SCAMS YOU SHOULD KNOW ABOUT:

Tax Scams and Identity Theft

Spring is prime season for many tax-related scams and identity theft. Watch out for the following red flags, and contact the IRS for assistance right away if you suspect you've been targeted for fraud.

- You receive a threatening call from someone claiming to be with the IRS. Some scammers pose as IRS employees to trick victims into paying fake tax debts. They may demand immediate payment, often in the form of gift cards or prepaid debit cards, and threaten you with arrest or other consequences if you don't comply. Don't fall for this — it's a lie, and any money you send will be lost.
- There is unauthorized activity on your IRS account. If the IRS notifies you of activities on your account that you don't remember taking — such as creating a new account in your name, accessing your account, or disabling your account — it might be a sign of identity theft.
- Your e-filed tax return is rejected due to duplicate filing. If you e-file your tax return and the IRS rejects it because there is a duplicate filing under your Social Security number, it could be a result of fraud.
- You receive a suspicious notice from the IRS. If you receive a letter from the IRS about a tax return you don't remember filing, it might mean that someone has stolen your personal information.
- Your IRS records include extra income you don't recognize. If you are asked to amend your tax return because the IRS has records of unlisted income, check to see if you actually received the income and forgot to include it in your tax return. If you don't recognize the income, it might be an indicator of tax-related identity theft.

Romance Scams

Romance or online dating scams often start out simple and take time to develop. These criminals are savvy and take their time gaining a victim's trust, often starting out with small deceptions before working their way up to major fraud.

- Internet dating scams tend to follow a similar pattern, so watch out for these red flags when you're getting to know someone new online:
- An attractive stranger gets in touch through a dating or social media site, claiming to live in another part of the country or overseas.
- They appear smitten and eager to get to know you, and they may quickly suggest moving your conversation to a more private channel, such as email or chat.
- Over time, the relationship may start to feel close, but your plans to meet always fall through for one reason or another.
- Eventually, they claim to have an "emergency" and ask to borrow money, usually in the form of gift cards, prepaid debit cards, or wire transfer.
- They promise to pay you back but never do, and instead they keep asking for more money.
- Keep the following tips in mind to help guard against romance fraud:

- Take your time getting to know someone new, especially online. Ask a lot of questions, and be wary of any inconsistencies.
- Don't give out personal details such as your last name or place of employment to someone you've only met online.
- Check the person's profile photo in an internet image search. If it shows up elsewhere with a different name attached, there's a good chance it's been stolen for fraud.
- Watch out for overly flirtatious or complimentary emails. When in doubt, paste the text into a search engine and see if any matches come up.
- Cut off contact immediately if you suspect someone may be trying to swindle you, and report that person to the dating app or website you are using.
- Don't assume you're safe just because you made the first move; many scammers create fake profiles as bait and wait for victims to get in touch.

Tech Support Scams

In this widespread type of fraud, criminals pose as tech support staff from a trusted company to gain access to your computer. They may call you on the phone, but most often they will contact you through a pop-up window in your internet browser, claiming that your data or security is at risk and urging you to call a toll-free number immediately. If this happens to you, STOP.

- Do not click on any links or call the phone number provided.
- Do not send any form of payment, including gift cards.
- Do not provide information about your bank accounts or credit/debit card.
- Do not let anyone take control of your computer.

Take these steps to further protect yourself:

- Report the incident at https://reportfraud.ftc.gov/#/ and include the phone number you were asked to call.
- Install security software from a reputable company and keep it up to date.
- If you need help with your computer, get help from a trusted professional; don't just rely on an internet search.
- Spread the word if you are targeted by this type of scam. Raising awareness can help keep others safe.

Delivery Notification Scam

If you receive an email or text message with the subject line "USPS Failed Delivery Notification" (or something similar), do not open it. These emails look almost identical to official notifications from legitimate shipping services like the USPS®, UPS®, or FedEx®, but they contain fraudulent information.

These messages instruct customers to click on a link to resolve a made-up delivery issue. Clicking on the link activates a virus, which can steal personal information such as usernames, passwords, or financial account information.

Online Gift Card Scam

Gift cards sold through online auction sites are often fraudulent or stolen. To avoid getting mixed up in a costly scam, it is safer to purchase gift cards directly from the merchant or retail store.

Stripped Gift Card Scam

Avoid purchasing gift cards “off the rack” at retail stores. If gift cards are not stored behind a counter, thieves may steal the gift card code or use a device to scan the magnetic strip on the back of the card. They will then monitor the card online until it is activated and redeem the card's value online without you or the recipient knowing.
When you buy a preloaded gift card, ask the cashier to scan the card to make sure the full amount is available. Also, check to make sure the packaging has not been tampered with or damaged. If you have the option, it is a good idea to register your gift card with the retailer as well.

Wi-Fi Network Scam

Using your laptop, tablet, or smartphone at Wi-Fi hotspots in public places is convenient, but often those networks are not secure. Information you send through an insecure Wi-Fi connection might be accessed by someone else and stolen.
One way scammers do this is by setting up a Wi-Fi signal with the same name as complimentary one; this is known as the “evil twin,” and it works similarly to a phishing scam. If you connect to an evil twin network, your personal or financial information can be intercepted by the scammer during normal-seeming transactions.
To protect your information when using public Wi-Fi hotspots, it is better not to use your credit card. Send information only to sites that are fully encrypted, and avoid using mobile apps that require personal or financial information while using a public network.

