

Safeguarding Client Data: 10 Critical Security Risks for Accounting Firms



Safeguarding Client Data: 10 Critical Security Risks for Accounting Firms

Accounting firms are prime targets for cybercriminals because they handle highly sensitive client data, financial records, tax filings, and payroll. Even a minor breach can be a jackpot for hackers and a disaster for your firm. On average, a data breach costs **\$4,800,000**—plus major losses in trust and reputation.

You may think that your firm is too small or insignificant to gain the attention of cybercriminals, but **over 40% of small businesses experienced an attack last year**. It's not a matter of if your firm will be targeted—it's a matter of when.

The best defense is preparation. Here are ten of the biggest data security risks for accounting firms and how you can start protecting your firm today.

1. Phishing

The Threat

Phishing attacks impersonate trusted contacts like firm executives or payroll departments to trick employees into sharing login credentials. They may also duplicate fraudulent login pages and emails from recognized programs and applications you use every day. They'll send an email saying you need to log back into your system and lead you to the fake landing page where your login information is stolen.

If an employee falls for the scam, attackers may gain access to a single system—or worse, use duplicated passwords to infiltrate more of your firm's sensitive data.

How to Protect Your Firm

Phishing scams are only successful when a member of your team isn't able to identify a threat. Training and educating your team about what to look for is the best defense. Some key identifications include:

- **Inaccurate email addresses.** Verify any unexpected emails from unfamiliar domains before clicking links or sharing information.
- **External links.** Be cautious of emails asking you to re-enter login details, especially if they contain an unexpected link to an external site.

2. Lack of Encryption

The Threat

Sending unencrypted emails is like mailing a letter without an envelope. Anyone can read it along the way.

Encryption helps protect your data in case it is intercepted or stolen. If a thief intercepts an encrypted email, rather than seeing the message, they will see indecipherable code.

How to Protect Your Firm

If your firm does not have an encryption solution, you must adopt one immediately. Without encryption, your firm and clients are vulnerable to data breaches and further cyberattacks.

Start by ensuring your firm uses encrypted email for all sensitive client communications. Ideally, encryption should cover all internal and external communications, as well as all stored files and documents.

3. Ransomware

The Threat

Just like a hostage situation, ransomware holds your firm's data for ransom. It is designed to shut down your firm, blocking you from accessing client data or essential applications until the ransom is paid.

How to Protect Your Firm

If you are targeted by ransomware, do not pay the ransom. Cybercriminals do not guarantee that they will give you control over your files, and your system will still be infected, putting you at risk for additional attacks.

Ransomware can't install itself; a user has to download it. To keep your firm protected, train employees to avoid suspicious files and links. Being cautious about downloaded files minimizes ransomware risks.

Regular, secure backups ensure you can quickly recover data without paying a ransom. Always check backups for infection before restoring to ensure you are reverting to a point free of ransomware.

4. Insecure Remote Workspaces

The Threat

Remote work is only possible when your employees can access your firm's database and client information remotely. Since **over a third of finance professionals work remotely**, firms must address the security risks associated with remote access.

Remote access creates a digital back door to your firm. It must be secured, or cybercriminals will exploit it.



How to Protect Your Firm

You can implement a few basic security solutions to ensure your firm is safe while enabling remote work.

The first line of protection is to ensure that remote workers use secure wi-fi connections. This creates a barrier to protecting data and helps stop cybercriminals from freely accessing your information.

Additionally, you can enable secure device practices, like mandating that a computer automatically locks after five minutes of being idle. If an employee steps away or is not actively using their computer, the system locks down, making it more difficult for cybercriminals to access sensitive information.

5. Data Breaches

The Threat

A data breach occurs when confidential information is stolen, exposed, or shared without your authorization. This can include internal information like login names and passwords or confidential client data like names, banking information, and other sensitive information, leading to fraud and legal risks.

How to Protect Your Firm

The best way to protect your firm from a data breach is to follow standard data security best practices.

- Require strong passwords for all users.
- Use multi-factor authentication.
- Use multiple levels of access to ensure sensitive information is only accessible by a limited number of users.
- Update passwords every three months.

