Educating users to take active precautions

Fraudsters are increasingly targeting companies that conduct online business, employing sophisticated tools designed to compromise your system and surrender control of your computer. Bank of America Merrill Lynch has a wide array of robust security features designed to help you reduce your exposure to certain types of fraud. To understand actions you can take to help your company reduce the risks associated with fraud, refer to the below online security tips and best practices to get started today.

**Online best practices**

- Be attentive during your online sessions. Know when and how the systems will prompt you to authenticate, whether at login or to approve a transaction. If you see prompts for entering your credentials that appear out of sequence or at points in a workflow that are not familiar, do not enter your data and contact your bank.
- Pay attention to the appearance of the application screens. If they are not consistent with what you are accustomed to or show unfamiliar data fields, this could mean your browser has been compromised. Stop your transaction and contact your bank.
- Use caution when visiting Internet sites from the same computer, or mobile device, where you carry out online banking activities. Access only trusted websites for business purposes because malware can be downloaded without your knowledge from unsafe or compromised websites.
- Install a dedicated, actively managed firewall, especially if there is a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
- Do not use your online portal passwords for other non-related websites that you access.
- Never share usernames and password information for online services with third-party vendors.
- Restrict computers from accessing personal email accounts.
- For the highest level of security, conduct all online banking activities from a standalone, hardened and completely locked-down computer system from which email and web browsing are not possible.
- Use notifications to alert you of transaction status changes including: pending payment and payment template approvals, positive pay exceptions, investment orders and account restrictions, as well as information reporting alerts for ACH outgoing payments.
- Leverage segregation of duties and dual approval for payments and entitlement changes.

**Email best practices**

- Do not open file attachments or click on web links in suspicious emails as that could expose your system to malicious code that could hijack your computer.
- Be on the lookout for grammatical errors, awkward writing and poor visual design. Typos and other errors are often the mark of fraudulent emails or websites.
- Be suspicious of emails that claim to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes or similar information.
- Sometimes criminals send email that looks like it has come from Bank of America Merrill Lynch or another trusted source. Be on the lookout for these requests in fraudulent emails:
  - Requests for personal information should raise a flag since trusted sources should never ask you to reply in an email with any personal information, such as your Social Security number, ATM or debit card PIN.
  - Urgent appeals, such as claims that your account may be closed if you fail to confirm, verify or authenticate your personal information, are common schemes to entice users to yield sensitive information.
  - Messages about system and security updates, and impending software upgrades, are also designed to trick users into providing sensitive company information.
  - Offers that sound too good to be true are frequent tactics used by fraudsters. These ploys ask the user to fill out a short customer service survey in exchange for a credit to your account. Then they solicit account numbers for proper routing of the supposed credit.
- When you see a suspicious email, show it to your employees and instruct them on its questionable characteristics.
System best practices

- Review users’ needs for administrative rights. If possible, limit administrative rights on computers to help prevent the inadvertent downloading of malware or other viruses.
- Install commercial anti-virus, spyware detection programs and desktop firewall software on all computer systems, specifically seeking products that protect your Internet browser. Free software may not provide protection against the latest threats compared with an industry-standard product.
- Make certain virus and anti-virus protection, security software and computers are updated regularly—including security patches for operating system and other applications.
- Verify that your browsers are connecting to all online banking sites via a secure session versus an encrypted session using HTTPS or Transport Layer Security (TLS) protocols, which encrypts information passed between the client (browser) and the server (website). Websites using this protocol will include https://.
- Avoid using automatic login features that save usernames and passwords when using online banking applications.
- Never leave a computer unattended while using any online banking or investing service.
- Never access bank, brokerage or other financial services information using public or shared computers at Internet cafes, public libraries or other unsecure locations. Unauthorized software may have been installed to capture account number and sign-on information, leaving the customer vulnerable to possible fraud. Additionally, avoid using public Wi-Fi networks when accessing online financial services. Fraudsters may target users of these networks.
- Understand your responsibilities for using all protection tools and the importance of layering security tools.
- Immediately escalate all suspicious transactions to your financial institution. Every minute counts to reverse and recapture lost funds.
- Establish procedures to identify and isolate computers from the network that become infected with malware. Make certain infected computers are fully remediated prior to reintroducing them for use to conduct online transactions.

Electronic payment best practices

- Set individual user limits appropriate for the payment and the user.
- Use maximum dollar amount per transaction for initiating and approving wires/ACH.
- Set maximum daily cumulative dollar amount for all wires initiated and/or approved.
- Review ACH and wire-transfer procedures on a regular basis and make sure that user credentials are updated and maintained to represent appropriate needs.
- Use repetitive wire templates to eliminate manual intervention and manipulation.
- Implement ACH Blocks to block incoming ACH transactions from posting to your accounts.
- Use ACH Positive Pay to monitor and control ACH transactions before they post to the bank account and allow transaction acceptance or rejection in real time.

Check payment best practices

- Reconcile accounts on a daily basis.
- Segregate internal duties for financial activities (audit/control).
- Consider migration from check payments to electronic payment products.
- Become fraud-focused on inquiries from other banks or institutions regarding legitimacy of checks.
- Safeguard check stock and consider using check stock security features.
- Consider outsourcing check processing to secured vendor.
- Consider using Positive Pay to prevent check fraud.

“Bank of America Merrill Lynch” is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., a member FDIC. Securities, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation (“Investment Banking Affiliates”), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and members of SIPC, and, in other jurisdictions, by locally registered entities. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA. Investment products offered by Investment Banking Affiliates are not FDIC Insured • May Lose Value • Are Not Bank Guaranteed. ©2015 Bank of America Corporation 01-15-8487