

## Email Scams

Protect yourself from Internet and email scams by keeping your private information secure. At American Continental Bank, your privacy is very important to us. That's why we want to let you know about an email scam on the Internet called "phishing" (pronounced "fishing") a technique fraudsters use to lure online consumers to fake corporate Web sites through links sent via email.

The message in the email often warns consumers that their account will be closed if their information is not updated or "verified." The links within the email are often pointed to Web forms that ask for bank account information, such as routing numbers, account numbers, PIN numbers, passwords and Social Security numbers.

It is American Continental Bank's policy to not send or request confidential account information through email because it is not a secure form of communication. You should never enter private, personal information in a form that was sent to you by email.

### Here are a few ways you can protect yourself from Internet and email fraud (phishing):

- Never click on links in unexpected emails that request confidential information. If updates to information are needed, always type the address for the institution's Web site into your browser.
- Before submitting confidential information through forms, make sure that you are using a secure Internet connection. There are two ways of determining if your connection to a Web site is secure. First, look at the address bar at the top of your browser. If the Web site address begins with "https://", then you have established a secure connection, but if it begins with "http://", then the connection is NOT secure. Second, look for a "lock" icon in your browser's status bar at the bottom right hand corner of your browser. The lock verifies that your connection to the Web site is secure.
- Make sure that you have installed and run updated anti-virus and anti-spyware software. Both viruses and spyware can leave your computer vulnerable to attack and intrusion. Anti-virus and anti-spyware software will keep your computer safe from malicious software that might have installed itself or may try to install itself on your computer. Anti-virus & anti-spyware software is especially important if you are using a broadband Internet connection like DSL, cable or satellite.
- Install a Firewall, either software or hardware. A firewall will prevent attacks on your computer through the Internet by determining if a requested connection is malicious or not. A firewall is especially important if you are using a broadband Internet connection like DSL, cable or satellite.
- Keep your Internet browser, anti-virus, anti-spyware and firewall up to date by visiting the manufacturer's Web site and checking regularly for software and security upgrades.
- Review and monitor your checking account, debit card, credit card statements and your credit report regularly to be sure all transactions are legitimate.
- Watch for misspelling or grammatical errors on forms requesting confidential information. Hackers often make errors while rushing to get bogus Web sites in place. If something doesn't look right, there is a good chance that it's not.

**American Continental Bank will NEVER request a customer's personal information (bank card number, account number, social security number, personal identification number or**

**password) through email or by phone. If you should ever receive an email or phone call requesting your personal, confidential information that appears to be from American Continental Bank, DO NOT respond and contact the Bank immediately at 1-626-363-8988.**