefully.

2. Fraudsters may send emails pretending to be from building contractors or vendors that provide services. They claim to have changed bank accounts and ask that the money to pay their bills be sent to the new account that is controlled by the BEC gangs.

Two vendor fraud scenarios have resulted in major problems not only for businesses, but also for colleges, universities and state and local governments. Information about state and local governments and the contracting process is all available online. Thus, if a city or college were building a parking garage, the information about who got that contract, who approved it and names of city managers or others involved in paying bills might all be readily available over the internet.

Armed with that information, fraudsters could send an email impersonating the building contractor providing a bill, stating that the bank account information where payments are to be made has changed and start receiving payments. If this succeeds once, the fraudsters may continue to receive payments for some time. For example, MacEwen University in Edmonton, Alberta, lost $11.7 million when a BEC email claimed that a vendor had changed its bank account. This is not limited to building contractors, but to anyone else providing goods or services.

In July 2019, there were reports that a North Carolina county government lost $1.7 million to a BEC fraud. In the same month, the Inspector General for the Department of Homeland Security found that several federal agencies had been impersonated in orders for computer equipment and other goods with hundreds of thousands in losses.

The nonprofit Center for Internet Security provides advice on BEC and other cybersecurity threats for state, local, territorial and tribal governments.

3. Tax information

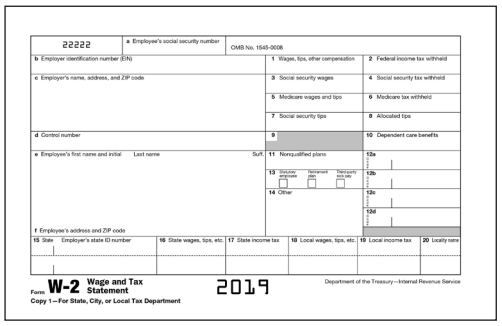
Unlike other types of BEC fraud, this version seeks information needed to commit a different fraud and does not require that a victim send money.

BEC emails may be sent "from" senior executives to human resources directors, claiming that they need employee W-2s -- in the U.S., a form that reports employee wages to the Internal Revenue Service and contain an employee's name, social security number, tax withholding information and overall pay -- and instructing HR to send these by email.

Armed with the W-2 forms, criminals can file bogus tax returns for those individuals, claim refunds and have those refunds deposited on stored value cards or deposited into bank accounts they control.

The IRS says it had a little over 100 reports of this in 2016, but in 2017 that rose to nearly 900. The volume dropped in 2018 to roughly 150, and so far in 2019 the W-2 scam has virtually disappeared.

There are several measures the IRS has taken that may account for the success in fighting this type of fraud. First, they publicized and warned of BEC fraud in a series of alerts. Second, they worked to shut down email addresses and domain names tied to this fraud by contacting service providers and worked with IC3 on another warning. Third, they set up a process and repository (dataloss@irs.gov) to receive information from victim organizations and immediately share it with criminal investigators. These efforts reduced the impact of the stolen data on affected taxpayers. The IRS has also partnered with other agencies and takes part in the BEC working group.



Aggressive efforts to prosecute those involved in stolen identity refund fraud has resulted in dozens of prosecutions, not all of them involving BEC.

Anyone who receives a bogus email asking for W-2 information should immediately report it to law enforcement.

4. Real Estate BEC

Another BEC fraud target involves the proceeds of home sales. When home sales close, buyers typically use bank-to-bank wire transfer to send money to the seller. Or the seller may use the money they get for the house to pay off the mortgage, again by wire transfer. When a home sale occurs, realtors, title companies, lawyers, buyers and sellers often communicate by email. With the introduction of Google Docs and DocuSign, important papers may come as email attachments. Logging into bogus phishing emails and opening those documents can allow fraudsters to steal email login credentials or release malicious malware programs.

Crooks insert themselves into this system to redirect the wire transfer to a bank account that they control. Thus victims may be devastated, losing hundreds of thousands of dollars, and may even be left with nowhere to live.

