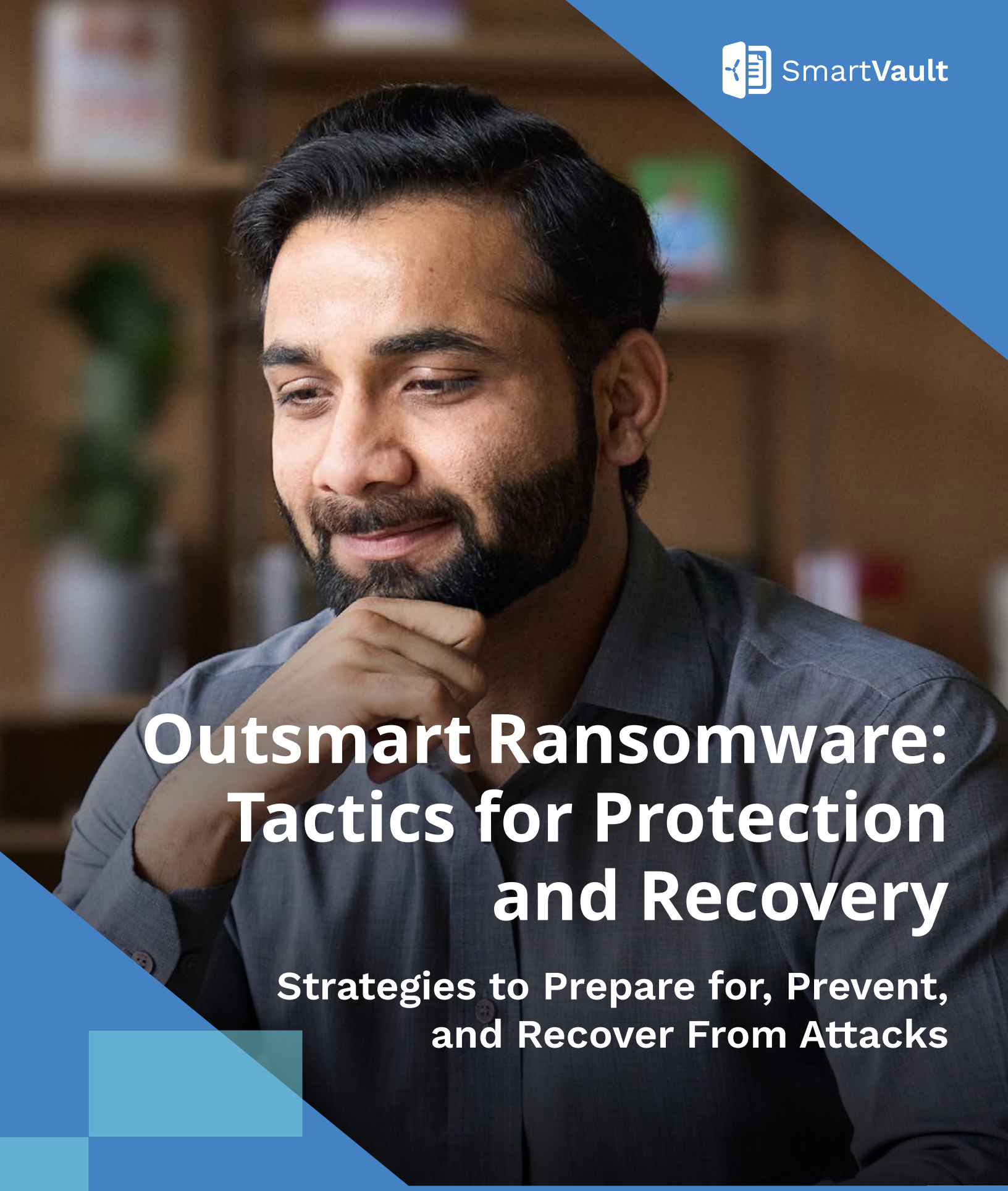
SmartVault



Outsmart Ransomware: Tactics for Protection and Recovery

Strategies to Prepare for, Prevent, and Recover From Attacks

Whitepaper

Table of Contents

Foreword

Criminals know your practice's database is a goldmine.

