Four Ways to Increase Cybersecurity and Safeguard Data

Learn how to confidently protect your business and client information in the cloud.

SmartVault

Table of Contents

STEP 1: Understand Your Risks: Cyberattacks Can Happen to Any Business Anywhere

Your clients trust you with their most personal information, and you're obligated to protect it. With cyberattacks happening more frequently than ever before, protecting your business and client data is a large obligation to meet — but it doesn't have to be overwhelming.

As a tax and accounting professional, you have the information thieves need to impersonate their victims, file fraudulent tax returns, apply for loans, and more. This puts you at *significant risk for cyberattacks*, especially if you work for a small-to-mid-size firm. Although cyberattacks target all industries and company sizes, hackers tend to think smaller businesses are the easiest targets, as many don't have proper processes in place to keep data secure.

Regardless of your firm size or who your clients are, prioritizing cybersecurity is a must. This eBook will teach you about cybersecurity and four actions you can implement to safeguard your business and client information from criminals.

8 Data Security Facts

Every 11 seconds a company is a victim to a ransomware attack, on average. *(Cyber Security Ventures)*

95% of breaches are caused by human error. *(World Economic Forum)*

22 billion records were exposed in 2021 breaches. *(Risk Based Security)*

Over 70% of US adults are concerned about data breaches when filing taxes online. *(PC Mag Tax Survey 2021)*

$5.05 Million is the average cost of a data breach in the United Kingdom. *(IBM)*

$9.44 Million is the average cost of a data breach in the United States. *(IBM)*

358% is the amount malware attacks increased in 2020. *(Help Net Security)*

435% is the amount ransomware attacks increased in 2020. *(Help Net Security)*

Know How Criminals Access the Data

The first step to creating a safer accounting practice is to *understand how cybercriminals access sensitive information.* Attempts can happen overnight, but mostly take days, weeks, or even months to be successful or discovered. Here are the most common ways cybercriminals gain access.

MALWARE

Cybercriminals design malware — short for malicious software — to steal your data and destroy and/or damage your computers and systems. Infections typically happen from clicking on a link or opening an infected email attachment. Malware includes things like viruses, spyware, and ransomware.

PHISHING

This type of attack lures people into disclosing their personal information, like passwords and social security numbers. Criminals accomplish this by making the victim believe the message and request are trustworthy. These attempts are usually performed via email or text message and appear to come from known, trusted sources, like your bank, loan provider, credit card company, or even places like big box stores.

MAN-IN-THE-MIDDLE (MitM)

Also known as eavesdropping, a perpetrator puts themselves between you and an application (i.e., your mobile device and its Internet browser). The victim is completely unaware that all the information they're passing to the application is going straight to the perpetrator. The attacker may even install software to access all of your information. People put themselves at risk for this when they connect to the Internet using an unsecure public Wi-Fi.

RANSOMWARE

A type of malware, ransomware makes its victims pay — literally. Ransomware keeps you from accessing your data by encrypting your files (making them unreadable). The criminals give you an ultimatum: pay a fee or lose the data indefinitely. Some attackers even demand a second ransom with the promise they won't sell your data online to other criminals. Ransomware is one of the final steps in a larger attack, as the criminal already accessed your network and data through an initial method, like malware or phishing.

Assess Current Policies

You need to pay attention to how you're handling sensitive information today. That means looking at the software and hardware you use, as well as evaluating your current operations. Think about your teams, both in-house and virtually, and the contractors or vendors who have access.

Review the flow of information you receive about and from your clients all the way through to when you are finished with the information and are ready to store it. Document as much as possible about how it is cared for and accessed. Consider things like where your data is stored. Is it online, off-line, locally, or in the cloud?

Identify all potential points of failure in your workflow, systems, or personnel. For example, if your business stores all vital information in only one place, what would happen if that access failed or was destroyed?

Let's say you have everything saved on an encrypted hard drive, but suddenly that computer is infected with ransomware — everything was lost. Could you recover the data from another secure, cloud-based backup? What happens if you can't?

This also applies to people. Perhaps your bookkeeper is the only one who knows vital or sensitive information about a client. If that person leaves your company, how would you recover those details — or would they just be lost?

We'll talk more about this in Chapter 2.

Review the flow of information and identify all potential points of failure in your workflow.

STEP 2: Mitigate the Risks: Have a Plan to Prevent Online Data Breaches

Paid tax and accounting practices that don’t have a plan in place are risking everything, and *they’re breaking the law*.

