Bank of Botetourt

April 2026

Tax Season Scams: How to Protect Your Money and Personal Information

Member FDIC

EQUAL HOUSING LENDER

Tax season is a busy and often stressful time for both individuals and businesses; and it's also one of the most active times of year for scammers. As filing deadlines approach, cybercriminals take advantage of urgency, confusion, and increased communication from financial institutions and tax agencies.

By understanding how these scams work and what warning signs to watch for, you can significantly reduce your risk.

Common Tax Season Scams

IRS Impersonation Scams
Fraudsters may call, email, or text pretending to be from the IRS or other government agencies. They often claim you owe back taxes or face penalties and demand immediate payment.

Phishing Emails and Text Messages
Scammers send messages that appear to come from legitimate sources, including tax preparation services or financial institutions. These messages may include links to fake websites designed to capture Social Security numbers, login credentials, or banking information.

Fake Refund or Stimulus Offers
Some scams promise unusually large refunds or additional payments. Victims are asked to "verify" their identity or provide financial details to receive the funds.

Connect with us!

(540) 591-5000

Continued on page 2

W-2 and Payroll Data Scams (Businesses)
Businesses may receive emails appearing to come from executives or trusted partners requesting employee tax documents or payroll data. These scams can lead to identity theft and financial fraud.

Warning Signs to Watch For

Scams often follow predictable patterns. Be cautious if you notice:

- Urgent or threatening language demanding immediate action
- Requests for payment through unusual methods such as gift cards, wire transfers, or cryptocurrency
- Emails or texts asking for sensitive personal or financial information
- Unexpected messages about refunds, tax issues, or account problems
- Slight misspellings or unusual email addresses and website links

Remember: legitimate organizations will not pressure you to act immediately or request sensitive information through unsecured channels.

How to Protect Yourself

Taking a few precautions can go a long way in preventing fraud:

- File taxes through trusted professionals or verified software providers
- Access tax-related websites by typing the address directly into your browser
- Do not click links or download attachments from unsolicited messages
- Never share Social Security numbers, account details, or login credentials
- Keep your devices updated and secured with antivirus protection
- Monitor your bank accounts and credit activity regularly

Additional Steps for Business Clients

Businesses should take extra precautions during tax season, particularly when handling employee or financial data:

- Verify all requests for W-2s, payroll data, or tax documents through a second communication channel
- Limit access to sensitive information to authorized personnel only
- Train employees to recognize phishing and social engineering attempts
- Establish internal procedures for handling financial and tax-related requests

When in Doubt, Pause and Verify

Scammers rely on urgency to push quick decisions. Taking a moment to verify a request; by contacting the organization directly using a trusted phone number; can prevent significant financial loss and identity theft.

If you suspect fraudulent activity involving your financial information, contact us immediately. Acting quickly can make a meaningful difference.

Source: OpenAI, ChatGPT, March 20, 2026
https://chatgpt.com

Designed by FreePik

Mobile Banking Safety: Protecting Your Finances on the Go

Mobile banking has become an essential tool for managing finances. From checking balances to transferring funds and paying bills, the convenience of banking on your smartphone is unmatched.

However, with this convenience comes increased risk. Mobile devices are a common target for cybercriminals, making it important to understand how to use them securely.

Secure Your Device

Your smartphone or tablet is often the primary access point to your financial accounts.

- Use a strong passcode, fingerprint, or facial recognition
- Enable automatic screen locking after a short period of inactivity
- Keep your device's operating system and apps updated

If your device is lost or stolen, these protections can prevent unauthorized access.

Download Apps Carefully

Not all apps are safe, even if they appear legitimate.

- Only download apps from official app stores
- Verify the app publisher before installing
- Read reviews and check for inconsistencies
- Avoid clicking links that prompt app downloads
- Fraudulent apps can be designed to capture login credentials or install malware.

Avoid Public Wi-Fi for Financial Transactions

Public Wi-Fi networks, such as those in coffee shops, airports, or hotels, may not be secure.

- Avoid accessing banking or financial apps on public Wi-Fi
- Use a secure, private network whenever possible
- Consider using a Virtual Private Network (VPN) for added protection

Be Alert to Mobile Scams

Mobile users are frequently targeted through text messages and app-based fraud.

- Do not click on suspicious links in texts or messages
- Be cautious of urgent alerts claiming to be from your bank
- Never share passwords, PINs, or one-time passcodes

If you receive a suspicious message, contact your bank directly using a trusted number.

Monitor Your Accounts and Enable Alerts

Staying informed about account activity is one of the most effective ways to prevent fraud.

- Enable transaction alerts and login notifications
- Review account activity regularly
- Report any unauthorized transactions immediately

Early detection allows for faster resolution and can help minimize financial loss.

Safe, Convenient Banking Starts with You

Mobile banking is a secure and powerful tool when used responsibly. By following these best practices, you can enjoy the convenience of managing your finances on the go while reducing your exposure to cyber threats.

If you have questions about mobile banking security or notice unusual activity, please contact us directly. We are here to help you stay protected.

Source: OpenAI, ChatGPT, March 20, 2026
https://chatgpt.com