Our Commitment to You

Standing Stone Bank wants to protect you and your accounts.

To achieve that goal, we use the latest security measures.

How do we accomplish that?

One shield is a firewall. This keeps unauthorized users from getting in. We also use a filtering router to be sure that all information goes only where it should.

For additional safety, our site requires customers to use a browser that supports 128-bit encryption. All of the well-known browsers will work inside our site.

Another shield is your user name, passcode, and security questions and answers that you will choose as you complete the application. After your application is approved and you have online access to your accounts, you can change your passcode whenever you want.

IF YOU WRITE DOWN YOUR PASSCODE AND SECURITY ANSWERS, PLEASE BE SURE TO KEEP THEM IN A SECURE LOCATION.

You can take some steps, too.

Always feel free to call us about our Web page.

Make your user name and passcode difficult. For example, use a combination of numbers, symbols, and upper- and lower-case letters.

Keep your user name and passcode a secret.

If anyone calls you for **ANY** private data, don't give it out. No one at Standing Stone will ever call you for your account number, user name, or passcode.

Don't send your confidential information to anyone through an email. Standing Stone will **NEVER** send an email to you that asks you to submit or confirm personal information.

To take full advantage of the latest technology, we strongly encourage you to keep your computer's browsers updated to the most recent version. Also, most browsers offer automatic updates.

Install an anti-virus program, keep it up to date, and run scans regularly. (Note: Experts recommend installing only one anti-virus program.)

Use and keep up to date an anti-spyware program, in the event that the anti-virus program does not have this feature.

Be careful downloading **ANYTHING** from the internet. If you don't trust the source, don't download it.

Be especially careful with email. If your email service has a spam blocker, consider using it.

Open email only if you're sure that you know the sender. Even if you do know the sender, use great care opening any attachments.

If you have any further questions regarding on-line security issues, please feel free to call us at 740-653-5115.

For additional information, you may also go to the Federal Trade Commission's website on Identity Theft: http://www.ftc.gov/bcp/edu/microsites/idtheft/.