From Social Security numbers to birthdates and addresses, your files have exactly what criminals need to steal identities, file fraudulent tax returns, and more. Many cybercriminals also sell the data on the black market for other threat actors to use as they wish.

So, how do they get your data? One of the most common methods is Ransomware, which experts warn is getting more aggressive and damaging.

"Ransomware deployments today are...designed to inflict maximum pain on the victim organization," Jake Williams, an information security expert and Senior SANS Instructor, warned in a 2022 SANS Institute report. "They typically have a single goal: getting the victim to pay by any means necessary."

This whitepaper will help you understand why ransomware is a significant threat and what experts recommend businesses do to prepare for, prevent, and recover from attacks.

Prepare:
Education is Your Best Defense

Ransomware is malicious software that encrypts your data and blocks you from accessing it. The attackers then threaten to publicly release the data or prevent your access to it unless you pay a ransom.

At the 2022 Tax Forum, the IRS made it clear that losing data is just one consequence of an attack: “Victims…may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for compromised employees and customers.”

You also must consider compliance requirements, penalties, fines, and the fact that your business (and source of livelihood) may never recover. Your reputation will severely decline, as clients will see you as a risk and quickly move their business elsewhere. These are just a few reasons why experts strongly encourage firms to be proactive about security rather than wait for disaster to strike.

The Growing Threat

Four companies fall victim to ransomware attacks every minute, . In 2022, there were over 236 million ransomware attacks across the globe, with 47% of those happening in the United States and nearly 6% in the UK.

Ransomware most commonly spreads through:

- Phishing emails with infected attachments or links
- Compromised websites that download malware onto devices
- Exploiting vulnerabilities in networks or software to gain access
- Brute force attacks on weak passwords

Once inside your system, the ransomware encrypts files and often spreads rapidly across your network. The victim(s) typically see a ransom note on their screens that details what will happen to their data if they don’t pay the ransom fee.

Attack Impacts

Lost data, productivity, & revenue

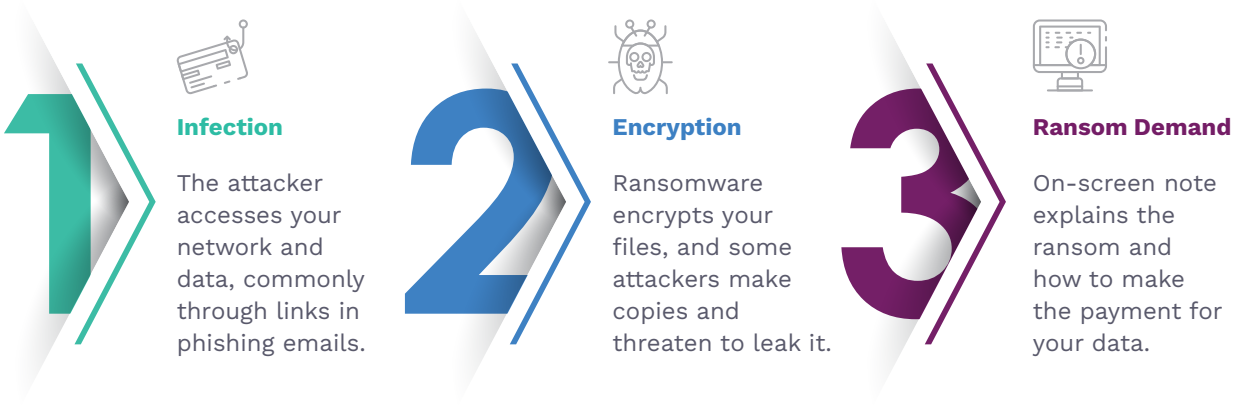
Damaged relationships & reputation

Penalties, fines, & costly recovery efforts

Significant stress & anxiety

Three Core Stages of Ransomware Attacks

While each type of ransomware has unique characteristics, most follow these three stages:



To Pay or Not to Pay

Whether or not to pay the ransom is a difficult choice. The FBI advises against payment to avoid incentivizing cybercriminals, and it's important to note that you could pay and still not get your data back.

