Security & Protecting Your Account

We at First Vision Bank encourage all of our customers to follow and use the following information, but we also know that this environment changes very quickly. Therefore, First Vision Bank assumes no responsibility or liability to our customers if they elect to use or not use any of the information listed below.

FIRST VISION BANK is strongly committed to protecting the security and confidentiality of our customer account information. First Vision Bank does not make contact with customers on an unsolicited basis to ask you for your personal electronic online banking credentials. If you get such a contact / request, DO NOT GIVE OUT INFORMATION, END THE CALL, and call your Customer Service Representative at First Vision Bank immediately to notify us of the contact.

FIRST VISION BANK uses state-of-the-art technology in the ongoing development of its Online Banking service to ensure this security. We use several different methods to protect your account information:

- You can only access FIRST VISION BANK's Online Banking with certain browsers that have a high security standard.
- Your account numbers are not displayed in full - only the last 4 digits can be viewed.
- You must have a valid Access ID and Password to logon. It must contain at least eight (8) alpha/numeric characters using upper and lower case, and at least one special character.
- If no action is taken for 10 minutes, you will be automatically logged off FIRST VISION BANK's Online Banking.

Your Responsibility:
You agree....

- Not to give out your identifying information such as your PC Password to any other person. First Vision Bank may rely on your Access ID to identify you when providing banking services to you.
- Never to leave your account information displayed in an area accessible by others.
- Never to leave your PC unattended while using FIRST VISION BANK's Online Banking.
- To always exit the system after using FIRST VISION BANK's Online Banking.
- To notify FIRST VISION BANK at 931-454-0500 or call collect immediately if you suspect that your Access ID or Password has become known to any unauthorized person, notice suspicious account activity, or experience any security related events. Ask for a Customer Service Representative to provide detail.

Fraud is a major threat and one that First Vision Bank takes very seriously. Nearly every day, users (the BAD guys) on the internet are continuously trying to hack your PC with infectious software or keystroke logging programs that can potentially provide the perpetrator with information so that they can profit illegally by the theft of your financial information and/or identity.

We urge you to fight back and protect yourself, your identity, and your information as best you can. There are several manufacturers of firewall and anti-virus software on the market. We suggest you use www.google.com or some other search engine to search for manufactures or retail sales locations that provide hardware and software products. Then, you can determine which product(s) best suit your needs. You can also read about protecting yourself online at sites like www.CNET.com or WWW.consumerreports.org.

Here is some information about Anti-Virus Software, Firewalls, and Spyware.

Anti-Virus Software – Viruses are simply programs or a piece of code that is downloaded to your computer without your knowledge. Viruses can and normally do replicate themselves and may quickly use up your computer's available memory and bring your operating system to a halt. Most of these viruses are disguised as email attachments. When the attachment is opened, the virus attaches itself to your system, without your knowledge in most instances.

There are many anti-virus software programs that have been written to assist in protecting your system from unwanted attacks. These programs are dependent up on your diligence to continuously update the program so it can watch for new viruses that come out from time to time. At First Vision, we always advise our staff to "KNOW the SENDER of email", and DO NOT open the attachment of a sender that is not known. We recommend you to do the same.

Firewalls – These devices are the first line of defense in protecting your PC and your privacy: identity / information. They are used to prevent access to your PC via the internet from the BAD guys. We recommend you have a firewall and keep it maintained and updated if you access the internet via cable or DSL. The firewall is designed to filter incoming and outgoing traffic between your PC and the internet provider's box. The firewall can be a configured to set the level of security so as to only allow information, email, and internet sites that meet your criteria to flow through to your PC. We recommend that you research for the right firewall solution to fit your needs.

Your operating system, programs installed, and other software that operates your PC need to be updated continuously to maintain a healthy and protected PC, helping to keep the risk level down for attempts to hack or take control of the PC by the BAD guys.

Know your information and stay on top of it. Watch your account(s) daily to make sure it only has transactions that you have originated and are aware of. You have the ability to review your Credit Reports. Sometimes you can get this information free, while in other instances, you may be charged a fee. The idea is to review the report to make sure there are no activities that are not yours. If you find information that is incorrect, or you don't understand, there are procedures to follow to get the incorrect information corrected.