Farmers Bank of Willards

INTERNET/MOBILE SAFETY TIPS

1. INTERNET BANKING

- ☐ Avoid using public computers to access your Online Banking.
- ☐ Do not give any of your personal information to any web sites that do not use encryption or other secure methods to protect it.
- ☐ Keep security software current on all of your devices; pc, tablet, smartphone, etc.
- ☐ Protect all devices that connect to the internet from viruses and malware.
- ☐ The Bank will ONLY ask for your user name if your password &/or security questions need to be reset.
- ☐ Remember the Bank would never contact or text message you asking for personal or banking information. Assume any unsolicited text request is fraudulent and do NOT respond.
- ☐ Never set your online banking &/or app to automatically log you in to your bank account. If your pc or phone is lost or stolen, someone would have free access to your account.

2. PASSWORDS

- ☐ Make passwords long and strong: combine capital and lowercase letters with numbers and symbols. Use paraphrases.
- ☐ Unique account, unique password: separate passwords for every account helps to thwart cybercriminals.
- ☐ Write it down and keep it safe: everyone can forget a password. Keep a list that is stored in a safe, secure place away from your computer.
- ☐ Do not use personal information for your user names and passwords like birth dates & SSN.
- ☐ The Bank will NEVER ask you for your password.

3. MOBILE BANKING

- ☐ Secure your phone: Use a strong passcode to lock your phone.
- ☐ Think before you app: Make sure the mobile apps you use are safe and legit. In fact, make it a golden rule for any app you want to download: go to trusted sites only, check the app's ratings and carefully read its permission requests and reviews from other users.
- ☐ Get savvy about Wi-Fi hotspots: Use caution with the type of business you conduct while on public Wi-Fi hotspots and adjust the security settings on your device.
- ☐ When in doubt, throw it out: Links in emails, tweets, and online advertising are often the way cybercriminals compromise your pc, phone &/or tablet. If it looks suspicious, it is best to delete or mark as junk mail.