Phishing

Phishing (pronounced "fishing") is a scam employed by cybercriminals to trick you into providing them with personal information that could be used to steal your identity. The scam usually works like this: You receive an email that appears to come from a reputable company - one you recognize and possibly do business with - like your Internet provider, a bank, credit card company, government agency, etc.

The language in the email will be designed to make you think you must respond immediately to solve a problem with your account, avoid cancellation, claim a valuable prize, etc. Most likely you will be asked to update or validate information - account number, password, Social Security number or other information that can be used to verify your account. You will be encouraged to click on a button to go to the organization's website. Don't do it!

If the email you received was part of a phishing scam, the link provided would take you to a fake website that looks just like the real thing. Or, it may actually be the real website, but will include pop-up windows designed to gather your personal information. Another objective of this scam may be to infiltrate your computer with a virus or software designed to spy on your Internet transactions.

It's never a good idea to open an email attachment you did not request or one from an unknown sender. And, you should never provide confidential information in response to an email or call you did not initiate.

If you are concerned about your accounts as a result of receiving an email, visit the company's website directly (don't cut and paste the address in the phisher's email), or call to find out if there is a problem and let the company know you received the email.

Bank OZK will never ask you for sensitive information via email or during a telephone conversation you did not initiate or request.