# EMAIL SECURITY: PROTECT YOUR BUSINESS FROM EMAIL SCAMS AND FRAUD

*Email Security for Your Small to Medium Business*

Email is a critical component of many business functions, including processing transactions, collecting orders, performing customer service functions and requesting wire transfers. Unfortunately, despite its popularity, email is usually the least secure of all business applications. In fact, many security experts agree, the primary source for the vast majority of cyber-attacks is through email.

## WHAT'S THE RISK?

Business Email Compromise (BEC) is an emerging form of financial fraud which uses a combination of Social Engineering and Spear Phishing to commit fraud by moving money to unauthorized recipients. According to the Federal Bureau of Investigation, since the Internet Crime Complaint Center (IC3) began tracking BEC scams in late 2013, it has compiled statistics on more than 7,000 U.S. companies that have been victimized—with total dollar losses exceeding $740 million. That doesn't include victims outside the U.S. and unreported losses. Since the beginning of 2015 there has been a 270 percent increase in identified BEC victims. Victim companies have come from all 50 U.S. states and nearly 80 countries abroad. The majority of the fraudulent transfers end up in Chinese banks.

The scammers are believed to be associated with organized crime groups located around the world. These attacks target specific individuals within a business, gaining access to the email accounts of authority figures in the company who are authorized to order money movement. Once these accounts are under the control of the criminals, orders for money transfers are sent via the compromised email account, and instead of making a payment to a trusted supplier, the offenders direct the payments to their own accounts.

### *Are All Email Accounts At Risk?*

Although all businesses are potentially at risk, the primary targets are businesses that work with foreign suppliers or regularly perform wire transfer payments.

If you believe your company has been victimized by a BEC scam, act quickly and notify Northern Trust immediately. Northern Trust will then attempt to contact the financial institution where the fraudulent transfer was sent. Next, call the FBI, and also file a complaint—regardless of the amount of monetary loss you believe you may have suffered.

### *What Can I Do To Reduce My Risk?*

According to the FBI, there are several steps businesses can take to reduce their risk.

- **Verify Changes.** Changes to vendor payment instructions should always be verified, and requests for transferring funds or processing payments should follow an outlined process which contains specific directions on managing the confirmation of new procedures or accounts.
- **Use Caution.** Avoid using free, web-based email accounts, which are easily compromised and frequently lack back-ups and two-factor authentication.

- **Be Alert.** Requests for wire transfers that include pressure to take action quickly or include a request for secrecy should be examined closely.

- **Use Two-Step Verification.** Implement procedures that outline and require two-step verification for wire transfer payments.

- **Implement Technology Controls.** Intrusion Detection Systems can be configured to flag emails that are similar, but not exactly the same, as your company email (.co vs. .com). It's also recommended that you register similar domain names to reduce the risk of a criminal gaining possession of or using those domains.

- **Train Your Employees.** Employees should not only be aware of the importance of verification and authentication procedures, but they should also receive training to identify anomalies in transaction requests and to flag behavior that is outside of the "norm" for clients.

- **Keep Your Computers "Safe."** Protect your company's information, computers and networks by installing the latest security software and operating systems. Whenever possible, use the most up-to-date web browser that you can. Ensure your virus software runs regularly, especially right after updates to the virus definitions are installed.

- **Manage Passwords and Authentication.** Configure systems to require strong, unique passwords, and force a password change on a regular basis. Implement controlled access — assign Unique User IDs, and maintain a policy which prohibits sharing passwords and accounts.

- **Maintain Documented Policies and Procedures Regarding Your Information Security Program.** The cornerstone of a solid Information Security Program, including your strategy for managing email, should be documented in appropriate policies and procedures, which are reviewed and updated on a regular basis and address the current threat landscape accordingly.