An IC3 alert from July 2018 states that this problem is increasing rapidly. The alert says that "reports of these attempts have risen 1,100% between 2015 and 2017, and in 2017 alone there was an estimated loss of nearly $1 billion in real estate transaction costs." FinCEN recently reported: "While real estate firms represented 9 percent of all targeted firms in 2017, they accounted for over 20 percent of fraudulent transaction amounts. Real estate firms have the highest average fraudulent

transaction amount of $179,001." Like the other types of BEC fraud, this is a worldwide problem, as illustrated in a New Zealand case.

Real estate fraud is complicated because real estate agents often work from home, change companies from time to time, and thus may have a variety of personal and work email accounts that they use regularly.

For fraud to work in this area, the fraudsters need to know who the parties are, the amount of money involved, and the timing of the closing. This information may not be publicly available. The fraud seems more likely to occur when its perpetrators have actually gotten the information needed to log into the email account of one of the parties. If fraud gangs can read the email of an appraiser, realtor, lawyer, or title company, they can discern who the parties are and get other crucial details. In at least some cases, the fraudsters have waited until the wire transfer instructions were sent (as an email attachment) and followed up a few moments later with a new email claiming there was an error in the previous instructions and providing a new bank account to send the money to.

The real estate industry is understandably concerned about this situation and has been attempting to train realtors to avoid this type of fraud. The National Association of Realtors has issued several educational pieces, which include fraud notices and three videos on recognizing scams, an alert for buyers, and information on how to avoid wire fraud. The CFPB has published a blog post on BEC real estate fraud.

In addition, a consortium of title companies and partners has recently set up a website, stopwirefraud.org, to educate and warn about real estate BEC.

The real estate industry says that wiring instructions should always be confirmed by phone with someone you know.

A realtor's story

Shawn, a real estate agent in Edwardsville, Illinois, sent closing instructions in July 2018 to a buyer for a home she helped sell. On the scheduled closing day a few days later, the buyer received an email appearing to come from Shawn. While Shawn did not send the email nor was it from her true email address, the amount requested was the actual closing price. Here is the email exchange, typos included:

Bogus realtor: "Hello, Please be informed that Escrow requires that you wire funds (($303,855.50) today prior to closing to avoid delay in closing. Kindly confirm if you are sending the wire today so I can provide you with our wire instructions."

Buyer: "I thought the email said I could bring a certified check."

Bogus realtor: "At the moment that's unacceptable because as I explained due to the account reconciliation. This matching process is important, because it proves that the general ledge figure for receivables is justified. However, you are required to send the wire today."

Bogus realtor, later that day: "Please find the wire instructions and endeavor to send me the confirmation of payment once processed."

A PDF attached to the email showed the letterhead of the real company handling the transaction, but the account to which the money was to be wired was fake.

Rather than wire the money as instructed in the email exchange, the buyer arrived at the closing with a cashier's check. Shawn and her client were shocked about the incident and the seller was deeply concerned about the near-loss of so much money.

Shawn wondered how the fraudsters found the actual sales figures, her name, her signature block and the name of the client. Since the bogus email did not come from her real address, she believes scammers may have obtained the information by hacking the buyer's email account.

Shawn reported the incident to her manager and the title company. Her company now warns clients to call the title company or real estate agent if they receive instructions to wire real estate closing money.

5. Direct deposit

BEC fraudsters are also after paychecks that are directly deposited into bank accounts or onto stored value cards. IC3 reports that this problem is increasing rapidly. In 2018, the IC3 received approximately 100 complaints with a combined reported loss of $1 million. This fraud is mainly being done on behalf of senior employees, presumably because they are paid more and so more money can be stolen.

Direct deposit fraud occurs with an email "from" an employee to the Human Resources office saying that the employee has changed banks, attaching a "voided check" for the new account and asking that future paychecks be deposited to the "new" account.

In addition to BEC fraud, the FBI is also concerned about a separate method of stealing paychecks. Fraud gangs sometimes use login information to get access to the employee's online payroll account with the organization and then change the direct deposit information so that it goes to an account they control. IC3 says that the institutions most affected by this scam have been education, healthcare and commercial airway transportation.

