LPL Financial

Scams to Expect for Tax Season

Tax scams involve bad actors — who impersonate the IRS, tax professionals, or government entities over the phone, through text, online, or by email — and are designed to trick you into providing sensitive information or sending money for taxes, penalties, and fees you don't owe.

According to the Internal Revenue Service's Criminal Investigation Team, they initiated 1,409 tax crime investigations and identified $5.5 billion in tax fraud in 2023. Tax scams peak the highest during tax season, therefore it is crucial to remain vigilant and verify the legitimacy of any communication or request related to taxes.

Tax Scam Methods

There are many methods cybercriminals use for tax scams, and they often deploy creative tactics to deceive their victims. The methods listed below are not the only methods a cybercriminal can use.

Fake Tax Refund: A new scheme that involves bad actors mailing letters impersonating and IRS letter. The letter claims that there is a notice in relation to an unclaimed tax refund.

IRS Call: Impersonation phone calls also known as vishing may occur, where callers will pose as IRS agents and use fake credentials in hopes of stealing taxpayer funds or personal information. These scammers may know a lot about their victims and will intimidate them into making a hasty decision.

Phishing email: Scammers will send several email alerts attempting to trick people into thinking their emails are legitimate notices from the IRS. These phishing emails will seek information related to refunds, filing status, confirming personal identity, and late payments.

How to Identify and Deal with Tax Fraud:

Tax scams become increasingly popular during tax season, but here are some ways to identify them:

- **Use caution with unsolicited communications.** The IRS typically initiates contact via traditional mail. Be wary of unexpected calls, emails, or texts claiming to be from the IRS or any tax authority, especially if they require immediate payment or threaten legal action.
- **Verify sources.** If you receive any communication claiming to be the IRS or a tax professional, verify its legitimacy by navigating to the official website or contact a verified phone number.
- **Be alert of phishing attempts.** Think twice before interacting with any email requesting for sensitive or financial information. Legitimate organizations like the IRS, will not ask for this information via email or phone.
- **Resist scare tactics.** Scammers will often use intimidation or urgency to bait victims into making a rushed decision, not in their best interest. We recommend you take your time, thoroughly evaluate requests, and verify all urgent requests.
- **Secure personal information.** Be sure to protect your information such as Social Security numbers and financial details to prevent identity theft and tax fraud.
- **Educate yourself.** Stay informed on the latest tax scams used by fraudsters. More awareness allows you mitigate risks and attacks.
- **Report Phishing Button.** If you receive any suspicious email, consider using the report phishing button to report the email to our security engineers for investigation. Our team can verify any emails and let

you know if it is a malicious or legitimate email. To receive access to the report phishing button, please contact securityawareness@lplfinancial.com.

I think I May Be a Victim of a Tax Scam. What Should I Do?

1. **Stop all communication.** If you are in contact with a scammer, cease communication immediately.
2. **Report the incident.** You can file a complaint with the IRS on their website. Additionally, you can report the incident to the Federal Trade Commission (FTC) on their website.
    i. You must report all suspected cases as soon as possible to PrivacyResponseTeam@lplfinancial.com or through the Report Incident Submission Form.
3. **Protect your identity.** Monitor your financial accounts, credit reports, and any other sensitive information for signs of unauthorized access and activity. With most accounts, you can place a fraud alert or a credit freeze to prevent further compromise.
4. **Document the incident.** Keep any record of communication and documentation related to the scam. This can be extremely useful when reporting the incident and resolving any issues with tax authorities.

Additional Considerations

If a scammer accessed your accounts...	Immediately change all passwords associated with the scam. Ensure the new password is strong and do not reuse passwords. Enable Multifactor Authentication (MFA) on all accounts.
If a scammer has access to financial information...	Contact your bank or credit card company immediately. They can help monitor your accounts for suspicious activity.
If a scammer has your social security number...	Place a fraud alert and initiate a credit freeze on your credit reports by contacting one of the three major credit bureaus. Additionally, file a report with the IRS and your bank so that they can protect your identity and monitor your accounts.

Please contact the Security.Mailbox@lplfinancial.com with any additional questions or concerns.