PROTECT YOURSELF FROM FRAUD & SCAMS

Beware of Spoofed Calls & Texts

Scammers may pretend to be the Bank, including spoofing the Bank's phone number, and:

- Claim a fake ACH, wire, or other account issue.
- Urge you to "act now".
- Send a link to "verify your identity" or "login".

Banks Will NEVER Ask For:

- Your online banking password.
- Your PIN.
- Your full account number.
- One-time passcodes.

If someone asks - hang up immediately.

Stay Safe

Do:

- Verify the website before logging in - even better, use a bookmark, favorite, or the Bank's official mobile app.
- Review your account often.
- Use multifactor authentication (MFA).
- Call us directly if something seems suspicious.

Don't:

- Click unexpected links.
- Share personal or account info.
- Use public computers for banking.

Mobile Safety

- Use strong passwords.
- Avoid saving passwords in your phone browser.
- Use a password manager or biometrics.

If Something Doesn't Feel Right

1. Do NOT click links or respond.
2. Call your bank using the number on their website or statement.
3. Report anything suspicious.

Your Security Is Our Priority.

Shore United Bank