cybercriminals target IRS-issued identification numbers to help impersonate practitioners as well as taxpayers.

Aug. 17, 2018

The IRS and the Security Summit partners warned tax professionals that savvy cybercriminals target IRS-issued identification numbers to help impersonate practitioners as well as taxpayers.

To help protect against this threat used on the Dark Web, the IRS, state tax agencies and the tax industry reminded practitioners that they must maintain, monitor and protect their Electronic Filing Identification Numbers (EFINs) as well as keep tabs on their Preparer Tax Identification Numbers (PTINs) and Centralized Authorization File (CAF) numbers.

This is the sixth in a series 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 between the IRS, states and the private-sector tax community — is making progress against tax-related identity theft, cybercriminals continue to evolve, and data theft at tax professionals' offices is on the rise. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder to detect.

Cybercriminals sometimes post stolen EFINs, PTINs and CAF numbers on the Dark Web as a crime kit for identity thieves who can then file fraudulent tax returns. EFINs are necessary for tax professionals or their firms to file client returns electronically. PTINs are issued to those who, for a fee, prepare tax returns or claims for refund. CAF

numbers are issued when tax practitioners or their firms file a request for third-party

EFIN, it is important that they keep their account up-to-date at all times. This includes:

- Review the e-File application periodically. Tax professionals' e-file application must be updated within 30 days of any changes such as individuals involved, addresses or telephone numbers. Failure to do so may result in the inactivation of an EFIN.
- Ensure proper individuals are identified on the application, and update as necessary. The principal listed on the application is the individual authorized to act for the business in any legal or tax matters. Periodically access the account.
- Add any new principals or responsible officials promptly.
- Update any business address changes, including adding new locations.
- EFINs are not transferable; if selling the businesses, the new principals must obtain their own EFIN.
- There must be an EFIN application for each office location; for those expanding their business, an application is required for each location where e-file transmissions will occur.

Monitoring EFINs, PTINs and CAFs

Tax professionals can obtain a weekly report of the number of tax returns filed with their EFIN and PTIN. For PTIN holders, only those preparers who are attorneys, CPAs, enrolled agents or Annual Filing Season Program participants and who file 50 or more returns may obtain PTIN information. Weekly checks will help flag any abuses by cybercriminals. Here's how:

For EFIN totals:

- Access the e-Services account and the EFIN application;
- Select "EFIN Status" from the application;

- Contact the IRS e-help Desk if the return totals exceed the number of returns filed.

authorizations up to date. Tax professionals should make an annual review to identify outstanding third-party authorizations for people who are no longer their clients. It is important that tax professionals remove authorizations for taxpayers who are no longer their clients.

See "Withdrawal of Representation" in Publication 947, Practice Before the IRS and Power of Attorney. Information also is available in the instructions for Form 2848, Power of Attorney and Declaration of Representative, or Form 8821, Tax Information Authorization, for additional information on withdrawing representation.

Protecting EFINs

The same good security habits for protecting client data also can protect the EFIN. Those include the use of strong anti-virus software, strong and unique passwords, two-factor authentication where available.

- Learn to recognize and avoid phishing scams; do not open links or attachments from suspicious emails, most data thefts begin with a phishing email.
- Secure all devices with security software and let it automatically update.
- Use strong passwords of eight or more mixed characters; use phrases that are easily remembered and password protect all wireless devices.
- Encrypt all sensitive files/emails and use strong password protections.
- Backup sensitive data to a safe and secure external source not connected fulltime to the network.
- Wipe clean or destroy old computer hard drives that contain sensitive data.

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. They can get help with security recommendations by reviewing the recently revised IRS Publication 4557,

Safeguarding Taxpayer Data, and Small Business Information Security: the