MICHIGAN ATTORNEY GENERAL

CONSUMER ALERT

IRS PHONE AND EMAIL SCAMS

Tax fraudsters strike quickly, often from overseas. They can cover, erase, or leave no tracks before taxpayers know they've been duped. Their goal is to steal money, take control of personal computers, or commit identity theft. IRS scammers trick their victims into giving them access to bank account information, Social Security numbers (SSN), or credit and debit card details.

You can avoid falling for an IRS scam if you know how to spot these scammers and their tricks, which starts with knowing how the Internal Revenue Service (IRS) contacts taxpayers. Here is a list of things a tax scammer will do but the **IRS will NEVER do**:

- Call, text, or email you and demand immediate payment.
- Demand payment without any chance to appeal or question the amount due.
- Threaten to have you arrested.
- Require a specific payment method, like a gift card, pre-paid debit card or wire transfer.
- Call, text, or email you and ask for your personal or financial information.

REMEMBER THIS: Anybody contacting you claiming to be from the IRS and asking you for personal or financial information is a crook.

IRS PHONE SCAMS

When tax season hits, IRS phone scams top the list of calls to the Attorney General's Consumer Protection Division. Phone tax scams come in many varieties. These tech-savvy crooks can spoof caller ID to make their calls look like they are coming from an official number or location. And they may even have some of your personal information when they call — like the last four digits of your SSN or your correct birthday and year. Don't confirm and don't offer any more information.

Reported IRS phone scams include:

- **Back Taxes or Penalty Phone Call** – High-pressure callers threaten legal action that can only be avoided by immediate payment. If you are tempted to pay, look for these clues: payment must be made by difficult-to-trace transfer methods, like a wire transfer or a pre-paid card; and, the payment must be made right away.
- **Debt Collector Contacts for Back Taxes** – The IRS occasionally uses debt collection agencies to collect some overdue tax debts. Consumers should be on the lookout for any unexpected contacts from anyone claiming to be collecting on behalf of the IRS. The Consumer Alert, Debt Collectors and the IRS provides additional tips to spot and stop these scams. IRS information on how to identify legitimate IRS private debt collectors and the private debt collection program is available at: irs.gov/businesses/small-businesses-self-employed/private-debt-collection.

- **Rebate Phone Call** — Aimed at seniors, the caller says they are an IRS employee and tells the targeted victim they are eligible for a sizable rebate for filing taxes early. The fake IRS employee then asks for the target's bank account information for direct deposit of the rebate. Don't do it! Sharing your bank account details gives criminals access to your funds.
- **Paper Check Phone Call** – A fake IRS employee calls and says that the IRS sent a check that has not been cashed and the IRS needs to verify the individual's bank account number. The only way the IRS collects your bank account details is if you choose to put them in your tax return.

DO THIS: If someone calls you and says they are from the IRS, hang up and call the IRS directly at 800-829-1040.

LISTEN AND LEARN

Click on this audio example of a real IRS phone scam call (mi.gov/ag/0,4534,7-359-82917_94178_95259_95299---,00.html). This caller claims to be from the IRS and tells you the IRS is filing suit against you for back taxes.

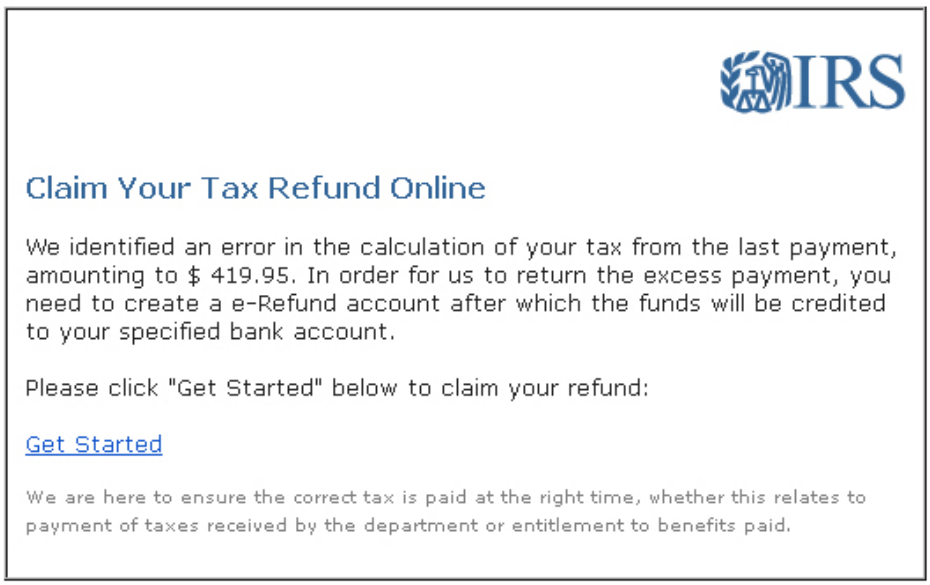
IRS EMAIL SCAMS

Identity thieves use phishing emails to trick recipients into giving up passwords and other information. Don't take the bait. Look for — but do not open:

- Emails that pose as a trusted source, like a bank or tax provider;
- Emails that use the official IRS logo or whole sections of text from the IRS website;
- Emails with an urgent message, i.e., update your account now;
- Emails with instructions to click on a link or open an attachment;
- Emails using a fake "from" address (see example below); and
- Emails using forms with numbers similar to those the IRS uses.

Keep your computer and mobile phone secure. Use security software and set to update automatically. Use strong passwords and 2-factor authentication. Give personal information only over encrypted websites — look for "https" addresses and back up your files regularly.

IF YOU GET A PHONE CALL OR EMAIL FROM "THE IRS"



First, if you don't owe taxes, hang up immediately or delete the email without opening it. Report any suspicious contacts to the Treasury Inspector General for Tax Administration hotline at 800-366-4484.

If you do owe on your taxes, call the IRS at 800-829-1040 if you need federal tax assistance.

You may forward emails to phishing@irs.gov, the address established by the IRS to receive, track, and shut down these scams. Detailed instructions for how to send the emails are available through the IRS. You may not receive an individual response to your email because of the volume of reports the IRS receives each day.

If you receive an illegal robocall from someone claiming to be from the IRS or pitching a tax scam, report the caller ID and callback number to the IRS by sending it to phishing@irs.gov and write "IRS Phone Scam" in the subject line. You can also report illegal robocalls to the Attorney General's Robocall Crackdown Team.

Report misuse of the IRS name, logo, forms, or other IRS property using the Treasury Inspector General's website or hotline at 800-366-4484.

Remember that the only genuine IRS website is irs.gov. You should never get to this site using a link embedded into an email - instead enter the address in your browser. A website link embedded into an email can easily take you to a fake site.

CONTACT THE ATTORNEY GENERAL'S OFFICE

If you have a general consumer complaint, you may file a complaint with the Attorney General's Consumer Protection Unit:

Consumer Protection Unit
P.O. Box 30213
Lansing, MI 48909
517-335-7599
Fax: 517-241-3771
Toll free: 877-765-8388
Online complaint form