The Federal Trade Commission requires paid tax and accounting professionals to have a robust data security plan. This plan — called a *Written Information Security Plan (WISP)* — details how they will protect their data.

Create a Compliant Data Security Plan

The Gramm-Leach-Bliley Act (GLBA) requires U.S. financial institutions to protect client data. As the Federal Trade Commission (FTC) implemented GLBA, it also issued the Safeguards Rule — a list of requirements financial institutions must follow. Tax and accounting professionals, real estate appraisers, lenders, check-cashing businesses, universities, and mortgage brokers are considered financial institutions under GLBA. The FTC requires each financial institution to choose at least one employee to coordinate their information security program. Even if you’re not obligated to comply, following their recommendations can help you develop a data security plan for your practice.

Other requirements include identifying risks to clients' data and evaluating the effectiveness of current safeguarding measures. You also need to create, implement, monitor, and routinely test the safeguarding program, as well as confirm that vendors and service providers maintain appropriate safeguards too. Lastly, you should update your plan as regulations, risks, or your business operations change.

To help tax and accounting professionals accomplish these tasks, the IRS joined forces with 42 state tax agencies and various members of the tax community (firms, payroll processors, financial institutions, and more) to create the *Security Summit*.

Include All the Required Details

When writing your WISP, consider your company's size, complexity, and scope. A large firm will have a longer, more robust plan than a smaller accounting firm — so there isn't a one-size-fits-all approach. However, there are three key areas each WISP should include:

1. Employee management and training
2. Information systems and technology
3. Detecting and managing system failures

The Summit's *template recommends* each practice have an Employee/Contractor Acknowledgment of Understanding document. This document helps keep track of training and is beneficial if you need to prove compliance and/or show accountability for your practice.

WISP Outline

Each WISP should follow this outline.

1. Define objectives, purpose, and scope
2. Designate who is responsible for creating, coordinating, and implementing your program, as well as list your authorized staff, their responsibilities, and what data they can access
3. Assess current risks and detail the types of information your firm handles, if you have any areas of potential data loss, and how you monitor and test these risks
4. List the hardware you use for work and where each piece is located
5. Detail your Employee Code of Conduct and your document safety policies, including those for:
    - Data collection, retention, and disclosure
    - User access on-site and remotely
    - Network protection, Wi-Fi access, and connected devices
    - Electronic data exchange
    - Reportable incidents
6. Include a signed implementation clause that states when you executed the WISP

3 Core Parts of a Compliant WISP

Let's take a deeper dive into the main sections.

Assess current risks and detail the types of information your firm handles, if you have any areas of potential data loss, and how you monitor and test these risks.

- Identify vulnerabilities and risks, such as unauthorized access, loss of information, and disclosure of information
- List the information your business handles
- Define potential data loss scenarios (i.e., computer is stolen or hacked, hard copy paper files are destroyed in a fire, etc.)
- Outline how you monitor, test, and respond to risks/threats

List the hardware you use for work and where each piece is located (on the cloud, in your primary office, at a staff member's home, etc.)

- Describe the hardware your practice uses to handle taxpayer data (i.e., desktop computer, cell phones, routers, printers, etc.)
- Explain what you use each item to accomplish
- List the location of each item and who accesses/uses them

Detail your Employee Code of Conduct and your document safety policies.

- Define the policies and procedures you use to secure data
- Consider both physical, hard copy data and electronic data
- Describe data collection and retention policies
- Describe data disclosure policies and network protection procedures
- Describe user and remote access
- Describe process for adding new devices or software to your network
- Include both an incident response plan and a breach notification plan
- Define the Employee Code of Conduct and policies like training and background checks and screening

Write a federally compliant WISP that protects your data.

▶ Download the Checklist

Don’t Forget About Recovery

When something goes wrong, will you or your team know what to do? Much like having a fire drill or evacuation route, there should be simple instructions and protocol that each person on your team knows about and has easy access to so that matters can be handled, protected, contained, and reported quickly and properly.

A strong incident response plan has these three components:

- Incident response team with clear assignments, objectives, and responsibilities
- Framework that outlines action items and procedures
- Information about external resources and how/when to contact them for response assistance

You also need to consider insurance beyond Professional Liability. Insurance is a necessary safety net in business. As accountants and bookkeepers, it is a best practice to carry professional liability/ errors and omissions insurance. But you should also seriously consider a cybersecurity policy as well. It can either be a separate policy or one added to your liability coverage.