Always confirm bank account or contact information changes by reaching out to the old phone or email address to confirm that the employee or client really wants the change as the Postal Service does when someone files a change of address form.

6. Gift cards

BEC fraud scenarios requesting gift card

purchases are exploding but involve smaller sums than frauds involving bank-to-bank wire transfers.

For example, two senior executives at the New York BBB received an email that appeared to be from Steve Bernas, president and CEO of BBB Chicago. The email read verbatim, in part:

"I need you to handle few things for me right away. I'm in the middle of something right now, got a hectic day ahead but I'm looking forward to surprising some of our staffs with iTunes Gift Card today.

I want you to keep it between us pending when they get it. So, therefore, I need iTunes Gift Card of $100 face value each, you can get them in Stores around(Best Buy, WalMart, etc....) (I need 50 pieces of the $100 amounting to $5000). I need you to get the physical card, then you scratch the back out and simply take clear pictures, attach the pictures showing the pins clearly and email them to me here.

I will be balancing up the funding account or Reimburse you immediately I'm done with things here."

The executives recognized the BEC scam and did not comply with the request.

The FTC has warned that many of these bogus emails claim to be coming from priests, rabbis or other clergy members.

An alert issued by IC3 on October 24, 2018, noted a recent explosion in reports to them where people were asked to buy gift cards. Average losses were $900. IC3 also reports that gift card BEC losses continue to grow rapidly and increased 61% in the first five months of 2019 over the same time period in 2018.

January 1, 2018 to May 31, 2018, IC3 BEC gift card complaints:
Victims: 7,391
Loss: $465,586,962

January 1, 2018 to May 31, 2019, IC3 BEC complaints:
Victims: 10,603 (+44%)
Loss: $750,273,494 (+61%)

A business' story

In spring 2019, Jane noticed her bank account was missing a payroll direct deposit entry. The senior executive for a Chicago-based corporation called her human resources department and learned her employer deposited her pay into a new account. They had received an email, supposedly from her, requesting that her pay be deposited into the new account. An email also contained an attachment containing an image of a blank check with the new account information.

After hearing from Jane, the company immediately contacted the bank where the money had been deposited. Fortunately, the bank flagged the account as possibly fraudulent. The company was able to get most of the money back, and Jane received her full pay.

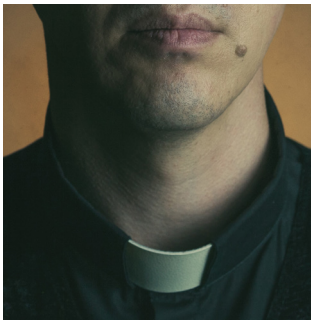
Jane was immediately concerned that she may have been a victim of identity theft. She had recently visited Russia on business, and she was worried other fraudulent activity using her name might occur. Free credit reports showed no problems, but she still placed a freeze on her credit. Fortunately, no other fraudulent activity happened. Her employer now requires employees to appear in person to request direct deposit account changes.

The FTC reports an increase in gift cards being used for many different kinds of fraud, occurring in 27% of complaints where the form of loss was reported – a 270% increase since 2015.

In the U.S., the most common gift cards used by fraudsters are iTunes and Google Play cards, Walmart, Target and Home Depot. Victims are usually asked to buy gift cards from Steam, iTunes and Google Play, according to Canadian law enforcement.

Fraudsters don't need to have the physical cards to get the funds. Instead they ask victims to scratch off the back of the card to reveal the code, take a photo of those numbers, and email or text the numbers back to the fraudster.

There are online marketplaces where people can redeem gift cards. Agari reports that one Nigerian BEC fraud gang enters the codes into the website of Paxful, which converts them to bitcoin. The bitcoin can then be converted into currency and deposited into the bank accounts of the fraud gangs. Agari reports that a gift card can be redeemed, converted, and placed in a bank account in Lagos, Nigeria, in less than four hours.



