# STAY SAFE ONLINE DURING TAX TIME

Tax season can be a stressful time for many Americans, and scammers are waiting for you to slip up so they can steal your personal information, money and identity. The National Cyber Security Alliance (NCSA) and the Internal Revenue Service (IRS) want to help you stay safe online while filing your taxes with these best practices, tips, and resources.


## DID YOU SPOT A SCAM OR PHISHING ATTEMPT?

You can help protect others by reporting it. Contact the following agencies to report a phishing or scam attempt:

- FTC - Report Fraud
- IRS - Report Tax Fraud
- IRS - Report Phishing to phishing@ irs.gov

## *BEFORE YOU GET STARTED: PREPARE YOUR DEVICES*

### LOCK DOWN YOUR LOGIN

Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by creating an extra layer of security, such as a unique one-time code sent to your phone. Most major email and online tax preparation services have this tool available.

### UPDATE YOUR SOFTWARE

Before filing your taxes at home or work, be sure that all internet-connected devices –including PCs, smartphones and tablets – are running the most current versions of software to improve the performance and security of your devices.

### BEWARE OF PUBLIC WI-FI

Public wireless networks are not secure. If you are filing your taxes online make sure you are doing it on a secure and personal network.  We advise the use of a Virtual Private Network (VPN) any time you need to operate on Wi-Fi.

# STAY SAFE ONLINE DURING TAX TIME

## *THINK BEFORE SUPPLYING SENSITIVE INFORMATION*

Unsolicited emails, calls, or texts that prompt you to click on a link or share valuable personal and financial information are very likely scams. With your personal data, online thieves can swindle funds and/or commit identity theft. Learn how to recognize a scam with the following tips:

## IRS COMMUNICATIONS: REAL VS. FAKE

**Be skeptical of any phone calls, emails, or texts claiming to be from the IRS, or other government agencies.** Almost all contact from the IRS will be initiated via the U.S. Postal Service. They will only call once they have established a line of communication with you via physical mail first. The IRS will not demand you make an immediate payment to a source other than the U.S. Treasury.

Unscrupulous callers claiming to be federal employees can be very convincing by using fake names or phony ID numbers. If you are unsure if the caller is legitimate, hang up, look up the direct number for the agency online, and call that source to verify.

### OTHER RED FLAGS

- **Requests for PII:** Personally Identifiable Information (PII) refers to any data that could potentially identify a specific individual.
  - For example: Bank account information, Social Security numbers, login credentials, mailing addresses
- **Urgency**: The sender uses an abnormal sense of urgency, or other scare tactics, to obtain information.
- **Attachments**: The message includes an attachment, such as a PDF. Never open attachments from a suspicious or unknown email address. It may download malware or viruses onto your device.

### TIP: WHEN IN DOUBT, THROW IT OUT

If an email or seems suspicious, even if you think you know the source, it's best to just delete it. You can also report IRS, Treasury or tax-related phishing scams to phishing@irs.gov, then delete it.

# STAY SAFE ONLINE DURING TAX TIME

## *WORKING WITH TAX PREPARERS*

### DO YOUR RESEARCH

Vet your tax preparer before handing over sensitive information and ask what steps they take to protect your information. Businesses of all sizes are susceptible to cyberthieves, so it is critical to choose a preparer who takes security seriously.

### CHOOSING A CYBER-SAVVY TAX PREPARER

Be selective about who you choose to file your taxes.
Consider asking them the following questions:

- How will we exchange files and sensitive information?
- Who at your firm has access to my data?
- Are our communications end-to-end encrypted?
- What types of network security have you implemented?
- How do you back up client data?

### SECURELY SENDING DOCUMENTS

The most secure way of transferring documents is physically, either handing them to your tax preparer in person or sending them through the mail. However, if you must transfer them electronically, be sure to do it as securely as possible:

- **Encrypt your files before sending them via email.** Encryption protect the content from being read by entities other than the intended recipients. Encryption features are available on most major email platforms.
- **Use a secure portal to upload documents.** Portals encrypt documents during transfer and storage and limit access to only approved individuals.

### TIP: BACK IT UP

Protect your valuable documents by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup.

**Use the 3-2-1 rule as a guide to backing up your data:**

- Keep at least three **(3)** copies of your data:
- Store two **(2)** backup copies on different storage media,
- With one **(1)** of them located offsite.

# STAY SAFE ONLINE DURING TAX TIME

## IDENTITY PROTECTION PIN (IP PIN)

An Identity Protection PIN (IP PIN) is a six-digit number that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps verify your identity when you file your electronic or paper tax return. Learn more.

## RESOURCES FOR TAX PROFESSIONALS

**Protect Your Clients; Protect Yourself**
Every tax professional is a potential target for highly sophisticated, well-funded and technologically adept cybercriminals around the world.

**Working Virtually: Protect tax data at home and at work with the "Security Six"**
Check out these basic "Security Six" protections that everyone, especially tax professionals handling sensitive data, should use.

## + *ADDITIONAL RESOURCES*

- ☑ **IRS**: Tax Security 2.0 – A "Taxes-Security-Together" Checklist:
- ☑ **IRS:** Tax Scams and Consumer Alerts
- ☑ **IRS**: Security Summit
- ☑ **IRS:** Unemployment Fraud
- ☑ **Federal Trade Commission:** Tax Identity Theft Awareness
- ☑ **Identity Theft Resource Center:** Tax Identity Theft