COMPTROLLER of MARYLAND
Serving the People

Peter Franchot

TAXPAYER *Tips*

Security Awareness for Taxpayers: The Tax Community Needs Your Help

ANNAPOLIS, Md. (January 10, 2017) – The Maryland Comptroller's Office and the federal Internal Revenue Service are doing everything they can to protect Marylanders from identity theft. But officials at both agencies urge Marylanders to take steps necessary to protect their personal and financial data.

Cybercriminals continue to steal enormous amounts of personal data from outside the tax system and to use that data to file fraudulent tax returns or commit other crimes while impersonating the victims.

Comptroller Peter Franchot urges Marylanders to take these steps to protect themselves and their data:

Keep Computers Secure

- Use security software and make sure it updates automatically; essential tools include using a firewall, virus/malware protection and file encryption for sensitive data.
- Treat personal information like cash, don't leave it lying around.
- Taxpayers should check out companies to find out who they are really dealing with.
- Give personal information only over encrypted websites – look for "https" addresses.
- Use strong passwords and protect them.
- Back up their files.

Avoid Phishing and Malware

- Avoid phishing emails, texts or calls that appear to be from the IRS, tax companies and other well-known business; instead, go directly to their websites.
- Marylanders should not open attachments in emails unless they know who sent it and what it is.
- Download and install software only from known, trusted websites.
- Use a pop-up blocker.
- Families should talk about safe computing practices.

Protect Personal Information

Citizens should not routinely carry their Social Security card or any documents with their SSN. They should not overshare personal information on social media. Information about past addresses, a new car, a new home and one's children help identity thieves pose as someone they're not. Maryland citizens should keep old tax returns and tax records under lock and key or encrypted, if electronic. They should shred tax documents before trashing.

The IRS urges citizens to watch out for IRS impersonators. Officials there say "the IRS will not call you with threats of jail or lawsuits. The IRS will not send you an unsolicited email suggesting you have a refund or that you need to update your account. The IRS will not request any sensitive information online. These are all scams, and they persistent and change frequently. Don't fall for them. Forward IRS-related scam emails to phishing@irs.gov. Report IRS-impersonation telephone calls at www.tigta.gov."

Additional steps:

- Citizens should check their credit report at least annually and check their bank and credit card statements often;
- Citizens should review their Social Security Administration records annually. They can sign up for My Social Security at www.ssa.gov.
- If someone is an identity theft victim whose tax account is affected, they should review http://www.irs.gov/identitytheft for details.

For more information, visit IRS.gov.

###