6. Distributed Denial of Service (DDoS) Attacks

The Threat

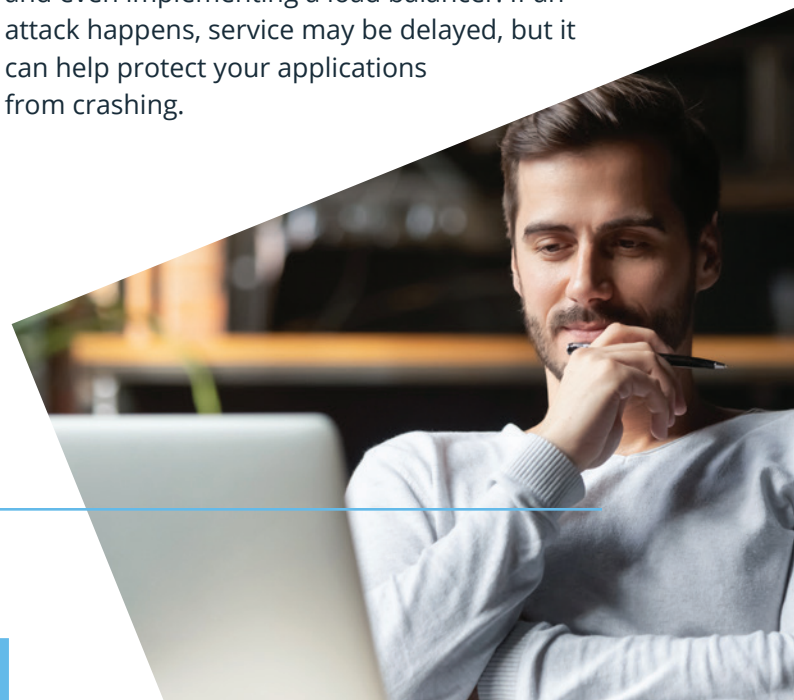
A DDoS attack is like flooding a restaurant with fake customers, preventing real ones from being served.

A distributed denial of service (DDoS) attack is when a cybercriminal or group of cybercriminals floods a website with web traffic and requests. This exhausts the application's resources, making it difficult or impossible for users to access the data and resources they need.

A small DDoS attack can slow your servers, making it difficult to complete basic tasks, but a large, targeted attack can shut down your applications and website and block you from using any of your digital resources.

How to Protect Your Firm

Implementing back-end security solutions is the best way to prevent DDoS attacks. These solutions reduce the locations where cybercriminals can send DDoS attacks, making it harder for an attack to succeed. Consider limiting the attack surface exposure by restricting traffic to specific locations, blocking communication from outdated or unused ports, and even implementing a load balancer. If an attack happens, service may be delayed, but it can help protect your applications from crashing.



7. Malware

The Threat

Malware, or malicious software, is designed to damage or disrupt your system. It's a broad term that includes viruses, worms, and Trojan horses.

Some malware aggressively attacks your system. It can delete files, block access, hijack your system, and even alter core computing functions. But not all malware is aggressive. Some malware acts as a spy in your system. It doesn't actively affect or modify the functionality of your system, but it does hunt down, track, and transmit sensitive or secure information such as your clients' personal data, login usernames and passwords, and your firm's banking and accounting information. This sub-genre of malware is referred to as spyware.

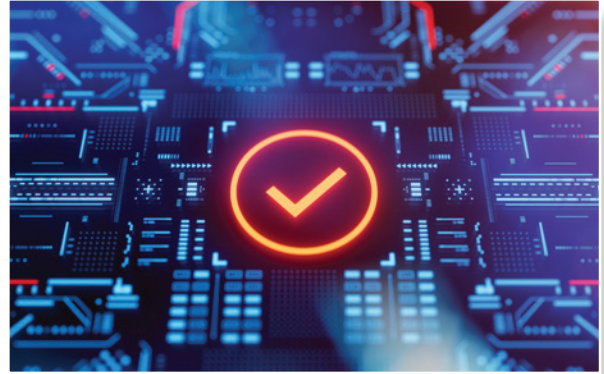
How to Protect Your Firm

While malware can be highly damaging to your firm, malware must be downloaded and installed onto your system before it can cause any damage. This one restriction is also the biggest strength of how you can protect your firm.

