business online banking
best practices

Avoid being a victim of a cyberheist or employee fraud. Most of today's cyberheists begin with malware that is spread via email attachments. Many of these threats can 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 include:

Out of band authentication at login and ACH/wire approval.

- You'll receive a phone call or text message with a Secure Access Code to be entered in Business Online Banking.

Session timeout:

- After 20 minutes of inactivity, you'll need to log back in with your username and password.
- After 40 minutes, you'll need to sign in with your username and password, even if you've been active during that time.
- The same rules apply for the Mobile App.

Other warnings:

- If your password is changed, we will send an email to you. If you didn't initiate the password change, please contact us immediately by calling our Business Member Service Center at (888) 200-7845.
- 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 can't use your current browser.

set up business online banking alerts

United recommends activating Business Online Banking alerts when using the ACH and/or wire modules: To set up alerts in Business Online Banking, go to Settings > Account Alerts; select New Alert, then select Online Transaction Alert. You will be provided several options for when you receive alerts, such as when an ACH and/or wire is:

- authorized
- cancelled
- drafted
- processed
- failed

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

avoid phishing, spyware, and malware

- Don't open email from unknown sources. Be suspicious of emails claiming 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, or similar information. United will never ask you for this information. Opening file attachments or clicking on web links in suspicious emails could expose your system to malicious code that could hijack your computer.
- Never respond to a suspicious email or click on any link embedded in a suspicious email. Call the source if you are unsure who sent an email. 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.

United FEDERAL CREDIT UNION we get U

Insured by NCUA. Equal Opportunity Lender. Equal Housing Lender.

computer and browser safeguards

- If an email claiming to be from United seems suspicious, contact us at (888)-200-7845.
- 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 your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.
- Install a dedicated, actively managed firewall, especially if you use 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're using. You can usually find this function in the browser's preferences menu.
- Don't use public or other unsecured computers for logging into Business Online Banking.
- Review account balances, detail transactions, and historical reporting 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.
- 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 them from inadvertently downloading malware or other viruses.
- Dedicate and limit the number of computers used to complete online banking transactions. For computers dedicated to Business Online Banking, don't allow Internet browsing or email 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 United to delete online user IDs as part of the exit procedure when employees leave your company.
- Segregate duties for online cash management services and monetary transactions by requiring separate entry and approval users.
- Establish transaction dollar limits for employees who initiate and approve online payments such as ACH, wire transfers, and account transfers.

Please call us at (888) 200-7845 if you have any additional questions!

United FEDERAL CREDIT UNION we get U

Insured by NCUA. Equal Opportunity Lender. Equal Housing Lender.