LIGHTHOUSE BANK

Online Banking Fraud Prevention Best Practices

At no time will the Bank contact you requesting your User ID and/or Password.

User ID and Password Guidelines

- Create a "strong" password with at least 8 characters that includes a combination of mixed case letters and numbers.
- Change your password frequently, at least every 90 days.
- Never share username and password information with other individuals or third-party providers.
- Avoid using an automatic login feature that saves usernames and passwords.

General Guidelines

- Do not use public or other unsecured computers for logging into Online Banking.
- Check your last login date/time every time you log in.
- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to us.
- View transfer history available through viewing account activity information.
- Whenever possible, use Bill Pay instead of checks to limit account number dissemination exposure and to obtain better electronic record keeping.
- Take advantage of and regularly view system alerts; examples include:
    - Balance alerts
    - Transfer alerts
    - Password change alerts

- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.

- Whenever possible, register your computer to avoid having to re-enter challenge questions and other authentication information with each login.

- Review historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.

- Never conduct banking transactions while multiple browsers are open on your computer.

Tips to Protect Online Payments & Account Data

- When you have completed a transaction, ensure you log off to close the Online Banking connection.

- Reconcile by carefully monitoring account activity and reviewing all transactions initiated by your company on a daily basis.

Account Transfer

- Utilize available alerts for funds transfer activity.

Tips to Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from any financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.

- Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail. Call the purported source if you are unsure who sent an e-mail.

- If an e-mail claiming to be from Lighthouse Bank seems suspicious, checking with your us may be appropriate.

- Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.

- Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.

- Ensure computers are patched regularly, particularly operating system and key application with security patches.

- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.

- Check your settings and select, at least, a medium level of security for your browsers.

- Clear the browser cache before starting an online banking session in order to eliminate copies of Web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browser's preferences menu.

Suspicious Activity or Security Breach

In the event that suspicious activity is detected, or you believe you may have experienced a security breach in your system, please contact the bank immediately to ensure further action can be taken to mitigate potential loss at (831) 600-4000, or by email at Lighthouse.Bank@lighthousebank.net.