STEP 3: Follow the Plan: Make Sure All Staff Know Your Data Security Processes

Your staff are your biggest risk when it comes to data breaches. They're also your first line of defense. You're only as strong as your weakest link.

As we saw before, 95% of breaches are caused by human error. It's critical that everyone who works at your practice — full time and seasonal employees — understand cybersecurity risks and their responsibilities in protecting data.

As technology continues to change, hackers will continue to look for new and more sophisticated ways to access sensitive information. Our best defense is continued education and implementation of best practice. We want to do whatever we can to protect our clients and ourselves against attack, as well as take steps to prepare for the worst and survive a breach if it happens.

"Tax professionals generally relax a little after filing season and many take a well-deserved vacation but don't let your IT defenses down," *said IRS Commissioner Chuck Rettig*. "Spear phishing remains one of the biggest threats to the tax industry and other client-based enterprises."

Train Your Staff to Stay Alert

Here are some things you can do to keep your data safe.

Use strong, unique passwords with at least 12 characters. The strongest passwords have letters, symbols, and numbers. It's also important not to use the same password across multiple devices or accounts. You can use a password manager to help you remember unique passwords or you can use "passphrases." These short sentences or phrases can mean something special to you, like iLove_Snick3rs!

Keep all hardware and software updated. If you fail to update your devices, browsers, software, etc., you're putting yourself more at risk for malware and ransomware infections. Consider upgrading your modems, routers, hardware firewalls, and computer CPUs at least every 3-5 years. Make sure your team configures devices to automatically update.

Recognize suspicious links. The most common way hackers get your information is when you click on something malicious. These links can be embedded in emails, social media posts, private messages, texts, pop-ups, and more.

Recognize and report phishing attempts. These emails, social media posts, and direct messages look like they're coming from a trusted source and may ask for things like credit card numbers or bank account passwords. Some have links or attachments to download. If something looks odd — misspellings or weird punctuation — or is even slightly suspicious, employees should promptly report it, delete it, and block the sender. Here are some signs a link may be a phishing attempt:

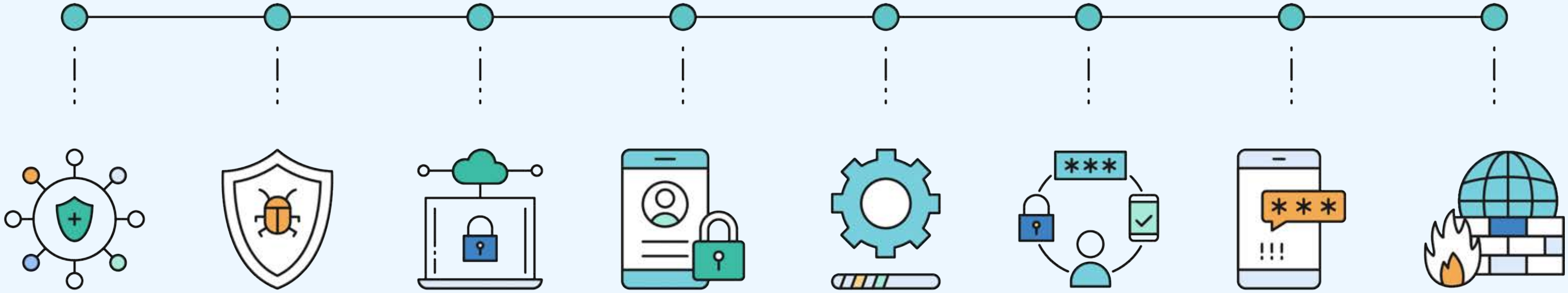
- The message is threatening or urgent
- There is weird spacing, bad grammar, and misspellings
- The email address has misspellings or doesn't match the display name
- It requests personal information or for you to complete a strange business request
- The offer is too good to be true

Be aware of social engineering. This is a very common type of attack that tricks the victim into completing a request or providing personal information. The attacker pretends to be someone they're not, like your manager, team member, or even a friend or family member. They may contact you online (email, social media, etc.) or through phone calls.

Be wary of public Wi-Fi. While it's great to empower your staff to work remotely, using public Wi-Fi can lead to serious consequences, like man-in-the-middle cyberattacks. If you must use public Wi-Fi, limit what you do online and don't log into your critical software or accounts. Using a personal hotspot or a virtual private network (VPN) would be a more secure option for working remotely in public areas like your library, café, or coffee shop.

