ADV 2018-33
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
AUGUST 8, 2018

Tax professionals offer suggestions to colleagues about data safety

Tips from victims in the tax community include cyber insurance, stronger private networks

PROVIDENCE, R.I. – As cybercriminals keep trying to steal data from tax professionals, the Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit are sharing lessons learned by victims in the tax community to help others avoid being targeted by identity thieves.

In recent years, hundreds of tax professionals have experienced data thefts or breaches that exposed their clients' personal information to cybercriminals and to tax-related identity theft.

Several of those tax professionals are now offering their suggestions to their colleagues, actions they wish they had taken to safeguard their customers and their businesses. The tips range from taking out cyber insurance to using stronger private networks.

These suggestions – pulled anonymously from victimized tax professionals -- offer an opportunity for the tax community to learn from these common mistakes and avoid a devastating data loss for their clients and their business.

Lesson: Get cyber insurance coverage

A common refrain from tax professionals who have been victimized by cybercriminals is that they were glad they had – or wish they had – insurance coverage for data loss.

Many tax professionals maintain business policies that may cover property and liability, but it may not fully cover data thefts. Tax professionals victimized by these crimes recommend also exploring cyber coverage for data breaches. This may require an addendum or rider to the policy. Practitioners also suggest that the dollar amount of the policy be large enough to cover expenses.

Some insurance companies provide teams of experts in the event of a data theft, assisting tax professionals in identifying the source of the data breach and resolving it. These teams may also help notify clients or provide extended protections. Just as important, these teams of experts may assist tax professionals proactively, helping make sure adequate safeguards are in place to prevent a data theft.

Another recommendation: If using cloud storage, ask the cloud service provider about cyber insurance coverage in case the provider's systems are breached.

Lesson: Password-protect each client account

Many tax software products also enable tax professionals to password-protect each client account. Tax professionals who have experienced data thefts acknowledge that this can be a hassle, but worth the trouble should they experience a breach. They suggest password-protecting every account as a critical safeguard against cyberthieves.

Strong passwords can help prevent cybercriminals from accessing computer systems and accounts. Passwords should be eight characters or longer, a mix of letters, special characters and numbers, include an easy to remember phrase, and be unique for each account.

See Protect Your Clients; Protect Yourself: Tax Security 101 for more information on passwords and encryption.

Lesson: Use a virtual private network (VPN)

Tax professionals who have been victimized also wish they had used a virtual private network (VPN) instead of remote access software. A VPN allows for teleworkers or branch offices to securely connect to the firm's computer system and to send and receive information.

There have been cases where cybercriminals have taken over remote access of a tax professional's computer systems. In one example, the thieves remotely accessed client accounts via the tax pro's computer, completed and e-filed pending returns, and changed the deposit information to their own accounts.

Technology media often provide lists of top VPN services.

About this announcement

This is the fifth in a series of Security Summit announcements called "Protect Your Clients; Protect Yourself: Tax Security 101."

The Security Summit awareness campaign is intended to provide tax professionals with the basic information they need to better protect taxpayer data and to help prevent the filing of fraudulent tax returns.

Although the Security Summit -- a partnership among the Rhode Island Division of Taxation, the IRS, and others in the tax community -- is making progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices is on the rise.

Thieves use stolen data from tax practitioners to create fraudulent returns that can be harder to detect and harder to distinguish from legitimate taxpayer returns.

Lesson: Keep all security software updated

Tax professionals who experienced data thefts also suggest that colleagues keep all security software up to date. This includes the computer operating system, anti-malware, anti-virus software, firewalls, etc. While most computers come with security software installed, tax professionals also can purchase additional security software products.

Updated software helps protect users from emerging threats that can lead to data thefts. Users can set the security software to update automatically.

In addition to these steps, the Security Summit reminds all professional tax preparers that they must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule.

Tax Professionals also can get help with security recommendations by reviewing the recently revised IRS Publication 4557, "Safeguarding Taxpayer Data", and "Small Business Information Security: the Fundamentals" by the National Institute of Standards and Technology.

Publication 5293, "Data Security Resource Guide for Tax Professionals", provides a compilation of data theft information.

The Rhode Island Division of Taxation office is at One Capitol Hill in Providence, R.I., diagonally across from the Smith Street entrance of the State House. It is open to the public 8:30 a.m. to 3:30 p.m. business days. To learn more, see the Division's website: www.tax.ri.gov.