But there's a lot more to it.

Williams warns that nonpayment could escalate the situation: "Some ransomware operators have...[contacted] business partners and even customers of the victim organization, trying to gain additional advocates for paying the ransom." Imagine how your clients would react if a criminal told them they plan to sell their personal information to other criminals – you'd surely get a lot of phone calls and emails from clients insisting that you pay the ransom fee.

The IRS also warned at the 2022 Tax Forum that many criminals create data leak websites to "publicly shame their victims and publish the files they stole." Known as double extortion ransomware, it is one of the most feared cyberattacks. The attacker first demands a ransom to decrypt the data so you can regain access. If you refuse to pay, they'll threaten to destroy the data, publish it online, or sell it to another criminal – unless you pay, of course. This gives attackers additional leverage.

"The decision to pay a ransom or not has to be a business decision," former cybercrime law officer and SmartVault Chief Information Security Officer Luke Kiely recommended on a Tax Rep Network podcast. Many business owners, especially those without data backups, may see no alternative when their business is on the line.

Remember, these are criminals. Before you consider paying, ensure that your data is actually encrypted and that a criminal isn't simply tricking you. Also, note that your computer will still be infected after payment; possibly worse, the criminal could just take your money and run.

Prevent:
Don't Become a Victim

> "The only thing worse than a data breach is multiple data breaches. Take steps so it doesn't happen again."
>
> Federal Trade Commission, *Data Breach Response: A Guide for Business*

The right processes can drastically decrease a ransomware attack's likelihood, cost, and impact on your business.

Create a Cybersecurity Plan

The first step is creating a cybersecurity plan for your business. This isn't just something nice to have – various regulations require it. The Federal Trade Commission (FTC) requires paid tax and accounting professionals to have a robust data security plan called a Written Information Security Plan (WISP). Firms must also comply with portions of the Gramm-Leach-Bliley (GLB) Act, which requires you to outline how you will protect your clients' personal information. Firms that fail to comply may lose their business licenses and damage their reputations. Your plan is the roadmap for protecting against threats.

Here are some things you should consider in your plan:

- Identify critical assets, data, and systems
- Perform risk assessments to find vulnerabilities
- Implement controls like firewalls, authentication, encryption
- Develop and implement security policies for access, BYOD, passwords, etc.
- Create incident response and disaster recovery plans
- Ensure employees are trained
- Continue to test your processes and stay updated on new regulations and threats

Your Complete Cybersecurity Checklist

While cybersecurity can be complex, and there isn't a one-size-fits-all approach, it doesn't have to be overwhelming. This checklist will help you build a robust cybersecurity program that protects your firm and clients' data from hackers.

Download the Checklist

Be Aware of Phishing

Ransomware is most commonly spread through phishing emails or text messages. These contain malicious links or attachments and lure victims into disclosing their personal information, like their passwords via fake login pages.

Criminals accomplish this by making the victim believe the message and request are trustworthy. These attempts appear to come from known, trusted sources, like your partner, client, bank, loan provider, credit card company, or even places like big-box stores.

