Safety Tips for Online Banking

Keep your Windows software updates current on your pc or mobile device.

Keep your anti-virus and anti-malware software current on your pc or mobile device.

Use a strong PIN (password) for your pc and (passcode) for your mobile device.

Use a strong PIN (password) for your online banking and mobile banking accounts (do not use names, nicknames, pet names, addresses, etc.)

Avoid writing down online banking or mobile banking User ID or PIN.

Internet browsers may save User ID's and PIN's.

For your security, please review your Internet browsers "Help" section, or contact their Customer Support, to see if this option is available and how to turn it off.

Look for https:// when signing onto the Farmers Bank web site home page: this means Farmers Bank has taken extra steps to protection your personal information.

Look for the 'small lock' when signing onto the Farmers Bank web site home page: this means that your information is being encrypted.

Avoid accessing your online banking using a public wireless connection.

If you are a mobile banking customer, download the 'FREE' Farmers Bank App (I Phone or Android) so you will not be directed to a fraudulent web site.

Commercial online banking customers, designate a pc that will be used only for online banking purposes (this pc should also be housed in a restricted, locked office at your business.

Look for the Customer Summary Information, once you have logged onto your online banking account page, it will display the last time YOU accessed your online banking!

Review your bank accounts using your online banking or mobile banking regularly.

Click on the 'Exit' when leaving the Farmers Bank web site or mobile banking app and always remember to close your browser session.

Farmers Bank will never send e-mails, text messages, or phone you directly asking for any account information.