

June 10, 2019

7 Ways to Help Keep Your Customer Data Safe as a Home-Based Business

Just because your business is small, doesn't mean you can't be protected. These tips may help keep your customer data safe.

Rodika Tollefson
Freelance writer and journalist



When you run a small business from home, or even from a small office with an employee or two, you likely don't have an IT person to help keep your data safe. Yet in the event of a data breach, you may still be liable to your customers if their intellectual property, financial information or other sensitive data is exposed.

Just because your business is small doesn't mean your chances of a breach are also small. "It makes no difference if you're a small or big organization—it's equally important for smaller organizations to have the same mindset when it comes to security," says Joakim Sundberg, founder and CEO of threat-protection company Baffin Bay Networks, which is based in Sweden and has a threat research center in Oregon.

Sundberg says that you don't need to do everything at once to secure your business, and go step by step instead.

"Sometimes it's better to do smaller things than look at the big picture," he says.

While there are many ways for a home-based business to approach cybersecurity, these are some of the more basic steps to help you improve your cyber hygiene.

1. Know your data.

Stephen Breidenbach, a greater New York City-area associate with the legal firm Moritt Hock & Hamroff LLP, says the first thing he recommends to his clients is to understand where they store their data.

ADVERTISEMENT

Product Solution

Keep better tabs on cash flow

We help simplify money management. American Express has the solutions to keep you on top of your spending.

[Learn More](#)

"Understand what you're collecting, what especially needs to be protected, and where you're housing that," says Breidenbach, a former cybersecurity professional who's his firm's co-chair of the Cybersecurity, Privacy and Technology Practice Group.

Once you have a clear picture of what sensitive data you store and where you're storing it—whether it's on your computer drive, in the cloud or in your email—then you can implement specific security protocols to protect it.

2. Keep your systems current and patched.

Better Business Bureau's "2017 State of Cybersecurity Among Small Businesses in North America" found that only 69 percent of small businesses patched their systems and applications (the report was based on a survey of 2,000 consumers and 1,100 businesses; 54 percent of surveyed businesses had zero to five employees). Yet outdated and unpatched devices and apps pose a high risk because cybercriminals take advantage of their vulnerabilities to gain access.



Just because you're a small business doesn't mean you don't have access to proper protection.

—Stephen Breidenbach, associate, Moritt Hock & Hamroff LLP

"Attackers exploit very simple mistakes that companies make," Breidenbach says. "They learn about exploits all the time because patches are released (by vendors) and they'll create a means of gaining access to a system using that vulnerability."

Using relatively recent devices, keeping them current with updates and turning on auto-updates are basic things that eliminate a lot of the risk, says Drew Cohen, an engineer and entrepreneur who's the president and CEO of MasterPeace Solutions Ltd, a cybersecurity company and technology accelerator in Columbia, Maryland.

"Running new operating systems (such as Windows 10) and keeping them patched is a good way to add in some cyber hygiene," he says. "And also avoid unnecessary apps, downloads and software on your devices because those are security risks."

3. Use strong authentication.

According to the BBB survey, victims of cyberattacks said their passwords and other authentication data were the most common type of data compromised. If you reuse the same passwords across different online or cloud-based services, that means you're essentially giving the bad guys the keys to your kingdom.

"Your password is the primary way to protect from brute-force attacks, which is one way that an attacker will try to get in, trying multiple types of passwords," Breidenbach says.

Sign up to receive the latest business insights

Enter your email address [Join](#)

By providing your e-mail address, you agree to receive the business insights newsletter from American Express. For more information about how we protect your privacy, please read our [Privacy Statement](#).

A password keeper is one way to use strong, unique passwords without having to memorize them. In addition to creating strong passwords, turn on two-factor (or multi-factor) authentication for any services that have it available.

In the BBB survey, only 64 percent of organizations adopted multi-factor authentication. Yet this protocol adds one more layer that a hacker would have to break to get in. A text message to your mobile phone is a common two-factor authentication method, but it's best to use an authentication app instead when that's an option.

4. Separate your computers.

Sundberg recommends a dedicated computer for accessing only online banking, cloud-based accounting platforms and similar websites. This doesn't require a large investment.

At the very least, don't use your business computer for personal activities, Breidenbach cautions.

"Let's say you let your kids use that business computer, and they install a game or an app from a site. They may inadvertently install a program and next thing you know, your computer is locked or an attacker got access to it."

5. Back up your critical data.

If your IT resources are compromised and you can't deliver on your projects, the consequences could be devastating. In the BBB survey, only 35 percent of businesses said they could remain profitable for more than three months if they permanently lost access to essential data.

"Backup is equally as important as passwords," Sundberg says. "Make sure you have a way to restore your data so you don't have downtime."

Cohen advocates using a cloud-based backup service from a reputable, leading vendor like Microsoft or Amazon.

"These cloud providers have the resources, and their security becomes part of your security," he says.

Avoid consumer-level cloud services, however, as they don't have the same levels of security and controls built in. Things to consider include encryption and multi-factor authentication.

