Concerned About the Cloud?

How the Most Reputable E-File Providers Handle Data Security

Brought to you by

FORMSTAX efile4biz™

It’s All About Security

When news of data breaches and identify theft make headlines, it’s not unusual to look at cloud-based services with a more critical eye. Take online tax filing. How can you be certain the sensitive information you capture from independent contractors and employees for 1099, W-2 and ACA filing doesn’t fall into the wrong hands?

Certainly, not all cloud-based businesses are alike – and it’s wise to question their security practices before you partner with them. With a greater understanding of the latest online security measures, however, you can more confidently select a reputable and safe e-file provider. Not only is the IRS stepping up its efforts to fight identity theft, but quality e-file sites are utilizing a handful of cutting-edge safety precautions. The result is a level of data protection that would thwart even the most sophisticated cyber criminals.

This e-guide will explore the growth of cloud-based tax-filing services – and what the best providers are doing to protect your data and earn your business.

What Exactly Is the Cloud?

A novel concept a couple decades ago, cloud processing is transforming how businesses run their operations and serve their customers.

For many employers, tax filing in the cloud is the next logical step from traditional software. If you're dependent on typical tax-filing software, you know it can be:

- Expensive, time-consuming and sometimes difficult to upgrade
- Limiting, because it's only accessible on the computer where it's stored
- Restrictive, because only one person has user access
- Difficult to get the customer support when you need it most

Cloud processing through an e-file platform allows you to go online to enter or upload your employee and independent contractor data and complete their filings – anytime, anywhere. With protected Internet access, you can prepare tax filings and submit them to the IRS or Social Security Administration right from your web browser. Plus, with the right e-filing provider, you don't have to print forms, stuff envelopes and visit the post office to distribute recipient copies by the end-of-January deadline. A full-service provider will print and mail forms directly to the employees and independent contractors from a secure, certified facility.

To be clear: Today's full-service, cloud-based filing is different from software you install on one computer, with limited access, and that only provides a handful of electronic filings. Now, you can conduct unlimited filing and distribution activities, and access all data, just by logging into and navigating a secure, specialized website – again, from any computer, laptop or tablet.

First Layer of Security: IRS Authorization

So you're interested in shifting from time-consuming paper filing to faster, more efficient electronic tax filing. But how can you be certain a cloud-based business is taking all the necessary security precautions?

There are several factors to consider when choosing an e-file provider. First and foremost, make sure you are working with an authorized IRS transmitter. To become an IRS transmitter, a tax return preparer or tax-reporting business must go through a rigorous three-step process.

1) Create an IRS e-services account — Before a business can submit an e-file application, it must create an IRS account, which allows electronic interaction with the IRS. In addition to providing specific identification details (Social Security number and phone number), the person creating this initial account must make sure every principal and responsible staffer in the business signs up for e-services. This point person also must confirm registration within 28 days of receiving an IRS confirmation code in the mail.

2) Submit an e-file application — A business can begin the application once all essential people are approved for e-services. Because the application is so comprehensive, it can take up to 45 days for the IRS to approve it.

3) Pass a suitability check — The business has submitted an application and related documents. Now the IRS can conduct a suitability check on the organization and each person listed on the application as either a principal or responsible employer. This may include a credit check, tax compliance check, criminal background check and/or a check for past

Upon this approval, the business gets an acceptance letter from the IRS and a Transmitter Control Code (TCC) that allows the business to offer e-filing.

As stated on the IRS website:

"The application process is not simple, but as a tax professional, you understand these steps are necessary to protect the integrity and security of the electronic filing system. We all have a stake in maintaining the highest standards for e-file providers."

Security Through Encryption of Sensitive Data

Next, a first-time user needs to know how the site handles confidential information, particularly through data encryption. Encryption is an advanced procedure that scrambles and locks information so it's unreadable and inaccessible without a private decryption key.

Only with the strongest encryption protocol recommended by the federal government – like Transport Layer Security (TLS) – can a provider effectively protect data as it's sent back and forth. There are a handful of reliable companies that issue encrpytion certificates guaranteeing information won't be stolen or compromised, including Symantec, DigiCert, Verisign and GeoTrust.

Print and Mail Facility Security

With cloud processing, data transmission is only half the necessary protection. The user has electronically filed with the appropriate government agencies, but now they need to send copies to employees and other recipients. And unless these individuals opted to receive an electronic version, the user will need to print and mail paper copies through their chosen provider.

Facilities that have achieved Service Organization Control (SOC) certification follow all the necessary precautions to protect data. This special certification by the American Institute of Certified Public Accountants (AICPA) means that every step of the e-filer's process has been thoroughly examined and approved to guarantee security.

Specifically, the AICPA examines these areas:

- **Security:** The entire system is protected against unauthorized access
- **Availability:** The system is functional and operates correctly
- **Processing integrity:** Data processing is complete and accurate
- **Confidentiality:** All sensitive information is protected
- **Privacy:** Personal information is collected, used, retained and disclosed in conformity with the AICPA's privacy principles

The certification process is costly and time-consuming. But in the end, it's a key indicator of a quality provider.

Security of Protected Health Information

Finally, if you're a business seeking an e-file provider for help handling Affordable Care Act (ACA) reporting, you need to check for one additional certification.

ACA forms include employee personal information, like Social Security numbers and birth dates, along with specific health insurance details. These details are considered protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) — and must be handled according to strict privacy and security rules.

