Union Savings Bank

10 Myths

about Small Business Cyber Security

LEARN HOW TO PROTECT YOUR BUSINESS

Table of Contents

Introduction 3

Myth #1
Cyber Criminals Don't Bother with Small Businesses 4

Myth #2
There's Only One Type of Small Business Cyber Attack 5

Myth #3
Cyber Fraud is Limited to Your Small Business Network 6

Myth #4
Older Systems are Safe from Cyber Fraud 7

Myth #5
Password Protecting a Small Business Wi-Fi Network is Bad for Business 8

Myth #6
You Can Tell the Moment a Small Business Network has been Breached 9

Myth #7
The First Thing to Do after Detecting a Breach is to Alert Your Customers 10

Myth #8
There's No Way to Prepare for a Security Breach 11

Myth #9
Small Business Employees Don't Need Online Training 12

Myth #10
There's One Person Responsible for Small Business Cyber Security 13

About Us

Thinking about the cyber attacks that make headlines will probably bring to mind well-known brands and global corporations shaken by data breaches and identity theft. At first glance, it seems obvious that a fraudster would choose to unleash a cyber attack on a large organization over a small one. After all, there is likely more to gain in terms of quantity of data and potential earnings. But in any given year, 43 percent of all cyber attacks target small businesses. These attacks range in size from small hacks to large scale assaults that can do enough harm to force small businesses to close their doors for good.

Even as advances in network security offer improved protection for businesses of all sizes, the best defenses against cyber fraud continue to be knowledge and awareness. This means that ongoing misconceptions about small business cyber security remain the biggest obstacles to protection and prevention.

In this guide, we will uncover the truth behind some of the biggest misconceptions about small business cyber fraud and discuss ways to protect your business.

Myth #1

Cyber Criminals Don't Bother with Small Businesses

As we learned from the introduction to this guide, small businesses are not immune to cyber attacks. Due to their size and allocation of resources, many small businesses do not have someone on staff dedicated to cyber security. And with the growing popularity of cloud-based data storage, small businesses with insufficient security can be prime and easy targets.

As a result, it's not uncommon for small businesses to be compromised and not realize it until it's too late, if ever. Even large-scale attacks on global corporations can fly under the radar, though these institutions often have teams of security professionals that can detect and manage a breach more effectively. These organizations are also more likely to bounce back financially following a cyber attack. When it comes to small businesses, however, 60 percent of companies that fall victim to cyber attacks are forced to close their doors within six months.

It's important to recognize that businesses of all sizes and revenues have data that could be valuable to fraudsters. This data can include anything from your customers' names and addresses to their payment information and dates of birth. You don't need to be a Fortune 500 company to have data that fraudsters are looking for.

60% of small businesses targeted by cyber attacks close their doors for good within 6 months.

Cyber criminals also set their sights on small businesses because they can carry out several attacks at once rather than channeling all of their resources into a single large target. You may never know it, but if your small business becomes a target, it could actually be one of many, all attacked by the same source. Keeping up to date with the latest cyber security news can help alert you to rising threats.

Myth #2

There's Only One Type of Small Business Cyber Attack

While you may have a picture of what a small business cyber attack looks like, there are many variations of cyber crime today. In one growing trend, fraudsters are bypassing networks altogether and going straight for your most vulnerable assets: your employees.

Social engineering cyber attacks attempt to get employees to divulge sensitive information and compromise business security. To reach that goal, hackers will do things such as study employees' social media or create email addresses that are very similar to company email addresses to look like they are part of the organization and therefore trustworthy.

In the case of a business email compromise attack, hackers will use the personal information they've gleaned about the business owner or upper management to contact someone else within the organization behaving like the individual they are impersonating. Using a combination of authority and urgency, hackers use fear tactics and play into their targets' sense of duty to their company to get what they want. In many real examples of business email compromise, hackers have used emotional pleas to steal information, including threatening the recipient's job if they don't comply or promising promotions as a thank you for their help. To avoid falling victim to such attacks, it's important to communicate to your employees how you will and will not ask them for information or assistance.

To avoid falling victim to social engineering attacks, it's important to communicate to your employees how you will – and will not – ask them for information or assistance.

