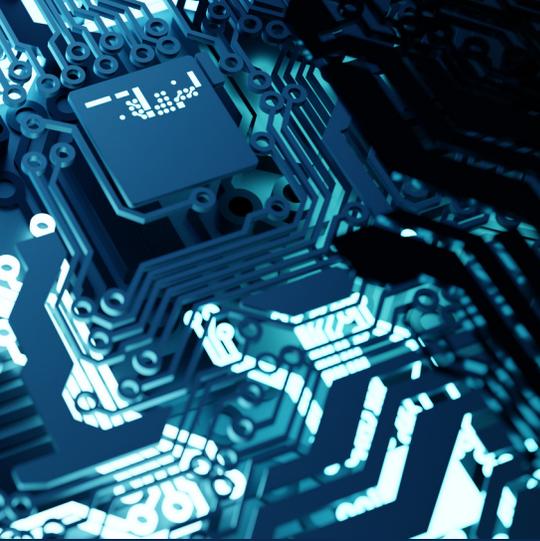


ELECTRONIC PAYMENT SECURITY

Identifying and Addressing Business Email Compromise (BEC) and Wire Fraud Attacks





INTRODUCTION

Formerly known as the “man in the email attack,” business email compromise (BEC) is a scam that takes control of a senior employee’s email account or even a trusted vendor’s email account with the goal to command unauthorized financial transfers. This type of attack is different from classic phishing campaigns because it targets one specific individual and is highly personalized in this sense. Indeed, it requires a thorough search from the cybercriminal, starting with the company’s publicly available information, such as the CEO email address, to the most confidential information such as bills and contracts. In addition, it generally escapes security measures that detect phishing because there is no link embedded in the scamming email nor any attachment.

Many BEC attacks request wire transfers because they often cannot be cancelled, but ACH and Bill Pay can be attacked as well. For example, a hacker starts to look for any sensitive information related to the CEO or vendor contact of a specific company and uses this information to get control of the person’s email account. From that account, the hacker searches for any invoice which is due soon and once he finds one, he sends a request to the finance department, pretending that it is urgent and that the bank account information for that payment has changed.

The hacker can amplify his story by giving arguments about the change, for instance by saying the supplying company was acquired by another entity, and the supplier of the company called him personally to make sure that the payment is on its way to the new account. The hacker can go even further by calling and pressuring staff in the finance department to make the request seem as real as possible. If the finance department doesn’t have procedures in place to check the trustworthiness of the request before ordering the payment, the hacker gets the funds and there is almost no way to get them back when the company realizes it was a scam.

Hackers target companies moving large sums of money on a regular basis. Commonly targeted industries include construction businesses, real estate related businesses, educational institutions, charities, companies buying inventory, businesses that use third party payroll providers that settle through wire transfer.