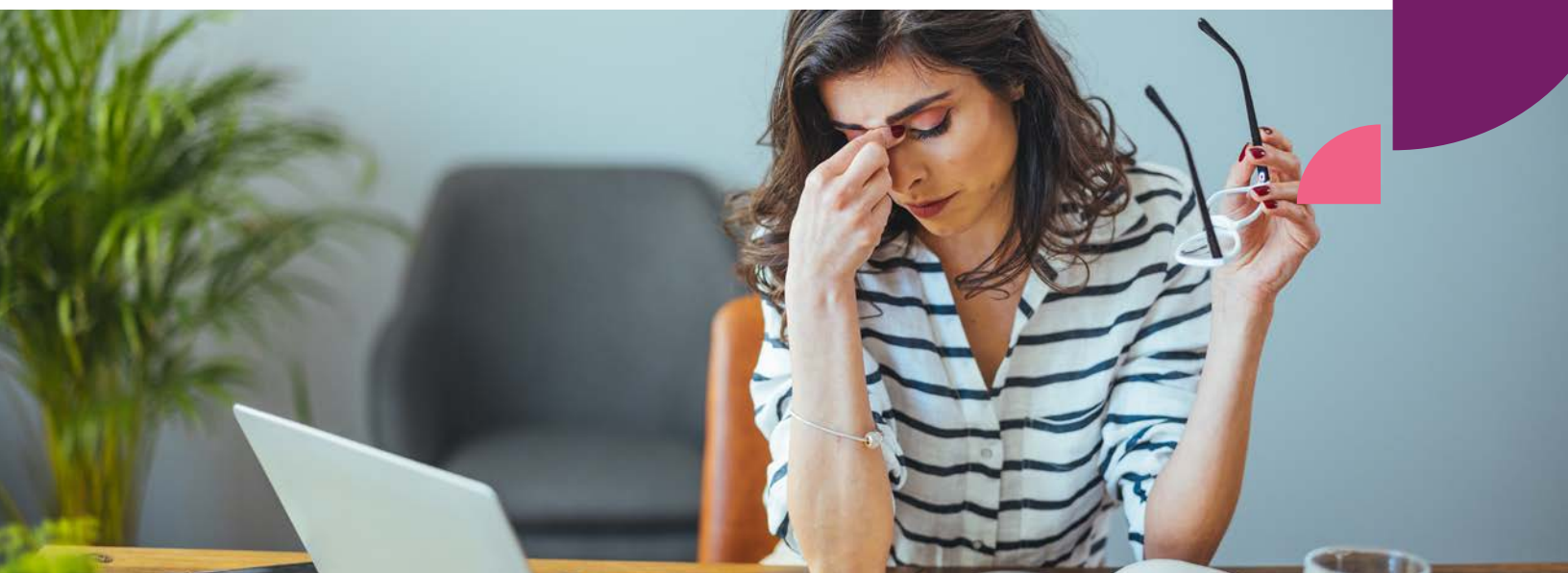
> According to the IRS, an estimated 91% of all data breaches and attacks begin with a phishing email.

Recognize Phishing

How can you tell if something is a phishing attempt? Phishing emails often have odd reply addresses, strangely worded content, and a sense of urgency – hackers frequently try to push people into responding hastily in order to get what they want. Ask yourself, 'Am I likely to get an email from a CEO asking to make a change to a bank account at 5:00 pm on a Friday?' Kiely suggests.

If something looks odd or is even slightly suspicious, you and your team should promptly report it, delete it, and block the sender. Here are signs a link may be a phishing attempt:

- The message is threatening or urgent
- There is weird spacing, bad grammar, or 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



Prevent Phishing

Here are some best practices to prevent falling for a phishing attack:

- Watch for red flags above
- Hover over links before clicking
- Don't open attachments from unknown senders
- Never enter credentials on websites reached from links
- Use secure connections and updated antivirus software
- Report suspicious emails to IT/security teams
- Train employees how to recognize, report, and avoid phishing attempts

Ensure Staff Understand Risks and Procedures

Patrick Schreiner, a business cybersecurity risk advisor at one of America's Big Three Index Fund Managers, says untrained staff are a big source of mistakes, because as we just learned, cyberattacks frequently start when someone clicks a malicious link in an email or downloads an attachment. Luke Kiely recommends managers remind their team members to examine things like emails carefully.