A Strong Cybersecurity Approach

Make sure your practice is prepared with these critical security components.



NETWORK SECURITY

ANTIVIRUS

VPN

PRIVACY

SOFTWARE UPDATE

TWO-FACTOR AUTHENTICATION

PASSWORD STRENGTH

FIREWALL

7 Warning Signs That You Were Hacked

You could be hacked and not even know it. According to the IRS, here are some common signs that you're a victim of an attack.

1. The IRS rejects your client's e-filed return because they've already received another return with their Social Security Number.
2. You receive e-file acknowledgments for tax returns you have yet to file or you receive more acknowledgments than returns you've filed.
3. Clients contact you about or respond to emails or other requests that you didn't send .
4. Your computer starts acting slow, unresponsive, or strange, including software taking longer to load, the cursor moving without you touching the mouse, and/or it locks you out of your computer or network.
5. Your clients tell you the IRS sent them authentication letters or a refund even though you haven't filed their tax return yet.
6. Your clients received a tax transcript that they didn't request or a message that someone created an online IRS account for them.
7. Your clients receive a message that someone has accessed their online account or that the IRS disabled their online account.

STEP 4: Secure How You Handle Data: A Document Management System Can Make All the Difference

Accounting practices will continue to face stronger security and compliance scrutiny by clients and regulators in the future. A document management system (DMS) that's built with security and compliance in mind will offer the following measures.

DOCUMENT STORAGE
Capture, organize, and securely store documents or files with ease of accessibility

ENCRYPTED FILES
Trust that all your most sensitive files are safe and secure thanks to 256-bit encryption technology

24/7 ACCESS
Access documents and files anytime, anywhere with cloud-based technology

INDUSTRY COMPLIANT
Stay compliant with industry regulations such as FINRA

Increase Your Data Security

Your DMS should:

1. **Encrypt data during transit and while at rest.** When sensitive data is at rest or being exchanged over the internet, it’s crucial that your data is encrypted every step of the way so no one can hijack your information and use it for malicious purposes. By using advanced encryption methods such as SSL and AES-256, a cloud DMS could *provide stronger protection for your data*.

2. **Provide controlled access to information.** How your information is stored and who has access to your information is critical to your overall security and compliance framework. With a security and compliance-first cloud-based DMS, you can easily set granular access permissions to folders and documents, and allow access to files via only authenticated logins. These added security and compliance steps help enhance your data and document security measures, which could increase your level of compliance to regulations.

3. **Have secure data backup.** Your documents and metadata are always stored using highly redundant replicated storage. Multiple copies of metadata and documents are stored in multiple geographical locations and backed up regularly to ensure data availability.

4. **Track all activity.** An activity log is an automatically generated, time-stamped trail of all activities that happened in your document management system. It tracks all events from all users such as document creation, download, and deletion and generates an audit trail of what’s happening in your account. No person, including the engineers of the platform can make any changes to this trail, making it the authoritative record for auditing purposes. This feature is a requirement from several industry-specific compliance regulations. Depending on your industry, it could very well be the single most important determining factor during your cloud DMS vendor selection process.

Staying on top of your cybersecurity doesn’t have to take an arm and a leg. With the right DMS, you can rest assured that your most valuable information is safeguarded by the strongest security measures.

▶ Choose the Right DMS

4 Ways a DMS Can Empower Your Practice and Your Clients

A powerful DMS can help you secure, optimize, and streamline your digital workflows.

1 **Save time and money by streamlining workflows.**

Standardize and digitize how you collect, manage, and share documents with software that's built for your unique security, compliance, and workflow needs. Your DMS should empower you to work smarter with unlimited storage and guest users, so it scales as your business grows. The security measures and access controls must also protect your data with the highest standards.

