CYBERSECURITY MADE SIMPLE FOR SMALL BUSINESS OWNERS

A Beginner's Guide to Keeping Your Business Safe

By: NDAY Security, Inc,

Published: 2025

TABLE OF CONTENTS

Your Guide to Staying Safe in a Digital World

Running a small business isn't easy. Whether you're brewing coffee, fixing cars, managing a salon, or running a neighborhood flower shop, you've got a lot on your plate: customers to help, employees to support, bills to pay, and a dozen other things demanding your attention. The last thing you want to worry about is a faceless cybercriminal halfway around the world messing with your computers, stealing your data, or shutting your systems down.

In today's world, cybersecurity is no longer just a concern for big corporations with big tech budgets and IT departments. Small businesses are one of the top targets for cyber-attacks. Why? Criminals know that most small business owners don't have the time, resources, or technical know-how to spot an attack or stop one before it causes serious damage.

But here's the good news: you don't need to be a technology expert to protect your business, your employees, and your customers. That's exactly what this little ebook is here for.

Think of it like sitting down with a trusted friend who happens to know a bit about cybersecurity, someone who can walk you through the basics in plain English, without all the jargon or scare tactics. We'll start with what's really happening out there on the internet, why it matters to you, and how these threats can sneak into your business without warning.

Then, we'll cover some simple, practical steps you can take, right now, to lock your digital doors, watch for warning signs, and put up some solid defenses. These are small things that can make a *huge* difference.

We'll also walk through what to do if the worst happens: if your systems are compromised or your data is stolen and how to recover quickly without losing your mind, your business, or your customer's trust. Finally, we'll share helpful resources you can turn to for support, guidance, and even free tools to stay protected in the future.

This guide was made for you the everyday business owner who's doing his/her/their best and just wants to stay safe in a world that's more connected (and riskier) than ever before.

Let's take it one simple, powerful step at a time.

Cybercrime and Your Business: What You Need to Know

Cybercriminals aren't just going after big corporations anymore. In fact, small businesses are now one of their favorite targets. Why? Because many small business owners assume they're too small to be noticed. They think, *"Why would anyone bother with my shop?"* But the truth is, cybercriminals are counting on your lack of preparedness.

They use a range of sneaky, increasingly sophisticated tactics to break into systems, steal data, or lock you out of your own files until you pay a ransom. These aren't just geeky hackers in dark basements anymore, this is big business. Organized. Fast. Ruthless. Profitable.

Here are a few of the most common ways small businesses get attacked:

Phishing Emails

You or your staff might get an email that looks legitimate; maybe it pretends to be from a bank, a delivery company, or even a coworker. It might ask you to click a link or open an attachment. Just one click, and malware can slip into your system, opening the door for a full-on attack.

Ransomware

Ransomware is like digital extortion. Criminals lock your files, including customer info, payment records, schedules, etc. and demand money (bitcoin) to give it back. These attacks can bring businesses to a screeching halt. And, if you pay the ransom, there's no guarantee you'll get your data back. Do you trust getting your data back from criminals?

Weak Passwords

Believe it or not, some of the most common passwords used are still things like "123456" or "password." Cybercriminals run software that can guess weak passwords in seconds. And if you use the same password in multiple places, it's like handing them a master key.

Unsecured Wi-Fi Networks

If your business's Wi-Fi isn't properly secured, someone parked outside could be snooping on your network, stealing data, or slipping malware into your system without ever setting foot inside.

Outdated Software

Old software, whether it's your website platform, payment system, or antivirus, often has security holes. Cybercriminals know how to find and exploit these weaknesses. If you're not updating software regularly, you're leaving the door wide open.

Why It Matters

You don't have to be a big company to suffer big consequences. A single cyberattack can cost thousands of dollars in lost revenue, repairs, and recovery time. It can scare away customers, damage your reputation, and take a huge emotional toll.

Worse yet, small businesses often don't survive a serious attack. Some are forced to shut down entirely.

