nebraska state bank
& trust company
P.O. Box 688
Broken Bow, NE 68822
www.nesb.bank

It has come to our attention that scammers are spoofing the NSB main phone line, 872-2466, and pretending to be from our fraud department.

If you receive a call from “Nebraska State Bank” never be afraid to say, “Let me call you back on another line” and hang up. Then you may call 872-2466 back and ask for the person who said they were calling. If that person is an employee you will be passed to them and you may continue the legitimate conversation.

Text message fraud alerts from NSB will always come from sender ID 32768 if you receive an alert from any other number just delete and do not respond.

Learn how to recognize fraudulent caller ID spoofing.

You are best served by learning how to recognize scams that use spoofing for yourself in order to avoid them entirely. Utilize these tips to help you:

- **Be skeptical of generic greetings**, such as ones that address you with “Dear customer,” as opposed to your real name.
- **Avoid answering unknown numbers**, as scam callers will regularly use unknown numbers.
- **Pay attention to the caller’s tone of voice**, and avoid giving information to a caller who seems pushy or demanding. This is a tactic employed by scammers to make matters appear urgent, thereby manipulating the human agency to react.
- **Be wary of the reason a caller gives you for needing your personal information.** If the caller says they need it for an event you had never previously heard of, hang up immediately.
- **Don’t stay on the phone line.** Trust your gut if you have any concerns regarding the legitimacy of the caller. Hang up immediately.

If you happen to fall victim to a spoofing attack then it is time to contact a government agency capable of investigating the incident and enforcing fraud statutes and fines.

Protect your personal information.

Many of the tactics used by scammers are employed to gauge your vulnerability. Scammers want to know how receptive you are to revealing information so that they target the right people. Each of the tips mentioned below will help you protect your personal information and avoid being the target of caller ID spoofing:

- **Don’t answer calls from unknown numbers**. If you do, hang up immediately.
- **Don’t hit any buttons**. If the caller asks you to, hang up immediately.
- **Don’t answer any questions**, especially ones regarding your personal information.
- **Never reveal personal information**, such as your Social Security number, mother’s maiden name, passwords, or credit card numbers.

- **Don’t assume they are who they say they are**. If you receive a call from somebody representing a company or a government agency, hang up and call back the phone number on the company or agency’s website. This will help verify the caller.
- **Don’t put your trust into the caller** until you can assure they are who they say they are.
- **Don’t panic**. Social engineers will see this as vulnerability and try harder in their attempts to manipulate you into revealing personal information.
- **Set a password for your voicemail account**. A scammer could hack into your voicemail if it is not properly secured with a password.

Any U.S. citizen who believes they are a victim of caller ID spoofing can file a report with the FCC Consumer Complaint Center. The FCC imposes a fine of up to $10,000 per violation.

Source: https://www.verizon.com/articles/caller-id-spoofing/

Thank you to everyone who let us know about this issue.

Kyle Stringham | AVP, IT & Security Officer