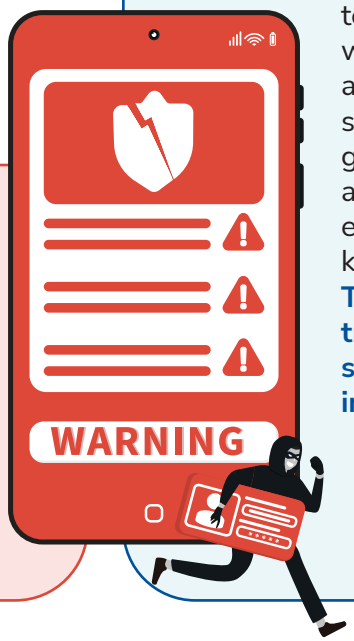
LOCK OUT FRAUD

# SPOOFING SCAMS:

## DON'T BE FOOLED BY A FAMILIAR NAME

## BEWARE OF SPOOFING

Spoofing occurs when scammers disguise a phone number, email, text message, or website to appear as a trusted source, such as your bank, a government agency, a utility company, or even someone you know. **Their goal is to trick you into sharing personal information, providing login credentials, or sending money.**




## WHY SPOOFING IS **DANGEROUS**

Spoofing scams can be very convincing because they appear to come from a legitimate source. Criminals often claim there is fraud on your account, that your account will be locked, or that you must act immediately to protect your money.

They may ask for passwords, PINs, one-time passcodes, or account information. Remember: caller ID, email addresses, and text messages can be spoofed. **A message that looks legitimate may still be a scam.**

**THE MOST IMPORTANT THING TO REMEMBER:**

**STOP. VERIFY.**

**Banks will never ask for your password.** A few minutes spent verifying a request by contacting your bank directly can prevent a costly loss.

## IF YOU'VE BEEN A VICTIM OF SPOOFING

Contact your bank immediately to report the incident. Change passwords for any affected accounts, especially online banking, email, and other financial services, and enable multi-factor authentication if it is available. Review your account activity carefully for unauthorized transactions and continue monitoring your accounts in the weeks that follow. Wisconsin consumers should also report the incident to local law enforcement and the **Wisconsin Department of Financial Institutions.** If personal information has been compromised, **visit IdentityTheft.gov** for step-by-step recovery resources and guidance. Most importantly, don't be embarrassed. Scammers are skilled at making fraudulent communications appear legitimate, and reporting suspicious activity promptly can help prevent additional losses.

## HOW TO **PROTECT YOURSELF**

- **Never share** passwords, online banking credentials, PINs, or security codes.
- **Hang up and call your bank directly** using a trusted phone number from its website, statement, or debit card.
- **Do not** click unexpected links or download attachments from unknown messages.
- **Enable** multi-factor authentication whenever available.
- **Use strong, unique passwords** and change them immediately if you suspect they have been compromised.
- **Trust your instincts.** If something feels suspicious, stop and verify before taking action.

Wisconsin Bankers ASSOCIATION