West Virginia Executive Branch
Privacy Tip

It's Tax Season again! Unfortunately, the scammers are out in full force. The IRS provides tips for taxpayers at https://www.irs.gov/uac/IRS-Tax-Tips

Scam Calls and Emails Using IRS as Bait Persist

IRS Tax Tip 2016-19, February 12, 2016

Scams using the IRS as a lure continue. They take many different forms. The most common scams are phone calls and emails from thieves who pretend to be from the IRS. They use the IRS name, logo or a fake website to try to steal your money. They may try to steal your identity too.
Be wary if you get an out-of-the-blue phone call or automated message from someone who claims to be from the IRS. Sometimes they say you owe money and must pay right away. Other times they say you are owed a refund and ask for your bank account information over the phone. Don't fall for it. Here are several tips that will help you avoid becoming a scam victim.

The real IRS will **NOT**:

- Call you to demand immediate payment. The IRS will not call you if you owe taxes without first sending you a bill in the mail.
- Demand tax payment and not allow you to question or appeal the amount you owe.
- Require that you pay your taxes a certain way. For example, demand that you pay with a prepaid debit card.
- Ask for your credit or debit card numbers over the phone.
- Threaten to bring in local police or other agencies to arrest you without paying.
- Threaten you with a lawsuit.

If you don't owe taxes or have no reason to think that you do:

- Contact the Treasury Inspector General for Tax Administration. Use TIGTA's "IRS Impersonation Scam Reporting" web page to report the incident.
- You should also report it to the Federal Trade Commission. Use the "FTC Complaint Assistant" on FTC.gov. Please add "IRS Telephone Scam" to the comments of your report.

If you think you may owe taxes:

- Ask for a call back number and an employee badge number.
- Call the IRS at 800-829-1040. IRS employees can help you.

In most cases, an IRS phishing scam is an unsolicited, bogus email that claims to come from the IRS. They often use fake refunds, phony tax bills, or threats of an audit. Some emails link to sham websites that look real. The scammers' goal is to lure victims to give up their personal and financial information. If they get what they're after, they use it to steal a victim's money and their identity.

If you get a 'phishing' email, the IRS offers this advice:

- Don't reply to the message.
- Don't give out your personal or financial information.
- Forward the email to phishing@irs.gov. Then delete it.
- Don't open any attachments or click on any links. They may have malicious code that will infect your computer.

More information on how to report phishing or phone scams is available on IRS.gov.

Each and every taxpayer has a set of fundamental rights they should be aware of when dealing with the IRS. These are your Taxpayer Bill of Rights. Explore your rights and our obligations to protect them on IRS.gov.

Additional IRS Resources:

- Identity Protection Tips
- Identity Protection Home Page

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.