

## West Virginia Executive Branch Privacy Tip

Periodically, the Privacy Office may issue tips for the purpose of assisting you in making informed decisions in your “away from work” life. The following tip is for that purpose.

### Tax Time Identity Safety Tips – Part Three

#### Beware of Bogus IRS Emails

(IRS Tax Tip 2013-19 [www.irs.gov](http://www.irs.gov))

The IRS receives thousands of reports every year from taxpayers who receive emails out-of-the-blue claiming to be from the IRS. Scammers use the IRS name or logo to make the message appear authentic so you will respond to it. In reality, it’s a scam known as “phishing,” attempting to trick you into revealing your personal and financial information. The criminals then use this information to commit identity theft or steal your money.

#### The IRS has this advice for anyone who receives an email claiming to be from the IRS or directing you to an IRS site:

- Ⓢ Do not reply to the message;
- Ⓢ Do not open any attachments. Attachments may contain malicious code that will infect your computer; and
- Ⓢ Do not click on any links in a suspicious email or phishing website and do not enter confidential information. Visit the IRS website and click on 'Identity Theft' at the bottom of the page for more information.

#### Here are five other key points the IRS wants you to know about phishing scams.

1. The IRS does not initiate contact with taxpayers by email or social media channels to request personal or financial information;
2. The IRS never asks for detailed personal and financial information like PIN numbers, passwords or similar secret access information for credit card, bank or other financial accounts;
3. The address of the official IRS website is [www.irs.gov](http://www.irs.gov). Do not be misled by sites claiming to be the IRS but ending in .com, .net, .org or anything other than .gov. If you discover a website that claims to be the IRS but you suspect it is bogus, do not provide any personal information on their site and report it to the IRS;
4. If you receive a phone call, fax or letter in the mail from an individual claiming to be from the IRS but you suspect they are not an IRS employee, contact the IRS at 1-800-829-1040 to determine if the IRS has a legitimate need to contact you. Report any bogus correspondence. Forward a suspicious email to [phishing@irs.gov](mailto:phishing@irs.gov);
5. You can help the IRS and other law enforcement agencies shut down these schemes. Visit the [IRS.gov](http://IRS.gov) website to get details on how to report scams and helpful resources if you are the victim of a scam. Click on "Reporting Phishing" at the bottom of the page.

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