Online Shopping Fraud

With more and more shopping being done online, customers often report that they have placed orders for products that never arrive. In many cases, this is the result of fraud. Scammers post listings online for products they do not actually own. When they receive an order, they use a stolen credit card to purchase the item from a third party and have it shipped directly to the buyer. Then they charge the buyer’s credit card and keep the purchase price for themselves. They may also use the buyer’s credit card information to make further purchases to perpetuate the scam.
If you purchase an item from an online seller but receive the shipment from someone else, it is a strong indication of fraud. To avoid these scams, use caution and don’t provide payment information directly to the seller. Instead, always use a legitimate payment service to ensure a safe, legitimate online purchase.

Package Delivery Scams

Online fraudsters pose as legitimate delivery services and offer reduced or free shipping to customers through auction sites. They provide fake shipping labels to the victim and

do not pay for delivery of the packages. Then the delivery service providers intercept the packages for nonpayment, and the victim loses the money they paid for the purchase.
To protect yourself, diligently check each seller's feedback ratings, along with their number of sales and the dates on which feedback was posted. Be wary of any seller with 100% positive feedback, a low number of feedback postings, or ratings that were all posted around the same date.

FNB North Impersonation Scams

Criminals are contacting FNB North customers by phone or text to trick them into revealing their financial information. They may ask for your online banking login information, ask you to provide or "verify" one-time passcodes sent by text, or ask for your card numbers and account balances. If this happens, hang up.
Remember, FNBN will NEVER call, text, or email to ask for your online banking login credentials, or for your credit/debit card information — including your PIN or the three-digit code on the back of your card.

Fake Calls From Amazon and Apple Support

Some scammers use the names of well-known companies like Amazon or Apple to gain your trust and then tell you there's something wrong with your account — a suspicious purchase, an account breach, or problems with an order or return. They will give you a phone number to call or instruct you to press 1 to speak with someone. Don't do either. Hang up. It's a scam, and they're trying to steal your personal information.

Travel Scams

Beware of offers for free or low-cost travel from companies you haven't heard of or done business with before—especially if they contact you out of the blue saying you've won a "free vacation." These so-called luxury travel packages often involve steep hidden fees or are entirely fake. Protect yourself by working only with travel companies you can verify are trustworthy, and by getting all the details (including cancelation and refund policies) in writing before you pay for anything. Beware of anyone who pressures you to "sign up to claim your prize," and never give out your credit card number to anyone who claims they need it to "verify" your identity.

Medical Scams/Fraud

Be wary of calls or emails from doctors or hospitals claiming to have treated a friend or relative for COVID-19 and demanding payment. If you suspect COVID-19 health care fraud, report it immediately online or call 800-HHS-TIPS (800-447-8477).

IRS Impersonation Scam Email

The Internal Revenue Service (IRS) warns taxpayers and tax professionals about a new IRS impersonation scam email. The email subject line may vary, but according to the IRS, recent examples use phrases like "Automatic Income Tax Reminder" or "Electronic

Tax Return Reminder". The emails include links that are meant to look like the IRS website with details about the taxpayer's refund, electronic return or tax account. The emails also contain a "temporary password" or "one-time password" that purports to grant access to the files. However, these are actually malicious files. Once the malware files are installed on your computer, scammers may be able to secretly download software that tracks every keystroke, giving the bad guys access to information like passwords to your financial accounts. Don't be fooled: the IRS does not send unsolicited emails and never emails taxpayers about the status of refunds.

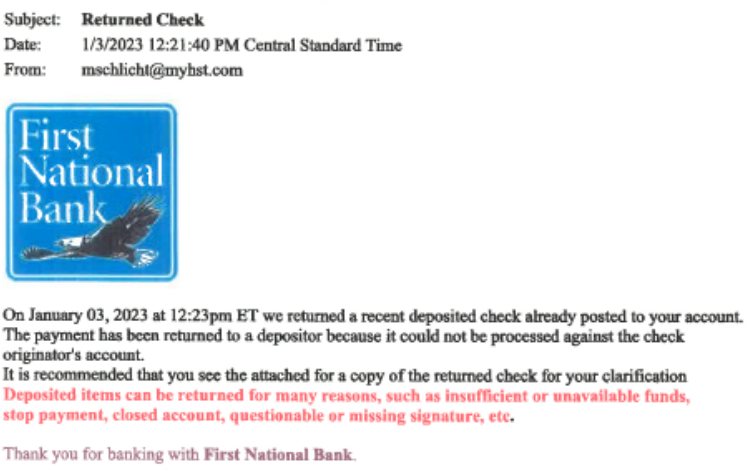
Zelle Scam

A common scam involves an email or text message asking a user to confirm a large, fake Zelle payment. When the user replies that they didn't authorize the transfer, the scammer follows up with a phone call pretending to represent the bank and spoofing the financial institution's phone number. They walk the caller through bogus instructions on how to reverse the unauthorized claims that instead actually transfer money to the criminals.

Another popular scam starts with a message claiming that your bank account has been compromised and that you need to take action immediately to resolve the problem. If you respond, the fraudsters follow up with a phone call, pretending to be your bank and guiding you through the process of transferring money.

Email Scam from First National Bank

An email is being sent which looks like is coming from the bank with a subject of "Returned Check", the email is asking you to click on the link to view the check which then brings the customer to the login section of our old website. Upon logging in it asks them to input their account number. This is a scam and FNBN would never email you to click on a link or ask you to input an account number or social security number.



Subject: **Returned Check**
Date: 1/3/2023 12:21:40 PM Central Standard Time
From: mschlicht@myhst.com

First National Bank

On January 03, 2023 at 12:23pm ET we returned a recent deposited check already posted to your account.
The payment has been returned to a depositor because it could not be processed against the check originator's account.
It is recommended that you see the attached for a copy of the returned check for your clarification
Deposited items can be returned for many reasons, such as insufficient or unavailable funds, stop payment, closed account, questionable or missing signature, etc.

Thank you for banking with **First National Bank**.