Business Online Banking

FRAUD PREVENTION

This document provides you with fraud prevention best practices you can use to educate your Business Online Banking users.

Union Savings Bank

With today's cutting edge technology and more people using online banking instead of traditional banking practices, you need to make sure that your business has the security to fend off online banking fraud. Small-to-medium-sized businesses are a highly targeted medium for online banking fraud because these businesses often do not use dual controls on their accounts nor have they adopted a strong information security posture to mitigate online banking fraud. We employ the most sophisticated technologies and best practices available to make certain that your sensitive information and accounts are well protected: online, over the phone, and in person.

USER ID AND PASSWORD GUIDELINES

» Create a "strong" password with at least eight characters that includes a combination of mixed case letters, numbers, and special characters.
» Change your password frequently.
» Never share user name and password information with third-party providers.
» Avoid using an automatic login feature that saves user names and passwords.

GENERAL GUIDELINES

» Do not use public or other unsecured computers for logging into Business Online Banking.

» Check the last login date/time every time you log in.

» If the system does not recognize your computer or location, you will be asked to provide additional information to log into Business Online Banking. This is called Out-of-Band Authentication via phone or SMS text.

» Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to your financial institution.

» View transfer history available by viewing account activity information.

» Whenever possible, use ACH instead of checks to limit account number exposure and to obtain better electronic record keeping.

» Take advantage of and regularly view system alerts; examples include:

  – Balance alerts
  – Password change alerts
  – Transfer alerts
  – ACH alerts
  – Wire alerts

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

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

» Never leave a computer unattended while using Business Online Banking.

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

» An FBI recommended best practice is to suggest that company users dedicate a PC solely for financial transactions (e.g., no web browsing, emails, or social media).

To report fraud please contact our   Call Center at **866.872.1866**

ADMINISTRATIVE USERS

» Prohibit the use of "shared" user names and passwords for Business Online Banking.

» Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.

» Dedicate and limit the number of computers used to complete online banking transactions; do not allow Internet browsing or e-mail exchange and ensure these computers are equipped with latest versions and patches of both anti-virus and anti-spyware software.

» Delete online user IDs as part of the exit procedure when employees leave your company.

» Assign dual system administrators for online cash management services.

» Use multiple approvals for monetary transactions and require separate entry and approval users.

» Establish transaction dollar limits for employees who initiate and approve online payments such as ACH batches, wire transfers, and account transfers.

» Implement IT policies to ensure online banking security and provide cybersecurity training to employees.

TIPS TO PROTECT ONLINE PAYMENTS AND ACCOUNT DATA

» Take advantage of transaction limits. Establish limits for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.

» When you have completed a transaction, ensure you log off to close the connection with the financial organization's computer.

» Use separate accounts for electronic and paper transactions to simplify monitoring and tracking any discrepancies.

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

» Keep confidential documents and personal information secured or locked up when not in use (i.e., secure network system, locked cabinets or off-site at a secure storage facility).

» Have a response program in place that specifies actions to be taken when there is unauthorized or inappropriate access to confidential information and account data.

To report fraud please contact our   Call Center at **866.872.1866**

ACH (AUTOMATED CLEARING HOUSE BATCHES)

» Use pre-notification transactions to verify that account numbers within your ACH payments are correct.

» Use limits for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.

» Review historical and audit reports regularly to confirm transaction activity.

» Use available alerts for ACH transfer activity.

» Use dual control for the establishment and approval of ACH files, templates and transactions.

WIRE TRANSFER AND ACCOUNT TRANSFER

» Use limits provided for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.

» Review historical and audit reports regularly to confirm transaction activity.

» Use available alerts for wire transfer activity.

» Use dual control for the establishment and approval of wire templates and transactions.

7

To report fraud please contact our   Call Center at **866.872.1866**

TIPS TO AVOID PHISHING, SPYWARE AND MALWARE

» Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as user names, 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 your financial organization seems suspicious, check with your financial organization.

» 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 systems, browsers, and key applications.

» 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 any Business Online Banking session 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.

» Be advised that you will never be presented with a maintenance page after entering login credentials. Legitimate maintenance pages are displayed when first reaching the URL and before entering login credentials.

» Business Online Banking does not use pop-up windows to display login messages or errors. They are displayed directly on the login screen.

» Business Online Banking never displays pop-up messages indicating that you cannot use your current browser.

To report fraud please contact our Call Center at **866.872.1866**

TIPS FOR WIRELESS NETWORK MANAGEMENT

» Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

» Change the wireless network hardware (router/access point) administrative password from the factory default to a complex password. Save the password in a secure location as it will be needed to make future changes to the device.

» Disable remote administration of the wireless network hardware (router/access point).

» If possible, disable broadcasting the network SSID.

» Ensure wireless networks are secured using WPA2 Encryption.

» If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.

» Business Online Banking error messages never include an amount of time to wait before trying to login again.

» Be advised that repeatedly being asked to enter your password/token code are signs of potentially harmful activity.

To report fraud please contact our Call Center at **866.872.1866**

Union
Savings Bank

866.872.1866
unionsavings.com