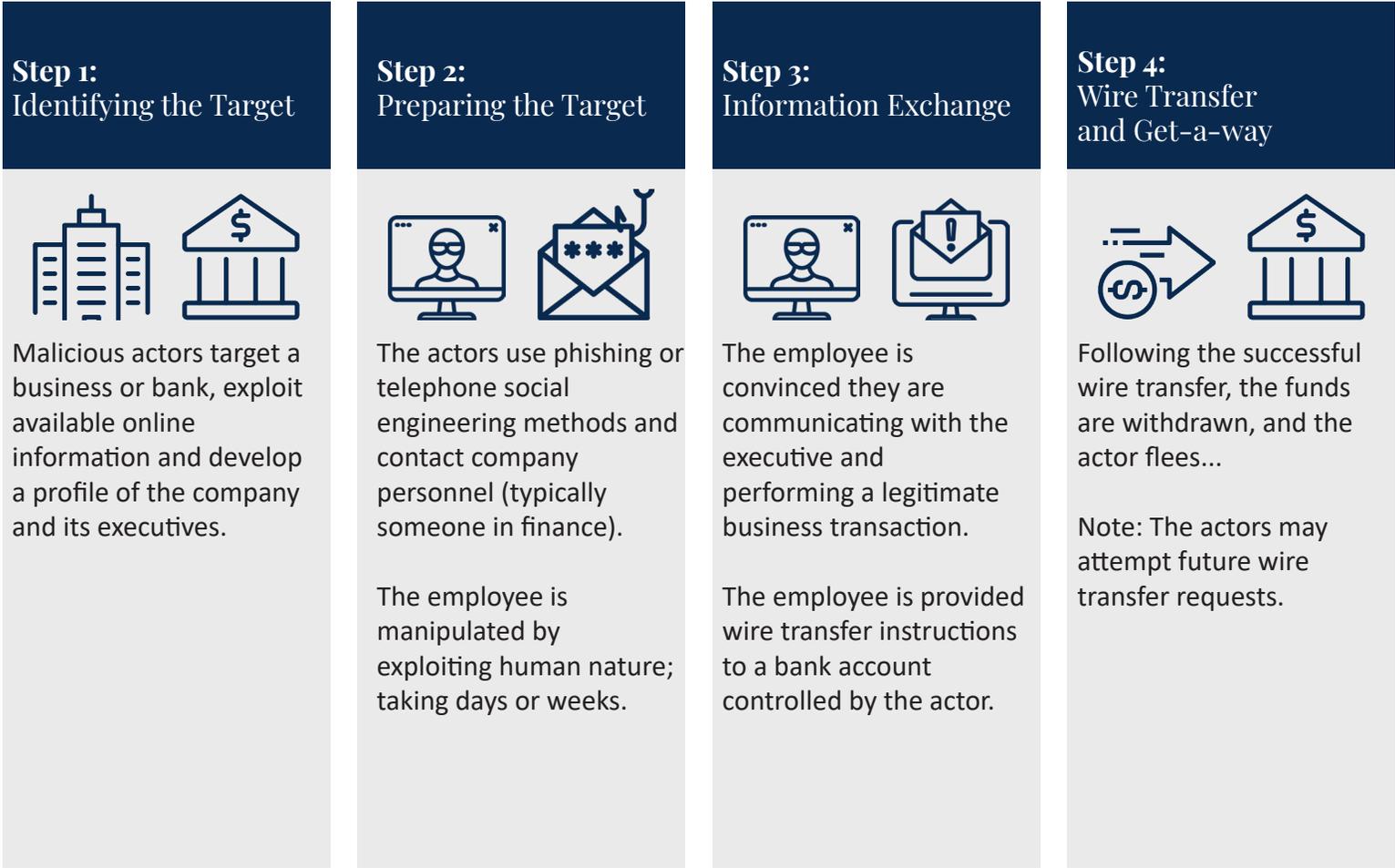
As the threat of wire fraud continues to grow, it’s important that businesses develop strategies to mitigate their risk and lessen the impact of attacks.

What is BEC?

Business Email Compromise (BEC):

A sophisticated scam targeting businesses working with foreign suppliers and companies that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

How BEC Works



What is the Financial Impact of BEC?

BEC is a business threat because it can lead to significant financial losses. Most importantly, it appears BEC attacks are constantly growing and becoming more elaborate.

How Criminals Carry Out BEC Scams

A Scammer Might Spoof an Email Account or Website

Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.

A Scammer Might Send Spear Phishing Emails

These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.

A Scammer Might Use Malware

Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.

How to Protect Yourself Against BEC

Employees should be educated about and alert to this scheme. Training should include preventative strategies and reactive measures in case they are victimized. Among other steps, employees should be told to:

- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII (personally identifiable information) in response to any emails.
- Monitor their personal financial accounts on a regular basis for irregularities, such as missing deposits.
- Keep all software patches on and all systems updated.
- Verify the email address used to send emails, especially when using a mobile or handheld device by ensuring the sender's email address appears to match who it is coming from.
- Ensure the settings on employees' computers are enabled to allow full email extensions to be viewed.