Agari also suggests that much of the increase in BEC gift card fraud emanates from Africa, noting: "Paxful recently told the online media outlet CoinDesk that it averaged $21 million a week in transactions in 2018—up from $8.5 million in 2017. It attributed the growth in part to its user base nearly tripling in Ghana and more than doubling in Nigeria to more than 300,000 accounts. In fact, African users make up nearly 35% of all Paxful accounts."

Companies that sell gift cards are learning how their products are being used for fraud. Gift cards are often used by other fraudsters who call consumers and claim to be from a government agency such as the IRS, DEA or Social Security. They threaten arrest if victims don't immediately pay money, usually via gift cards. The FTC has posted the phone numbers of companies that offer gift cards so that victims can report fraud to them.

Apple recently instructed its employees to tell customers that its gift cards cannot be used to pay taxes or purchase non-Apple electronics and hardware. App Store & iTunes Gift Cards can be used only to purchase goods and services from the iTunes Store, App Store, Apple Books, for an Apple Music subscription or for iCloud storage. Apple Store Gift Cards can be redeemed only on the Apple Online Store and at Apple retail stores.

Who is responsible for BEC fraud?

At least 90 people have been arrested or charged for BEC fraud in the U.S. over the last three years, and the majority of the defendants in those cases are of Nigerian origin. There is broad consensus among law enforcement and internet security companies that 90% of BEC groups operate out of Nigeria. Other Nigerian fraud groups operate from the U.S., Canada and many other countries around the world. Ghana is also a significant source of activity. IC3 reports that the gangs may also work with Eastern Europeans or other organized crime groups.

Nigeria has a long tradition of consumer fraud. It also has a great deal of political corruption, which may help shield fraud operators. Over the last 20 years or more, many educated Nigerians have left the country and now live in the U.S., Canada, Malaysia, China, India and other countries. Some of these individuals are actively involved in a worldwide network of fraudsters.

Most people have encountered the Nigerian "dead dictator" letters and emails, written in poor grammar and wildly unbelievable. These continue to draw victims into elaborate fraud schemes. Unfortunately, there may be a tendency to conclude from these that the fraudsters are unsophisticated, and their frauds are easily avoided by exercising just a smidgen of common sense. Both of these are untrue.

Many Nigerian fraudsters have college degrees. The frauds they operate are well organized. Today these groups use computer programs to correct grammar, hire professional writers, and operate organized crime businesses.

In addition, at least some of these activities are controlled by violent organized crime groups like Black Axe, which was formed on college campuses in Nigeria but now operates around the world, including in the U.S. and Canada. There are reports that Black Axe is deeply involved in BEC fraud as well as working with the mafia and controlling prostitution in Italy. One internet security company has issued a report looking closely at this phenomenon.

A close look at one BEC group

Internet security company Agari has issued several fascinating reports looking closely at who is involved in BEC gangs, how they evolved and how they operate. One, which they dub Scattered Canary, apparently began with one young man and a mentor in 2008. The main player, "Alpha," began in 2008 operating Craigslist frauds involving fake checks, a topic of an earlier BBB study. With eight victims per month, he was making $24,000 a month.

Alpha then branched out to do romance fraud, and in 2015 he began targeting organizations with BEC fraud. The romance fraud victims provided key help by setting up bank accounts, and another person joined the group to manage this process, with the title "mule herder."

As the group grew, they also engaged in a large phishing effort, using a Google Docs phishing page to get email login credentials. They gathered more than 3,000 account credentials from these efforts, almost all in the U.S. and Canada. In addition, the group signed up for several seven-day trials at Lead411.com to gather information on potential victims. They also began registering domain names for their efforts, so that BEC emails would look real. The group now numbers at least 35 people.

In addition to the group's BEC activities, Scattered Canary continued to engage in romance fraud, fake check frauds, filing bogus tax returns to get refunds applying for benefits from social security. Scattered Canary also sought FEMA disaster funds, "sold" nonexistent vehicles advertised for sale on the internet and ran mystery shopping frauds. They expanded BEC efforts to include direct deposit and gift card fraud. They laundered the gift cards through Paxful.