But here's the good news: **most cyberattacks can be prevented with just a few basic precautions**, things that don't require a full-time IT team or expensive technology.

That's what this guide is all about: showing you how to recognize the risks, take simple protective steps, and respond quickly and smartly if something goes wrong.

Practical Tips

- Learn the Basics: Watch beginner-friendly videos or read articles about scams like phishing and ransomware.
- Recognize You're a Target: Assume your business could be next, and act accordingly.
- Stay Informed: Set aside time monthly to check news or alerts on cybersecurity trends.
- Ask a tech-savvy friend or team member to explain key threats.
- Be cautious with suspicious emails and links.

Common Questions Answered

Q: What are AI-driven threats?
A: *Attacks using smart automation to mimic legitimate users.*

Q: Do I need to hire someone, or can I manage this myself?
A: You can manage the basics yourself — and that's a great place to start, especially if you're on a tight budget. Once your business starts growing, or if you're dealing with sensitive customer data, it's worth consulting an IT professional or managed service provider. But at the beginning, a little awareness and good habits go a long way.

Q: Do I need to do something with my firewall? What does it do?
A: *A firewall acts like a security guard for your internet connection. It watches all the data coming in and going out of your network and decides what's safe and what's not — based on rules you set or it already knows. For a small business, the firewall in your router + the one on your computer is usually enough to start. Just make sure both are turned on and updated regularly.*

Building Basic Cyber Defenses – What You Need to Know

Think of this chapter as installing locks, alarms, and smoke detectors for your digital workspace. You wouldn't leave your office doors wide open overnight, so why leave your business data vulnerable to hackers, scammers, or software bugs? You want your business to be harder to get into than your neighbor's, just like your security at home. Don't be the easy target for the least sophisticated or experienced attacker.

What You Need to Do Right Now

Use Strong, Unique Passwords

This is your first line of defense. Don't reuse the same password everywhere. Use passwords that are at least 12 characters long, and don't include easy-to-guess info like your business name or "1234." An easy complex password to remember is a phrase you like. Use only the first letter of each word, alternate capital letters and change some letters into numbers. For example:

PHRASE: " In order to know your enemy, you must become your enemy." - Sun Tzu, The Art of War

PASSWORD: i0tKy3YmBy3SttA0w

Pro tip: Use a password manager, many are free or low-cost, to generate and store passwords for you.

Turn on Two-Factor Authentication (2FA)

Think of 2FA as a deadbolt on your digital door. It adds an extra layer of protection by requiring a code from your phone (or another method) in addition to your password. Most email services, bank websites, and cloud tools offer 2FA. Turn it on wherever possible.

Keep Software Updated

Outdated software is one of the easiest ways for cybercriminals to get in. Always install updates for your operating system, antivirus software, and apps, even if it's annoying. These updates often patch security holes that hackers love to exploit.

Back Up Your Data

If a cyberattack or hardware failure wipes out your data, a recent backup is your lifeline. Make sure your files are backed up regularly to an external drive or a reputable cloud service. Ideally, use both for extra safety. And test your backups! Make sure you can accurately restore files if needed.

Install Antivirus or Antimalware Software

Good security software helps catch threats before damage occurs. Even basic free antivirus tools can offer solid protection. Just make sure it's from a reputable company and keep them up to date.

Train Your Team (Even If It's Just You)
Most attacks start with human error—clicking a bad link, opening a fake invoice, or sharing a password. A little training goes a long way. Teach yourself (and all employees) to spot suspicious emails, avoid shady downloads, and ask questions when something feels off.

Practical Tips

- Backup Regularly: Save important files weekly to a USB drive or cloud storage.
- Secure Cloud Storage: Use platforms like Google Drive or Dropbox, secured with strong passwords.
- Set a reminder to back up data weekly.
- Turn on 2FA for email and banking.
- Use built-in antivirus, if necessary, but plan to upgrade.
- Check for software updates monthly.

