Oak Bank

You can't be the best, if you're only the same!

SECURITY UPDATE - FEBRUARY 2022

Vishing and Smishing

Have you ever been hesitant to reply to an unknown text message? Maybe you are getting those anonymous calls with the caller ID showing as "unknown." Cybercriminals are always looking for new ways to steal your personal information using vishing (phishing + voicemail) or smishing (phishing + SMS) or texting. We share ways to identify these kinds of scams and how to prevent them below.

What is vishing?

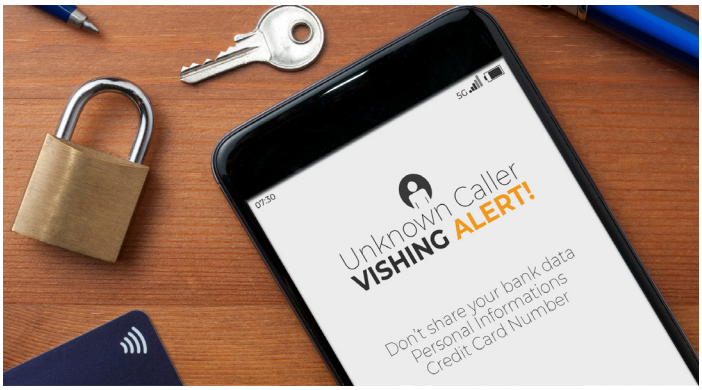
Vishing is a form of phishing where a phone call or voicemail message appears to be from a trusted source. A vishing phone call may claim to be from your bank, the IRS, the Social Security Administration, Apple, Amazon or Medicare.

How to protect yourself from vishing?

- **Do not answer the phone if you don't recognize the number and let it go to voicemail. Most caller IDs can be faked.**
- **Do not respond to any questions if you pick up a call and think it's vishing. Instead, hang up and block the number.**
- **Never provide personal information that you wouldn't give a stranger.**

Types of vishing scams:

- **Compromised bank accounts**
- **Credit/debit card scams**
- **Unsolicited loan or investment offers**
- **COVID-19 information emails**
- **Medicare or Social Security scams**
- **IRS tax scams**



What is smishing?

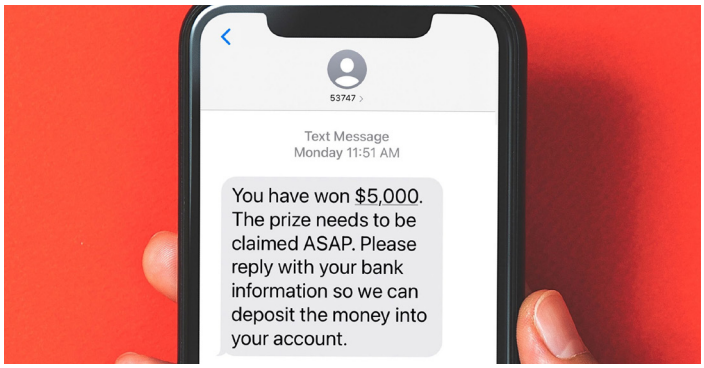
Smishing is another form of phishing. Rather than an email or phone call, a text message is sent to the user's cell phone that appears to be from a trusted source to encourage them to click on the link.

How to protect yourself from smishing?

- **Do not click on links in text messages when you don't recognize the phone number.**
- **If you get a text message from a company, make sure the information is the same on their website, with their phone number and their text.**
- **If the text message contains a routing number associated with a package, look for altered URLs. (Ex: ama.zon.com vs. amazon.com)**
- **Scammers often use location data. You can "spoof" your location by using a VPN for your mobile device.**

Types of smishing scams:

- **Messages about your credit card or bank account that are "urgent."**
- **Notifications that you have won something.**
- **Fake survey links.**
- **Fake messages that a package was delivered from a trusted brand.**



Remember!

Oak Bank will never ask clients to send personal information by phone or text.

If you receive an unsolicited phone call or text message requesting your Oak Bank account information, report it immediately by calling 608.441.6000 or sending an email to bank@oakbankonline.com.

*For additional security information you can visit **Oak Bank's Security Information** on our website.*