



Information Security Commitment and Awareness

Our Commitment to You

AmeriFirst Bank understands that your trust in us depends on how well we keep your personal, business and account information secure. Our Corporate Information Security Program is comprehensive and proactive to ensure your information is secure whether you choose to bank with us through banking offices, ATMs, telephone or the Internet.

AmeriFirst Bank utilizes industry-accepted security practices that are appropriate for the way you choose to bank with us. For your protection, no matter which channel you choose, we verify you are who you say you are before granting you access to your accounts. Additionally, our systems use firewalls and encryption to protect your information from others.

We will never send e-mails asking you to provide, update or verify personal or account information such as passwords, Social Security Numbers, PINs, credit or debit card numbers, or other confidential information.

Security Is Everyone's Responsibility

At AmeriFirst Bank, we take the safeguarding of your information seriously. In fact, we believe keeping your information safe and secure is every employee's responsibility. We also encourage you, the customer, to take steps in protecting your personal information. An excellent source of information on how to prevent identity theft and what to do if you are a victim of identity theft is the Federal Trade Commission Web site.

For more information on how we protect your information online and our approach to privacy, please see our Privacy Statement.

Security Controls and Browser Requirements

We understand the security of your personal and account information is important to you. To assist us in offering financial services in a secure manner, we employ a number of controls described below. These controls allow us to properly authenticate your identity when you access these services and protect your information as it travels over the Internet between us and your access device (such as PC or wireless device). Many of the financial services we provide use access codes, such as your login ID, Customer Access Code (CAN), password or Personal Identification Number (PIN).

Our Internet Banking and Online Bill Payment services require the use of secure browsers to protect you while you access our online services. Secure browsers allow you to communicate with these services in a protected session by encrypting information that flows between you and the site. To verify your session is secure, look for https: instead of http: in the URL address line, and a secure symbol (for example, closed padlock or key) on the status bar of your browser located on the lower part of the screen. For greater security when viewing your account information over the Internet, we recommend you use a browser with 128-bit encryption.

To provide additional protection, a timeout feature is used on selected services. This feature automatically logs you out of your account after an extended period of time. Re-establishing and authenticating your credentials for your online session helps to reduce unauthorized access to your accounts with us.

The Web site uses firewalls to protect our computer systems and your information. Firewalls can be thought of as a selective barrier that permits only specific types of traffic (transactions) through to our systems.



Information Security Commitment and Awareness

Here Is How You Can Help

While we at AmeriFirst Bank continue to provide security controls to protect your information, we believe it is extremely important for you to share in the responsibility for security. The following are some ways you can protect yourself and your accounts:

- Never share your access codes with anyone. Remember, a bank representative will never ask you for your PIN.
- We recommend you change your access codes on a regular basis. If you think your access codes have been compromised, change them and contact us immediately.
- Use only the secure e-mail service when sending or requesting account or personal information.
- Consider using a personal firewall to prevent hackers from invading your personal computer, especially if you are using DSL or a cable modem to access the Internet.
- Install virus protection software and scan all downloaded software, as well as all diskettes, before use. Also, delete e-mails with attachments from unknown sources.
- When you have completed your transactions, always click on the Logoff button on the Web site to exit the application and prevent further access to your account. When using a public PC (such as in a library or school), also close the browser when you are finished.