Another frightening type of cyber attack targeting small businesses are ransomware attacks. As the name suggests, hackers executing a ransomware attack will hold a business' data ransom in exchange for amounts of money that their targets typically cannot pay. As a result, one in five small businesses hit by this type of attack is forced to shut down operations.

In many cases, these small business cyber attacks use sophisticated data encryption software, leaving a small business unable to access their own network. With the data at their disposal, hackers may be able to access customers' personal data and other types of sensitive information, stripping the business of any and all control over how it's used or where it could be sold.

Many security experts will advise against complying with the hacker's demands as there is no guarantee that they will actually cooperate. Depending on how the information has been confiscated or encrypted, it may be possible for an expert to regain access to the network. This does not necessarily prevent or reverse any damage hackers may have done to your network, however, so the best remedy is prevention. Look for tips about policies, procedures and training employees later in this guide.

Myth #3

Cyber Fraud is Limited to Your Small Business Network

Imagine a fraudster gaining access to small business data and an image of a shady figure typing into a laptop might come to mind. It's the visual we have gained from movies and television and while hacks certainly can and do happen in this manner, tapping into your network is not the only way a fraudster can gain a foothold.

A small business' physical property, whether it's a brick and mortar storefront that's open to customers or a manufacturing warehouse with employee-only access, can open the door to fraudsters.

In a storefront that accepts credit card payments, fraudsters sometime utilize devices called skimmers. Skimmers are extremely sophisticated devices that hackers hide on credit card readers, ATMs, gas pumps, etc. for cyber attacks that mirror the exact layout of the machine and read and store credit and debit card information. Some customers have even pulled the skimming device off the top of the machines themselves.

Warehouses and manufacturing plants that use connected machinery and equipment are also potential targets. The culture of bringing your own device (BYOD) and the Internet of Things (IoT) means that everyone from your employees to your vendors expect to be able to connect effortlessly when they need to, whether it be to review delivery status or remotely check inventory.

A small business' physical property can open the door to fraudsters.

This connected equipment can help your employees and service providers perform their duties more efficiently, but it can also leave gaps in your network security. Just like you update your mobile apps and personal devices, you need to update your business equipment to get the latest security software and patches. These updates help fix known security flaws and bugs that could otherwise leave you vulnerable to small business cyber attacks.

Myth #4

Older Systems are Safe from Cyber Fraud

With all the talk of BYOD and IoT, it may seem like the safest course of action is for small businesses to stick to older hardware and software. But just as outdated operating systems can leave security gaps in your personal devices, using outdated hardware and software can leave your small business network vulnerable.

Is your small business using desktop computers, laptops and other hardware that are no longer able to be updated with the latest operating system or application patches? Then your business is at risk. Considering that today's cyber criminals have technology to hack into some of the most complex systems, running your small business on outdated software can make hacking into your network a breeze. While antivirus and cyber security software can't prevent every attack, the latest program updates can add a layer of security which, when paired with other tips in this guide, can help you protect your business.

Keeping your small business hardware and software up to date is one of your first lines of defense against cyber attacks

As long as operating systems and equipment are still supported, companies will generally issue updates and security patches as needed. Keeping all connected equipment up to date is extremely important. Just as you would remove outdated and unsafe products from your shelves, you should maintain your small business' cyber security by safeguarding your system and updating and upgrading when necessary.

Myth #5

Password Protecting a Small Business Wi-Fi Network is Bad for Business

Offering free Wi-Fi access to customers has proven to increase profit and gain customer loyalty. In fact, as many as 62 percent of businesses reported that customers spent more time in their establishment when free Wi-Fi access was available, and 50 percent spent more money while there.

62% of businesses offering free Wi-Fi access reported that customers spent more time in their establishment

50% of consumers spent more money at businesses where free Wi-Fi was offered

Creating a barrier to entry for customers may seem counterintuitive, but opening up your small business Wi-Fi network for anyone and everyone to use can leave your network vulnerable to attack. Customers are accustomed to – and certainly expect – reliability and security, so should their personal information get hacked, it can cost your business and customers money.

