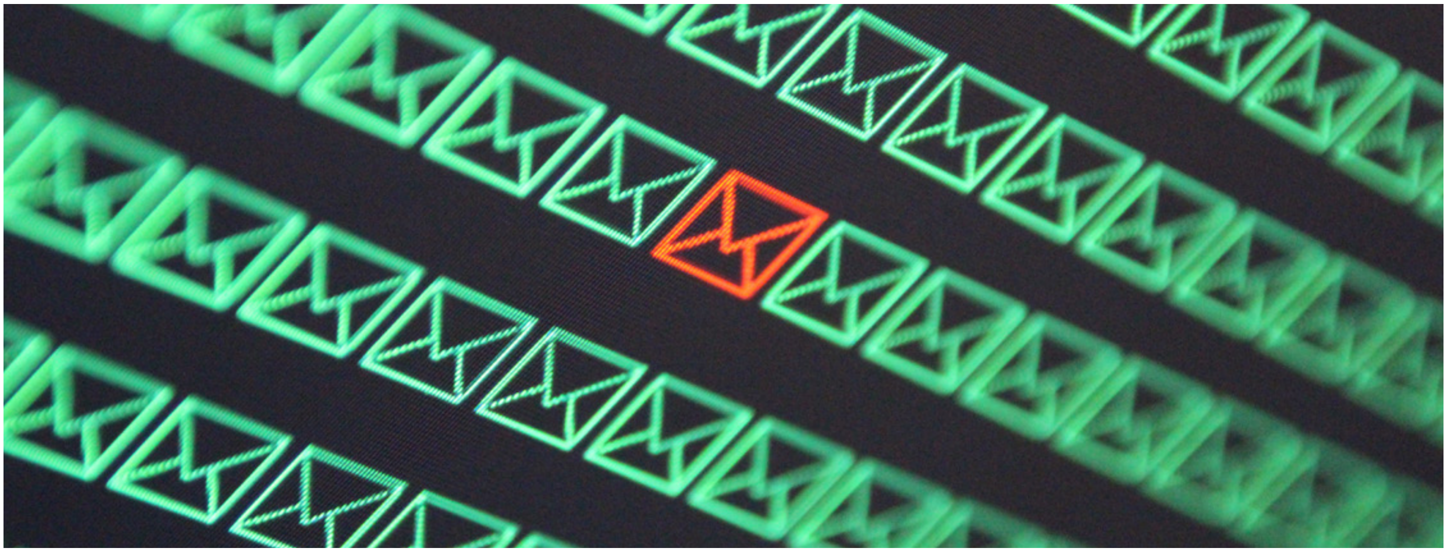
Santander Commercial Banking

November 2017

Combating Cyber Fraud Threats To Your Business

Kathleen Kenslea *Senior Vice President, Cash Management Sales*
kathleen.kenslea@santander.us



Online attacks on companies are on the rise, and business leaders have come to view them as one of the top risks organizations face today. Cyber fraud can have consequences far beyond that of direct financial loss—including compromise of confidential information, loss of business, remediation costs, and reputational damage.

Phishing and the Business Email Compromise

As technology continues to evolve, so does the sophistication of cyber-attacks, which can range from malicious software embedded in emails, ransomware, distributed denial-of-service, and more.

Email phishing is one of the most common types of cyber-attack. In this form of fraud, criminals send emails in which they masquerade as a trustworthy person or business to acquire sensitive information, such as passwords, that can then be used to initiate fraudulent payment transactions. Phishing is also used to persuade unsuspecting employees to send payments to accounts controlled by criminals. This type of scam is known by a number of names, including “imposter fraud,” “masquerading” and the “business email compromise” (BEC).

The Association for Financial Professionals (AFP) reports that BEC fraudsters conduct extensive research in order to create convincing profiles of company managers. Using these detailed profiles, fraudsters masquerade as a company’s CEO or CFO and send emails with specific payment instructions to Accounts Payable employees.

In another variation of the BEC, fraudsters pose as vendors in emails and request that their payment information be changed because of a new banking relationship, which again can result in payments being made into accounts controlled by criminals.

In other cases of phishing, cyber thieves start by casting a wide net: mass-distributing phishing emails that either directly ask for sensitive information or try to lure victims to a bogus website designed to extract such information. Once sufficient data is acquired, the perpetrators zero in on promising targets.

Protecting Your Organization

Phishing is a particularly prominent and dangerous form of cyber fraud, but there are a number of best practices companies can adopt to minimize their risk.

First and most importantly, educating employees and creating greater awareness of phishing tactics will significantly decrease the risk of the company falling prey to a phishing scam. For example, companies should train employees to automatically challenge the authenticity of any emails containing payment instructions. If an email purporting to be from the CEO or CFO asks a treasury employee to make a large wire payment to a new bank account number, the employee should know to pick up the phone or walk down the hall to find out if the executive actually sent the request.

In addition to educating employees, companies can adopt the following basic security measures to offer protection against phishing scams:

- Have employees delete any emails that look questionable. Employees should watch for inaccuracies in the sender's address (e.g., slight misspellings), a sense of urgency accompanying the requested action, threats if the recipient doesn't act, or a link in the email that doesn't match the URL in the status bar.
- When initiating transactions through an Internet-based payment system, always institute dual control, which requires multiple users to initiate and release a payment.
- Set up alerts to notify managers of payments initiated above a threshold amount.
- Establish transaction limits for employees who initiate and approve online payments.
- Document vendors eligible for payment and set dollar limits on their payments.
- Never provide information such as account numbers or online banking credentials—personal IDs or passwords—over the Internet.
- Carefully monitor account activity. Review all transactions initiated by your company on a daily basis for authenticity.

Of course, email phishing is just one way in which cyber criminals target businesses. Companies must also consider instituting additional cyber-security measures—such as installing firewalls and various types of anti-virus and anti-malware software, and ensuring that servers are kept up to date with the latest software patches—to better protect themselves against other forms of cybercrime.

If your business experiences a cyber-attack, get in touch with the electronic crime investigators at the U.S. Secret Service. For more information about resources that help deter cyber threats, contact your Santander relationship manager.

Santander

This information has been provided by Santander Bank, N.A. for general information purposes. Statements contained herein do not constitute endorsements or guaranties of information provided by the Institutions referred to herein, the Trade Portal or Trade Club. Nothing contained herein creates any client, advisory, fiduciary or professional relationship between you and Santander Bank, N.A. Neither Santander Bank, N.A. nor any affiliate, in connection with the information herein, is engaged in rendering auditing, accounting, tax, legal, advisory, consulting or any other professional service or advice to you. Finally, the information contained herein should not be considered a substitute for your independent investigation and your sound technical business judgment after consulting with your own professional advisors.Santander, Santander Bank and the Flame Logo are trademarks of Banco Santander, S.A. or its subsidiaries in the United States or other countries. All other trademarks are the property of their respective owners.