CYBERSECURITY EDUCATION

Business Email Compromise (BEC) Scam

The Business Email Compromise (BEC) Scam is the fastest growing form of payment fraud occurring in the world. According to the FBI's most recent Internet Crime Report (ICR), losses from BEC scams amounted to **over $1.2 billion and involved over 20,000 BEC-related complaints**. BEC is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments. While there are several variations of the BEC Scam, the most commonly seen are: CEO Impersonation, Vendor Impersonation, and Payroll Scam.

CEO Impersonation 	The fraudster poses as a company executive and initiates an ACH or wire payment or requests to change payment instructions. The email will be similar to the targeted business' actual domain, and is usually sent with a sense of urgency and secrecy. *From: CEO@ABGCompany.com (fake); CEO@ABCCompany.com (real)* *Subject: Wire Transfer ASAP* *Please process a wire transfer payment in the amount of $250,000. Wiring instructions attached. I'm in a meeting all day and have little access to email/phone. Let me know once complete.* *Sent from my iPad*
Vendor Impersonation 	The fraudster poses as the vendor and sends an email to inform the company that the vendor has a new bank account where future electronic payments should be sent. A fake invoice could even be attached to the email. The fraudster could also send an email notifying the company of an address change so that check payments are rerouted to the fraudster's account. The fraudster now has access to the account information on a legitimate check to make counterfeit checks. *From: ABC Company* *Subject: New Bank Account Information- Update* *Hi! We've recently changed bank accounts. Please update your records and send all future payments to the referenced bank account. Email if you have any questions.*
Payroll Scam 	The fraudster poses as an employee and sends human resources an email to change their bank account. Once changed, payroll is routed to the fraudster's account and the company is on the hook for replacing the stolen funds. *From: Employee* *Subject: Payroll- Assistance Needed* *Hi, I changed my account and I need you to help me update my direct deposit information with the new account details. I would be very happy if the changes could be made effective for the current pay period. What information do you need from me?*

What can you do to protect yourself?

While fraud schemes are getting more sophisticated and becoming harder to detect, there are ways that you can protect both yourself and your company. Below are a few helpful tips to keep in mind:

- ✓ Educate and train employees
- ✓ Carefully check the email domain portion of an email sender's address (.net, .com, etc.) for any replacement characters, such as a "0" or zero instead of the letter "O" or "l" (lowercase "L") in place of "I" (uppercase "I")
- ✓ Authenticate requests by telephone
  - o Use known contact information to authenticate payment or change requests
  - o Use caution if the request for payment is from a personal email account instead of the company email
- ✓ Review your accounts frequently
- ✓ Never provide password, username, authentication credentials, or account information when contacted
- ✓ Do not provide non-public information on social media
- ✓ Specifically regarding company email policies:
  - o Avoid free web-based email accounts
    - ▪ A company domain should always be used to establish company personnel emails
  - o Consider registering domains that closely resemble the actual company's domain
  - o Do not use the 'reply' option when authenticating emails for payment requests. Instead, use the 'forward' option and type in the correct email address or select from a known address book
- ✓ Use antivirus software and keep it updated
  - o Make sure your business's computers are equipped with antivirus software and antispyware and updated regularly
- ✓ Secure your networks
  - o Safeguard your Internet connection by using a firewall and encrypting information
- ✓ Consider a dedicated computer for important financial transactions
  - o Restrict e-mailing, social media, or surfing the web on this computer

Questions?

If you suspect that you are a victim of a BEC Scam, notify your bank immediately. Gather all documentation regarding the transaction, emails, and invoices, and report the incident to your local police department as soon as possible. Additional information can also be found at:

- International Criminal Police Organization (www.interpol.int)
- Federal Bureau of Investigation (www.fbi.gov)

First Choice Bank™
First in Speed | Service | Solutions

17785 Center Court Drive, Suite 750
Cerritos, CA 90703
(877) 256-9809 or (562) 345-9092
www.FirstChoiceBankCA.com