Protecting Your Money
Tips to Avoid Scammers

From Your Friends at
Bank of Eastern Oregon / Bank of Eastern Washington

June-2023

Hello Valued Customers.
Here are some tips to help you protect your money and avoid some popular scams.

PHISHING: Scammers use email or text messages to try to steal your passwords, account numbers or Social Security numbers. You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank, credit card or utility company. These messages will often say your account is on hold because of a billing issue and will ask you to click on a link to update your payment details. ***Don't do it!*** You can contact the company directly using a phone number or website you know is real.

Four Ways to Protect Yourself from Phishing
- Protect your computer by using security software. Set the software to update automatically so it will deal with any new security threats.
- Protect your cell phone by setting software to update automatically. These updates could give you critical protection against security threats.
- Protect your accounts by using multi-factor authentication. This makes it harder for scammers to log into your accounts if they do get your username and password.
- Protect your data by backing it up on your computer and cell phone, to an external hard drive or in the cloud.

PEER TO PEER PAYMENTS (P2P): Allow consumers to transfer money using their bank accounts, debit cards or credit cards through a website or mobile app such as Cash App, Paypal, Google Pay, Venmo, or Zelle. Younger customers are more likely to engage in electronic transfers such as these.

Three Ways to Protect Yourself from P2P Scams
- Remember a bank will never ask you to send money to anyone, not even yourself. Scammers will try and convince you to send money to yourself or "the bank's address" but you'll actually be sending money to an imposter.
- Scammers posing as a legitimate business may request a P2P payment for a product or service. Once they receive your money, you never receive what you paid for. Treat P2P payments like cash »» **don't pay until you receive the product!**
- A scammer "accidentally" sends you money through a P2P service and asks you to send the money back. Never send back the money, and instead contact the P2P service about the error.

LOTTERY / SWEEPSTAKES SCAMS: Often begin with scammers telling the victim they've won a lottery or sweepstakes raffle. The consumer is issued a check worth more than the amount owed and instructed to pay taxes and fees before receiving a lump sum payment. Unfortunately the check, in addition to the raffle, is bogus.

Four Ways to Protect Yourself from Lottery/Sweepstakes Scams
- Don't be fooled by the appearance of the check. Scam artists are using sophisticated technology to create legitimate looking counterfeit checks.
- Never "pay to play". There is no legitimate reason for someone who is giving you money to ask you to wire back or send you more than the exact amount »» that's a red flag that it's a scam. If a stranger wants to pay you for something, insist on a cashier's check for the exact amount, preferably from a local bank or one with a local branch.
- Verify the requestor before you wire or issue a check. It is important to know who you are sending money to before you send it. Just because someone contacted you doesn't mean they are a trusted source.
- Ensure a check has "cleared" to be most safe. Just because you can withdraw the money doesn't mean the check is good, even if it's a cashier's check or money order. Be sure to ask the bank if the check has cleared, not merely if the funds are available before your decide to spend the money.

RESOURCES:
https://www.beobank.com/fraud-protection • https://www.beobank.com/senior-fraud-resources
Please contact your local branch whenever you have a question about a suspicious email, text, phone call, or mail.

Remember, anytime someone tells you to keep a transaction secret or not talk to your bank about it, that's a huge red flag. Please talk to your local banker about any transaction that seems suspicious.

We are here to help you Keep Your Money Safe!