Think Before You Click: How to Spot Email Scams

In recognition of National Email Week, it is a good reminder to talk about something that continues to affect individuals and businesses every day: email scams.

Scammers have become increasingly sophisticated in how they create fraudulent emails. Many of these messages look like they come from trusted companies, financial institutions, government agencies, or even people you know. Their goal is often the same: create a sense of urgency and convince you to click a link, open an attachment, or provide personal information.

Watch for Common Warning Signs

Many scam emails share similar characteristics. Be cautious if you receive a message that:

- Claims there is a problem with your account that needs immediate attention
- Asks you to verify personal or financial information
- Includes unexpected attachments
- Contains links that direct you to unfamiliar websites
- Creates pressure by saying you must act immediately

For example, you might receive an email that appears to be from a package delivery company claiming your shipment is delayed and asking you to click a link to update your address. Another common scam involves messages that appear to come from a bank asking you to confirm your online banking credentials.

Slow Down Before You Click

One of the best ways to protect yourself is to pause before taking action. If an email seems unusual, take a closer look at the sender's email address. Scammers often use addresses that look similar to legitimate companies but contain small differences. You can also contact the company directly using a phone number or website you know is legitimate rather than using information provided in the email. A good rule of thumb is simple: if you were not expecting the email, be cautious about clicking links or opening attachments.

Your Bank Will Never Ask for Sensitive Information by Email

At Bank of Lake Mills, protecting your financial information is a top priority. We will never ask you to provide sensitive information such as passwords, account numbers, security codes, or online banking credentials through email. If you receive a message claiming to be from the bank and are unsure whether it is legitimate, contact us directly before responding 920-648-8336.

Stay Alert

Email scams continue to evolve, but their purpose remains the same: gaining access to your personal information. Taking a few extra seconds to verify a message, check the sender, and think before you click can help prevent fraud and keep your information secure.

When it comes to email, slowing down and taking a second look can make all the difference.