Working with a qualified company can lessen cyber security threats and ensure that the network you use for your business operations is not accessible from the network your customers are using. Working with a professional can also ensure all proper firewalls and encryption and protection services are installed correctly. Businesses may also want to consider limiting Wi-Fi access to their hours of operation in order to prevent someone nearby from using the hotspot as their personal network.

Ensure that the network you use for your business operations is not accessible from the network your customers are using

Myth #6

You Can Tell the Moment a Small Business Network has been Breached

Even with the most robust security measures, a security breach or cyber attack can still happen to any business. Unfortunately, most small businesses learn they have been hacked after their customers start complaining of extraneous charges on cards they have recently used at the breached business. Other signs are even easier to dismiss such as web pages failing to load or general sluggishness on the business Wi-Fi network.

Most small businesses learn they have been hacked only after their customers start complaining.

Cyber criminals can be very discrete when hacking into small business networks, but there are some signs you can look out for. Slower than usual network speeds and strange pop-up messages that appear without warning can be indications that someone is maliciously accessing your network. An influx of suspicious emails, especially password reset requests that you did not initiate, should raise red flags as well. This is a maneuver hackers may use to gain easy access to your network and stay there undetected while wreaking havoc to your business.

Detecting a breach as early as possible is paramount to protecting both your business and your customers. Make sure your customers know what types of communication you will use to reach them and collect information. If your business uses email to confirm orders or appointments but your customers report receiving online messages, it's time to take a look at your network. Spotting these subtle changes early on can help prevent serious damage in the event of a cyber attack.

Myth #7

The First Thing to Do after Detecting a Breach is to Alert Your Customers

Honesty is always the best policy, but that doesn't mean that alerting your customers the moment you detect a network breach is the best course of action. In fact, it can cause even more panic and an onslaught of questions that you may not be prepared to answer quite yet.

If you know your business has been breached, the first thing you should do is contact law enforcement and try to contain the breach. You want to get law enforcement involved as soon as possible regarding a recent data breach so that they have fresh information to work with. In some cases, law enforcement may have to let the breach continue to trace it.

If your customers' information was breached, you need to notify them once you have adequate information to explain what happened. There are laws that require businesses to follow certain protocols that vary by state. In the state of Connecticut, businesses are required to notify customers that their personal information has been breached within 90 days unless law enforcement requests that the notification is delayed or if law enforcement determines the cyber attack will not harm the customer.

In the state of Connecticut, businesses are generally required to notify customers that their personal information has been breached within 90 days.

Begin alerting your customers by sending them a written notice, outlining what happened, how it happened, how their data was affected, how you are preventing future attacks and what action they can take. In addition to these actions being required by law, you want your customers to trust you. You may have to take steps to earn their trust back.

You may also want to hire a private cyber forensic firm to investigate the breach. They can look at your network and determine what was lost, when it was lost, how the criminals got into the system, how long they were in your system, if they are still in your system and if they can get back into your system.

Myth #8

There's No Way to Prepare for a Security Breach

Becoming a victim of a cyber security breach is an unnerving and violating feeling. Trying to sort through these emotions while simultaneously dealing with law enforcement and preparing to alert your small business customers can leave you and your business without clear direction. While no two security breaches are the same, you can be ready to react by preparing a crisis response plan.

A cyber security crisis response plan should include:

- Contact information for law enforcement
- Detailed instructions for how to secure your small business data, including any data saved in servers offsite
- Directions for how to respond in the case of a ransomware attack
- A list of people within your organization and at outside firms who should be notified
- Information about products and/or equipment that may be impacted by the breach
- Drafted notifications to be sent to customers, when you are ready
- The names and contact information of the people responsible for each step of the plan

Your crisis response plan needs to be updated regularly based on what is happening and changing in the cyber security world. A plan from 2013, for example, may no longer be sufficient to fully address and resolve a breach that occurs today. Hackers are constantly evolving, so your small business cyber security plan needs to evolve with them.

The best way to make sure your cyber security incident response plan will work when it's needed is to put it to the test. Ensure that the information for your designated point of contact is still valid, and test the speed of response. If anyone listed in your response plan is no longer working for your business, remove their names and contact information and replace them with current employees. The same goes for any outside vendors that assist with network security; if contracts have expired or you are employing a different agency, include current information in an updated plan and test the communication.