Common Questions Answered

Q: Do I really need antivirus if I use a Mac or Windows with built-in protection?
A: It depends on how you use your devices — but in most cases, yes, especially for a business. Both Windows Defender (built into Windows) and XProtect (built into macOS) offer decent basic protection, but neither are foolproof. They don't always catch newer or more sophisticated threats like phishing, ransomware, or targeted malware, which are increasingly aimed at small businesses. If you're on a tight budget, some trusted free options can still give you stronger coverage than built-in tools alone.

Q: Why are updates important?
A: *Software updates are important because they fix security holes that hackers can exploit, protect against the latest viruses and ransomware, and help your systems run smoothly by fixing bugs and improving performance. They also help your business stay compliant with data protection laws and show customers you take security seriously. Turning on automatic updates is a quick, easy way to keep your devices and data safe.*

Q: Is cloud storage safe?
A: *Cloud storage is safe if you use it the right way. Most major providers use strong security to protect your data, often better than storing it on your own computer. To keep it secure, use strong passwords, turn on multi-factor authentication, and be careful about who has access. If you follow those steps, the cloud is a reliable and safe way to store your business files.*

Empower Your Team with Cyber Awareness, What You Need to Know

Your employees aren't just part of your business, they're also your first line of defense against cyber threats. While firewalls, antivirus software, and strong passwords play important roles, even the most secure systems can be compromised by human error. Cybersecurity is a team effort and when your employees understand the risks and feel confident in what to do, they become one of your business's biggest assets in staying secure.

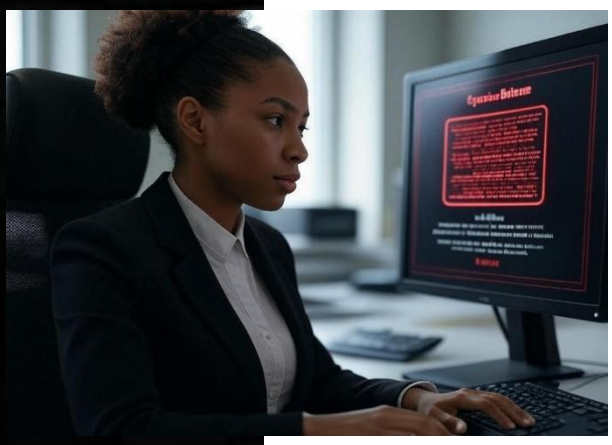
Why It Matters

Cybercriminals often see small businesses as easy targets because they know many small teams don't have dedicated IT staff or advanced security systems. Instead of attacking big corporations with strong defenses, attackers look for less time-consuming targets and that often means small businesses with just enough data and money to make it worth their time.

It only takes one click, one mistake, or one moment of trust in the wrong source to open the door to serious consequences like a data breach, stolen customer information, system downtime, lost revenue, or damage to your brand's reputation.

Practical Tips

- Run Cybersecurity Training: Training doesn't have to be dry or overwhelming. Make it part of your culture annually, not just a checkbox.
- Secure Remote Work: Require secure Wi-Fi and keep work devices updated, encrypted, and locked when unattended.
- Vet Third-Party Vendors: When you work with third-party vendors, whether it's an accountant, marketing agency, cloud service, or payment processor, you're not just sharing services, you're also sharing responsibility for your data.
    - Only give them access to what they need and nothing more.
    - Review all contracts for data protection language.
    - Regularly discuss cybersecurity with your third-party vendors, especially if they handle sensitive customer info, payments, or business operations



- Have a Response Plan: Outline what to do if something goes wrong. Every employee should know there's a clear, simple plan to follow if something seems suspicious or goes wrong. The faster they act, the less damage your business will experience.
- Protect Customer Data: Not every employee needs access to all customer data. Give team members access only to what they need to do their job and use permissions or roles in your systems to control who can see or edit sensitive info. Remove access immediately when someone changes roles or leaves the company

Common Questions Answered

Q: What role does training play?
A: *Training helps prevent mistakes before they happen*

