

5 ways to keep your small business cyber-safe

How to hack-proof your onsite and virtual workspaces



Your guide to the importance of cybersecurity in your small business

We're happy to see you here, digging into another educational resource developed to offer you valuable information on how you can keep your small or midsize business (SMB) secure against cybercrime.

The state of SMB cybersecurity

How "cyber-secure" is your small business? Before you answer, "100%!" consider that we're in a time when many small businesses are working both onsite and remotely. Even if you don't have to worry about remote employees, cybercriminals have become more sophisticated—and relentless—than ever.

Recent [CNBC/Survey Monkey polling](#) showed that only about half of SMB owners have installed antivirus or malware software, made passwords stronger, or backed up their files to an external hard drive. And just a third have enabled automatic software updates or multifactor authentication (MFA), while only a quarter installed a virtual private network (VPN).

Aren't they worried they'll be the target of a cyberattack? Well, the same poll found that cybersecurity ranks lowest on small business owners' lists of worries, behind inflation, supply chain disruptions, COVID-19 and labor shortages. As a result, while small businesses may not contain the treasure trove of data a large company would, what they do offer are easier targets for attack.

That's why we've created this eBook, to help you keep your business and data safe from cyberattacks that could compromise your customers or clients...and even bring down your business.



About half of SMB owners have installed antivirus or malware software, made passwords stronger, or backed up their files to an external hard drive.

If you think you're too small to be cyberattacked... think again

It used to be the case that large companies were almost exclusively the targets of cyberattacks.

That's no longer true.

Somewhere along the line, cybercriminals realized that security in an SMB tends to have more gaps than in a large company. This is because many owners figure they can handle IT and security issues on their own to avoid what can be a complex and expensive process. As a result, SMBs have become more frequent targets—and it's why [Verizon's 2021 Data Breach Investigations Report](#) (DBIR) found that 46% of breaches affected small and mid-sized businesses.

Why SMBs don't have cybersecurity measures in place

59% My business is too small to be a target for cyberattacks

25% Our online business is limited

19% It's too expensive

16% No one on staff knows about cybersecurity

8% We don't have time to implement cybersecurity

6% The threat of cyberattacks is overblown

Digital.com survey, 3/28/22

That's almost *half*. Not exactly promising odds that your small business won't find itself in a similar situation. This can lead to possible outcomes like these for your business:

- In the CNBC/Survey Monkey poll, 55% of people in the U.S. say they'd be less likely to do business with brands that have been victims of a cyberattack.
- Verizon's DBIR found that the average cost of 95% of SMB breaches fell between \$826 and \$653,587 (yes, you read that last number right).
- According to the [National Cybersecurity Institute](#), 60% of SMBs that are hit with a cyberattack go out of business within six months.

Verizon's 2021 DBIR found that 46% of breaches affected small and mid-sized businesses.

Now, let's be fair about this. Implementing the type of cybersecurity measures that are an accepted cost of doing business in a large company can be prohibitively expensive for a small business—which is why they so often don't get done.

The problem is that unless you're an IT security wizard, most SMB owners don't know enough about cybersecurity to manage it effectively. And they can't afford to hire someone who does. That's when you end up with 51% of small businesses that have no cybersecurity safeguards for their systems, according to a recent [Digital.com survey](#).

Okay. That's enough gloom and doom. Now, let's get to the good stuff.

Five steps you can implement quickly to keep your small business cyber-safe

It goes without saying that you don't want to be one of the 60% who goes out of business within six months of a cyberattack. But you also don't have the budget or the personnel to handle cybersecurity on the scale it admittedly needs. So, is there anything you can do right now, without spending a fortune, to keep your business safer?

We're glad you asked. Here are five easily implemented and relatively affordable ways to help defend your business against cyberattacks.

1 Have a plan ready

Once a business has been breached, panic tends to ensue. And panic often leads to spur-of-the-moment (aka potentially bad) decisions.

Creating a written security plan now—while you have time to consider each step carefully—will give you a set of instructions to follow and one less thing to think about when you're in the heat of a cyberattack. You don't have to start from scratch; Google "template for a small business cybersecurity plan" to find free templates you can use to build your plan. Start with this [Cyberplanner](#) from the Federal Communications Commission (FCC). And here are some critical points to get you thinking:

Detail how you'll follow cybersecurity best practices

You don't have to pull these out of thin air, either. The [FCC](#) has a simple and non-intimidating list of best practices for small businesses on its website.

Implement formal security policies for all staff

Include the importance of strong passwords, identifying and reporting suspicious emails, activating MFA, and not clicking on links or downloading email attachments from anyone—even if it appears to be a known sender.

Pay special attention to security around remote or hybrid workers

When they're not in the office, do you want employees using their own devices, or should they only use business-issued equipment? Can they work at a public location using a VPN?

Develop and practice an incident response plan

It may feel a little silly at first, but along with your staff, pretend you've been attacked and then go through the steps of a response. How do you know it's happened? What's the first action to take? Who will you call for help? How will you communicate any issues to your customers/clients? Thinking through all of this in advance will enable you and your staff to quickly identify and handle a cyberattack before too much damage is done.

Reinforce your plan with regular meetings, and be sure all new employees are brought up to speed as soon as they join your business.