ACA reporting requires greater security than other IRS forms. Third-party vendors, such as payroll and e-file providers, should be HIPAA-compliant and, therefore, contractually bound to encrypt and safeguard electronically transmitted PHI.

Additional Security Steps You Can Take

Although your choice in an online e-file provider is the most important factor with data security, there are additional steps you can take to increase cyber safety in your workplace:

1 Use robust passwords

Oftentimes, passwords are too simple, making it easy for hackers to tap into accounts and steal personal information. The key to avoiding problems is making sure passwords are complex, unpredictable and impossible to guess.

One way to test a program's security is to create a mock account with a very simple password and see if the program accepts it. A website or online service that doesn't prompt you to create a more sophisticated password may not be trustworthy. Strong passwords typically require eight characters containing at least one number, one letter and one special character such as "!","@", "#", or "%."

2 Build a solid firewall

Firewalls (whether installed as software or built into devices as hardware) act as a screening device for information coming in and out of computer networks. They can block leaks of private information and prevent outside threats such as viruses from coming in. They will also prevent users from visiting webpages that could be potential threats. You can make adjustments as needed, such as allowing exceptions for certain sites or lowering the firewall's sensitivity.

3 Keep antivirus and anti-malware software up to date

This is something many businesses overlook, even after they've made the effort to build a strong firewall. Unless you're staying on top of the latest versions or patches, you could open the door to new scams, phishing attacks and other risks.

4 Limit access to the appropriate individuals

Only allow approved individuals to access sensitive data and systems. Require administrator's logins and set up screen savers that request passwords after a period of inactivity, all of which help keep information out of the wrong hands – from your internal staff as well as the outside world.

Read the Fine Print on the Site

You can check a few additional elements on the site itself to determine if you're dealing with a trusted provider:

HTTPS: The S in HTTPS (Hypertext Transfer Protocol Secure) stands for "Secure" and indicates the site uses TLS encryption. If there's no S in the URL, proceed with caution.

Lock icon: Appearing as a padlock icon on the left or right side of the URL bar (depending on the browser), this icon also indicates SSL encryption. A "security report" pop-up should appear when you click on it, showing web permissions and security certificates.

Badge verification: You should see a "Verified by" graphic somewhere on the site. It typically displays the name of the business verified, as well as the date of the last security scan. Look for a pop-up page here, too, with confirmation of the site's security and identity.

Website privacy policy: A carefully designed policy includes disclosures on how your data is collected, how it's used and the security measures in place. Be wary of any site that doesn't highlight its privacy policy somewhere on the site.

Why efile4Biz Is the Ultimate Choice

Many businesses are coming out of the woodwork right now, claiming they can help employers with mandatory information reporting. Truth is, some are only taking advantage of an emerging opportunity – and don't have the expertise or sophistication to meet your needs and keep your information safe. Worst still, others are downright scams.

Here are three factors to consider – and why efile4Biz.com is the clear choice for your 1099, W-2 and ACA tax filing:

1 Is the business experienced?

Without the credibility or background to handle your filings, a new business is asking you to take a leap of faith and trust they'll do the right thing. This is no time to test a new business or assume they have your best interests in mind.

***Efile4Biz.com** is an industry leader and pioneer, backed by a team of highly qualified and dedicated experts. Seasoned tax professionals ensure a practical tax-filing process from start to finish, and a legal staff keeps abreast of the latest tax-filing requirements.*

2 Is the business compliant?

Working with a provider that isn't authorized by the IRS is asking for trouble. 1099s, W-2s and 1095s are all IRS tax forms with very specific requirements, so why would you choose a tax-filing service that isn't approved by the IRS itself? The risk of incomplete or late filings – and the related penalties – is too great.

***Efile4Biz.com** is an IRS-authorized transmitter that underwent a rigorous screening process to become an official IRS transmitter. Many tax return preparers or online tax-filing services don't ever undergo this process – or were denied, but continue to operate without IRS authorization.*

3 Is the business secure?

In today's digitally focused world, data security is vitally important to avoid breaches, identity theft and other cyber threats. Yet many e-file providers are nothing more than mom-and-pop businesses storing sensitive data, such as SSNs and tax IDs, in homegrown databases. Just as alarming, they may print and mail forms out of their garages.

*All sensitive data you enter on **efile4Biz.com** is encrypted under strict IRS guidelines and printed from a high-security, SOC-certified and HIPAA-compliant print and mail facility. You can be confident your sensitive data is guarded against tampering and identity theft through the latest, most stringent business practices.*

But That's Not All ...

A More Detailed Look at Our Threat-Prevention Measures

With a commitment to unparalleled data security, efile4Biz takes a series of physical, electronic, contractual and managerial steps to safeguard information. Among them:

- Distributed Denial of Services (DDOS) systems to thwart attacks aimed at disrupting operations or compromising systems.
- Multi-factor Authentication (MFA) that provides additional security to verify your identity and ensure secure access to your account.
- Intrusion Prevention Systems (IPS) that monitor networks for malicious activities.
- Firewalls that provide multiple DMZs (also known as perimeter networks) to shield systems from both the Internet and efile4Biz's private network.
- Antivirus software installed (and on servers) to protect from virus and malware attacks.
- Use of a third-party PCI authorized scanning vendor to perform periodic vulnerability scans from the Internet to detect potential exposures exploitable by hackers.
- Internal scanning of servers with assessment tools to identify any vulnerabilities that may make a system susceptible to an intrusion.
- Performance of web application penetration tests by certified penetration testers.

FORMSTAX efile4biz™

©Copyright Efile4Biz.com