SIX IRS AUDIT RED FLAGS FOR RETIREES

The Internal Revenue Service (IRS) audited almost 1.1 million tax returns in 2017, representing approximately 0.5% percent of all returns filed in the previous calendar year. According to the IRS, the majority—70% of audits—were conducted via correspondence and the remaining 29.2% were conducted in the field.[1] However, selection for an audit does not always suggest there's a problem. That's because the IRS uses several different selection methods:[2]

- **Random selection and computer screening**—returns are selected based solely on a statistical formula. Tax returns are compared against "norms" for similar returns, which are developed from audits of a statistically valid random sample of returns, as part of the National Research Program conducted by the IRS.
- **Related examinations**—the IRS may select your returns when they involve issues or transactions with other taxpayers, such as business partners or investors, whose returns were selected for audit.

While the IRS does fewer full-blown audits each year, certain red flags on taxpayers' returns may still generate IRS inquiries and examinations. Common red flags for retiree tax returns include:[3]

1. Failure to report all income, including Social Security benefits and retirement plan distributions
2. Failure to take required minimum distributions (RMDs) for taxpayers over age 70 ½ with assets in certain qualified retirement plans, or reporting an incorrect RMD
3. Taking disproportionately large deductions relative to other taxpayers at your same income level
4. Reporting disproportionately large charitable deductions relative to your income level
5. Taking large rental losses
6. Failure to report lottery, sweepstakes, or gambling winnings

Beware of IRS impersonators

While the odds of being audited by the IRS are low, the odds of being targeted by the "IRS Impersonation Scam" continue to grow, especially for retirees who remain a chief target of this type of fraud. In fact, the IRS reports that they generally see a surge in this particular scam during tax filing season.[4] This is an increasingly common scam where individuals impersonating IRS employees make unsolicited telephone calls to taxpayers, using the threat of arrest to obtain money from victims by falsely stating that the victims owe back taxes or other fees. The perpetrators generally demand that the victims send them money via gift cards, prepaid credit or debit cards, money orders, or bank wire transfers.

It's important to know that if your return is selected by the IRS for audit, the IRS will notify you by mail. They will *not* initiate an audit or other inquiry by telephone. If you receive a phone call from someone saying they're from the IRS asking you to provide personal information or send money—hang up immediately. If you believe you have been a victim of an IRS Impersonation Scam, contact the U.S. Treasury Department to file an incident report.

[1] https://www.irs.gov/statistics/enforcement-examinations
[2] https://www.irs.gov/businesses/small-businesses-self-employed/irs-audits
[3] https://www.kiplinger.com/slideshow/taxes/T056-S010-red-flags-that-raise-audit-chances-for-retirees/index.html
[4] https://www.irs.gov/newsroom/phone-scams-remain-serious-threat-no-2-on-the-irs-dirty-dozen-list-of-tax-scams-for-2017

WHY SOCIAL MEDIA USERS ARE MORE LIKELY TO BECOME VICTIMS OF FRAUD

Keeping up with friends and family and sharing pictures of the grandkids and your most recent travel destination online may seem pretty tame. But according to several recent studies, social media use may leave you more vulnerable to financial fraud. According to a Harris Poll survey, nearly two in three U.S. adults with personal social media profiles believe they've been hacked.[1] A separate study conducted by Javelin Strategy & Research reported that a 46% higher risk of account takeover and fraud is associated with active users of social media accounts versus those who are not active on social networks, due in large part to the following:[2]

- Seventy-five percent of consumers fail to use virtual private networks (VPNs) to protect their Wi-Fi connections
- Eighty-seven percent of mobile users report engaging in high-risk activity via public Wi-Fi, such as accessing corporate email and conducting online banking via mobile phones and laptop devices

How can you help protect your finances and your identity online? Consider the following tips:

- Secure your home Wi-Fi network
- Install anti-virus and anti-malware programs on all your devices and networks
- Limit the use of unsecured networks when away from home or the office
- Use multiple passwords; avoid using the same passwords across devices and accounts
- Use a combination of upper- and lower-case letters, numbers, and characters for passwords
- Do not open emails or links if they're not from a trusted source and can't be verified as such
- Properly remove data from all devices before selling, donating, recycling, or discarding

If you believe you're a victim of online fraud or cyber theft, don't wait to act.

- Contact your bank or financial institution immediately to report lost or stolen cards, or fraudulent accounts or charges
- Consider placing a fraud alert on your credit if you suspect fraudulent activity
- Close any accounts that have been tampered with or opened fraudulently in your name
- Notify the Federal Trade Commission (FTC)

Protecting your online security requires many of the same steps as protecting your physical security. Remaining vigilant, cautious, and informed can help safeguard your finances and your good name from would-be cyber criminals. If you have questions about ways to help protect your lifestyle in retirement, contact the office to schedule time to talk.

[1] https://www.phoenix.edu/news/releases/2016/04/uopx-social-media-hacking.html
[2] https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new