Online Security

Online Banking has multiple layers of security to keep your information secure. Some of these items include:

- Advanced firewalls and filtering routers.
- Multi-Factor authentication. Unregistered computers our devices will prompt users to reply to a challenge question.
- 128-bit encryption. All information is encrypted at rest and when traveling over the internet.
- Auto logout. If your account is not logged out within 10 minutes, we will do this for you.
- We require you to choose a unique Online Banking password and user ID.
- Last login notification. On the summery page, there is a date of time displayed of your last login to help alert you of authorized access.

Things you can do to increase security:

- Always use a strong password consisting of at least eight characters including numbers, capital letters and symbols. Do not write your password down where it will be easy for others to find or share it with others.
- Change your password frequently—every thirty days is recommended.
- Never disclosure your personal information or password.

Do Not Disclose your Personal Information

- Farmers State Bank will never send you an e-mail asking for personal or account information. Never disclose personal information by e-mail.
- E-mail unless encrypted is not a secure form of communication and should not be used for sensitive information such as social security or account numbers.
- Always log out when you are finished viewing account information.
- Do not respond to any e-mail that threatens to close or suspend accounts unless you "verify" your information. Criminals send e-mails designed to look like official communications from banks or government agencies, but these e-mails are scams designed to acquire your personal information such as access IDs, passwords and other personal information.

Use Anti-Virus Software and Keep your OS and Browser Up to Date.

- Configure your computer to automatically download and install operating system updates. These updates contain important security patches and other stability enhancements.
- Make sure you keep your web browser updated as well for your security.
- Install reliable anti-virus software and keep it up to date to protect your computer from viruses, spyware and keystroke loggers, which can be used to steal your personal and financial information. These programs often come in a suite that also contains spam filters, pop-up blockers and a firewall. Make sure that the product you select has those features.
- Be sure to configure your anti-virus software to regularly run virus and malware scans.

Customer Responsibility

These are some items that are outside our control and are your responsibility:

- Customer input errors.
- Negligent handling or sharing of Online Banking account numbers by the customer.
- Leaving computers or devices unattained without properly logging off.
- Failure to report known incidences of password theft or unauthorized Online account access within 2 business days of discovery.

Contact Us Immediately If You Notice Anything Suspicious

- Review all accounts regularly to detect unauthorized activity.
- Notify us at 509.996.2244 immediately if you suspect that your Access ID or Password has become known to any unauthorized person.