Fraud Alert

Posted 5-23-17

CEO and Business Email Compromise (BEC) Fraud Awareness

What is CEO Fraud?

CEO Fraud, also known as Business Email Compromise (BEC) Fraud, is a type of targeted attack that commonly involves a cybercriminal pretending to be the CEO or another senior executive from your organization, then tricking you into releasing highly sensitive information or initiating a wire transfer. Click here to find out how CEO Fraud is carried out and ways to avoid it.

Posted 3-7.17

Federal Trade Commission

The Federal Trade Commission has long provided advice to consumers about steps they can take to avoid phishing scams. On March 6, 2017, the FTC released tips and a video for businesses on how to respond if they are impersonated as part of a phishing scam. Among the steps businesses should take include notifying customers as soon as possible through social media, email or letters; contacting law enforcement; providing resources for affected consumers; and reviewing the company's security practices. Please visit the Federal Trade Commission's website for more details.

Posted 4-20-16

FDIC Consumer News

What Consumers Can Do ... and What Banks and Regulators Are Doing ... to Help Prevent Online Fraud and Theft

- Safety precautions for Internet banking or shopping
- How to avoid identity theft online
- The roles of banks and the government in protecting customers
- Additional resources from the FDIC that can help educate consumers

Posted 3-29-16

IBM® Security Trusteer Rapport™
FREE downloadable fraud protection

Online fraud protection software that provides extra security while you are signed on to FBHP online banking. It works in conjunction with your current anti-virus solution but is not meant to replace it.

The Internet offers massive advantages, conveniences and opportunities convenient for you or your business. With such access, various security risks are unearthed for cybercriminals. That's why you need Trusteer Rapport.With Trusteer Rapport you can remove and prevent financial malware infections, stop phishing attacks, and protect your sensitive data.

Protect yourself today! When you login to your online bank account, you will be asked to download Trusteer

Fraud Alert

Rapport. Once you click the "Download Now" button, the software will download within seconds and work in the background to protect your account.

Here are some tips from the FBI that you can use to avoid becoming a victim of cyber fraud:

• Do not respond to unsolicited (spam) e-mail.
• Do not click on links contained within an unsolicited e-mail.
• Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Always run a virus scan on attachment before opening.
• Avoid filling out forms contained in e-mail messages that ask for personal information.
• Always compare the link in the e-mail to the web address link you are directed to and determine if they match.
• Log on directly to the official Web site for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
• Contact the actual business that supposedly sent the e-mail to verify that the e-mail is genuine.
• If you are requested to act quickly or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act impulsively.

ID Theft & Fraud

For your online safety, First Bank of Highland Park will never email passwords or account number(s) and we will never ask for your password or account number(s) in an email. Do not use the links in an email, instant message, or chat to get to our web page or to your online bank/bill pay account.

FDIC Scam Alert

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports from consumers who received an e-mail that has the appearance of being sent from the FDIC. The e-mail informs the recipient that "in cooperation with the Department of Homeland Security, federal, state and local governments..." the FDIC has withdrawn deposit insurance from the recipient's account "due to activity that violates the Patriot Act." It further states deposit insurance will remain suspended until identity and account information can be verified using a system called "IDVerify." If consumers go to the link provided in the e-mail, it is suspected they will be asked for personal or confidential information, or malicious software may be loaded onto the recipient's computer.

This e-mail is fraudulent. It was not sent by the FDIC. It is an attempt to obtain personal information from consumers. Financial institutions and consumers should NOT access the link provided within the body of the e-mail and should NOT under any circumstances provide any personal information through this media.

The FDIC is attempting to identify the source of the e-mails and disrupt the transmission.