Best Practices for Employee Training

Your cybersecurity plan should include employee training processes, such as these:

- Require staff (full-time, contractors, and temp workers) to read the program and complete training during onboarding and at least twice each year
- Regularly remind employees of your policy and their legal obligation to protect customer data
- Ensure all employees pass a background check and submit references
- Develop and implement non-disclosure agreements and privacy guidelines
- Ensure terminated or separated employees do not continue having access to your network and data

Regularly Backup Your Data

Having reliable backups makes ransomware recovery possible without paying the ransom. Yet, many businesses still operate with one computer that contains all their client data. This could lead to a significant problem, as Luke warns: “If you can no longer access your data, you can no longer deliver service. The business stops, and you start losing money.”

Data Backup Best Practices

The best way to backup your data is to store it all in the cloud. Cloud providers store your data on multiple remote servers, which they maintain and back up regularly. It happens automatically, so you don’t even have to think about it.

Cloud vendors also have greater resources and invest heavily in ensuring their customers’ data stays safe. You’ll benefit from advanced security measures like bank-level encryption, granular access controls, and multi-factor authentication (MFA). These measures help prevent criminals from gaining access to your files in the first place.

Leverage Document Management Systems

A robust document management system (DMS) will give you peace of mind that all valuable information is protected and will be readily accessible if you fall victim to a ransomware attack. Here are some things you should look for in a DMS:

- Automated cloud backups for availability if your local systems are damaged, lost, etc.
- Version control and activity tracking to preserve history and access previous versions
- Encryption at rest and transit and robust access controls to restrict who can view, edit, and delete documents
- Mobile access so you can access and collaborate on documents from anywhere
- Indexing and search to find the documents you need quickly
- An integrated client portal for clients to collaborate with you online
- Integrations with the tax prep, accounting, and admin programs your firm already uses

Follow Security Best Practices

Cyberattacks are becoming more sophisticated, but basic protection remains the same. Here are some additional practices to consider:

Strong, Unique Passwords

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. Set passwords to expire regularly and ensure your vendors have appropriate password requirements and policies.

Set Access Permissions

Your DMS should offer advanced user permissions that let you granularly separate access to data and folders and actions each person can take (read-only, edit, delete, etc.). You must set granular permissions for internal staff, including temporary or seasonal workers, and for external collaborators like your clients. This helps reduce risk of unauthorized access and malicious attacks.

Leverage Antivirus and Anti-Malware Software

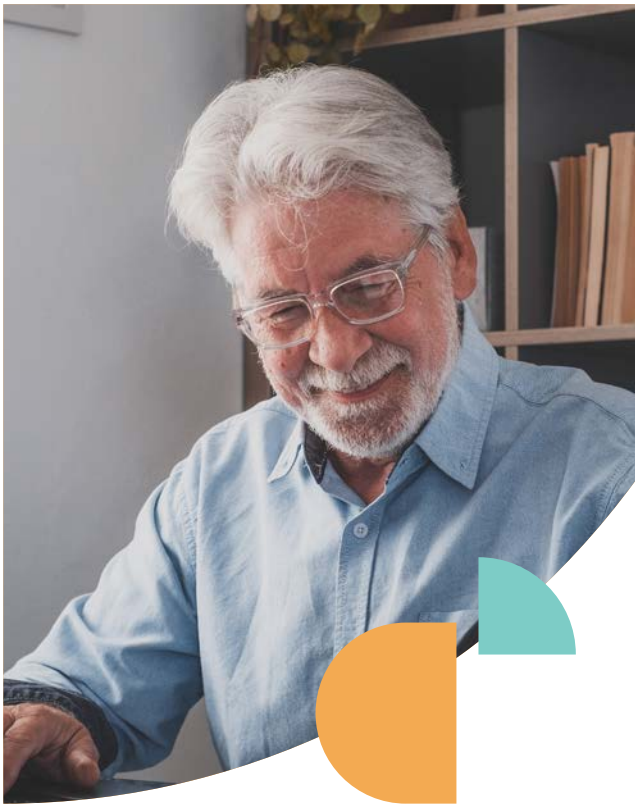
Having up-to-date antivirus and anti-malware software is critical for protecting devices and systems from malicious threats. Antivirus software helps detect, block, and remove viruses before they can infect a system. Anti-malware programs identify and neutralize other forms of malicious software. Running comprehensive antivirus and anti-malware scans regularly allows you to proactively catch and mitigate threats before they have a chance to do harm.

