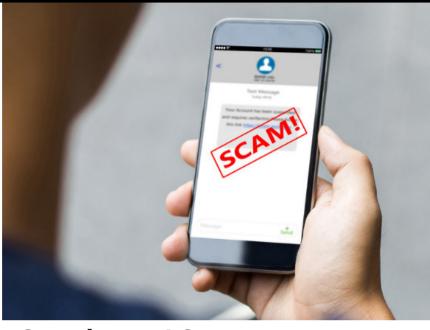
Bank of Hays

Fraud Update



Grandparent Scam

Fraudsters will call claiming to be a family member in serious trouble and in need of money immediately. The scammer might say he is stranded or has been mugged and call in the middle of the night to add to the urgency and confusion. Once the money is sent, the victim later finds out that it wasn't their grandchild, it was a criminal. Here are four tips to help avoid the grandparent scam:

- Confirm the caller: Verify the caller by calling them back on a known number
- Don't be afraid to ask questions: The more questions you ask the more inclined they will be to ditch the scam if they suspect you're on to them
- Never give personal information to anyone over the phone unless you initiated the call and the other party is trusted
- Never rush into a financial decision and trust your instincts: Don't be fooled - if something doesn't feel right, it may not be right

Over \$8.8 billion dollars stole by scammers last year!

Watch for these five flags of phishing in emails, calls and text:

- 1. They ask you to open a link
- 2.They use urgent or fear-inducing language
- 3. They send an attachment
- 4. They request personal info like PINs, passwords, or social security numbers
- 5. They pressure you to log into, or send money with payment apps

Online Dating Scams

Has an online love interest asked you for money? THAT'S A SCAM! Scammers know millions of people use online dating sites. They are there, too, hiding behind fake profiles. Some signs of an Online dating scam would be, professes love quickly and claims to be overseas, asks for money and lures you off the dating site, and claims to need money for travel. In 2023 over One Billion dollars was lost due to this scam. Several things you should do to make sure you are not a victim of this scam is:

- Slow down

-Never transfer money

-Contact your bank right away

Zelle Fraud

Here are some examples of Zelle Fraud:

- Financial Institution Impersonators A scammer pretends to be from a bank and claims they need updated account information or to verity a transaction, with the goal of getting you to click on a link
- Business Account Scam Consumers attempting to receive money are contacted by a scammer claiming they need to pay for an account update to collect the funds
- Refund Scam A Scammer claims to be a
 Zelle agent flagging a fraudulent
 transaction on your account. During the
 "refund" process, you're asked to pay to
 retrieve the money you never lost

Here are some good rules of thumb when using Zelle:

- Only use Zelle to pay family, friends or other people you trust
- Be cautious about unsolicited or urgent request
- Be suspicious if someone demands you use Zelle

Fake Check Over-payment

The Scammer offers to give you a check for more than the selling price. They tell you to deposit the check and send the difference back to them.

The check is fake, but if you deposit it, it'll appear in your account balance. That's because banks must make your money available quickly, usually within two days.

When a bank says the check cleared, that doesn't mean it was a good check. It can take weeks for the bank to figure out the check was fake. By that time, the scammer has the item you sold and the money you sent back. The bank then takes the money from the fake check out of your account because you are responsible for the items you deposit to your account.



Lottery or Sweepstakes Scam

You get a call, email, or letter saying you won a sweepstakes, lottery, or prize - like an iPad, a new car, or something else. But you can tell it's a scam because of what they do next: they ask you to pay money or give them your account information to get the prize. If you pay, you'll lose your money and find out there is no prize.

Who doesn't dream of winning a lot of money or a big prize? That's why scammers still use the promise of a prize to get your money or personal information. The good news is that there are ways to tell you're dealing with a scam.

Here are three signs of a prize scam:

- You have to pay to get your prize. But real prizes are free. So if someone tells you to pay a fee for "taxes," "shipping and handling charges," or "processing fees" to get your prize, you're dealing with a scammer. And if they ask you to pay by wiring money, sending cash, or paying with gift cards or cryptocurrency to get your prize, don't do it. Scammers use these payments because it's hard to track who the money went to, and it's almost impossible to get your money back.
- They say paying increases your odds of winning. But real sweepstakes are free and winning is by chance. It's illegal for someone to ask you to pay to increase your odds of winning. Only a scammer will do that.
- You have to give your financial information. There's absolutely no reason to ever give your bank account or credit card number to claim any prize or sweepstakes. If they ask for this information, don't give it. It's a scam.