Business Online Banking Best Practices

Avoid being a victim of a cyberheist or employee fraud. A majority of today's cyberheists begin with malware that is spread via email attachments. Many of these threats will go undetected by antivirus tools in the first few days after the virus has infected your computer.

Basic Business Online Banking Security

Our Security Practices:

- Out of band authentication at login and ACH/Wire approval
  - Receive a phone call or text message with a Secure Access Code to be entered in Business Online Banking
- Session timeout
  - The session will timeout after 20 minutes and you will need to enter a password to resume.
  - If the session is inactive for 40 minutes you will need to sign in with your user name and password.
  - In the Mobile App the timeout will happen after 20 minutes of inactivity.
- Other warnings
  - If your password is changed, an email will be sent to you. If you did not initiate the password change, please contact us immediately by calling our Business Member Service Center at (888) 200-7845.
  - Be advised that Business Online Banking will never present you with a maintenance page after 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.

Set Up Business Online Banking Alerts

UFCU recommends activating Business Online Banking alerts when using the ACH and/or Wire modules:

To set up alerts in Business Online Banking, go to **Preferences**>**Alerts**>select the **Add** button>select **Add Transaction Limits**. You will be provided several options for alerts such as when an ACH and/or Wire is:

- Authorized
- Cancelled
- Drafted
- Processed Successfully
- Processing Failed

These alerts are real time and can help you stop fraudulent transactions before the funds leave the credit union. You can be alerted by a phone call, email or text message. These can be changed or updated at any time.

Avoid Phishing, Spyware and Malware

- Do not open email from unknown sources. Be suspicious of emails purporting to be from a financial institution, government agency, or other organization requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. UFCU will never ask you for this 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 link embedded in a suspicious e-mail. Call the purported source if you are unsure who sent an e-mail. Do not use the number in the email itself as this may be fraudulent as well. If you have any questions, call our Business Member Service Center at (888)200-7845.

Business Online Banking Best Practices
(continued)

United
FEDERAL CREDIT UNION

Computer and Browser Safeguards

- If an e-mail claiming to be from UFCU seems suspicious, contact us at (888)-200-7845 to see if it is legitimate.
- 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 with security patches, particularly operating system 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.
- Do not use public or other unsecured computers for logging into Business Online Banking.
- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to United.
- Do not use your social security number, or other account or personal information, when creating account nicknames or other titles.
- Review 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.
- Prohibit the use of "shared" usernames 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. For computers dedicated to Business Online Banking, do not allow Internet browsing or e-mail exchange and ensure the latest versions and patches of both anti-virus and anti-spyware software are installed. If email is viewed on the PC, set email to display without HTML formatting if possible.
- Remove any unneeded software from dedicated systems used to access the credit union's site
- Contact UFCU to delete online user IDs as part of the exit procedure when employees leave your company.
- Segregate duties 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.