Scattered Canary also outsources some of its efforts to develop leads and template emails. This is a highly organized enterprise, and it is just one of hundreds of such groups.

Agari also suggests that instead of a focus just on a particular type of fraud, a more effective approach for law enforcement might be to recognize that these fraud groups are engaged in a wide variety of frauds at the same time, and to consider concentrating efforts on the gangs behind it instead of just concentrating on one type of fraud.

What is being done?

Criminal Prosecutions of BEC

The U.S. Justice Department has been very active in addressing BEC fraud. They have brought at least 22 cases in the last three years, with 453 individuals arrested or charged. One prosecution involved a Lithuanian, but almost all the rest involved people from Ghana or of Nigerian origins. Six of those cases also charged defendants with romance fraud. Losses in those cases were at least $200 million. Many of these cases were announced as part of a collective enforcement effort dubbed "Operation Wire Wire."

A September 2019 Operation Wire Wire follow-up effort, dubbed "Operation reWired," resulted in 281 arrests world-wide. The FBI, U.S. Secret Service, U.S. Postal Inspection Service, ICE's Homeland Security Investigations, IRS Criminal Investigation and U.S. Department of State's Diplomatic Security Service participated in the investigation. State District Attorneys in Texas and Arkansas have ongoing investigations related to this four-month

operation that included cooperation with officials in multiple countries.

Since BEC frauds operate around the world, there have also been investigations or prosecutions in other countries, including Canada, the United Kingdom, Japan, Australia, and Nigeria, as well as two cases in France.

Efforts to recover funds stolen in BEC fraud

The FBI and FinCEN have worked together to freeze bank accounts and get money back to victims of BEC fraud. FinCEN reports that since 2014, it has recovered over $500 million by working with banks, law enforcement and partners in 164 countries around the world.

In addition, IC3 set up an asset recovery team in February 2018 to help recover BEC funds that went into U.S. bank accounts. They report that in 2018 they recovered $192,699,195, for a 75% recovery rate.

Public/private partnerships

Several years ago, Agari's Ronnie Tokazowski set up a BEC working group to share and analyze BEC information, seek patterns of activity, and assist enforcement efforts. The group currently includes over 600 people from at least 35 organizations such as the FBI, the IRS, the Secret Service, Google and a number of internet security companies. Since 2015, this group has "helped stop millions of dollars in wire transfers, taken down thousands of romance accounts and contributed to well over 100 arrests." It received an award for these efforts in October 2018.

New York University and Agari have created a visualization tool, called Beagle, to track connections in data and to help identify BEC groups. It is available for free to law enforcement.

Better Business Bureau

BBB also has been active trying to help address this problem. It has issued past alerts on BEC. In addition, the BBB Scam Tracker system has a category for BEC fraud which collects reports of this type of activity. Moreover, BBB has organized conferences for local business that provides education on BEC fraud and how to avoid it. BBB urges employees at retail locations selling gift cards to warn potential victims that these are commonly used as payment methods for frauds.

Internet security companies

A lot of work in this area has been done by the Internet security industry. In addition to protecting their clients from BEC and other cyber threats, they have also done a great deal of research on this industry and how it operates. Many of those studies are cited in this study.

Banks

A large St. Louis bank calls all of its customers requesting wire transfers to confirm that the request is real and is not for fraud. With these simple phone calls – not emails or texts – they let their clients know that they are watching out for them. They have successfully stopped many BEC frauds with these efforts. Many banks have similar practices.

Recommendations

What can you do to protect your organization from BEC fraud?

All organizations face a serious risk of BEC fraud, and the fraud gangs are very smart and innovative. They need only succeed in a small number of their attempts to make this fraud profitable. And organizations that have not suffered a loss may believe the steps they have been taking are effective, even though the frauds are evolving and increasing.

