Best Practices for Client Online Banking

Computer Security

- Ensure the operating system is up to date and patches are installed regularly
- Remove administrative rights from users' workstations which may prevent the unintentional installation of malware, viruses or spyware
- Install, run and update on a regular basis an anti-virus, anti-malware and anti-spyware software program
- Install a firewall on all computers, in addition to your computer network
- Power off computers when not in use; do not use the computer's sleep or hibernation modes
- Limit online banking activities to secure computers only; public computers (Internet cafes, libraries, etc.) and public WiFi hot spots should be used with caution; also consideration should be made when retrieving banking information (account history, statements, etc.) on public computers as the information may be stored within the computer's memory or cache
- Consider using a standalone computer to conduct all online banking activities; prevent access to email and other websites to ensure the security of this standalone computer

Email Security

- Be cautious and vigilant when receiving suspicious emails, even emails from known parties, particularly when there are attachments or links; never open the attachment(s) or click on the link(s)
- Look out for phishing attempts in which the sender requests information such as account numbers, PINs, passwords, secure token numbers, etc.; many phishing attempts are made to look like they are coming from banks/credit unions, NACHA – The Electronic Payments Network (NACHA administers the ACH Network operating rules, but processes no ACH transactions on behalf of banks), transport companies like FedEx, UPS, or USPS, or government agencies such as the IRS, FDIC, or FBI
- If you receive a suspicious looking email, do not reply; delete it immediately
- If you respond to a suspicious email with any banking information or credentials, contact us immediately so that we can take the necessary steps to limit any potential fraudulent activity

Internet Security

- Verify you are using a secure internet session (look for https rather than http) for all online banking activities
- Do not store or allow your browser to "remember" your online banking credentials, including your user name and password
- Watch for any pop-up windows asking for your credentials, warning you of a virus or that your virus protection has expired; these techniques are designed to scare you into divulging your information or downloading malware on your computer
- When your online banking activities are complete, log out of the session and completely close out of your browser

Best Practices Continued ▶

Best Practices for Client Online Banking

Password Security

- Passwords should be strong, utilizing a combination of upper and lower case letters, numbers, special characters like #, *, &, ~, etc.
- Passwords should not be easily identifiable, such as your name or using the word "password" or any combination of the word "password" with numbers (e.g. Password123)
- Do not reuse your password for multiple sites that you access; consider using a different unique password for each site that you access, particularly those relating to online banking
- Passwords should be changed often, e.g. every three months
- Do not share user names and passwords

Account Security

- Every effort should be made to utilize dual control when initiating funds transfers (e.g. account transfers, wire transfers and ACH origination); one person should initiate the funds transfer request while a completely separate person should approve the funds transfer
- Your accounts should be reviewed and reconciled daily; if you do not recognize a transaction, contact us immediately as there is a limited window of opportunity to recover funds and notice to us may prevent further loss
- You should review, periodically, the users granted access and permission to the online banking application, as well as funds transfers; this will ensure only active, employed and known users are performing activity on your behalf
- You should set user-specific limits on all funds transfers, including wire and ACH, to the lowest level necessary to complete normal operating functions; this will reduce your exposure to fraud or loss
- Consider purchasing cyber fraud insurance designed to protect your business from any fraud losses resulting from compromised and unauthorized access to your online banking account(s)

Mobile Banking Security

- Always lock your device when not in use
- Store your device in a secure location
- Never disclose banking information and/or credentials via text message; if you receive a text message asking for this information, delete it immediately
- If you replace your existing device for a new one, delete all mobile applications or "apps" that are used for mobile banking before discarding your device
- Use caution when using public WiFi hot spots as they may not be secure
- When your mobile banking activities are complete, log out of the session and completely close out of the app

816.220.8600 • www.lead.bank

Lead BANK® Member FDIC