Q: Do I need a response plan?
A: *Yes, absolutely! Some pro tips:*

- *Assign roles and responsibilities. Know who's in charge of reporting, investigating, communicating, and restoring systems.*
- *Include a clear reporting process. Make it easy for employees to report problems without fear.*
- *Create communication templates. Prepare messages for customers, employees, or partners if a breach occurs. This saves time and keeps messaging consistent.*
- *Practice your plan. Run drills or tabletop exercises a few times a year to make sure everyone knows what to do.*
- *Keep it updated. Review your plan regularly, especially when tools, vendors, or staff change.*

Q: How do I assess vendors?
A: *Ask about their cybersecurity practices. These questions will help get the conversation started:*

- *How do you protect our data? They should be able to explain how they store, secure, and control access to your information.*
- *Do you use encryption? Encryption scrambles data to make it unreadable to hackers. It's a must for anything stored or shared online.*
- *Who has access to our data? Only the people who need it should be able to see or use it. Make sure they have controls in place.*
- *What happens if something goes wrong? They should have a plan for dealing with breaches and notifying you quickly if your data is affected.*
- *Are you following any industry standards or laws?*
  They don't need to be experts, but they likely follow basic rules like GDPR, HIPAA, PCI DSS

Q: What should I do if I think I clicked something suspicious?
A: First, don't panic. The sooner you act, the better. Pro tips:

- *Don't keep clicking or navigating around.*
- *If a file downloaded, don't open it.*
- *If you're on a suspicious website, close the browser tab immediately.*
- *Report it to your manager, IT person, or business owner right away. Include details on what you clicked, when it happened, and anything unusual that popped up.*
- *If you got an email, don't delete it*
- *Unplug your Ethernet cable or turn off Wi-Fi. This can help stop malware from spreading or sending out data*
- *Don't try to fix it yourself. Follow the plan*

Monitor for Threats and Staying Alert, What You Need to Know

Constant vigilance is key. Just like a security camera protects a physical store, monitoring your digital environment helps you catch suspicious activity early before it turns into a major problem.

Why It Matters

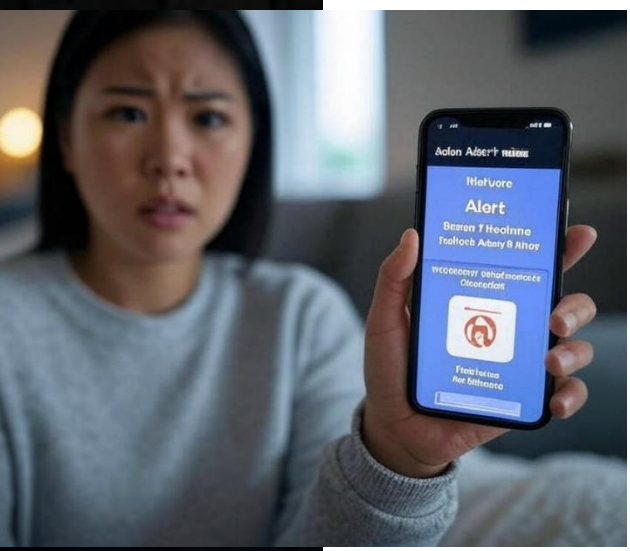
Cyber threats don't always announce themselves. Many attacks start quietly with things like a strange login, an unauthorized data transfer, or a phishing email that went unnoticed. The faster you spot these red flags, the more control you have over the outcome.

Whether it's malware, a compromised account, or unusual behavior on your systems, early detection means less data lost, less downtime, lower recovery costs, and faster response time.

Security isn't just a one-time setup; it's a daily habit. Monitoring helps catch small issues before they become big breaches. Whether it's a team of IT pros or just a watchful employee, staying vigilant protects the whole business.

Practical Tips

- Watch for Red Flags. Here are some examples:
  - Slower-than-usual systems - Your computer or network suddenly becomes sluggish, programs take longer to open or crash unexpectedly.
  - Strange pop-ups or error messages - Unfamiliar alerts may appear, especially ones asking you to click a link or download software or fake antivirus warnings are a common scam tactic.
  - Unexpected restarts or system behavior - Devices restart on their own, freeze, or behave oddly. Settings or files change without explanation.

