

NEWS BRIEF

IRS Offers Ways to Protect Tax Data for Cybersecurity Awareness Month



October is Cybersecurity Awareness Month, and the IRS is using the occasion to urge taxpayers to make online security part of their daily routine. In [a recent press release](#), the agency said a few simple habits can go a long way toward keeping personal, financial and tax information out of the hands of identity thieves and scammers.

The IRS is joining the Cybersecurity and Infrastructure Security Agency (CISA) and Security Summit partners in the effort. CISA offers [cybersecurity resources](#) for individuals, families and organizations, and the IRS stresses that these practices should continue long after the month ends.

Simple Steps to Strengthen Security

The IRS recommends that everyone, including employees at work and at home, start with these basics:

- **Use strong, unique passwords.** A password manager can help.
- **Turn on multifactor authentication** for an extra layer of account protection.
- **Update software and devices**, with automatic updates enabled when possible.
- **Recognize and report scams.** Be wary of unexpected messages that pressure you to act immediately.
- **Protect tax records by storing them securely**, encrypting sensitive files and backing up important information.
- **Use secure networks.** Avoid public Wi-Fi for financial accounts, tax records or IRS online services.

Why Vigilance Matters

These habits are your first line of defense against scammers who impersonate the IRS by mail, email, text, social media and phone, often promising bigger refunds or demanding immediate payment. The IRS normally makes first contact by mail and will never call to demand immediate payment, threaten arrest or tell taxpayers they are due a refund.

Your workplace can be a target too, since payroll and HR teams are frequent targets of phishing, fake invoices and W-2 schemes aimed at employee data or funds. If you get a request to change sensitive employee or payment details, verify it through a trusted channel before acting. The IRS also offers an [identity protection PIN](#) you can use to block fraudulent returns filed in your name, and suspicious tax-related mail, emails, texts or social media messages can be reported through [IRS.gov/SubmitATip](https://www.irs.gov/SubmitATip).

Looking Forward

Cybersecurity Awareness Month is a good time to revisit these habits, but the risks don't end after October. Continuously practicing these habits, verifying unusual requests and knowing where to report suspicious activity can help you protect yourself, your co-workers and your employer's data year-round.

The content of this News Brief is of general interest and is not intended to apply to specific circumstances. It should not be regarded as legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice. © 2026 Zywave, Inc. All rights reserved.