If a part of your incident response plan includes sending internal or external alerts, make sure that when you test the alert functionality, you do so on a small control group and give them advance notice. You may also want to test your web alerts after hours as not to raise alarm, and include a message that the alert is for testing purposes only. Other aspects of your plan, such as shutting down access to the internet until the issue is resolved or filing a formal report of a breach, may be more difficult to test on a regular basis, however the series of events should be reviewed for accuracy.

Myth #9

Small Business Employees Don't Need Online Training

To prepare for – and ideally prevent – a cyber security breach before it happens, your small business should have policies and procedures in place. Cyber security policies and procedures dictate how your small business employees conduct themselves in the digital landscape, and they should be reviewed and updated frequently.

Think of your policies and procedures not only as cautionary materials, but as supportive and instructional ones too. They can offer you and your employees guidelines to follow to ensure that everything within your small business is done as securely as possible.

Your small business digital policies and procedures should include:

- Rules about social media usage, emphasizing that employees represent your business both on the premises and off
- A list of employees who have access to your small business data
- How business data is shared and by whom
- Names and contact information for employees responsible for maintaining your website
- How often your employees must change their passwords
- Which personal devices are allowed on the premises
- Which websites and apps are not allowed at your small business
- A process for opening your business at the start of the day and one for closing up

Other policies and procedures may be necessary based on your small business size, type and industry, but these are good places to start. As your company grows and changes, your policies and procedures should too, but do not wait until this happens to review and update them.

Myth #10

There's One Person Responsible for Small Business Cyber Security

This is perhaps the most widespread and dangerous cyber security misconception of all. Assuming that only one person is responsible for small business cyber security can be just as damaging as a full-fledged cyber attack. Without a sense of accountability, it becomes harder to enforce cyber security policies and procedures. And if an attack does occur, employees may not feel responsible for reporting issues because they've identified that as someone else's problem.

The safety and security of your small business network is everyone's responsibility. As we discussed at the start of this guide, knowledge and awareness are the most powerful defenses against cyber attack. Arming your employees with information about how to protect the business and how to act at the first signs of trouble is your best line of defense.

The safety and security of your small business network is everyone's responsibility

If handled correctly, cyber awareness and security awareness training can be an engaging and effective process. To protect your company and avoid unintentionally opening any backdoors to your network for hackers, employee training should include understanding the company policy on the following.

- **General technology use** - Be clear with your employees regarding internet security and what technology they may use on the business network, including what programs and websites they may access and how they may use their personal devices.
- **Password management** – In general, having a complicated password that is stored in an encrypted password vault is better than having simple passwords that are updated regularly.
- **Data handling procedures** – Hackers will sometimes steal files and encrypt them, holding them for ransom, so making backups of important files regularly can save your business a lot of time, money and stress. Store these backups using the 3-2-1 rule. Create 3 copies of all data which include the original and two copies. Make sure to use 2 different media types for the backups. Lastly, store 1 backup offsite in case of a data security breach.
- **Incident response plans** – Make sure your employees know what to do in the event of a cyber attack. This includes knowing who to notify, how to contain the breach and how to prevent future breaches.
- **Social engineering techniques** – Many well-intentioned employees are fooled by hackers using social engineering techniques to gain their trust and use them as a security breach to access the network. Keep your employees informed about the latest social engineering news so they can more easily spot security risks.

Knowledge and awareness are a small business' best line of defense against cyber attack. Breaking down the misconceptions about small business cyber security and empowering your small business team with the right information is a big step toward protecting your business and keeping it running smoothly for years to come.

At Union Savings Bank, we work closely with small businesses and commercial institutions as they make some of their most important decisions. With every loan taken, every business check deposited, and every storefront that has broken ground, we know that protecting your small business is critical – because it's our goal, too.

About Us

We offer one stop for the flexible solutions you need to reach your business goals.

As part of the local business community, we take special pride in being able to offer personal service and customized business banking solutions to area businesses.

Some of our business product offerings to support your business include:

- Business Checking
- Business Lending
- Online and Mobile banking with Bill Pay
- Remote Check Deposit
- Business Credit Cards
- Merchant Services
- And more…

Let us help you grow your business today.

Get Started