

One of Pendleton Community Bank's top priorities is protecting your company's financial information when banking online. When you apply for a business and/or non-profit online banking and bill payment account, the bank performs multiple steps to confirm your identity prior to opening the account. The commercial and/or non-profit organization is responsible for reviewing and abiding by the terms in the Agreement and Disclosure for 24/7 Online Banking.

Pendleton Community Bank will NEVER ask for your company's online banking credentials by phone, email, in person or any other means of communication. DO NOT provide your company's online banking credentials to any request online, by phone or in person. Providing this information may allow a criminal to compromise your company's deposit accounts. Immediately contact your nearest Pendleton Community Bank office if you are contacted and asked to provide your company's online banking credentials.

State of the art technology is used to keep your information secure. All passwords and personal information is encrypted and access requires passwords only employees at your company know. Your account numbers, tax id numbers and/or social security numbers are never displayed in the online banking system. If your company utilizes the Wire and Payroll features of online banking, the bank has strict operating procedures in place to assist in confirming that wire transfers and payroll file activity is not fraudulent.

Within online banking is a secure email portal. The bank may use this secure email portal to respond to online banking, bill payment, cash management and payroll assistance. Sensitive information can be securely communicated using this secure online banking email system.

Pendleton Community Bank utilizes multifactor authentication and pictures for your online banking protection. During your online banking setup, you will pick a unique picture that appears on every page in online banking and you are asked to setup three questions and answers. Always verify that your unique picture shows when you log into your online banking account. Certain activities in online banking may require you to provide the answer to the questions you created.

Your company and/or non-profit organization is NOT protected under Reg E from financial loss if your company's online banking credentials are fraudulently used. The amount of the loss you can incur if your business and/or non-profit accounts are compromised depends on how quickly your business contacts Pendleton Community Bank. Refer to the *Agreement and Disclosure for 24/7 Online Banking, Customer Liabilities – Commercial and Non-Profit Customers Only* for losses you may be responsible for.

You choose an employee as Administrator of your commercial/non-profit online banking accounts. Business online banking may include ACH, Wire and Payroll features. Your company Administrator is responsible for setting up and monitoring employee access to the online banking system. Your online banking Administrator will remove/add employees in the system and ensure that all employees with access understand the importance of not sharing log on credentials. We recommend you train your employees to practice safe internet banking. You and/or your online banking Administrator should immediately contact us if you suspect an employee has committed fraudulent activity with your company online banking accounts.

Online banking creates an opportunity for criminals (hackers) to get access to business accounts to transfer money. Pendleton Community Bank uses out of band authorization for both online wire transfers and payroll transfers. This simply means that the bank requires a phone call from your business prior to sending a wire or payroll file. Pendleton Community Bank highly recommends that businesses install anti-virus/anti-spyware on computers and keep the software up-to-date. However, the bank is not responsible for providing anti-virus/anti-spyware protection for your business pc's or errors or issues with anti-virus/anti-spyware software currently running on your business computers. Nor is the bank responsible for employee setup in the online banking system.

Protect Your Computer

Below are suggestions on how to keep your business computers safe for online banking, bill payment, ACH, wire transfers and payroll transactions.

- (1) Have a dedicated computer used only for business online banking. Do not use this computer for email, web browsing or file sharing. This lessens the chance of Trojans, viruses, spyware, and other malware being installed on the pc.
- (2) Install anti-virus and anti-spyware software on the computer and keep the software up-to-date.
- (3) Learn how to use the computer's personal firewall.
- (4) Install the latest updates and/or patches for your web browser (Internet Explorer, Firefox, etc.).
- (5) Disable the option in your browser that remembers your username and password, thus allowing automatic log on.
- (6) Disable file sharing software so unauthorized users cannot access your computer and its data.

Commercial Online Banking Best Practices

- (1) Train employees to create strong passwords. [Click here](#) to view tips for creating a strong password and tips for keeping passwords secure.
- (2) Train employees in how to recognize 'phishing' and 'pharming' and how to safely bank online.
- (3) Never leave a computer unattended once logged into the company's online banking account and ensure no one is watching when the employee enters their online banking ID and PIN.
- (4) Sign out of the online banking account, clear the web browser cache and close the web browser when the employee has completed the online banking transactions.
- (5) Ask employees to not give the business bank account number, online banking password or user ID to anyone requesting it, regardless if the request comes via an email or telephone call. Pendleton Community Bank will never call or email you requesting this information.
- (6) [Click here](#) to view a guidance on physical and cyber security published by the Department of Homeland Security.
- (7) Know who you are dealing with. Access the online banking account by typing the bank's address in the web browser (www.yourbank.com). Ask employees to Never go to a website from a link in an email and then enter their user ID or PIN. Report any unusual account activity immediately to Pendleton Community Bank.
- (8) [Click here](#) to visit StaySafeOnline for a list of resources to assist you and your employees about internet security for businesses.
- (9) [Click here](#) for a list of Pendleton Community Bank offices and contact information.