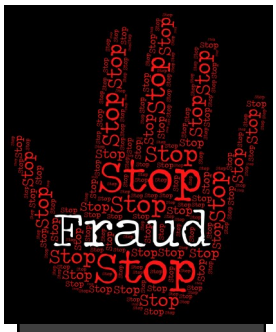

Protecting Your Account From Fraud

Checking

Online

Debit Cards

Have you received a check that is:

...payment for something you sold on the internet:
...made payable for an amount more than you were expecting?
...connected to someone you have only communicated with by email?
...commission or payment to receive a larger deposit or transfer additional money through your account?
...drawn on a business or individual account that is different than expected?
...an initial payout for a loan, or lottery, where you are asked to purchase gift cards, wire money, or return some of the funds in order to get the rest of the loan amount or winnings sent to you?

You could be involved in fraud or a scam!

Protect Yourself from Identity Theft:

- Keep your computer and mobile devices up to date
- Establish strong passwords; mix upper and lowercase letters, numbers and symbols.
- Keep your personal information personal; hackers use social media to figure out answers to security questions like maiden names, pet names, birthdays, etc.
- Secure your connection; don't send private information over public Wi-Fi connections, and protect your home wireless network with a password.
- Look for secure sites: website addresses should begin with https, and a tiny padlock symbol should appear on the page.
- Watch out for fraudulent links. Do not click a link to confirm or provide private information that has been sent to you in an email.
- Do not provide your online banking or account information to an unknown third-party.

Protect Your Card:

- Keep your card in a safe place, just like you would cash or checks.
- Immediately notify Landmark if it is lost or stolen.
- Keep your Personal Identification Number (PIN) a secret. Never write it down anywhere, especially on your card.
- Never give any information about your card or PIN over the telephone, unless you are authorizing a purchase.
- If you are asked to provide your card number for a free trial, you'll probably get charged later for an automatic renewal, shipping, or other unexpected costs.
- Be aware of your surroundings at a payment terminal or ATM. Make sure no one is watching you enter your PIN.

LANDMARK NATIONAL BANK

Common Scams

Emergency Scam

What is it?

Scammers pose as a family member or friend, claiming they were in an accident or have been arrested and need emergency money.

Stop it!

Ask questions a stranger couldn't answer

Verify the story by calling other family or friends in your circle. Use telephone numbers you know are correct—not numbers provided by the caller.

Romance Scam

What is it?

Scammer professes love quickly, often claiming to be overseas for military service or business. Asks for money for travel or other emergency and promises to visit soon.

Stop it!

Be careful what you post on social media sites. Criminals use personal information to manipulate.

Research the person's photo and profile using online searches.

Never send money to someone you have not met personally.

Lottery/Prize Scam

What is it?

Scammer gives you notice that you have won a lottery or large prize. Asks you to send money for taxes or processing fees.

Stop it!

If you didn't enter—you didn't win. Ignore all calls, emails and letters.

Never provide your social security number in order to claim a prize. Never send money for fees.

Never agree to buy a "winning" ticket from someone. It's likely fake.

Member FDIC

Remember, Landmark National Bank will never call you or email you to confirm your account number, social security number, or debit card number. We may ask you those questions if you call us to verify your identity, but you should only call us on published numbers. Here's the best way to reach us:

By Phone: 1-800-318-8997

By Email: LNBMail@banklandmark.com

(please, never put private information like account numbers in your email!)