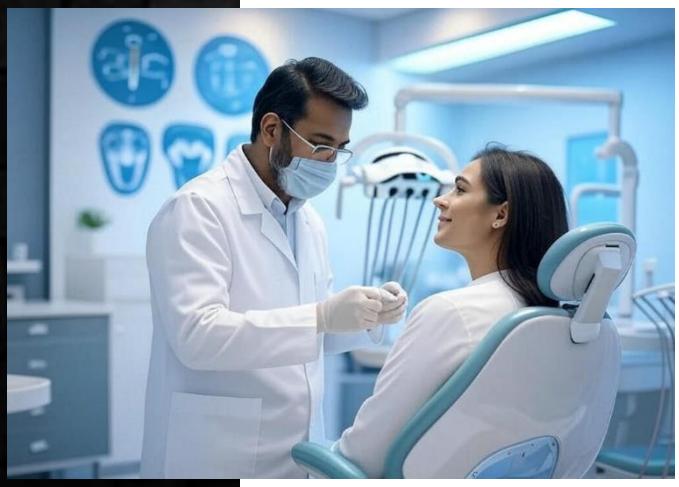


  - Suspicious emails or messages - Emails with odd grammar, urgent requests, or strange links (even from known contacts), unexpected attachments or requests for sensitive info (passwords, payment details, etc.) are all warning signs.
  - Login issues or lockouts - You're locked out of an account or receive alerts about logins you didn't initiate could be a sign that someone may be trying to gain unauthorized access.
  - Missing, encrypted, or renamed files - Files go missing, appear with weird names, or can't be opened. This is a common early sign of ransomware.
  - Unusual network activity- Internet or network slows dramatically for no reason or devices send/receive large amounts of data unexpectedly.
- Limit Access: Only allow trusted users to access systems.

- Run Security Tests: Free security testing tools can help you spot weak points in your systems *before* cybercriminals do. These tools act like a digital "check-up," scanning for common problems like outdated software, open ports, weak passwords, or misconfigured security settings.
- Secure Smart Devices: Change default passwords on cameras, printers, etc.
- Use Alert Tools: Some apps notify you if something suspicious happens. Set up alerts for critical accounts, like email, cloud storage, admin panels, and payment systems first. You don't need to monitor everything, just the tools that matter most to your business.
- Speak up if something feels off: Examples we have discussed are a weird email, a slow system, or a strange popup.
- Don't ignore software or security alerts - report them immediately.
- Follow safe habits: Lock your screen when you step away from your computer, logging out of shared systems, and double-checking email senders are great habits.

Common Questions Answered

Q: What is zero trust?
A: *Don't automatically trust anyone and verify everything. Zero Trust is a modern cybersecurity approach that assumes no one, not even someone inside your business, should be trusted by default. Instead, everyone and everything must be verified before being allowed access to data, systems, or applications. It's a big shift from the old way of thinking, where companies trusted people or devices just because they were "inside the network."*



Q: How do I secure IoT devices?
A: *Start by changing default settings and passwords. IoT devices are great for convenience and automation, but they can also be easy entry points for hackers if not secured properly. Many of these devices come with default usernames and passwords that are publicly known or easy to guess, and hackers scan the internet looking for them. Keep the device's firmware updated and consider a separate network for these devices. Turn off features you don't use and stay vigilant, keep an eye on device behavior.*

Q: How often should I test my defenses?
A: *At least quarterly. Cyber threats don't take breaks, and neither should your security strategy. Regularly testing your defenses ensures everything is working as it should, meaning your antivirus is active, your backups are usable, your systems are updated, and your team knows what to do in case of a threat.*

Q: Why monitor daily?
A: *To catch issues before they escalate and minimize business impact.*

Preparing for the Unexpected, What You Need to Know

No one expects a cyberattack until it happens. And when it does, the impact can be fast, chaotic, and costly. That's why preparation isn't optional, it's a business essential.