According to the National Cybersecurity Institute, 60% of SMBs that are hit with a cyberattack go out of business within six months.

2 Increase password strength and use MFA

According to the 2022 Verizon DBIR, stolen usernames and passwords are involved in more than half of cyberattacks on small businesses—and about half of the attacks on businesses in general. Emphasize to your staff the importance of strong, complex passwords, and remind them to:

- Make passwords complex—at least 14 characters.
- Never share passwords.
- Use uppercase and lowercase letters, numbers and symbols.
- Use hard-to-guess nonsense phrases (e.g., "CaptainEntropyAimsWestward") and replace or add random letters, numbers and symbols.
- When it's time to change a password, don't just add or change one number/letter.
- Never use the same password in more than one place.

Consider using a password manager to help eliminate the frustration of forgetting a password.

And most important, adopt MFA. This will require users to log in and then verify the login on another device, like a mobile phone or tablet, to gain access. Yes, it's an extra step, but it's a step that has been shown to prevent [up to 90% of cyberattacks](#).

3 Train employees on what to look for

According to Verizon's DBIR, 82% of data breaches start with a human clicking on a malicious link or inadvertently handing over confidential or personal information to bad actors. So, you can implement every technology in the world, but it will only be as effective as the people who use it. Malware, ransomware, phishing, spear phishing, spoofing,

smishing...cyberattackers have so many ways to burrow into your business's systems that it's nearly impossible to keep up.

That's why security training is a must for all employees and company leaders. And it doesn't have to be expensive; the federal government offers free tools and training at the following sites:

- Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA): <https://cisa.gov/stopransomware>
- CISA's Stop. Think. Connect. campaign: <https://stophinkconnect.org>
- The U.S. Department of Commerce's National Institute of Standards and Technology (NIST): <https://nist.gov/itl/smallbusinesscyber>
- National Cybersecurity Alliance: <https://staysafeonline.org/resources>
- U.S. Small Business Administration: <https://sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity>

Cybersecurity training shouldn't be a one-and-done occurrence. Consider ongoing training to keep your employees up to date on new security vulnerabilities and to help them recognize and avoid scams, understand the importance of creating strong passwords, and to stress the necessity for protecting sensitive customer and company information.

Multifactor authentication has been shown to prevent up to 90% of cyberattacks.


④ Keep your software updated

Whatever software and apps you use, KEEP THEM UPDATED! (We're not yelling, we just want to make sure you understand how important this is.) We're talking about the software you need to run your business: accounting software; other financial apps; security applications like antivirus, firewalls and malware (and if you don't use those, we need to talk); operating systems such as Windows; and anything else that is used on a daily, monthly, quarterly or yearly basis.

Cybercriminals love outdated software—and they're so prolific at taking advantage of vulnerabilities that software makers continually issue security patches. If you don't immediately patch your system, you're leaving yourself open to attack until that patch is applied (ever hear of a [zero-day exploit](#)?).

This can especially be an issue if you have remote workers. You may be foggy on their security setup, especially since other technologies like servers, browsers, VPNs, printers, scanners, routers, computers, tablets and smartphones also need constant updates.

If it sounds like a big job, it is. But it's also essential. If you're not sure you or anyone else in your business is up to the task, it may be worthwhile to investigate outsourcing some of your IT support and management.



In addition to a regular backup, your data should also be accessible off-site in case of an incident that takes down your system.

⑤ Back up your data

Even if your network has only a few computers, one of the best things you can do to keep your system secure is to regularly back up your data. While it won't prevent a cyberattack, it will protect you from data loss.

In addition to a regular backup, your data should also be accessible off-site in case of an incident that takes down your system (a cyberattack that wipes or encrypts data, a natural disaster, or other unexpected issues that make access to your business data impossible). It can make the difference between restoring your data quickly and being up and running again...or being unable to conduct business at all.

Some owners back up their data to external hard drives that they take home with them each night (or whenever their backups are scheduled). You can also transfer that physical backup to a cloud solution for storage, but you'll want to be sure it's not accessible from your business network so that an attack won't affect those files. And don't rely exclusively on the cloud; always be sure you have a physical copy available as well in case you're unable to access the internet due to an infrastructure failure.

Another option is to use automated backup software, in case you forget or are unable to manually perform the regular backup of your business's important data.

In addition to frequent backups of your data and your most critical business applications, it's a good idea to test the recovery of data from your backups regularly to be sure there are no glitches—especially if you've added new programs or systems since your last recovery test.

Summing it all up

While there is no guarantee that all these steps will prevent your firm's systems from ever being breached, preparation will put you ahead of at least half of the small business owners in the U.S.

If you take the time now to up your cybersecurity game, when cybercriminals try to tell you it's "game over," you'll be ready to show them they've messed with the wrong business.

We hope this guide has demonstrated why cybersecurity should be top of mind for any business—large or small. Remember, it's up to you to ensure your business's data (especially sensitive customer, client and employee information) is safeguarded from cyberattacks. It's a big job, but we have every confidence you'll be able to handle it with the assistance of the resources provided in this eBook. And as always, we're here to help. Let us know if we can provide additional guidance or information.

Finally, check with us if we can help you in any way with your business finances or an action plan for business growth.

Just click the **GET IN TOUCH** button and complete the brief form or give us a call.

We look forward to hearing from you!

