



News Release

Media Relations Office

Washington, D.C.

Media Contact: 202.317.4000

www.irs.gov/newsroom

Public Contact: 800.829.1040

IRS Warns Washington D.C., Maryland, Virginia Residents of New Phishing Scam Targeting National Capital Area

IRS YouTube Videos

Tax Scams: [English](#) | [Spanish](#) | [ASL](#)

Security Summit Identity Theft Tips Overview: [English](#)

Be Cautious When Using Wi-Fi: [English](#)

Update Your Password Regularly: [English](#)

IR-2016-55, April 6, 2016

WASHINGTON — As reports of phone scams as well as email phishing schemes continue across the country, the Internal Revenue Service warned taxpayers of a new phishing scam targeting Washington D.C., Maryland and Virginia residents.

This time, the email scammers are citing tax fraud and trying to trick victims into verifying “the last four digits of their social security number” by clicking on a link provided. The criminals specifically state that this is for tax filers in the District of Columbia, Maryland and Virginia. As a further attempt to trick residents of the Capital region, the email scam even suggests that information from recent data breaches across the nation may be involved.

“As we approach the final days of this filing season, we continue to see these tax scams evolve.” said IRS Commissioner John Koskinen. “We don’t send emails like this, and there’s no special effort underway for people in the District, Virginia and Maryland. As these criminals shift their tactics, the IRS remains committed to quickly warning the taxpayers who may be targeted. Taxpayers should be on the lookout for these scams.”

Last February, the IRS announced a 400 percent increase of these scams being reported when compared to the same period last year. As the email scams increase, the IRS continues its efforts to protect taxpayers, and has teamed up with state revenue departments and the tax industry to make sure taxpayers understand the dangers to their personal and financial data as part of the [“Taxes. Security. Together”](#) campaign.

In general, the IRS has added and strengthened protections in our processing systems this filing season to protect the nation's taxpayers. For this tax season, we continue to make important progress in stopping identity theft and other fraudulent refunds.

Protect Yourself

Phishing is a scam typically carried out with the help of unsolicited email or a fake website that poses as a legitimate site to lure in potential victims and prompt them to provide valuable personal and financial information. Armed with this information, a criminal can commit identity theft or financial theft.

If a taxpayer receives an unsolicited email that appears to be from either the IRS or an organization closely linked to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), report it by sending it to phishing@irs.gov. Learn more by going to the [Report Phishing and Online Scams](#) page.

It is important to keep in mind that the IRS generally does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels. The IRS has [information online](#) that can help protect taxpayers from email scams.

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.

Don't be fooled by scammers. Stay safe and be informed.