Think of it like a fire drill for your digital operations. You hope you'll never need it, but when disaster strikes, the steps you take beforehand can make all the difference. Preparation minimizes downtime, limits financial loss, and helps your team stay calm and focused under pressure.

Why It Matters

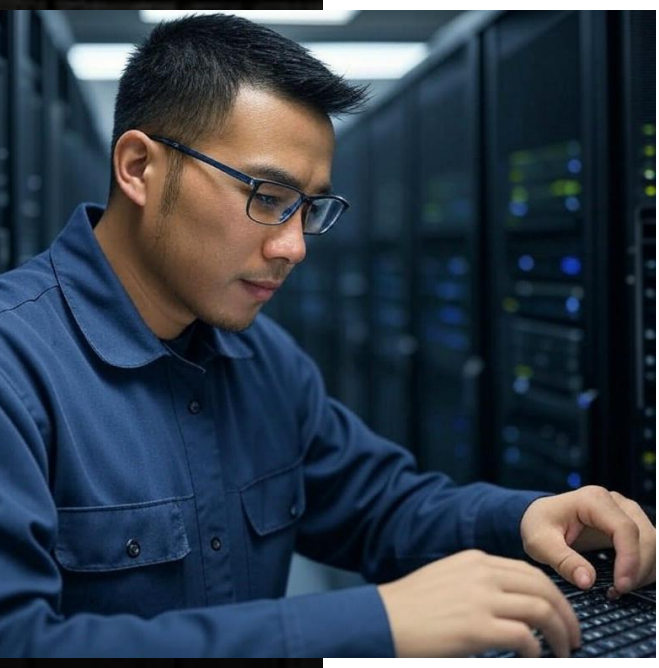
Even a small cybersecurity incident, like ransomware, a data breach, or a system outage, can lead to:

- Lost income from downtime or canceled customer orders.
- Legal trouble if customer or employee data is exposed. In addition to financial penalties, companies may be legally required to notify affected individuals, offer credit monitoring services, and implement corrective measures. Legal actions may also include class-action lawsuits if multiple individuals are affected.
- Reputation damage that's hard to fix once trust is broken.
- Stress and confusion if no one knows what to do next.

Practical Tips

- Identify Vulnerabilities: List your key systems and weak points. Begin by mapping out all critical systems, data repositories, and digital infrastructure. This includes servers, cloud platforms, employee devices, and third-party integrations. Conduct regular risk assessments to identify weak points, like outdated software, poor password practices, or lack of encryption. Then prioritize them based on potential impact.
- Consider Cyber Insurance: Cyber insurance can provide a financial safety net in the event of a breach, covering expenses such as legal fees, notification costs, data recovery, and business interruption losses. Evaluate different policies to ensure coverage aligns with your specific risks and operational needs.
- Understand the Cost of Inaction: Investing in cybersecurity may seem expensive upfront, but it's significantly less costly than dealing with the aftermath of an attack.
- Know the Laws: Familiarize yourself with local and industry regulations. Different regions and industries have specific data protection and privacy requirements. Stay informed about applicable laws such as GDPR, CCPA, HIPAA, or PCI-DSS. Non-compliance can lead to fines, legal action, and loss of customer trust.

- Create a Business Continuity Plan: Know how to recover quickly. Prepare a detailed plan outlining how your business will respond to and recover from disruptions, including cyberattacks. This should include data backups, communication protocols, recovery time objectives (RTO), and designated roles. Testing and updating the plan regularly ensures you're ready when it counts
- Protect most-used systems first.
- Start an emergency savings fund is a proactive step toward financial resilience. This fund acts as a financial cushion to help your business weather unexpected events such as cyberattacks, equipment failure, economic downturns, or other operational disruptions. Ideally, it should cover several months of essential operating expenses, including payroll, rent, utilities, and critical services.
- Use free resources to learn about business regulations. Government websites such as the Small Business Administration (SBA), IRS, Department of Labor, and your local chamber of commerce often provide guides, webinars, templates, and checklists tailored for small and medium-sized businesses. You can also find free courses and articles through platforms like Coursera, edX, SCORE, YouTube, and local Small Business Development Centers (SBDCs).
- Backup key data to multiple places.



