INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.317.4000
www.irs.gov/newsroom | Public Contact: 800.829.1040

IRS, States and Tax Industry Warn of Last-Minute Email Scams

IR-2017-64, March 17, 2017

WASHINGTON – The Internal Revenue Service, state tax agencies and the tax industry today warned both tax professionals and taxpayers of last-minute phishing email scams, especially those requesting last-minute deposit changes for refunds or account updates.

As the 2017 tax filing season winds down to the April 18 deadline, tax-related scams of various sorts are at their peak. The IRS urged both tax professionals and taxpayers to be on guard against suspicious activity.

The IRS, state tax agencies and the tax industry, acting as the Security Summit, enacted many safeguards against identity theft for 2017, but cybercriminals are ever evolving and make use of sophisticated scams to trick people into divulging sensitive data.

For example, one new scam poses as taxpayers asking their tax preparer to make a last-minute change to their refund destination, often to a prepaid debit card. The IRS urges tax preparers to verbally reconfirm information with the client should they receive last-minute email request to change an address or direct deposit account for refunds.

The IRS also suggests that tax professionals change and strengthen their own email passwords to better protect their email accounts used to exchange sensitive data with clients.

This is also the time of year when taxpayers may see scam emails from their tax software provider or others asking them to update online accounts. Taxpayers should learn to recognize phishing emails, calls or texts that pose as familiar organizations such as banks, credit card companies, tax software providers or even the IRS. These ruses generally urge taxpayers to give up sensitive data such as passwords, Social Security numbers and bank account or credit card numbers.

Taxpayers who receive suspicious emails purporting to be from a tax software provider or from the IRS should forward them to phishing@irs.gov. Remember: never open an attachment or link from an unknown or suspicious source. It may infect your computer with malware or steal information. Also, the IRS does not send unsolicited emails or request sensitive data via email.

The Security Summit maintains a public awareness campaign for taxpayers – Taxes. Security. Together. – and an awareness campaign for tax professionals – Protect Your Clients; Protect Yourself – as part of its effort to combat identity theft.

— 30 —