Some businesses may be concerned that money spent on IT precautions is simply additional overhead. But BEC fraud prevention is just as important as door locks, fences and other efforts to protect physical assets.

However, we can't rely solely on technology to prevent phishing emails. We need to learn how to recognize and avoid responding to them. Fortunately, there are several key steps that are free or cost very little and that will go a long way in preventing BEC fraud.

IT and technical precautions

Require multifactor authentication. First, and perhaps most important, organizations can keep fraudsters from logging into email systems by requiring "multifactor authentication." Examples include sending a text message with a code that must be entered to log in, answering a phone call to a number designated by the user or using thumbprints to unlock smartphones. One very strong system requires a token that continuously generates new number codes that must be entered to log in.

Change settings so that all emails coming from outside an organization are flagged with a warning. Email systems offer features that can help stop BEC emails from reaching inboxes, often available for no cost. For example, one setting identifies emails from outside the organization, and when delivered, a line is added in red type stating: "This email comes from an external email address."

Monitor email rules used when someone else is in an account. In situations where someone has hacked into email accounts,fraudsters often set rules that automatically forward all emails to them and prevent the real email account owner from noticing. Administrator

tools can automatically check for such unusual rules.

Limit the number of times people can enter incorrect login information without having to contact an administrator. This will stop brute force attacks that try many different passwords until they find one that works.

Enable systems that authenticate emails. Systems called DKIM and DMARC will authenticate that emails are authentic. The FTC provides helpful information explaining how these systems work.

Verify changes in information about customers, employees or vendors. Crooks can log into online accounts and change account information, phone numbers and email or mailing addresses to ones they control. If an employee or vendor claims that their contact information has changed, ensure that the old contact information is no longer active by trying to reach the person using the old information.

Other useful tips can be found at staysafeonline.org, by the National Cyber Security Alliance, a public/private partnership to help with online safety.

Culture/Training

Confirm requests by phone before acting. Several people interviewed for this study highlighted a "secret weapon" to fight BEC fraud – the telephone. Most BEC fraud could probably be stopped if employees who were directed to send money simply called the person supposedly asking them to send money and ask them to confirm it. Emails aren't sufficient to ensure you are talking to the right person. Pick up the phone or walk down the hall. In this age of electronic communications, many people may be reluctant to do so. Senior executives need to develop a culture that encourages this.

Anyone involved in a home closing should confirm wiring instructions by phone before wiring proceeds. And internal organization policies should require that at least one other person be required to authorize unusual transactions -- and through a means other than email or text message.

Train all employees in internet security. Busy executives may just label this "an IT issue" and leave it to the staff to handle. IT staff may not be aware of the scope of risks, and some IT measures require comprehensive staff training in order to be effective.

Insurance/malpractice

One potential precaution for organizations is to buy cyber insurance. Unfortunately, most policies exclude coverage for "social engineering" losses, presumably because they are concerned that employees may be participants in the fraud. Riders that cover social engineering are available at an extra cost. But organizations rarely purchase this coverage.

What can law enforcement and other agencies do to curb BEC fraud?

- There is a strong need for more international cooperation between law enforcement agencies.
- Email system providers should consider enabling additional features to help prevent BEC fraud, including default settings with more security.
- Law enforcement should recognize that BEC fraud gangs engage in many varieties of the fraud at the same time and focus on the key actors in the frauds, not just supporting actors such as money mules.

What should you do if your organization has lost money to a BEC fraud?

- If an organization finds that it has been a victim of a BEC fraud, it needs to immediately call its bank to stop the payment and report it to the FBI in the U.S. or the Canadian Anti-Fraud Centre in Canada. If a report is filed within 48 hours, there is a chance the money can be recovered.
- Complain to the FBI's Internet Crime Complaint Center. IC3 also asks people to report unsuccessful BEC attempts as well. Information from attempts may help establish patterns or identify mule bank accounts.
- Complain to the Canadian Anti-Fraud Centre: 1-888-495-8501.
- Report fraud to BBB Scam Tracker.

By C. Steven Baker, International Investigations Specialist