How well does IRS Direct File protect taxpayers and their data?

To understand how tax filing alternatives stack up in terms of safety, reliability, and risk, let's consider how vulnerable each solution is, on average, from a cybersecurity perspective. Risk rankings are based on the likelihood of a threat scenario to expose the greatest number of taxpayers to immediate and longer-term financial losses and/or credit and reputational damage.

Let's examine cybersecurity risk, in order of prevalence and impact, based upon the three primary principles of cybersecurity - **confidentiality, availability, and integrity**:

- Threats that could expose private, **confidential** taxpayer data generally impact the greatest number of individuals all at once and can cause the most enduring harm to the taxpaying public,
- Compromises to the **integrity** of data that could contribute to fraudulent tax filings, pilfering tax refunds and/or spoofed IRS emails that could quickly lead to financial losses for targeted individuals, and
- Loss of **availability** triggered by data loss/destruction, or system/ support inaccessibility may cause delays and confusion for tax filers resulting in distress, audits and/or fines.

Below are key scenarios that highlight the connection between the cybersecurity principles and the potential harm to the greatest number of taxpayers, and risk rankings for each filing method based on potential sources of vulnerability characteristic of each method.

How to use this information

Keep in mind that while most tax-filers won't qualify for this year's limited pilot of Direct File, we may see Direct File expand beyond the types of income currently supported or increase the household income cap.

Choose the method with the best cost/ benefit/ risk tradeoff for your household. Keep vigilant for signs of identity theft and refund fraud.

If you have concerns, reach out to your tax professional, online filing provider, or the IRS support desk to ask how they protect your data and verify that it's kept secure and private.

Follow me on LinkedIn and check out my other articles covering risks to data and technology.

Tax filing gone wrong could compromise taxpayer data, leading to:

- **Confidentiality/ Privacy**
  - Disclosure/theft of sensitive personal and financial information and sign-on credentials to spoof your identity
  - Exploitation of personal income, demographic and lifestyle data for unwanted, unsavory advertising
- **Integrity/ accuracy**
  - Theft of tax returns by committing online or mail fraud
  - Exposure to targeted phishing and social engineering scams
- **Availability/ Accessibility**
  - IRS or state tax authority enforcement actions triggered by late, inconsistent, or incorrect filings

Taxpayer Security/ Privacy Vulnerability

Greatest Risk → Least Risk

	Online for-profit tax prep/ filing	For-profit tax professionals	Postal Mail Paper Tax Filing	IRS Direct File online filing
Use of 3rd party processing via contractors and suppliers	(C)onfidentiality	C	C	
Accountability for hardcopy paperwork and/ or refund checks		C	C	
Excessive online tracking/ snooping	C			
Motivation to monetize user activity and data	C	C		
Complexity of filing/ multi-step data entry and processing			(I)ntegrity	I
Tax filing approach familiarity/ novelty				I
Availability of reliable support	(A)vailability		A	A

** This risk ranking assumes that all practitioners, software providers, and agencies take reasonable and appropriate precautions, employing a comprehensive, compliant framework of technical, operational, and administrative data protection practices and techniques to secure data in transit, at rest, and during processing.*