Protecting Data During Tax Season

WithMe

In the first four months of every year, **cybercrime spikes.**

Tax season is a veritable feeding frenzy for hackers. People hand over their Social Security numbers, bank information, W-2s ,and pay stubs without a second thought. Not surprisingly, tax-related fraud continues to rise every year. In 2025 alone, millions of Americans fell victim to financial scams, leaving a $10.59 billion trail of damage.

Each one of those breaches has the same origin story. Someone trusted the wrong system with sensitive information. We've seen it time and time again in multifamily, hospitality, and commercial offices just like yours. Tax season is every organization's biggest data stress test, and most businesses are set up to fail before it even begins.

Cybercriminals will exploit every weak link in the chain, from emails that reside on employee devices to something far less obvious, like a shared printer. The billions lost last year? That wasn't just money, it was also a loss of trust. And trust is fragile. One misstep, one unsecured document, and suddenly, your organization is front-page news for all the wrong reasons.

Tax season is the time of year when vigilance is paramount, because one slip can lead to hefty regulatory fines, irreparable reputational damage, or a full-blown data breach.

Where Your Data Is Most Vulnerable

When it comes to protecting sensitive information, most organizations focus on obvious targets. Hackers. Malware. Phishing emails. But the truth is, your data faces threats from multiple directions. Some you can see, and some you might never notice.

Physical documents

Paper might seem old school, but it remains one of the most vulnerable ways sensitive information is handled. Printed records are everywhere. On desks. In filing cabinets. Sitting in shared office trays. Left unattended, misplaced, or improperly disposed of, these documents can be accessed by anyone within close physical proximity, creating risk that digital safeguards can't prevent.

During tax season, the surge in printed sensitive information, and the greater likelihood of human error, makes exposure far more likely.

Emails and digital communication

Tax season is prime time for phishing and social engineering attacks. Cybercriminals masterfully craft emails that appear authentic, often impersonating government agencies, financial institutions, or even internal staff. The goal is to trick employees and residents into clicking malicious links, downloading infected attachments, or handing over private login credentials.

One careless click could be a mistake that compromises an entire network, exposing payroll data, resident information, bank accounts, and other personally identifiable information (PII).

Employee devices

Laptops, tablets and smartphones are often overlooked gateways to some of your organization's most sensitive data.

When devices are lost, stolen, or inadequately secured, cybercriminals can exploit them to gain direct access to internal systems, bypassing traditional network defenses. Risks are compounded when software isn't regularly updated, passwords are weak or reused, or employees connect to unsecured Wi-Fi networks.

Third-party systems

Vendors, cloud platforms, and external service providers are essential to daily operations, but they can also introduce security blind spots. Any time sensitive information is shared with a third party, your risk footprint expands beyond your own environment. The real question isn't whether you trust them, it's whether you can verify they're protecting your data to the same standard you expect internally.

Weak access controls, unpatched software, or inconsistent security practices on their side can create openings for attackers, turning a trusted provider into an unintended point of compromise.

Best Practices for Protecting Sensitive Information During Tax Season

Protecting data requires a multi-layered, proactive approach. Here's how property teams can reduce risk and safeguard trust:

Limit access and enforce permissions

Start by controlling who has access to sensitive information. PII shouldn't be accessible to every employee. Implement role-based access controls and restrict file permissions so only those who require information for their work can access it. Regularly audit access logs to catch any anomalies or unauthorized attempts.

Strengthen digital security measures

Digital channels are the most common entry points for attacks during tax season. Make sure employees are trained to identify phishing attempts, social engineering tactics and suspicious attachments. Enforce strong password policies, enable multi-factor authentication (MFA) wherever possible, and keep all software, devices, and systems patched and updated.

Vet third-party vendors carefully

Your vendors and cloud service providers are extensions of your organization. Before sharing sensitive data, verify they uphold rigorous security standards. Establish contracts that clearly define data handling responsibilities, including breach reporting protocols.

Protect printed materials from unauthorized access

Ensure sensitive documents are stored securely in locked cabinets or access-controlled areas. Implement strict check-in/check-out procedures for printed materials, and train staff to never leave documents unattended in shared spaces. When disposing of documents, use cross-cut shredders or secure disposal services to prevent data from falling into the wrong hands.

Train, reinforce, repeat

Human error is a major factor in most breaches. Regular training sessions, short refresher courses and simulated phishing tests help employees recognize threats and respond appropriately. Encourage a culture of vigilance. Employees should feel empowered to question suspicious activity and follow protocols without hesitation.

Monitor and audit continuously

Security isn't "set it and forget it." Regularly review your systems, network logs and document-handling practices. Look for unusual access patterns, failed login attempts or missing documents. Continuous monitoring helps you catch risks early before they escalate into breaches or compliance violations.

Document your policies and protocols

Clear, written policies on how to handle sensitive information demonstrate your organization takes data security seriously. This not only helps your team follow best practices consistently, but also shows regulators and auditors that you have proactive measures in place.

Plan for incident response

Even the best defenses aren't foolproof. Have a well-defined incident response plan so your organization can act quickly if a breach occurs. Define roles, communication protocols, and steps for containment, investigation, and notification.