Simple software protections like firewalls and antimalware software play an important role in protecting your firm, but your team must also be informed and vigilant.

Software protection is adequate, but a bad user can ruin everything.

- Be cautious with email.
- Do not click on links or attachments from unknown or suspicious senders.
- Avoid pop-ups.
- Always avoid risky or questionable websites.



When your team takes the measures to avoid questionable digital activity, your protection and detection software can handle the rest.

8. Outdated Software

The Threat

Skipping software updates may seem harmless, but it leaves your system open to cybercriminals exploiting known vulnerabilities.

Good software companies want to help protect you from malicious attacks. When they discover a weakness in their program (either through internal research or a hacker exploiting a weakness), they will send out a patch to help strengthen and protect your system from falling victim to an attack. Avoiding updates means missing crucial security patches, leaving your system vulnerable.

How to Protect Your Firm

The only way to combat outdated software is to ensure that all of your software is up to date regularly and consistently.

If you receive a notification about an update, prioritize it. At the very least, set the update to run at the end of your workday so you can return to work with a fully updated system.

9. Cloud Data Security

The Threat

Cloud-based applications and storage decentralize your data and move data usage to the cloud, but they are not immune to security threats.

Cloud-based computing allows your data to be accessed remotely and through many different systems simultaneously. If a cybercriminal can take advantage of that system, they can access sensitive information at any time from any location.

How to Protect Your Firm

Your cloud security depends on the provider and configuration you choose. As an accounting firm, you are dealing with highly sensitive client data and information; your cloud-based systems should include the following:

- Encryption
- Authentication
- Data obscuring
- Data erasure

An additional step you can take to protect your data is to use a private cloud. This helps further isolate your data, making it more difficult for third parties to access it. Typically, private clouds also include a high level of security through firewalls and internal hosting.

10. Weak Passwords and Security Training

The Threat

It's common for users to be the weakest point in your data security. Even the best firewall can't protect against weak or reused passwords.

Data security can feel cumbersome or annoying because it can slow down authorized users' access to the data they need to do their work. However, those same processes stop unauthorized users from accessing your database, so it is worth the cost of having a longer password with a mix of lowercase, uppercase, numbers, and special characters because it helps protect your company.

Security training also covers how computers and applications should be used and managed. This includes training on how to identify a fraudulent email and on locking and securing computers when users walk away from them, even for a quick water break.

How to Protect Your Firm

The best way to improve data security is to fully embrace it and make the changes mandatory. There is a big difference between sending an email reminding people to update their passwords every three months and making it a system requirement that all users update their passwords or be locked out of their accounts.

One way to simplify data security training and password management is to partner with a software provider that includes security options. This removes the responsibility from you to manage password updates and reminders, and allows them to automatically happen within your firm's software.





Strengthen Your Security with IRIS

With over 40 years of industry experience, IRIS provides secure, professional software solutions for accounting firms. Our solutions complement your security needs, helping to protect confidential and sensitive information while streamlining data management, making it easier for you to do your job.

Our document management solution creates a secure, custom database for your firm. It uses AI and automation solutions to minimize

manual data entry, errors, and duplication. This saves time and ensures you can quickly find and access the documents you need, exactly when you need them.

Get started today and discover the difference IRIS can make.

[Contact now](#)

The IRIS logo consists of a stylized bar chart icon with three vertical bars of increasing height, followed by the word "IRIS" in a bold, sans-serif font.

IRIS Americas is part of IRIS Software Group. IRIS payroll solutions exist to take the pain out of processes and enable professionals working in CPA firms and payroll service bureaus businesses comply with regulations, improve efficiency and drive growth. IRIS Americas brands include IRIS Star Practice Management, IRIS Global Workforce, IRIS Innervision, IRIS Practice Engine, Doc.It, PSI Payroll, IRIS HCM, Apex, AccountantsWorld, Senta and Conarc.

IRIS partners with thousands of CPA firms, payroll service bureaus and small to midsize businesses across North America, including 52 of the top 100 US CPA firms. We offer innovative Payroll and HR solutions, making us the preferred partner in the region. Globally, IRIS serves over 100,000 customers, with 80% having tenure of five or more years.