If you discover you are the victim of a fraudulent incident, immediately contact your bank to determine a course of action.

In addition, as soon as possible, file a complaint regardless of the amount with www.ic3.gov or, for BEC/EAC victims, BEC.IC3.gov.

What is Wire Fraud?

Wire Transfer:

An electronic payment method to move money—domestically or internationally—from one person to another using a bank or a nonbank provider, such as a transfer agency.

Wire Fraud:

Any fraudulent activity that occurs over interstate wire communications, which includes the telephone and internet. In many cases, the fraud attempt occurs over email. If such payment request is not authenticated, it can result in a fraudulent transfer of money.

Methods of Wire Fraud

Malware	Phishing	Voice Phishing (Vishing) and SMS Phishing (SMShing)	Business Email Compromise (BEC) or Email Account Compromise (EAC)
 <p>Malware occurs when a user opens an email or clicks on a link that redirects to a website that downloads malware and infects the computer operating system. Criminals can also send malware through removable media, such as a USB flash drive. After the removable media is inserted into a computer drive, criminals can gather user credentials to gain access to payment systems.</p>	 <p>Phishing occurs when criminals send emails that appear to be sent from a known company or vendor, such as a bank. The criminal asks the user to reply to the email or visit a website that looks similar to the company's domain and submit a username, password, account number or other personal information.</p>	 <p>Voice phishing (vishing) and SMS phishing (SMShing) use live or automated calls (vishing) or text messages (SMShing) to intimidate callers into providing personal information by threatening to close or freeze their bank accounts. The personal information is used to gain access to payment systems or take over accounts.</p>	 <p>Business Email Compromise (BEC) or email account compromise (EAC) occurs when cybercriminals use stolen credentials, look-alike domains, spam or phishing to gain access to an email account. Cybercriminals may impersonate a known vendor or C-suite executive officer, and direct another employee to transfer funds to a fraudulent account.</p>

How Can You Prevent BEC with a Secure Wire Transfer or Vendor Payment Procedure?

Secure wire transfer and vendor payment procedures are one of the key ways you can prevent BEC. Although the scammer can have email account access and/or personally identifiable information, employees following secure transfer procedures will stop most BEC scams targeting your business. Every company has the duty and the ability to develop procedures to address the growing BEC threat. Here are seven suggestions to help you secure your organization's payment process.

1. Use a Secure Payment Method

Above all, your company should use a secure payment method. Different ways to do so are available depending on the budget and needs of your business. Examples are electronic signatures and accreditation of the transfer by a competent organization when the payment is made online.

2. Verify All Payment Requests

Your finance department should follow-up on payments to ensure that they are done properly and sent to the appropriate bank accounts. The department should also verify client accounts on a regular basis. This helps monitor the security and the safety of the payment process and detect possible breaches, so the company can quickly respond if needed. In addition, employees should confirm every wire transfer request and/or payment face-to-face whenever possible. This is particularly important in some specific situations, i.e., if the cybercriminal has control of a company email account or phone number.

3. Note and Verify Any Account Changes Before Approving Transfers

When a wire transfer is requested with an email address and the email sender asks for payment changes, employees should verify the identity of the person. Hackers often ask for bank account information changes, as their aim is to receive the funds elsewhere. Therefore, the employee in charge of the transfer should contact a trusted person from the company requesting the changes (with a verified contact method) to check if these changes are genuine. Never respond back to an email request as a form of confirmation.

4. Balance Authorizations and Control Procedures

Even though your company should crosscheck payment requests and changes by involving at least two authorized employees, it is not recommended many individuals have such authorizations inside the company. In fact, it increases the risk of fraud since many employees can be a juicy target for cyber-attacks. Therefore, make sure only a limited number of authorized employees can give approvals for payments and find the right balance between risk of exposure and adequate control measures.

5. BEC Reporting Procedure

Your company should consider allocating the responsibility to report suspected scams to a specific department or responsible person. This department or person can then represent the company legally with external bodies and enforce action with the bank, for example, in an attempt to reverse payments, if possible.

