

SPECIAL ALERT ON EMAIL SCAMS DURING TAX SEASON



Tax filing season can cause anxiety and confusion for many taxpayers. While you are locating your receipts and forms, be on guard for scam artists impersonating the IRS in emails.

These email messages may appear convincing, but it is important to remember that the IRS does not initiate communications through email. Emails using the IRS name and logo are fraudulent attempts to download malware or steal your personal information to gain access to your financial accounts. If you provide your personal information to these impostors, you will be at risk for identity theft and financial fraud. The most common tax season email scams:

W-2 Form Update

This spam email attack pretends to be the IRS asking you to update your W-2 due to "important changes." The instructions encourage you to open an attached file to access the new form. However, clicking the attachment will download malware to your computer, enabling a remote hacker to access your hard drive and any confidential data it contains.

Tax Refund

The most frequent impersonation of the IRS involves an email message informing you that you are eligible to receive a tax refund for a specified amount. To claim the refund, the email says you must open an attachment or click on a link. The attachment will download malware, and the link will direct the you to a fake IRS website. It will request your personal and financial information like passwords, PINs, Social Security Number, bank account and credit card numbers.

Tax Audit

You may receive an alarming email claiming that you are being audited for "Tax Avoidance." The email will provide you with a link to a fraudulent website where you will be asked to complete an investigation form requesting your personal information. Some of these links will also download malware to your computer.

Online Survey

This message claims that you have been randomly selected to participate in an online satisfaction survey of the IRS. You will be promised a monetary incentive for completing the "survey." Unfortunately, instead of receiving a credit for providing feedback, you will now be at risk for identity theft.



Protect Your Identity

If You Receive Emails Claiming to be from the IRS

1. Do not open any attachments, click any links, or enter your personal information.
2. Forward the suspicious email to phishing@irs.gov and delete the message.
3. Visit the real IRS website at www.irs.gov or call 1-800-829-1040 to verify a claim or to check information.

Protect Your Information

Filing income taxes requires the disclosure of a great deal of confidential information. Avoid being victimized by scam artists this tax season. Ignore suspicious emails and obtain official tax information directly from the IRS at www.irs.gov. Choose a reputable tax preparer or efilng software, like [TurboTax®](#), that offers password-protected access and industry-standard SSL encryption. And dispose of any documents containing personal and financial information with a cross-cut shredder.

If You Responded to a Scam

If you believe you have provided your personal information to a scam, you can quickly minimize the potential damage:

Place a "Fraud Alert" on your credit report by calling the toll-free fraud number of one of the three consumer reporting companies:

- TransUnion 1-800-680-7289
- Equifax 1-800-525-6285
- Experian 1-888-EXPERIAN (397-3742)

Review your credit report and close any accounts that you know or believe to have been tampered with or opened fraudulently.

File an identity theft report on the [Federal Trade Commission](http://www.ftccomplaintassistant.gov) website at <https://www.ftccomplaintassistant.gov> or call 1-877-ID-THEFT (438-4338).

BBT.com/about/privacyandsecurity