



04 | 14 | 20

## **IRS, Security Summit partners warn tax professionals on scams, urge additional security measures to protect taxpayer data**

IR-2020-71

WASHINGTON – The Internal Revenue Service and its Security Summit partners today urged tax professionals to take additional security steps immediately to protect taxpayer data as more practitioners telework and security risks increase.

The IRS, state tax agencies and the nation’s tax industry continue to see an upswing in data thefts from tax professionals as cybercriminals try to take advantage of COVID-19 and Economic Impact Payments to create new scams.

“Identity thieves view the pandemic as a chance to exploit tax professionals as well as taxpayers,” said IRS Commissioner Chuck Rettig. “They are using every trick of their criminal trade to con people as well as steal valuable personal and financial information to help enable tax-related identity theft. In many ways, tax pros are one of the first lines of defense. We urge the entire tax community to take additional steps and protect their sensitive data.”

The partners in the Security Summit – including the IRS, state tax agencies and private-sector tax industry – continue working closely together to watch for new threats during the coronavirus.

In addition, IRS Criminal Investigation is actively working to combat scam artists trying to exploit Economic Impact Payments and other provisions related to coronavirus. So far, the scams CI has already seen look to prey on vulnerable taxpayers who are unaware of how the payments will reach them. IRS CI is prioritizing these types of investigations to help protect taxpayers and the tax system.

### **Tax Pros: Use a Virtual Private Network for extra security**

All tax professionals who are teleworking should be using an encrypted Virtual Private Network or VPN. A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the internet and the company network.

Cybercriminals can exploit various weaknesses, whether by using a phishing email or an unsecured network, to gain control of a tax professional’s computer. Once they have remote control, they can either steal data or complete and file client tax returns but change the bank account information for refunds.

The government cannot recommend a VPN provider, but tax professionals can ask trusted colleagues or search for “Best VPNs” to find a legitimate vendor. Major technology sites often

provide lists of top services. Never fall for “pop-ups” on websites for VPN or any kind of security software. Those generally are all scams.

### **Multi-Factor Authentication helps protect data**

This year, most tax software providers for tax professionals and for taxpayers are offering the option of multi-factor authentication. Security Summit partners urge the use of this option. Multi-factor authentication means a returning user to the software product must enter not only their credentials (username/password) but also a security code, generally sent as a text to a mobile phone. The idea is the thief may compromise log-in credentials, but it is unlikely they will have stolen the mobile phone as well.

Multi-factor authentication protects the software account from being breached and from client data being stolen. Tax professionals should activate this feature immediately.

### **Avoid phishing scams**

Identity thieves have stepped up phishing scam efforts to capitalize on COVID-19 and Economic Impact Payments. Crooks are targeting tax professionals as well as taxpayers.

Tax professionals should beware of emails from criminals posing as potential clients. As people practice social distancing these days, criminals may exploit this process to try to trick tax practitioners into opening links or attachments. For example, crooks may present themselves as a new client and ask the practitioner to view the wage and income information they have in an attachment.

The Security Summit reminds tax professionals of simple steps to remember: Know your customers. Use the phone to confirm identities. And, don't take the bait.

Thieves also seek to impersonate tax software providers, cloud storage providers banks and others. Remember, phishing emails generally have an urgent message, i.e. your account password expired, and direct you to a link or attachment.

Taxpayers can report suspicious emails posing as the IRS to our \*PHISHING mailbox at [phishing@irs.gov](mailto:phishing@irs.gov).

### **Watch out for IRS impersonation scams**

The IRS will not call, email or text anyone about Economic Impact Payments. These are impersonation scams by thieves seeking to steal bank account or other sensitive data. Do not fall for these scams.

### **Don't forget security software**

Everyone, especially all tax professionals, should be using broad-based security software that protects not just their computers but mobile phones as well. Security features will help identify and stop potentially dangerous malware that can infect digital networks.

For more help, the IRS and the Security Summit partners urge tax practitioners to review the security measures outlined in [Publication 4557](#), Safeguarding Taxpayer Data.