Common Questions Answered

Q: How do I assess my risk?
A: *Start by identifying which data and systems are most vital to your business. Think about what you store (i.e. customer info, financial records, or proprietary data) and what you use daily, such as email, point-of-sale, or inventory systems. Ask yourself:*

- *What data would be most damaging if lost or exposed?*
- *What systems would disrupt operations if they went down?*
- *Who has access to sensitive information, and how is it secured?*

Once you know your key assets, assess their risks to include cyberattacks and accidental loss. Then identify weak points.

Q: What laws apply to me?
A: *The laws you need to follow depend on your industry, location, and the type of data you handle. For example, healthcare must follow HIPAA, retailers need PCI-DSS, and businesses with customer data may fall under GDPR or CCPA. You'll also need to comply with tax, labor, safety, and licensing laws at the local, state, and federal levels.*

Protecting Personal and Financial Information, What You Need to Know

Keeping your personal and business financial information separate and secure is a critical step in maintaining both your personal identity and the integrity of your business. This means having separate bank accounts, credit cards, digital wallets, and accounting systems for your business and your personal life. Mixing the two not only creates confusion at tax time but also increases your risk exposure if either side is compromised.

For business owners, especially those operating as LLCs or corporations, maintaining this separation is also key to preserving limited liability protection. If personal and business finances are intertwined, it could "pierce the corporate veil," leaving your personal assets vulnerable in the event of a legal dispute or audit.

Why It Matters

One breach can trigger a chain reaction. If a hacker gains access to an account that links both personal and business data, they could steal money, commit fraud, access sensitive client or employee data, and even compromise your identity. This could lead to:

- Financial loss: drained accounts or unauthorized transactions
- Reputational damage: loss of client trust and business credibility
- Legal issues: lawsuits, fines, or regulatory investigations
- Operational disruption: system downtime and recovery costs

Separating accounts helps contain the damage. If one side is breached, the other remains protected. It also makes it easier to detect suspicious activity early and take swift action.

Practical Tips

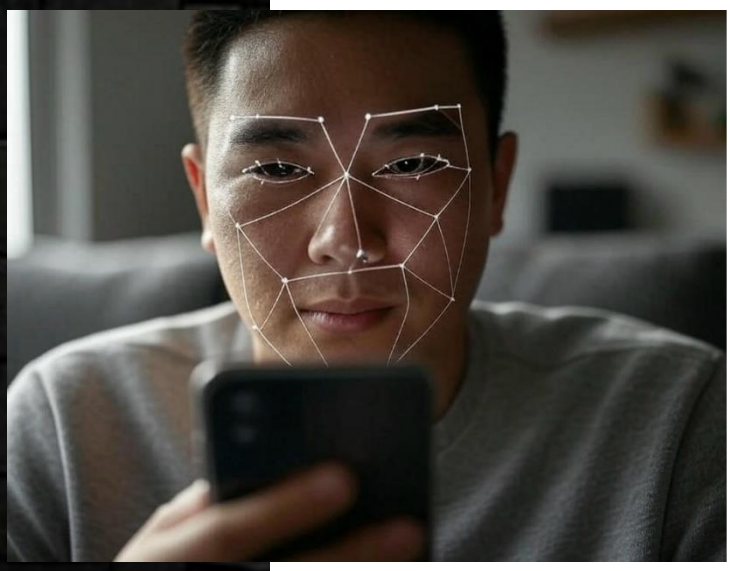
- Use a Dedicated Device for Banking: Don’t mix business with personal browsing. For example, use your phone (not business PC) for banking.
- Create Unique Logins: Never reuse usernames or passwords for banking sites.
- Enable 2FA for Financial Accounts: For financial accounts, such as online banking, payment processors, bookkeeping platforms, and business credit cards, 2FA should be **non-negotiable**. It's one of the easiest and most effective ways to prevent financial loss. Pro tip: Use an authentication app instead of SMS when possible. It’s more secure and less vulnerable to SIM-swapping attacks.
- Avoid Password Reuse: Across family, work, and personal life. Talk to your family about password safety.
- Change financial account logins. Regularly updating the usernames and passwords for your business and personal financial accounts is a simple but powerful way to protect against unauthorized access.

