Signature Bank

5 Tips to Prevent Fraud this Holiday Season

'Tis the season for holiday fraud. Like Santa's elves, fraudsters are busy this season creating new and more sophisticated ways to perpetrate cyberattacks. We've seen an uptick in these fraud attempts with several of our small business customers. While small businesses are an especially attractive target for hackers, there are many steps you can take to make sure your business is protected.

1. **Verify the approval chain of any wire or transfer of funds requests.**
   Don't be shy about conducting due diligence to verify a request.

2. **Be wary of suspicious emails or phone calls.**
   Spoofed emails often contain grammatical errors or awkward language. If it doesn't sound like something the person would write, place a phone call to confirm.

3. **Do not set up an out-of-office alert.**
   Hackers love out-of-office alerts, especially when they reveal sensitive company information like chain of command. Business Email Compromise (BEC) scammers can infiltrate a system and wait until the time is right to strike.

4. **Strengthen your password to a passphrase.**
   Pick your favorite song lyric or quotation to use as your passphrase. Not only does a passphrase typically meet the minimum character requirement, it also is easier for you to remember and harder for hackers to guess.

5. **Act quickly if you think you've been hacked.**
   If you think you've been the victim of financial fraud, contact Signature Bank immediately. You can also file a complaint with the Federal Bureau of Investigation Internet Crime Complaint Center or IC3 at www.IC3.gov.

Real-world fraud attempt: Recently, the newly hired CFO at a company received an email from what appeared to be the CEO of the company asking him to wire funds internationally as soon as possible. When the CFO forwarded the chain to Signature Bank to process, Commercial Lender Tim Hanson found the pattern suspicious. The company does not usually do international wires and the urgency of the request raised a red flag with him. Tim asked the CFO to call his boss, who was traveling at the time, to verify the request. Indeed, the CEO's email had been hacked and it was a fraudulent request.

Lessons Learned: Always stop and ask another question. If it seems suspicious, it probably is suspicious.

Signature Bank

If you have any concerns about your business accounts as we head into the holidays, don't hesitate to call us immediately at 773.467.5600.