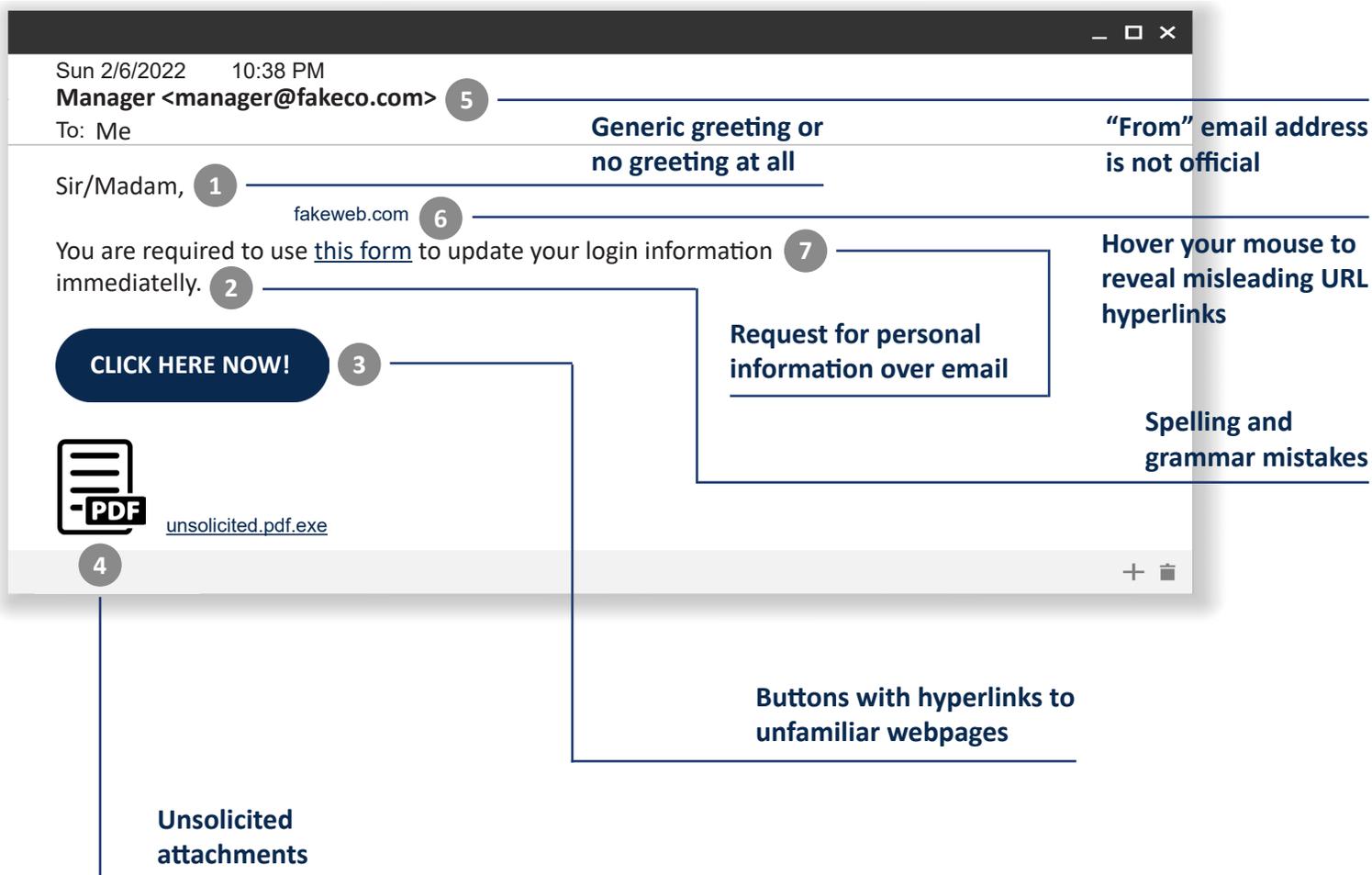
6. Educate Employees About BEC and Transfer Approval Policies

