From: Awareness
Cc: Awareness; SETA Team
Subject: SETA Newsletter - February 2026
Date: Monday, February 23, 2026 10:23:22 AM

Awareness
+2
Monday, February 23, 2026 · 6 min read

View in Outlook Newsletters

SETA Newsletter - February 2026

February may have fewer days, but scammers make every one of them count. Whether it's IRS-style emails boasting unbelievable refunds, social-media tax myths dressed up as "insider secrets," or melodramatic threats telling you to "pay now or else," scammers somehow manage to keep coming up with new ways to make tax season even more stressful. Incidentally, if the IRS ever threatens to arrest you by email... congratulations, you've just met a scammer.

For additional information on current tax scams, visit: Tax scams | Internal Revenue Service

Cybersecurity Tips for Tax Season: How to Protect Your Identity and Refund

Online Safety and Privacy | National Cybersecurity Alliance | February 17, 2026

Tax season comes with lots of stress - deadlines, paperwork, confusing forms, money on the line, high stakes if mistakes are made...Unfortunately, it's also a prime time for cybercriminals.

Every year around April, scammers ramp up phishing attacks, fake IRS

messages, and tax-related identity theft attempts, hoping to steal personal information or redirect refunds.

Importantly, though, these scams can occur at any time of the year.

But the good news is that a few habits can dramatically reduce your risk. Whether you file on your own or work with a tax professional, these tax season cybersecurity tips can help keep your data, identity, and your refund safe.

Why cybercriminals target tax season

Tax filings contain some of your most sensitive personal data, including your Social Security number, income details, and banking information. Criminals know this and often impersonate the IRS, tax preparation services, or financial institutions to trick people into handing over information or clicking on malicious links. They also know it's a stressful time and a lot of money is at stake for many of us.

Being prepared and cautious can make a huge difference. Resolving tax identity theft is usually time-consuming and stressful, so prevention is critical.

ESSENTIAL CYBERSECURITY TIPS FOR TAX SEASON

1. File your taxes early

One of the simplest and most effective ways to prevent tax fraud is to file as early as possible.

Criminals sometimes use stolen Social Security numbers to file fraudulent returns and claim refunds before the real taxpayer submits their return. Filing early reduces the window of opportunity for scammers. Employers are required to send W-2s and 1099s by January 31, so once you have your documents, don't wait. Remember, once it's done, it's done!

If you discover someone has already filed using your information, contact the IRS immediately.

2. Use an IRS Identity Protection PIN (IP PIN)

The IRS offers an Identity Protection PIN (IP PIN), a six-digit code that helps prevent unauthorized tax filings using your Social Security number and helps prevent identity theft.

The fastest way to get an IP PIN is through your online IRS account. You get a new IP PIN every year.

When you have an IP PIN, the IRS will reject any tax return filed without it –

even if a criminal has your Social Security number. The program is available to anyone who wants the extra protection – which should be all of us!

This step is especially important if your personal information has been exposed in a data breach, especially your Social Security number. Keep your IP PIN private and only use it when filing your return.

3. Enable multifactor authentication (MFA)

Multifactor authentication (MFA) adds an extra layer of security to your accounts by requiring more than just a password to log in.

Enable MFA on:

- Your IRS online account through ID.me
- Tax preparation software
- Bank and financial accounts

This additional step, which can include a face scan, authentication app, or one-time code texted to your device, makes it much harder for attackers to access your accounts, even if a password is compromised.

4. Watch out for tax scams pretending to be the IRS

Tax-related phishing scams are extremely common, especially early in the year. Scammers often pose as the IRS. They will also pose as tax preparers and financial institutions to steal information and money.

Look out for red flags:

- Unexpected IRS messages: The IRS does not initiate contact by email, text message, or social media.
- Urgent threats: Scammers may threaten arrest, fines, or immediate account action to pressure you into responding quickly.
- Requests for sensitive information: Never share your Social Security number, bank details, or login credentials via email, text, social media, direct messages, or phone.
- Suspicious links or attachments: Phishing emails often include links or files that can install malware on your device. If you suspect phishing, never click links or download attachments – report the email to your work IT department. If the suspicious message was sent to your personal email, report it to your email platform and delete it.

When in doubt, don't click. Go directly to official websites by typing the web address yourself.

5. Ask your tax preparer about their cybersecurity

If you work with a tax professional, their cybersecurity practices matter. Your data is only as secure as the systems that protect it.

Some good questions to ask are:

- How do you protect client data?
- Do you use encrypted portals for document sharing?
- Who has access to my information?
- How are tax records backed up?
- How long are records stored?

A reputable tax preparer should use encryption for documents and communications, limit internal access to sensitive information, and store records securely for an appropriate period (typically three to seven years). If your tax preparer doesn't follow these best practices, shop around for a safer competitor.

6. Exchange tax documents securely

Avoid sending tax documents as regular email attachments. Email is not a secure way to transmit sensitive information.

Use encrypted email or a secure file-sharing portal

- Follow your tax preparer's secure upload process
- If mailing documents, use a trusted courier with tracking
- Taking a few extra steps when sharing documents can significantly reduce the risk of data exposure.

7. Back up your tax records

Create both digital and physical backups of your tax documents. Store electronic copies in encrypted cloud storage, on an external hard drive, or both (both is great!). Keep paper copies in a secure location, such as a locked file cabinet or safe.

The IRS generally recommends keeping tax records for at least three years, but certain situations may require longer retention. Backups help protect against data loss from device failure, theft, or ransomware.

Please report scams to the IRS at its website!

SMART HABITS FOR A SAFER TAX SEASON

Tax season doesn't have to be a stressful nightmare...or, at least, you can have peace of mind that your risk of identity theft is reduced. Filing early, using available IRS protections, enabling MFA, and staying alert for scams

can go a long way toward protecting your identity and your refund.

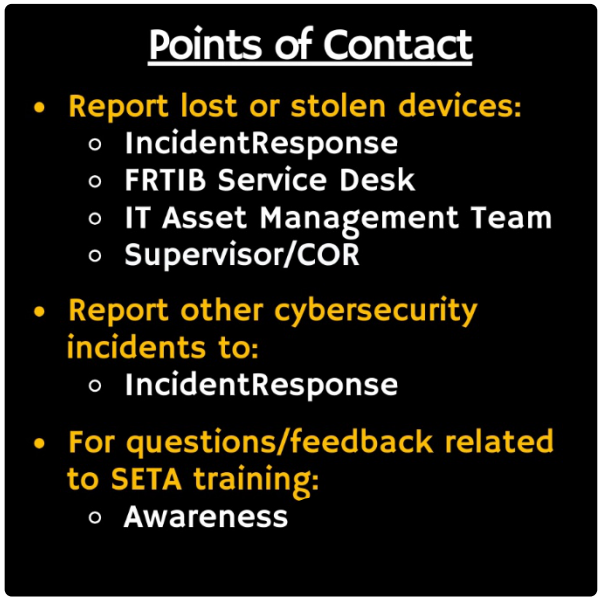
Full Article: [Cybersecurity Tips for Tax Season: How to Protect Your Identity and Refund - National Cybersecurity Alliance]

News:

Annual Role-Based Training campaign for those with an assigned NICE Role will begin 3/11.

Reminders:

Executive and Executive Role-Based Training is due 2/27



For additional information and resources, please visit the SETA Site on the FRTIB Town Center under Offices > OTS > IT Security Management Division > Security Education, Training, and Awareness (SETA).

Add Comment