"The big thing is to make sure that what the vendor is telling you is actually what they're doing and that you know how they're storing your information," Breidenbach says. (The same is true for any other vendor that you entrust with your sensitive data.)

If you prefer backup to a physical drive, choose one that offers both encryption and password-protected access.

6. Use encryption as much as possible.

Encryption renders your lost or stolen data useless to a cybercriminal without a decryption key. Besides your backup, you may want to encrypt your hard drive, as well as your email.

Breidenbach also recommends file-level encryption for your most sensitive documents. But, he cautions, do extensive research before you choose a tool.

"Use reputable sites and make sure there's a significant amount of reviews for the product," he says. "And then attempt to use it and test to see that it encrypts."

7. Monitor and secure your network.

Large organizations commonly segment their networks to limit attackers' ability to move laterally once they get in. If your home-based business uses the same network and internet access as your household computers and smart devices, your risk escalates.

"The problem with network security is that one bad device that gets infected is the entry point for the infection to spread to other devices," Cohen says.

New devices are coming to the market that provide micro-segmentation, including consumer-grade routers that could help protect your home-business network—so Cohen recommends keeping an eye on new technologies.

The Federal Trade Commission's cybersecurity basics for small businesses also include securing your router by changing user name and password, turning off remote management and logging off as an administrator once the router is set up. Additionally, ensure that the router uses encryption and that it's turned on.

A Few Other Basics

Website hosting: If you gather sensitive information via your website, avoid using a web platform that gets frequently attacked. "We see so many hacks because of online publishing software that's not safe," Sundberg says.

Email authentication: Email is a primary phishing vehicle, so be suspicious of attachments or links from even legitimate-looking companies. Before you click on an unknown URL, check it against malicious site blacklists.

FTC authentication technology also makes it harder for scammers to spoof your emails. FTC recommends choosing an email provider that uses three safeguards: a sender policy framework (SPF), domains keys identified mail (DKIM) and domain-based message authentication, reporting and conformance (DMARC).

Public Wi-Fi: If you take your business on the road and use your laptop at coffee shops, hotels and other public places to catch up on work, use a virtual private network (VPN) before you check email, log into accounts and so forth.

Lack of resources is often a hindrance for small businesses but, as Sundberg notes, some security vendors cater specifically to small organizations and have affordable costs.

Breidenbach agrees. "Just because you're a small business doesn't mean you don't have access to proper protection," he says.

As a small business, you also have an advantage because you're not storing your customer data in very many places—making it easier to secure.

"With some of these security things, even if you're not a tech person, you can Google, 'How do I secure X?' and follow those steps," Breidenbach says. "And at least then you could show you've made an effort."

In addition to the FTC, you can also find free resources for small businesses from agencies like the Federal Communications Commission, Homeland Security and US-CERT.

Photo: Getty Images

Want to Dig Deeper?

- [Digital Tools](#)
- [Rodika Tollefson](#)
- [Getting Customers](#)

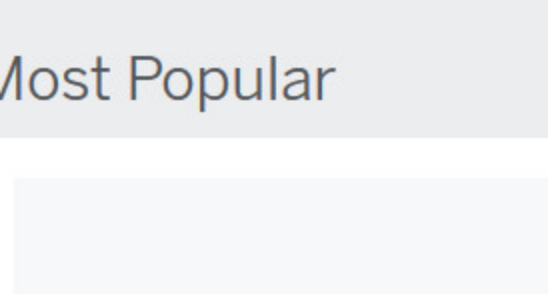
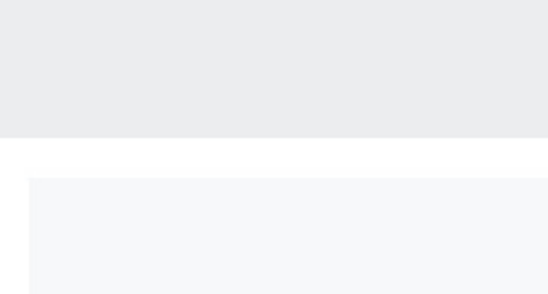
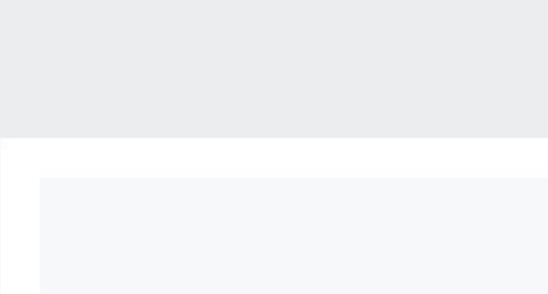


About the Author



Rodika Tollefson
Freelance writer and journalist

Most Popular

 <p>7 Ways To Promote Your Business Online For Free</p> <p>Kim Bhasin • 3 min read</p> <p>Read Article</p>	 <p>How 16 Great Companies Picked Their Unique Names</p> <p>Glen Stansberry • 3 min read</p> <p>Read Article</p>	 <p>12 Ways to Hook an Audience in 30 Seconds</p> <p>Bruna Martinuzzi • 6 min read</p> <p>Read Article</p>
--	--	--