Common Questions Answered

Q: Do I legally have to separate business and personal finances?
A: *If you're a sole proprietor, it's not legally required, but it's* strongly recommended*. For LLCs, corporations, or partnerships, yes, mixing finances can put your personal assets at risk and even invalidate your limited liability protection.*

Q: How safe are digital wallets? And why are they considered secure?
A: *In general, digital wallets are quite safe when used correctly. They use advanced security measures to protect your payment information, often making them safer than carrying physical cards or cash. Some key safety features include:*

- *Encryption & Tokenization: Your actual card number isn't stored or shared during transactions. Instead, it's replaced with a one-time-use "token" that hides your real account info.*



- *Biometric Authentication: Most wallets require Face ID, fingerprint, or a passcode before authorizing any payment, making it hard for someone else to use your wallet even if your phone is stolen.*
- *Remote Lock/Wipe Options: If you lose your device, you can usually lock or erase your digital wallet remotely using tools like Find My iPhone or Google Find My Device.*
- *No Physical Card Info Stored on the Device: Your actual card details are not stored on your phone or transmitted to merchants, reducing the risk of theft during transactions.*
- *Fraud Protection: Most major digital wallet providers (Apple Pay, Google Wallet, Samsung Pay) partner with banks and credit card companies that offer fraud monitoring and zero-liability protection for unauthorized charges.*

Q: How do I start separating my finances?
A: *Open a business bank account using your EIN (or SSN for sole proprietors). Get a business credit/debit card for purchases. Start paying yourself a salary or draw from the business account. Track all income and expenses separately using accounting software.*

CONCLUSION

You made it! You don’t need to be a tech wizard to keep your business safe.

Running a business isn’t easy, and let’s be real: cybersecurity probably isn’t the most thrilling part of your day. Think of this like locking up your shop at night, it’s the same idea, just online. Pick one simple tip from each section to start, like creating strong passwords (no more “1234!”) or making sure your files are backed up. These are your digital baby steps and they *really* add up.

At the end of the day, you’re the boss. You’ve built something amazing, and you deserve to protect it without stress or confusion. With a little care and a pinch of confidence, your business will keep growing, safely.

Sleep better knowing you’ve got this.

NDAY Security, named after the "n-day" vulnerability, fortifies the human element of cybersecurity by addressing known vulnerabilities and social engineering attacks before they become liabilities.

The NDAY platform, AttackN takes a proactive approach to offensive security. Built with an AI-infused backbone, AttackN reduces the risk of costly breaches, transforms users into informed defenders, and enables CISOs to allocate precious dollars and resources elsewhere.

Developed by experienced offensive security professionals who got their start as white-hat hackers and have supported three letter agencies, NDAY is led by a team who have led some of the largest commercial offensive security organizations, and were executives at pivotal times in the development of well-known security technologies.

NDAY Security is backed by over 40 years of combined experience in offensive security. Known for staying ahead of evolving cyber threats, NDAY leadership has held senior roles at top firms like Deloitte, PwC, SecureWorks, Trustwave SpiderLabs, Raytheon Foreground, BAE Systems, and General Dynamics.

NDAY leadership also holds a Master’s in Applied Information Technology from NSA-recognized Towson University, a Bachelor’s in Sociology from McDaniel College, and certifications from Harvard Business School and CISSP—underscoring their role as a respected leader in the field.

NDAY™

www.NDAYSecurity.com