COLONIAL
Banking | Home Loans Insurance

Colonial Online Banking Fraud Prevention Best Practices

Colonial is committed to providing you secure online banking by using 128 bit encryption, SSL, layered security, and browser and intrusion testing to protect your personal and account information. The most important element of the security, fraud prevention, and identity theft prevention plan is you! Here are some tips to ensure your privacy and security when accessing Colonial Online.

User ID and Password Guidelines

* Create a strong password with at least 8 characters and includes at least one uppercase character, one lowercase character, and one number. Create a unique password for online banking.

* Do not use easily guessed personal information when selecting user name and password.

* Change your password frequently.

* Never share your username and password with others.

* Avoid using an automatic login feature that saves username and passwords.

General Online Use Guidelines

* Do not use public or unsecured computers for online banking.

* Do not leave your computer unattended if you are logged into online banking.

* Do not conduct banking transactions while multiple browsers are open on your computer.

* Monitor the sign on/failed sign on information provided on the account overview screen.

* Review your account balance and transaction history on a regular (daily) basis and notify us of any fraudulent items as soon as possible by contacting any Colonial Savings banking center or calling 817-390-2000.

* View your cleared checks to monitor for fraud.

* Take advantage of available alerts; balance, transfer, information changes, and e-mail address updates.

* Electronic statements via online banking reduce the risk of fraud and identity theft.

* Consider using online bill pay through online banking to help reduce the chance of mail fraud.

* Out of band authentication (OOBA) uses known information to verify your identity when logging in the system. Please keep your phone numbers updated.

* Colonial online banking has a digital server certificate by VeriSign that your browser uses each time you sign on to verify that you are connected to us.

* When you have completed a transaction, ensure you log off to close the connection to online banking.

* If you are using a wireless network, change the wireless password from the factory default to a complex password.

* E-mail is not a secure way to send information. Do not include any personal or account information in general e-mails. Please use the secure messaging available in online banking to communicate with us.

Cash Management ACH and Wire Transfer Users

* Use ACH pre-notes to verify that account numbers within your ACH payments are correct.

* Review transaction reporting regularly to confirm transaction activity.

* Utilize available alerts for ACH and other account activity.

* Consider requiring approval of transactions prior to submission for processing.

Tips to Avoid Malware, Spyware and Phishing

* Install anti-virus and spyware detection on all computers and keep them updated.

* Operating system and software updates, sometimes known as patches or service packs should be installed as soon as possible.

* Check your setting and select at least a medium level of security for your browsers.

* Install a dedicated, actively managed firewall, especially if you are using broadband, DSL or cable. A firewall limits the potential of unauthorized access.

* Clear the browser cache before starting an online banking session in order to eliminate copies of web pages stored on the hard drive. See your browser's Help section for instructions on how to clear the cache.

* Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from banks or government agencies that request account, personal or financial information, user names or passwords. Opening files attachments or clicking web links from suspicious e-mails could expose your system to malicious code that could highjack your computer. Call the source if you are unsure who sent an e-mail.

* Pop-up advertisements requesting personal or account information are likely fraudulent and could introduce malware to your computer. Colonial will never ask for personal information in a pop-up.

* If an e-mail claims to be from Colonial and seems suspicious, please contact us.

Mobile Banking Tips

* Criminals may develop and publish fake mobile banking applications in an attempt to steal your online banking credentials. Do not download apps being promoted by a third party or somewhere other than the official application store for your mobile device. The author or the application must be Colonial Savings F.A.

* Colonial Mobile banking applications require you to enter your online banking user id and password for access to mobile banking.

* Mobile phones offer convenience, but are easily lost or stolen. You should password protect your device and enable an automatic screen locking program. Keep a record of your device's make, model and serial number.

* You should disable your mobile device through online banking or contact us as soon as possible if your device is lost or stolen.

* Some devices support anti-virus products.

* Stay security minded when using the convenience of mobile devices. Do not use public unsecured Wi-Fi to access online banking.

Additional identity theft, fraud and computer safety links are available on the Colonial website.