



Spoofing scams are getting trickier and more frequent.

Spoofing scams are on the rise. Fraudsters are getting more skilled at posing as trusted financial service providers to gain access to your private information. Here at Oak Bank, we want to help you understand scammers tricks so you can keep your information safe.

This is how a Spoofing Scam works:

- You receive an unsolicited call that appears to be from Oak Bank or some other service provider that you are associated with. (Your caller ID may even say “Oak Bank” or show Oak Bank's phone number.)
- If you hesitate to provide their requested personal info, the scammer tries to convince you they're legitimate because of the “real” phone number – saying “Look at the number, it says this call is from Oak Bank!”
- If you ask the scammer a question about the bank or to provide more information, they hang up.

And here's a trickier scheme scammers use to appear more trustworthy:

- The scammer claims they've noticed fraudulent charges on your account and asks for your username and password to “fix” the situation.
- After accessing your account, they'll reset your username and password, prompting a one-time PIN (OTP) to be sent for you to verify the change. The scammer assures you providing this OTP is just part of the process.
- The scammer then uses that OTP to validate a new device or to gain full access and control over your account (which may stop you from being able to log in to your account).



Remember, Oak Bank will never reach out to you randomly requesting one-time passwords (OTPs), debit or credit card numbers, PINs, or username/passwords.

Take the following steps to protect yourself:

- Hang up on any unsolicited caller asking for personal or account information.
- Do not click any links in an unsolicited text or email asking for personal or account information.
- Be sure not to call, text or email any contact information given to you by the caller.

More tips to help you stay safe:

- Know who you're talking to. If you have any doubts that you are speaking to an associate of the service provider that they say they represent, hang up and call the number you have for them in your personal contacts.
- Take a moment. Think about what they're asking for, and verify they are who they say they are, especially if it feels urgent or pressured — it could be a scam.
- Be extra careful when sending money. It's important to verify you're not sending money to a scammer. Once you send money you may not be able to get it back.

Please reach out to us right away at 608.441.6000 if:

- You think you've given out your personal information to someone posing as Oak Bank or another questionable contact, or
- You've experienced a fraud attempt, or
- You've heard about a scam you'd like to report.

For additional security information, you can visit [Oak Bank's Security Information](#) on our website.



Need help with your account?

Email: bank@oak.bank

Call: 608.441.6000

- If your Oak Bank Debit/ATM Card has been misplaced, call 877.755.2957.
- If you have misplaced your Oak Bank Visa Credit Card, call 800.423.7503.

[VISIT OAK BANK ONLINE](#)



608.441.6000
877.625.2265 Toll Free



Lobby
M - F: 8 a.m. - 5 p.m.



Drive-up
M - F: 8 a.m. - 5 p.m.





Oak Bank | 5951 McKee Road, Suite 100 | Fitchburg, WI 53719 US

[Unsubscribe](#) | [Update Profile](#) | [Our Privacy Policy](#) | [Constant Contact Data Notice](#)



Try email marketing for free today!