



Rhode Island Department of Revenue

Division of Taxation

ADV 2021-49
SECURITY SUMMIT

ADVISORY FOR TAXPAYERS AND TAX PROFESSIONALS
DECEMBER 2, 2021

Tax pros should be wary of information-stealing scams

National Tax Security Awareness Week - Day Four

PROVIDENCE, R.I. – The Rhode Division of Taxation, the Internal Revenue Service (IRS), and other partners in the Security Summit today warned tax professionals that they face additional security risks from cybercriminals seeking to use the pandemic-related industry changes and scams to steal sensitive client information.

As more tax preparers work from home or remote locations because of COVID-19, professionals may need to take extra steps to safeguard client information and secure tax data. The Security Summit partners urge tax professionals to increase their focus on these security issues. They have released the 'Security Six' - six simple steps that can make a big difference for tax pros as well as taxpayers:

- Use anti-virus software and set it for automatic updates to keep systems secure. This includes all digital products, computers and mobile phones.
- Use firewalls. Firewalls help shield computers from outside attacks but cannot protect systems in cases where users accidentally download malware, for example, from phishing email scams.
- Use multi-factor authentication to protect all online accounts, especially tax products, cloud software providers, email providers and social media.
- Back up sensitive files, especially client data, to secure external sources, such as external hard drive or cloud storage.
- Encrypt data. Tax professionals should consider drive encryption products for full-drive encryption. This will encrypt all data.
- Use a Virtual Private Network (VPN) product. As more practitioners work remotely during the pandemic, a VPN is critical for secure connections.

Tax professionals are especially urged to be wary of scam emails from criminals masquerading as the IRS or related agencies. Anyone who receives such an email should save the email as a file and then send it as an attachment to phishing@irs.gov. They also should notify the Treasury Inspector General for Tax Administration at www.TIGTA.gov to report the IRS impersonation scam. Both TIGTA and the IRS Criminal Investigation division are aware of these scams.



Remember: never email documents that would disclose taxpayer identities and sensitive information. Criminals can use this information to file fraudulent returns by impersonating tax professionals. Emails where criminals also pose as potential clients could be especially effective this year due to the volume of remote transactions during the pandemic.

Summit partners also remind tax professionals - large and small - that they are all required to have a security plan in place. [Publication 4557, Safeguarding Taxpayer Data \(.pdf\)](#), provides tax professionals

with a starting point for basic steps to protect clients, and the [“Taxes-Security-Together” Checklist](#) is available to help tax professionals identify the basic steps they should take. Additionally, tax professionals should consider an emergency response plan in the event they experience a breach and/or data theft.

IRS [Publication 5293, Data Security Resource Guide for Tax Professionals \(.pdf\)](#) provides a compilation of data theft information available on IRS.gov, including the reporting processes.

About the Security Summit

The Security Summit consists of the IRS, state tax agencies, and the tax community -- including tax preparation firms, software developers, processors of payroll and tax financial products, tax professional organizations, and financial institutions. Partners in the Security Summit help protect taxpayers from identity theft and refund fraud. See <https://www.irs.gov/newsroom/security-summit> for more details.

The Rhode Island Division of Taxation is open to the public from 8:30 a.m. to 3:30 p.m. business days. For more information, contact the Division of Taxation at (401) 574-8829 or see <http://www.tax.ri.gov/contact/>.
