American Continental Bank
美 國 大 陸 銀 行

Online Banking Security

AMERICAN CONTINENTAL BANK is constantly developing and implementing security enhancements to ensure the integrity of our Online Banking system. Our goal is to protect the confidentiality of your account and personal data and comply with all applicable banking regulations relating to the safeguarding of your data. The use, collection and retention of client information is detailed in our ***Privacy Notice***, however, there are certain topics related specifically to online banking we would like to share with you.

Security Measures

We strive to insure the security of your banking information online. These standards include:

- Your banking information never travels the internet without encryption protection. When you click on "Login", we encrypt your Online Banking ID and Password using Secure Sockets Layer (SSL) technology. The secure connection is established before your User ID and Password are transmitted and maintained for the duration of your online banking session.
- After initial login, we require you to change your online banking password before any transactions can be requested.
- Password *guessing* is deterred with a lock-out feature. The system will automatically lock a user out of the banking system when an incorrect password is used three times consecutively.
- We provide the date and time of last access to the system after login for your own monitoring purposes.
- Login sessions have a time-out limit requiring you to login again after a fifteen-minute period of inactivity.
- We have implemented a security feature which will provide additional checks to verify your identity once you are logged in to your accounts.

In addition, there are steps that you can take to protect your account and personal information while performing online financial transactions. While we continue to do everything possible to ensure the security of our system, we are not responsible for any breach of security that is outside of our control.

Online Banking Security Guidelines

- Create a strong unique online banking password comprised of 8 to 16 alphanumeric characters.
- Select a password that is hard to guess by using random letters, numbers and symbols. Do not use a word that can be found in the dictionary. Do not use readily identifiable information such as your name, birth date, child's name, etc.
- Your User ID and (temporary) password are assigned to you and verify who you are when you begin an online banking session with AMERICAN CONTINENTAL BANK. Do NOT share your password with anyone else.
- Do NOT use the *save password* option on your computer.
- Do NOT write down your password or reveal it to anyone, including bank associates.

If you feel your Online Banking User ID or Password have been stolen or compromised, change your password and notify AMERICAN CONTINENTAL BANK *immediately* at (626) 363-8988.

- Change your password regularly. We recommend changing your password every 60 to 90 days (Note: you will be prompted to change your password every 90 days).
- Remember to sign-off when you're finished banking online or leave the room for a few minutes.
- Avoid using Public Internet Access Terminals when conducting your online banking session.

Personal Computer Security Guidelines

- Use a current Internet browser with 128-bit encryption that supports secure and private transactions. Use the built-in security features that some browsers provide. Choosing certain security settings and options will help protect the privacy of your accounts and personal information. The Help Option or Properties on your browser should provide you with the security options available on your system.
- Keep your operating system and Internet browser updated with patches from the vendor's website. For example, use Microsoft's Windows Update feature and install the Critical Updates and Service Packs since these address critical security issues.
- Use virus and spyware protection software and update the software regularly in order to detect new threats.
- Use personal firewall software, especially if you connect to the Internet with a broadband (i.e. cable or DSL) connection.
- If your computer is on a wireless network, ensure that the router settings are secure.
- Use caution when downloading files, installing software, or opening e-mail attachments from unverified or unknown sources.

Internet Fraud

"Phishing" is a method developed by scammers and hackers to get unsuspecting victims to reveal their personal information and is a contributing factor to the rise in identity theft. The most common method of phishing involves cleverly designed e-mails which claim to be from reputable companies with whom the recipient may or may not have a relationship. The bogus e-mail requests the recipient to confirm personal information such as User ID, passwords, account numbers, etc. The e-mail may instruct you to "update" or "validate" your personal information via e-mail or direct you to a phony web site that looks like a legitimate web site.

- **AMERICAN CONTINENTAL BANK will not ask you to enter your personal information in an e-mail link or send such information in an e-mail. If you receive such a request in an e-mail, notify AMERICAN CONTINENTAL BANK immediately at (626) 363-8988.**
- Look for secure web pages when entering your password or financial information. Using Internet Explorer, most secure web pages begin with https:// and display a padlock icon in the bottom right corner of the browser window. A locked padlock, or a key, indicates a secure connection and an unlocked padlock, or a broken key, indicates an unsecured connection. If this is not apparent, you can review the Properties of the web page to verify that it is secure. If you are not using Internet Explorer, consult the Help Option or Properties on your browser to determine the security of web pages on your system.
- Look for legitimate web pages when entering your password or financial information. Non-legitimate web pages may use a common misspelling of the company's name in the web address or may add a word, symbol, or number before or after the name.
- For additional information on phishing, including how to protect yourself and steps to take if you fall victim, visit www.fdic.gov.