BEWARE COMMON FRAUDS TO WATCH FOR

Fraud can take many forms, and staying alert to these schemes is essential to protecting yourself. Below are some common tactics used by scammers and steps you can take to stay safe.

Imposter Scams
Scammers often pretend to be someone trustworthy, like a company representative, government official, or even a loved one, to steal your personal information or money. They may reach out via phone, email, or text. Examples include grandparent scams, romance scams, and robocalls.

How to Protect Yourself:
Never share personal details or click on suspicious links from unknown contacts. Always verify the identity of someone asking for sensitive information by contacting the company or organization directly – even if the request seems legitimate.

Online Shopping Scams
These scams involve fake websites, excessive charges, undelivered orders, or broken guarantees. Be cautious of online stores with unusually low prices, suspicious web addresses, or ads with high-pressure tactics like countdown timers or limited-time deals.

How to Protect Yourself:
Always verify the authenticity of the website before making a purchase. When shopping online, use payment methods that offer purchase protection so you can recover your money if a seller turns out to be fraudulent. Be cautious of requests to pay by gift cards. This is not typical of a legitimate transaction.

Fake Prizes, Sweepstakes and Lotteries
Fraudsters may claim you've won a contest, sweepstakes, or lottery to trick you into providing personal information or payment. If you're notified of a win for something you never entered, it's likely a scam.

How to Protect Yourself:
Legitimate contests don't charge fees to claim prizes, nor do they ask for personal data. Ignore messages that claim rewards you didn't enter or require a payment or sensitive information to receive a prize.

Investment Scams
These scams promise quick wealth through tips, courses, or guidance on high-yield investments such as cryptocurrency, stocks, or real estate. Often, scammers charge fees for training or advice but fail to deliver any real value.

How to Protect Yourself:
Avoid offers that guarantee returns or sound too good to be true – real investments always carry some risk. Use tools from regulatory organizations, like the Financial Industry Regulatory Authority (FINRA), to research opportunities before committing.

Fraudulent Jobs/Business Opportunities
Some scammers offer work-from-home scams, franchise opportunities, pyramid schemes, and fake job postings. They may pose as legitimate companies to steal your personal information through application forms or request fees for supplies, training, or placement services that are never fulfilled.

How to Protect Yourself:
Research any job or business offer thoroughly before proceeding. Look for complaints or negative reviews about the person or employer and trust your instincts. If someone promises you a job in exchange for payment, it's likely a scam.

If in doubt, STOP and do your research!
Stay informed to avoid falling victim to these and other prevalent scams.

FNCBank
Member FDIC

POST SCAM CHECKLIST

Here's a checklist of tasks to follow if you've been scammed:

IMMEDIATE ACTIONS

- [ ] **Stop Communication:** Cease all contact with the scammer immediately.
- [ ] **Secure Your Accounts:** Change passwords for any accounts that may have been compromised.
- [ ] **Freeze Your Credit:** Contact credit bureaus (Experian, Equifax, TransUnion) to place a fraud alert or freeze on your credit.
- [ ] **Cancel Payments:** If you sent money, contact your bank, credit card company, or payment service (e.g., PayPal, Venmo) to cancel the transaction or dispute the charge.
- [ ] **Report Unauthorized Transactions:** Notify your bank or financial institution of any unauthorized charges.

REPORT THE SCAM

- [ ] **File a Report with Local Authorities:** Report the scam to your local police department for an official record.
- [ ] **Contact the Federal Trade Commission (FTC):** File a complaint at reportfraud.ftc.gov.
- [ ] **Report to Relevant Platforms:** Notify the platform where the scam occurred (e.g., social media, e-commerce site, etc.).
- [ ] **Use IC3 for Online Scams:** Report internet-related scams to the FBI's Internet Crime Complaint Center at ic3.gov.

PROTECT YOUR IDENTITY

- [ ] **Monitor Your Credit:** Periodically check your credit report for suspicious activity.
- [ ] **Set Up Fraud Alerts:** Request fraud alerts from credit bureaus to be notified of unusual activity.
- [ ] **Consider Identity Theft Protection:** Use a service to monitor and protect your identity.

RECOVER AND EDUCATE

- [ ] **Document Everything:** Keep records of all communications, transactions, and reports related to the scam.
- [ ] **Educate Yourself:** Research common scams to recognize red flags in the future.
- [ ] **Spread Awareness:** Share your experience with friends, family, or online communities to help others avoid similar scams.

Taking these steps quickly can help minimize the damage and protect you from further harm.

This tip sheet provides general information on common scams and fraud prevention. It is not an exhaustive list of all potential scams, and following these precautions does not guarantee complete protection against fraud. Always stay vigilant and consult trusted resources for additional guidance.