PHISHING REMINDER

Unfortunately, there are a lot of very creative people out there that would love to get their hands on your sensitive and confidential information. Fidelity Bank would like to remind you of a few things that you can do to help protect your information from fraudsters:

- **Passwords:** NEVER provide your passwords to anyone. That information is yours, and yours alone, and you should be suspicious of the intent of anyone that asks for it. As a reminder, Fidelity Bank will never ask you for your passwords.

- **Websites:** You should never type confidential information (including your password) into a website that is unsecure. Any website that starts with http://, and not https://, is not secure. In addition, your browser (depending on which one you use) will normally indicate whether a site is secure by displaying a locked padlock in the address bar.

- **Emails:** The days of emails using broken English that are relatively easy to identify as a scam/phishing attempt are gone. Even if an email looks and sounds official, if the email is coming from an unrecognized email address, or uses terms that aren't typically used in the email's context, be suspicious of it. Do not click on any links that are in the email until you verify the validity of it.

- **Phone Calls:** If you cannot verify the identity of the person on the other end of the phone line or the purpose of their call, don't provide any confidential information to them. The fraudster will try all kinds of tricks (including playing on your emotions), and may even drop a name or two of people at the Bank, but be suspicious.

Having to use the word "suspicious" above is unfortunate, but it is a part of the world that we live in now. The importance of maintaining a cautious level of suspicion is critical. Keeping the above in mind daily will help to avoid fraudulent situations.