



# Protect your business from tax scams

## Watch for these common signs of tax-related scams

- Fake requests for W-2s.
- Tax advice from misleading social media messages and posts urging you to:
  - File fraudulent tax documents.
  - Use tax software to manually prepare a Form W-2, Wage and Tax Statement, with false income information.
  - Pay fees to a preparer based on your refund amount.
  - Misrepresent your eligibility for tax credits.

## Don't ignore these signs of possible identify theft

- You're unable to e-file a return because one was already filed with the same EIN or SSN.
- You receive a rejection notice for a routine extension to file request because a return with duplicate EIN or SSN is already on file.
- You receive an unexpected tax transcript or IRS notice that doesn't match anything submitted.
- You receive **Letter 6042C** or **5263C** from the IRS.
- You aren't receiving expected or routine correspondence from the IRS because the business address has been changed.

## Safeguard your systems and data with strong security actions

- Add anti-malware/anti-virus security software with automatic updates enabled on all devices.
- Use responsible passwords and multi-factor authentication when available.
- Enter personal data only on secure sites with web addresses that begin with "https."

## Educate your employees

Help employees protect themselves and your business with information about data security. Visit [IRS.gov/idtheft](https://www.irs.gov/idtheft) for steps to protect their account or share the [Taxpayer Guide to Identity Theft](#).

## Safeguard your EIN

Keep your Employer Identification Number (EIN) safe and the application up to date with accurate, responsible party and contact information. Use Form [8822-B](#) to update your EIN.

## Report scams and tax fraud

You can help prevent fraud in the following ways:

- Report suspected tax fraud, scams, identity theft, or other tax-related wrongdoing at [IRS.gov/submitatip](https://www.irs.gov/submitatip).
- Tell us about data losses related to W-2 scams by emailing [dataloss@irs.gov](mailto:dataloss@irs.gov) and providing contact information. In the subject line, type "W2 Data Loss" so that the email makes it to the right people. Don't attach any employee personally identifiable information.
- Notify states of any disclosures of W-2s or other identity information by emailing [StateAlert@taxadmin.org](mailto:StateAlert@taxadmin.org).

For more information, visit [IRS.gov/taxscam](https://www.irs.gov/taxscam) or scan the QR code.

