



Online Banking Security and Safety Tips

Simple habits. Stronger protection.

Online and mobile banking make managing your money convenient. A few everyday precautions can help protect your accounts, personal information, and devices. Use these tips to recognize common scams and bank with greater confidence.

Protect your passwords and sign-in codes

Use a long, unique password for online banking that you don't use for any other account. Avoid names, birthdays, and other information someone could easily guess. A reputable password manager can help you create and store strong passwords.

Keep your password, PIN, and one-time sign-in codes private. Never share them with someone who contacts you unexpectedly, even if they claim to represent your bank. Only enter a sign-in code when you are signing in through the official website or app. Do not approve a login request you didn't initiate.

Add another layer of protection

Enable multifactor authentication wherever it's available, especially for your email account. Your email can be used to reset passwords for other services, so protecting it is an important part of protecting your finances.

Use a screen lock on your phone, tablet, and computer. Enable fingerprint or facial recognition on supported devices when appropriate, and don't leave an unlocked device unattended.

Go directly to Farmers Bank

Start your online banking session by typing gofarmersbank.com into your browser or using a bookmark you created from the official site. For mobile banking, use GoFarmers Mobile and follow the app-store links on our website when downloading it.

Check website addresses carefully before entering information. A familiar logo or professional-looking page does not prove a website is genuine. HTTPS helps protect information in transit, but even a fraudulent website can use it. Never ignore a browser security warning.

Pause before you click scan or respond

Scammers use emails, text messages, phone calls, and QR codes to trick people into revealing information or sending money. Be cautious of unexpected messages that:

- Claim your account is locked or a payment failed
- Pressure you to act immediately or keep the conversation secret
- Ask you to verify information through a link or attachment
- Tell you to install software or give someone remote access to your device
- Request payment by gift card, cryptocurrency, or an unfamiliar payment method

If you're unsure, stop and contact the organization using a number you already trust. Don't use the phone number or link in the suspicious message. Caller ID can be faked, so a familiar name or number is not proof of who is calling.

Watch for safe account scams

Be suspicious of anyone who tells you to transfer or withdraw money to "protect" it from fraud. An unexpected caller may impersonate a bank employee, government agency, or technical support representative.

End the conversation and contact Farmers Bank directly before taking action. Never let pressure or urgency replace an independent check.

Keep your devices up to date

Install updates for your operating system, browser, banking app, and security software promptly. Turn on automatic updates when available. Download software only from trusted sources, and avoid using devices that no longer receive security updates.

Bank from a device you control

Use your own updated device whenever possible. Avoid signing in on shared or public computers. When choosing a connection, prefer your trusted home network or cellular data rather than an unfamiliar Wi-Fi network.

Sign out when you finish banking. Before selling, trading in, or recycling a device, remove your personal information and follow the manufacturer's instructions for securely resetting it.

Keep an eye on your accounts

Review your transactions regularly and read your monthly statements. Use available account alerts to help stay informed, and keep your contact information current so important notices can reach you.

Report unfamiliar transactions or unexpected account changes promptly. Don't wait for your next statement if something looks wrong.

Double-check before sending money

Confirm the recipient and payment details before sending a transfer or person-to-person payment. If a friend, family member, or business unexpectedly asks for money or changes payment instructions, verify the request through a trusted phone number. Messages can come from compromised accounts, and voices can be imitated.

Contact us promptly if you think something is wrong

If you notice an unfamiliar transaction, share information with a suspected scammer, or believe someone has accessed your account:

1. Stop communicating with the suspected scammer and contact Farmers Bank at **479-996-4171** during normal business hours. Explain what happened so we can help you determine the next steps.
2. From a trusted device, change any exposed passwords and any other accounts that use the same password. Secure your email account, too.
3. Save relevant messages, receipts, and transaction details. Do not send passwords, PINs, or full account numbers through ordinary email or a website contact form.
4. Report the scam at [ReportFraud.ftc.gov](https://www.ftc.gov/identitytheft). If your identity may have been stolen, visit [IdentityTheft.gov](https://www.ftc.gov/identitytheft) for recovery guidance.

Lost or stolen debit or ATM card

For a lost or stolen Farmers Bank debit or ATM card, call **479-996-4171** during normal business hours or **1-888-297-3416** after hours.

When in doubt, pause and call. We're here to help you take the next step.