GPSbank
GREAT PLAINS STATE BANK
Member FDIC

COMMON FRAUD EXAMPLES

Advance Fee Fraud

- A scammer requests fees upfront or personal information in return for goods, services, money, or rewards that they never supply.
- Scammers invent convincing and seemingly genuine reasons for requesting payment, such as to cover fees or taxes.
- They often ask for payment by international wire transfer.
- These scams are commonly mass-marketed with scammers sending them out to thousands of people all over the world at the same time, usually by mail or email.

Lottery Sweepstakes and Competition Scams

- An email, letter or text message from a lottery or sweepstakes company arrives from out of nowhere stating you have won a lot of money or are to receive fantastic prizes in a lottery or sweepstakes competition that you did not enter.
- These scams try to trick you into giving money upfront or your personal details in order to receive the prize.
- Scammers typically claim that you need to pay fees or taxes before your winnings or prize can be released.
- You may also have to call or text a premium rate phone number to claim your prize.
- Remember you cannot win a prize if you haven't entered.

Romance and Dating Scams

- Scammers create fake profiles on legitimate dating websites.
- They use these profiles to try to enter a relationship with you so they can get a hold of your money and personal details.
- The scammer will develop a strong rapport with you then ask for money to help cover costs associated with illness, injury, travel or a family crisis.
- Scammers seek to exploit your emotions by pulling on your heart strings. Sometimes the scammers will take months and months to build up the rapport.

Computer Hacking

- Phishing emails are commonly used by scammers to trick you into giving them access to your computer.
- They 'fish' for your personal details by encouraging you to click on a link or attachment.
- If you click, malicious software will be installed, and the hacker will have access to files and information stored on your computer.
- A phishing email often appears to come from an organization that you know and trust, like a bank or financial institution, asking you to enter your account password on a fake copy of the site's login page.
- If you provide your account details, the scammer can hack into your account and take control of your profile.

USPS Package Text Scam

- Scammers send you a text alerting you your package has arrived at the warehouse and cannot be delivered due to an incomplete address.
- The text indicates you must confirm your address in the link provided.
- Do not click on the link or visit the website as this is a scam to release your address as well as your bank account information.
- The USPS will never send you a text for your package.

Banking, Credit Card and Online Account Scams

- Scammers send emails or text messages that appear to be from your bank, a financial institution, or an online payment service. They usually claim that there is a problem with your account and request that you verify your details on a fake but convincing copy of the bank's website.
- Card skimming is the copying of information from the magnetic strip of a credit card or automatic teller machine (ATM) card. Scammers skim your card by putting a discreet attachment on an ATM or POS machine. They may even install a camera to capture your pin.
- Once your card is skimmed, scammers can create copies and make charges to your account.

Small Business Scams

- If you own a small business, you can be targeted by scams such as the issuing of fake invoices for unwanted or unauthorized listings, advertisements, products or services.
- A well-known example is receiving an invoice for a listing in a supposedly well-known business directory.
- Scammers trick you to sign up by disguising the offer as an outstanding invoice or a free entry, but with a hidden subscription agreement in the fine print.
- Scammers can also call your business pretending that a service or product has already been ordered and ask for payment over the phone.

Job and Employment Scams

- These scams involve offers to work from home or set up and invest in a business opportunity. Scammers promise a job, high salary or large investment return following initial upfront payments.
- These payments may be for a business plan, training course, software, uniforms, security clearance, taxes or fees.
- These scams are often promoted through spam email or advertisements in well-known classifieds, including websites.

Charity and Medical Scams

- Scammers are unscrupulous and take advantage of people who want to donate to a good cause or find an answer to a health problem.
- Charity scams involve scammers collecting money by pretending to work for a legitimate cause or charity, or a fictitious one they have created.
- Often times, scammers will exploit a recent natural disaster or crisis that has been in the news.
- Scammers play on your emotions by claiming to collect for a cause that will secure your sympathy, for example to help sick children.

Online Ads, Classified and Auction Scams

- A scammer will sell a product and send a faulty or inferior quality item or send nothing at all. They may also pretend to sell a product just to gather your credit card or bank account details.
- A scammer will place a real item in the classifieds or auction sites and sometimes under a legitimate business name. The scammer will send payment instructions (usually a wire) and you will never receive the item.
- These scams can also be found on reputable online classified pages or auction magazines.
- An online auction scam involves a scammer claiming that you have a second chance to buy an item that you placed a bid on because the winner has pulled out. The scammer will ask you to pay outside of the auction site's secure payment facility.
- If you do, your money will be lost and the auction site will not be able to help you.

Help fight fraud: report a scam, a company, or an unwanted call to the Federal Trade Commission at reportfraud.ftc.gov