STOP THE SCAMS – June 2022

Criminals today are becoming more creative, using emails, phone calls, and text messages in their scam attempts. A common tactic is for cyber-criminals to impersonate companies, especially banks, even spoofing phone numbers and email addresses designed to trick you.

Here's What You Can Do:

- **If a phone call seems suspicious, hang up right away.** You can always call back using a known phone number, such as the number listed on a company's website or on the back of your bank card.

- **Text message or email seem odd?** Never click links or open attachments, and delete these communications right away. If a message asks you to take action urgently, that's a red flag. Also, check email addresses and wording closely for misspellings – this is another indication of a scam.

- **Only use payment apps to send money to people you know and trust.** Additionally, your bank will never ask you to send money using a payment app.

Remember, LincolnWay Community Bank will never send you an unsolicited email, text message or phone call asking you to share your account or PIN number, social security number, password, or security questions.

If you notice suspicious activity or feel your LincolnWay account has been compromised, notify us right away at 815-462-4300 or contactus@lwcbank.com. As a reminder, NEVER include sensitive account or personal information in an unencrypted email.