Awareness Is The Best Protection.

PUT A LOCK ON FRAUD AND IDENTITY THEFT

SCAMS ARE ON THE RISE. HERE'S WHAT YOU SHOULD NEVER DO.

DO NOT

trust every email you receive. Fraudsters will try to grab your attention by pretending to be a well-known bank or company. They will create emails and texts with the logos and colors of reputable companies so they look legit.

DO NOT

click on links in an unexpected email, text message, or direct message that asks you to send money. Delete suspicious emails, texts and social media messages right away.

DO NOT

give out your username, PIN or password. Scammers can spoof phone numbers, too. If a phone call seems suspicious, hang up right away and call the company back using a known number on the company website or the back of your credit or debit card.

DO NOT

send money to someone you do not know. When using Mobile Payment Apps such as Zelle, Venmo, Google Pay, PayPal and Cash App, verify that you know the person. These payment apps are just like cash and once you send the money, it's gone. Consumers have limited protection from fraudulent and unauthorized activity from these apps.

Protect Your Accounts. Here's What You Should Do.

- Keep your contact information up to date within Online Banking
- Use multi-factor authentication
- Set up alerts within Online Banking
- Activate card controls within your Mobile App
- Never share your credentials
- Check your payment app and bank accounts regularly
- Create the strongest possible passwords
- Keep your devices up to date with the latest browsers and operating systems
- Enable fingerprint sign-in or facial recognition
- Know the red flags that signal a scam
- Know which third parties have access to your account information

PrimeSouth Will Never Ask You For:

- **One-time passcodes**
- **Passwords of any kind**
- **Full Social Security number**
- **PIN number**
- **Debit or credit card 3-digital security code or exp. date**
- **Online banking secret word of password**
- **Account number**

As your bank, we already know this information. If we contact you, we will always use your name or account information. If anything sounds unusual, trust your gut! Hang up and contact us using a trusted channel!

WHAT TO DO IF YOU ARE A VICTIM OF FRAUD

1. **Contact us right away!**

2. Report it to the payment app or service and ask to reverse the transfer.

3. Report it to the Federal Trade Commission at **reportfraud.ftc.gov.**

PRIMESOUTH BANK

Find Your Prime

Member FDIC