SECURITY

Reliance Bank is committed to keeping your personal and financial information secure. We know that security and confidentiality are a significant concern, and we want you to feel safe and have confidence using all our digital banking applications. We take all the necessary measures to ensure the safety of your information. Here are some simple online security precautions you can take to help conduct your financial transactions safely.

DIGITAL SECURITY BEST PRACTICES:

- Regularly update and use strong passwords for all online accounts
- Connect to secure Wi-Fi
- Use your mobile devices securely: install Apps from trusted sources, keep your device updated, avoid sending sensitive personal information over text message or email
- Learn about Phishing Scams – be suspicious of email from unknown senders, don't open email from people that you do not know, know which links are safe and which are not, when in doubt don't click on the link
- Review your online accounts and credit reports regularly for changes

An important reminder, Reliance Bank will NEVER ask for personal information like the PIN or 3-digit security code on the back of a card. If at any point you are uncertain about questions being asked or just uncertain about a call, text or email itself, call Reliance Bank directly.

HOW DO YOU KNOW IF ITS PHISHING?

You might have heard about online scams or phishing, when a person receives an email to their regular inbox or spam inbox that looks like something official. Often, these “phishers” do a very realistic job to make their communication look genuine, but it is not. How do you know if an email is malicious?

Phishing emails are designed to be rather tricky and difficult to differentiate from safe emails. The address where the message is from could say the name of a bank, company, or even a government agency. However, legitimate companies have domain emails. Check the email address by hovering your mouse or cursor over the ‘from’ address. Make sure no alterations have been made (for instance additional numbers or letters transposed).

Phishing emails can have realistic logos, colors, text or other visual elements that are designed to trick you. Always keep in mind that legitimate companies will not request your sensitive information via email, will usually call you by your name, and will not use bad grammar (possibly the easiest way to recognize a scam). Most importantly legitimate companies will not send emails with unsolicited attachments. If you were not expecting the link or attachment best practice is to not open it.