SCAM REPORT

MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING MARCH 11, 2024

Prepared by Arnold H. Shifrin, RPh

Current Tax Scams - A Quick Review

Tax scams are ongoing throughout the year but tend to peak now as we approach the April 15 filing deadline. Figures are not yet available for 2023, but victims of tax scams lost $5.7 billion to criminals in 2022. You can avoid being a victim by understanding common tax scams, the tactics used by criminals, and how the IRS operates.

Common tax scams

- Phishing emails and websites: Scammers send bogus emails or create official-looking IRS websites to lure victims into providing personal and financial information.
- Telephone scams: Scammers claiming to represent the IRS demand immediate payment of a "past due" tax bill and threaten immediate legal action or arrest for non-compliance.
- Filing false returns: Fraudsters steal the personal and financial information of unsuspecting victims and file false tax returns claiming refunds on behalf of the victims.
- Fake charities: Scammers create fake charities and solicit victims for "tax-deductible" donations.
- Corrupt tax return preparers: Dishonest tax preparers steal a client's identity. They also underreport incomes or inflate deductions to reduce taxes or obtain larger refunds for their clients.

How to protect yourself

- File your taxes early and electronically to prevent a scammer from fraudulently filing a return in your name and receiving a refund to which you are entitled.
- Be cautious of unsolicited emails or phone calls claiming to be from the IRS. The IRS initiates contact with taxpayers about outstanding tax bills by US Mail.
- If you receive a call and the Caller ID displays a Washington, D.C. area code (e.g., 202), the call may have originated from another number. Technology enables scammers to display any number they wish on your Caller ID.
- If you pay your taxes by check, use a gel pen or other permanent ink. Mail the checks inside the post office.
- If an "IRS agent" contacts you and asks for personal information to "update your account," do not comply. The agency will contact you by US Mail if this information is legitimately needed.
- If an "IRS agent" threatens to cancel your SSN for any reason, you are dealing with a scammer. The IRS does not make such threats.
- Scammers posing as IRS agents attempt to create a sense of urgency and threaten arrest or legal action to pressure victims into acting quickly. Do not let this approach force you to respond foolishly.
- If you are told by an "IRS agent" that your outstanding tax bill must be paid by wire transfer, gift card, debit card, or cryptocurrency, you are dealing with a scammer.
- If you use a tax preparer, verify their credentials. Be sure the preparer signs the return before filing.
- Verify that charities to which you contribute are registered with the Illinois Attorney General's Office and accredited by the Better Business Bureau.
- Before responding to an email message, verify the sender's identity and that the website is secure and encrypted (e.g., the "tune" icon precedes the URL in the address bar).
- Do not click on links or open attachments in messages you receive from unknown senders.
- Use strong, unique passwords for your accounts and change them frequently. Use 2FA if it is offered.
- Monitor online financial accounts often for suspicious activity. Do not wait for monthly statements.
- Verify that the operating system and browser versions installed on your devices are current.

If you were a victim of this scam, file a report with the following agencies

• Federal Trade Commission (*ftc.gov*) • Internal Revenue Service (*irs.gov*) • Better Business Bureau (*bbb.org*) • Illinois Attorney General Senior Citizens Consumer Fraud Helpline (telephone: 1-800-243-5370; email: *seniorhelpline@ilag.gov*) • Your bank and credit card companies (your accounts will be monitored for suspicious activity) • Your local police department

[Sources: IRS, FTC]