Software Updates

Too many people increase their vulnerability by ignoring or postponing software updates on their devices. Even though updates can be time-consuming and frustrating, they're necessary because viruses and malware change and adapt constantly. Upgrade your modems, routers, hardware firewalls, and computer CPUs at least every 3-5 years. Make sure your team configures devices to automatically update.

Be Wary of Public Wi-Fi

While empowering your staff to work remotely is great, using public Wi-Fi can lead to serious consequences. 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) is the most secure way to work in public areas like your library, café, or coffee shop.



Plan For Today and Tomorrow

It's not enough to plan for risks you're aware of right now: Technology changes quickly, and if you don't stay current, cyberthieves will remain one step ahead of you. When you partner with the right vendor, they can take on that responsibility for you. Since it's their products you're using to keep your data safe and since their reputations are incumbent on their solutions being as secure as possible, they'll be up to date on the latest risks and can help you maximize their solution to ensure you're not vulnerable.

Recover:
Quickly Get Back on Your Feet

Let's say the worst-case scenario has come true: You find yourself staring at a ransom demand on your computer screen. Now what? The answer depends greatly on your business and the attack details.

This chapter summarizes guidance from the IRS and the Federal Trade Commission (FTC). Every state also has legislation that dictates how to respond to and notify others of data breaches. Check your state and federal laws for specific requirements.

Secure Your Operations

In their data breach response guide, the FTC says, "The only thing worse than a data breach is multiple data breaches," which is why number one on their list is to secure your systems and fix vulnerabilities. To prevent the malware from spreading to other systems, you should disconnect infected computers from all networks. But, don't turn the computer off – doing so may result in the computer losing some of its memory, which will make it harder to recover.

Contact Authorities

You must immediately report data losses, thefts, or ransomware attacks to the IRS. They can help you take appropriate precautions. They'll also help protect your clients by preventing fraudulent returns from being filed in their names. Here are some of the IRS recommendations:

- Report data breaches to your local stakeholder liaison at the IRS
- Contact the FBI and Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS)
- File a police report with your local police office
- Contact the Attorney General's office for every state in which you prepare returns
- Reach out to security experts and your insurance company

Alert Others

The FTC advises businesses to have a “comprehensive plan that reaches all affected audiences — employees, customers, investors, business partners, and other stakeholders.” State laws mandate what you can and cannot provide in your communication; many allow you to include:

- How the breach happened and what information the attackers received
- What actions you’ve taken to help recover and/or remediate the situation
- What actions you plan to take to protect the victims, such as offering credit monitoring services

Access Your Data Backup

“Backups are ultimately the only thing that can save an organization’s data after a ransomware attack,” the IRS said at the 2022 TaxForum. If you’re working with a vendor for data backups, contact them to get started on recovery.

Keep Your Data and Business Safe

While ransomware is scary, being proactive and having the right tools in place make a big difference. SmartVault provides accounting professionals with a cloud-based document management system and client portal that prioritizes security and compliance.

SmartVault automatically backs up your data, making recovery easy. Built with bank-level security, SmartVault also encrypts data both in transit and at rest and has robust user access controls that allows you to restrict and track data access. Two-factor authentication provides an added layer of protection.

smartvault.com