Oak Bank

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

SECURITY UPDATE - MAY 2022

Watch out for 'phishy' emails!

The average person gets 100 emails a day. And not all those emails are legitimate. Some are purposefully designed to steal your personal information. Learn how to recognize these fake emails and keep your information private by reading more about email phishing.

What is phishing?

Criminals use emails, and other methods, to impersonate legitimate businesses or individuals and steal your personal information.

Hints something might be email phishing:

- Instead of addressing you by your name, the email uses a generic greeting like "Dear Customer."
- There is an urgent tone to the email that requires you to act immediately (ex: fraud on your financial account).
- You receive an email with an attachment you didn't expect, and the email says you need to open it right away.
- The email or response requires sensitive information such as your credit card number or password.
- A link in the email doesn't look legitimate and takes you to a different URL than you were expecting.

Prevent email phishing:

- Never provide personal information in response to an email request.
- Be cautious when opening unsolicited attachments or links.
- Verify the destination of links in email messages, even if it came from a trusted source.
- Watch out for tricky URLs like www.am.zon.com.

Remember:

- Phishing email attacks are straightforward and require little effort from scammers, which is why they are so prevalent.
- Oak Bank will never email you asking for your personal banking information. If you think you have been involved in a phishing attack, email oak@oakbankonline.com or give us a call at 608.441.6000.

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