2 **Future-proof your practice by going paperless.**

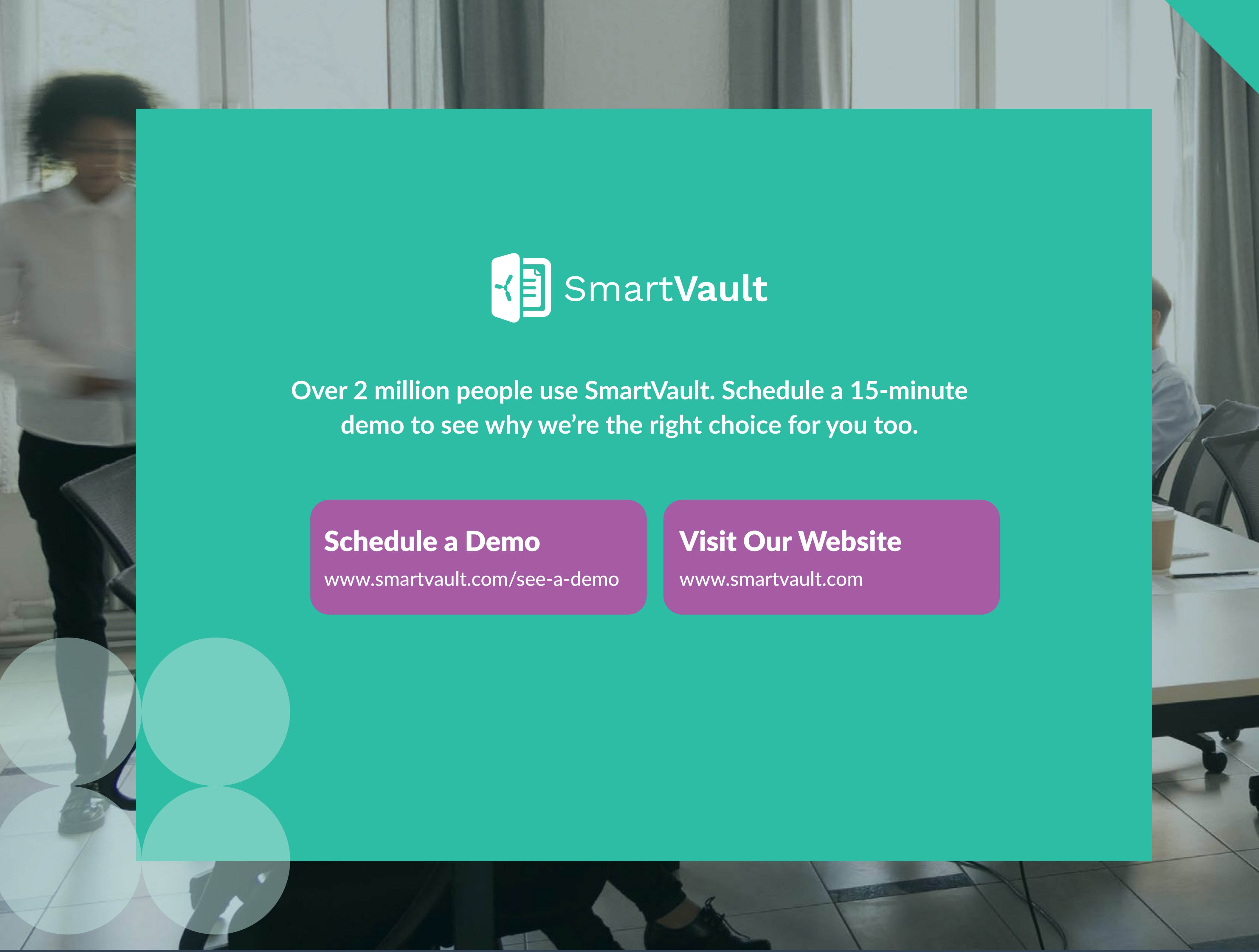
Your DMS should let you and your clients upload, access, delete, and share files from any web-enabled device. With a click of a mouse, you can send clients — whether it's one, twenty, or a thousand — an email requesting exactly what you need and receive a notification when they complete that request. The most powerful DMS include an autofiler, meaning you don't have to worry about chasing emails or manually saving documents to the right place. The DMS would take care of that for you.

3 **Increase customer satisfaction and collaboration.**

A custom-branded, online portal gives your clients a secure, easy, and professional way to collaborate with you from wherever they're located. It's easy to invite clients to the portal, and they can access the portal directly from your website. Customizable folder templates automatically put the right folders in each client portal, making onboarding a breeze.

4 **Reduce manual tasks with powerful integrations.**

Your DMS should integrate with the leading accounting and tax applications you already use and trust like Lacerte, ProSeries, QuickBooks, and more.



SmartVault

Over 2 million people use SmartVault. Schedule a 15-minute demo to see why we're the right choice for you too.

Schedule a Demo

www.smartvault.com/see-a-demo

Visit Our Website

www.smartvault.com