Once secure procedures are developed, employees need to be trained. Any employee in direct contact with external parties should be not only be aware of the scam risks, but also how to mitigate them. For instance, the company can send reminder emails frequently about the tricks used by scammers, what makes a payment request suspicious, the company's wire transfer control procedures and the contact person to whom to report suspicious requests. It is always good to remind employees that they will never be asked to go out of the scope covered by the company's wire transfer control procedures to make an urgent or confidential payment, and inform them about the consequences on their job in case of non-compliance. Educational tools such as online courses and simulations are also strong ways to raise awareness among employees.

7. Assess Risk Through Regular Audits, Fund Transaction Policies and Processes

As the BEC problem grows globally, companies dealing with this kind of transfer should implement appropriate procedures to minimize the risk of financial loss. Different procedures exist to secure wire transfers. These procedures range from the most basic such as the use of secure methods, to more complex and broader ones such as verifying payment requests, implementing a reporting procedure and raising awareness among employees.

7 Signs of a Phishing Email



Other Methods of Internet Fraud

Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them. Internet crime schemes steal millions of dollars each year from victims and continue to plague the Internet through various methods. Several high-profile methods include the following:

Data Breach:

A leak or spill of data which is released from a secure location to an untrusted environment. Data breaches can occur at the personal and corporate levels and involve sensitive, protected, or confidential information that is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

Denial of Service:

An interruption of an authorized user's access to any system or network, typically one caused with malicious intent.

Email Account Compromise (EAC):

Similar to BEC, this scam targets the general public and professionals associated with, but not limited to, financial and lending institutions, real estate companies, and law firms. Perpetrators of EAC use compromised e-mails to request payments to fraudulent locations.

Malware/Scareware:

Malicious software that is intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds from victims.

Phishing/Spoofing:

Both terms deal with forged or faked electronic documents. Spoofing generally refers to the dissemination of email which is forged to appear as though it was sent by someone other than the actual source. Phishing, also referred to as vishing, SMSing, or pharming, is often used in conjunction with a spoofed e-mail. It is the act of sending an e-mail falsely claiming to be an established legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website. The website, however, is not genuine and was set up only as an attempt to steal the user's information.

Ransomware:

A form of malware targeting both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through spear phishing emails to end users, resulting in the rapid encryption of sensitive files on a corporate network. When the victim organization determines they are no longer able to access their data, the cyber perpetrator demands the payment of a ransom, typically in virtual currency such as Bitcoin, at which time the actor will purportedly provide an avenue to the victim to regain access to their data.

Response Planning

Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. Establishing an incident response capability should include the following actions:



Creating an incident response policy and plan



Developing procedures for performing incident handling and reporting



Setting guidelines for communicating with outside parties regarding incidents



Selecting a team structure and staffing model



Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)



Determining what services the incident response team should provide



Staffing and training the incident response team

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. One of the benefits of having an incident response capability is that it supports responding to incidents systematically so that the appropriate actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data. An incident response capability also helps with dealing properly with legal issues that may arise during incidents.

In addition to this guide, we also offer a Cybersecurity Guide and a free basic Risk Assessment to help your organization start an incident response plan to help identify, prevent and address cybersecurity-related attacks. Contact our Treasury Management team to obtain the self-assessment tool by email at tm@pbofca.com or by calling (949) 732-4050. For additional information or questions about how to protect your company from BEC and wire fraud attacks, visit our Resource Center on pbofca.com or contact support@pbofca.com.



partners bank
of california

MISSION VIEJO

Corporate Headquarters
27201 Puerta Real, Suite 160
Mission Viejo, CA 92691

(949) 732-4000

BEVERLY HILLS

8484 Wilshire Blvd., Suite 520
Beverly Hills, CA 90211

(323) 556-3137

pbofca.com

© 2022 Partners Bank of California. All rights reserved.