Adopt secure printing solutions

Printers don't usually make the security checklist, and that's exactly the problem.

Especially during tax season, printers process highly sensitive information, from internal records to documents that residents need for tax filing. And unlike other systems in the tech stack, printers often operate in the background, unchecked and unmonitored.

Here's the uncomfortable truth: many traditional printers store data, transmit files without encryption, and even monetize user information. As state-level privacy laws grow more stringent and enforcement becomes more aggressive, this creates serious risk, which falls into three clear categories:

- **Data breaches:** Hackers, rogue employees or even well-meaning staff can unintentionally expose sensitive documents. The fallout can include legal consequences, operational disruption and erosion of trust.
- **Non-compliance:** Privacy regulations increasingly require transparency, consent and the ability to honor data rights such as deletion and correction. Printers that store or mishandle data can put organizations out of compliance.
- **Overstated security claims:** If vendors claim full security without substantiating it, regulators like the FTC can, and will, step in.

This is why secure printing is essential.

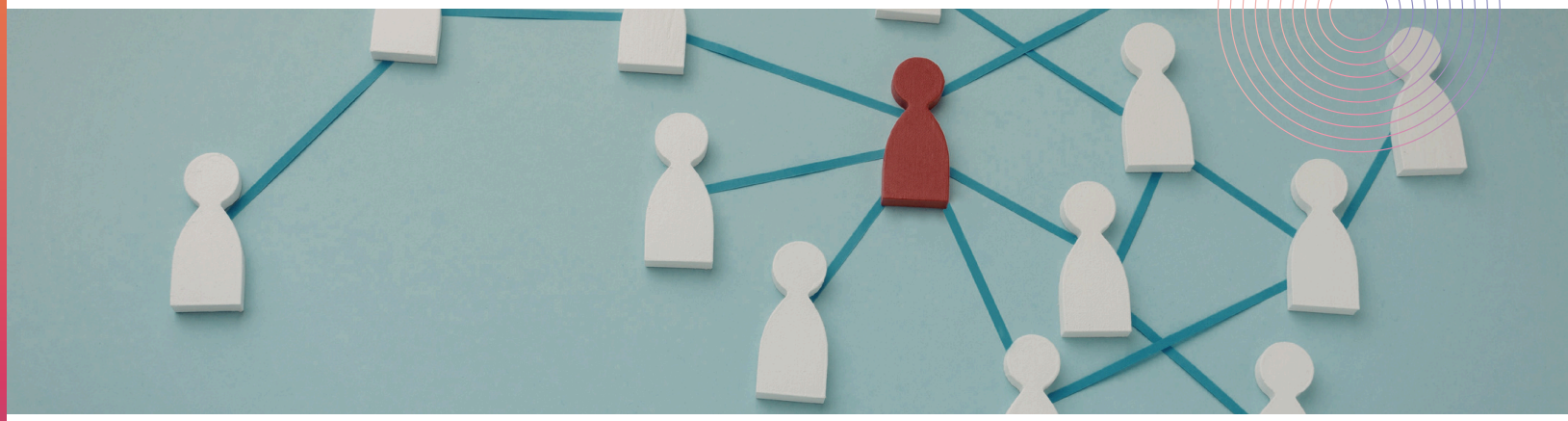
Imagine this:

A resident prints their W-2 on a shared office printer. Long after the job completes, that information can linger, stored in the printer's memory, in print queues, or in an inbox, viewable or retrievable by anyone with the ability to reach it. And then there's the most visible part of all: the hard copy itself, sitting on the output tray in a shared space until someone picks it up. It's like leaving your front door wide open so everyone in the neighborhood can see what's going on inside.

Modern, privacy-first printing solutions are designed to eliminate risk at every stage of the print lifecycle. With PrintWithMe, every print job is encrypted end-to-end, securely released only to authorized users, and automatically deleted once completed. There's no lingering data, no hidden storage and no ambiguity about how information is handled.

Transparent data practices and compliance with privacy laws like CCPA are built into the experience, not added as an afterthought.

In 2025 alone, 1.1 million people used PrintWithMe printers to securely print more than 33 million pages. That level of activity highlights just how much sensitive information can flow through shared printers every day, and, even more, how critical it is to protect it. Expand that lens to other verticals like hospitality or government services, and the potential risk and responsibility only grows.



Secure printing solutions also reduce operational burden. Centralized management makes scaling simple, plug-and-play installation removes complexity, and flat-rate, all-inclusive pricing eliminates budget surprises. Auto-shipped paper and toner removes a routine headache from teams, and outsourced support and service gives everyone peace of mind.

Data is only as safe as the weakest link in your organization, and **tax season has a way of exposing gaps** that usually go unnoticed. Sensitive information moves through more systems than most teams realize, and even everyday tools like shared printers can introduce risk when they're not properly secured. Paying attention to these overlooked details is how organizations protect both their data and the trust that depends on it.

Overtaxed teams need fewer security worries, not more.

Let's talk about how PrintWithMe can protect sensitive resident and business data during tax season - and all year long!

withme.com

sales@withme.com