

Financial institutions nationwide are reporting a surge in spoofed calls and texts from criminals impersonating bank employees. These scams are sophisticated, using technology to make calls appear as though they're coming from a legitimate financial institution, then pressure clients into sharing sensitive account information before they have time to think it through. They use fear of fraud or compromise to create a sense of urgency.

What does a spoofed call or text look like?

The caller or sender typically claims there's urgent activity on your account like a suspicious transaction, a security breach, or a login attempt. Then they ask you to verify your identity by providing account numbers, passwords, PINs, one-time passcodes, or login credentials to “block a compromised profile” and set up new access. The urgency is key, so you’ll act before you question whether the request is legitimate.

How can you protect yourself?

- **Even if the call appears to come from a trusted number**, never share account numbers, passwords, PINs, Social Security numbers, or one-time passcodes over an unsolicited call or text, regardless of who the caller claims to be.
- When in doubt, hang up and call your bank directly using a number you already have on file.
- Scammers rely on urgency, so slowing down is your best defense.
- Remember that First Business Bank and other financial institutions will never ask for sensitive personal information through unsolicited calls or texts.
- If you receive a suspicious communication, do not engage, document any contact information you can, and report it to our Treasury

Management support team at 608-232-5938 or
tmsupport@firstbusiness.bank.

Please [visit our website](#) to learn more about trending scams on the rise. Your reports help us track active threats and protect all our clients. Thank you for your vigilance.