BANC OF CALIFORNIA | TOGETHER WE WIN™

BUSINESS EMAIL COMPROMISE (BEC)

More sophisticated scams require more comprehensive protection.

Business Email Compromise (BEC) is an insidious, increasingly common scam.

BEC fraud, an email phishing scam that targets individuals at businesses and other organizations and cons them into making wire transfers to bank accounts controlled by the criminals, is a growing scourge. According to the FBI, 80% of businesses received at least one BEC email attack.

The FBI has identified six different kinds of BEC Fraud.

1. CEO to CFO or other Payment Officer

The traditional BEC involves an email that appears to be from the CEO to the CFO or other person who can send wire transfers, asking them to send money right away. They time these emails for when the CEO is away, and often claim that the matter is urgent. Believing the email is from the boss, employees may send the money without checking it out first.

2. Vendor Impersonation Fraud

This is a growing trend in BEC, in which scammers target vendors or suppliers with phishing emails, study their billing and payment patterns and processes, then send authentic-looking invoices to their customers. These invoices are for payments that are about to be made and look normal in every respect except that the bank account number has been “updated”. This type of fraud often involves impersonating smaller companies that provide products or services to larger companies. The company receiving the invoice is the one that suffers the loss.

3. W-2 Scams

In W-2 scams, BEC emails appearing to be from senior executives instructing human resources directors to email employee W-2s. The fraudsters can then file fake tax returns, and have tax refunds deposited onto stored value cards or criminal-controlled bank accounts. The IRS has taken measures to combat this type of fraud and appears to have succeeded so far in 2019.

4. Real Estate BEC

This type of fraud typically targets homebuyers but it does apply to commercial real estate transactions. The fraud works when scammers log into the email account of one of the parties and redirect the wire transfer to a bank account that they control.

5. Direct Deposit

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

6. Gift Cards

BEC fraud scenarios requesting gift card purchases are growing. The FTC has warned that many of these bogus emails claim to be coming from priests, rabbis or other clergy members, but scams sometimes are represented as requests by company executives.

If you fall victim to a business email compromise scam:

- Contact Banc of California Client Services immediately to notify us about the fraudulent transfer
- Contact your local Federal Bureau of Investigation office immediately; they may be able to freeze or return thhe funds if notified quickly
- File a complaint, regardless of dolars loss, at www.IC3.go

For additional questions regarding fraud, please contact Client Services at 877-770-BANC (2262) or your Relationship Manager.

BE AWARE OF HOW BEC WORKS AND BE WARY OF EVERY EMAIL

How does BEC work?

There are essentially three steps to operating a BEC fraud:

- Obtaining the names, job functions, email usernames and passwords of people within an organization, learning who is in charge of the organization and who controls payments
- Sending emails impersonating a trusted superior, partner or vendor and requesting money or change in payment account information
- Devising a way to obtain money sent by victims

To do that, they use online tools and sophisticated techniques:

Spoofing email accounts and websites: Fraudsters use slight variations on legitimate addresses to create fake accounts that appear authentic, then use a spoofing tool to direct email responses to accounts they control.

Spear-phishing: Fraudsters send bogus emails that appear to be from a trusted sender and that prompt victims to reveal confidential information.

Malware: Fraudsters use malware to infiltrate company networks and gain access to victims' passwords and financial information, and email threads about billing and invoices. They use that information to make requests for fraudulent wire transfers appear routine.

How do scammers impersonate people?

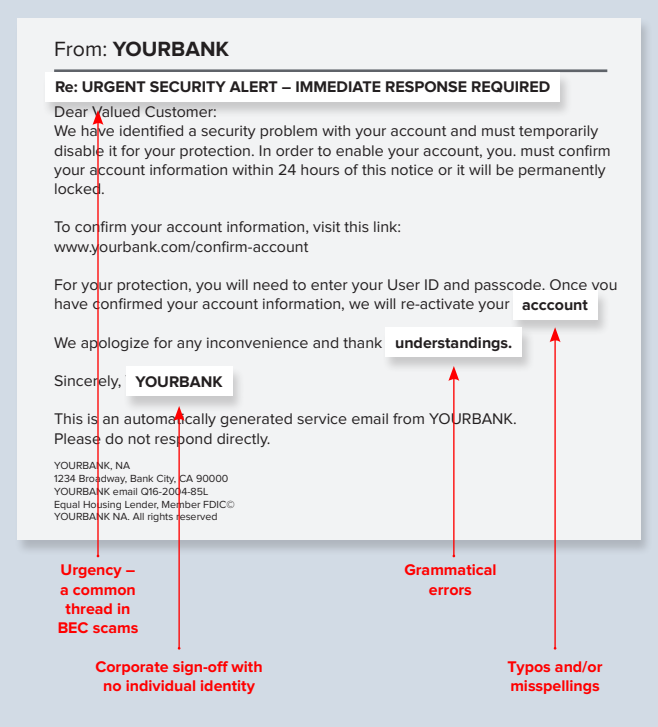
Scammers use a variety of techniques to adopt false identities.

One is to put the name of a real person in the "From" line of an email, assuming that the recipient will not notice any differences in the domain name.

A second way is to 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 they are impersonating. For example, an email like johndoe@samplecompany.com might be approximated as "johndoe@sample.company.com", a domain name the criminals would have registered.

A third is to get access to a real person's email account through malware or phishing attacks or may purchase them on the dark web. Then they meticulously study the organization's vendors and billing systems, the targeted executive's style of email communication and even his or her travel schedule so they can time their scams for when the target is away to send a bogus email from the CEO to a targeted employee in the finance office requesting an immediate wire transfer to a trusted vendor, using an account number that is just slightly different.

This example email illustrates four warning signs of a scam:



TIPS FROM THE FBI ON GUARDING AGAINST BEC FRAUD:

- Verify the authenticity of requests by speaking directly to the requesting executive in person or on the phone.
- Create intrusion detection system rules that flag emails with extensions that are similar to company email.
- Create an email rule to flag email communications where the "reply" email address is different from the "from" email address shown.
- Color code virtual correspondence so emails from employee/internal accounts are one color and emails from non-employee/external accounts are another.
- Verify changes in vendor payment location by adding additional two-factor authentication such as a secondary sign-off by company personnel.
- Confirm requests for transfers of funds by using phone verification as part of a two-factor authentication; use previously known numbers, not the numbers provided in the email request.
- Carefully scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary.

BANC OF CALIFORNIA | TOGETHER WE WIN™

EQUAL HOUSING LENDER FDIC

TM03W1019