cloudnexus

# SMALL BUSINESS SECURITY:

## How To Keep Your Business Safe From Cyber Crime

Table of
# CONTENTS

# INTRODUCTION

We live in a technology-driven world. Technology is an amazing asset to most small businesses today, but at the same time broad technology adoption can also lead to increased cyber crime.

As a small business owner, your livelihood depends on keeping your business safe. This ebook will provide the foundational knowledge you need to protect your business from cyber threats.

At CloudNexus, we understand how devastating it can be for small businesses to experience a cyber threat. Our primary goal is to inform small business owners and give them the tools to protect themselves and their livelihoods.

This is not just a technology view into the things you can do to prevent cyber attacks. Although technology helps, employee readiness training and building standard operating procedures are cornerstones to any cyber security plan.

In this ebook, we'll provide an overview of the top forms of cyber crime, including what makes your small business a target, how to keep your data safe with secure password techniques, and what you can do to protect your business from threats like ransomware.

# CHAPTER 1

## *Cyber Crime 101:*
## 4 Reasons Why Your Small Business Is An Easy Target

Have you had your identity stolen or heard the horror stories of someone you know who had their identity stolen? If you have, you can begin to understand the headache involved to get your money or identity back. You would have to contact your banks, credit card companies, credit bureaus, utility companies and anywhere else that you pay for services. It could take a few months to clear up all of the issues. During that time you won't be able to open new credit cards, take out a mortgage or an auto loan. Basically, your financial life is put on hold until you go through the miles of red tape necessary to get back to normal.

Now, can you imagine if one of your clients called to let you know that their data breach was traced back to your business? Are you liable or open to litigation? Have you violated some compliance standard, such as HIPAA or PCI, and are now open to fines?

"My company is too small for hackers to bother with, there are bigger fish in the sea." might be your stance. Unfortunately, the opposite is true. As a small business, hackers are more likely to be interested in your business and clients for a number of reasons.

Cyber criminals love unsuspecting small businesses. And the unfortunate reality is that many small businesses have already been hacked and don't even know it.

At CloudNexus, we understand how devastating it can be when a small business has been attacked. We don't want you to delay implementing protection steps because you think it won't happen to you.

Let's talk about four common reasons why your small business is an easy target for a cyber attack.

1. NOT HAVING AN I.T. BUDGET LINE ITEM - When small businesses come up with their yearly budgets, little to no money is set aside for cybersecurity. Some small businesses don't think they are large enough to put aside money in the budget. In contrast, others don't even believe that they would be subject to an attack, so it never crosses their mind to budget money for it. Unfortunately, a minimum of 33% of customers leave when a company has a breach of data. It's not difficult to understand why. You are the steward of your clients' data and you broke their trust. Which is more expensive? Spending money on preventative measures or recovering revenue with a damaged reputation?

2. NOT HAVING AN I.T. SECURITY POLICY AND PROCEDURE - Cyber attackers understand that large companies have mature cyber security programs in place. They know how hard they would have to work to get into their systems. Unfortunately, hackers know how easy it is to crack small business networks. With no policy or procedure in place, computers go unpatched, firewall subscriptions lapse, security bulletins regarding your wireless access points go unread, backups go untested, communication plans become outdated, the list goes on. But you are not alone. You have a day job and it is to build widgets or provide services and technology management is an afterthought.

3. STORING IMPORTANT DATA - Hackers know that small businesses keep a lot of essential customer data. This data includes credit card numbers, emails, insurance information, and personal data. What about product designs or patents? Engineering drawings? Sales proposals and bid information? All of this data has value to the right people.

4. **HIGH RETURNS VS. LOW RISK** - The amount of risk associated with hacking a small business is minimal compared to the high return of information gained for the hacker. The fact is, those small businesses that are attacked rarely report them. If they do, the hacker is seldom caught, because attackers can attack from anywhere in the world. There are also many instances where a small business has already been attacked and a bot is sitting on a PC, smartphone or server undetected listening to your network and sending that traffic back "home" to bad-guy HQ.

If any of these situations apply to you, it's time to take a second look at your business and implement steps to protect yourself and your clients.

# CHAPTER 2

## *Passwords:*
## The Easiest Target

So let's start with the weakest link. Employees. This is not out of malice but from not knowing any better. An employee's job is to work effectively and efficiently and to many employees, steps like entering a password or asking permission to access a file or directory are just impediments to them doing a good job for you. So they do things like writing simple passwords down on sticky notes and stick them to their monitors or ask and receive administrator rights so they can get to files that they cannot currently anticipate a need for, but maybe someday....

Employees also use passwords that they might use at home for their work computers. If their GMail account gets hacked, it is hacker common practice to try the same password for other accounts, work or otherwise. Many of these passwords can also be easily guessed and they change infrequently.

Because passwords are the easiest target for hackers, it is also the quickest way to raise your security profile. With proper passwords in place and a good password expiration policy, your data has a greater chance to remain secure from potential cyber attackers.

In this chapter, we will discuss easy methods you can use to create secure passwords for your business.

**FIRST, A GENERAL RULE:** NEVER use any public information in your password or security question.

Anything that you've answered on social media quizzes or senior yearbook pictures is off-limits when it comes to creating a secure password for your business. With a simple Google search, a potential hacker can find a lot of information about you, and it's best to avoid giving them anything they can use to predict your password.

If you are like 70% of users, a hacker can guess your password or the answer to your security question using your high school, favorite sports team, pet names and kids' birth dates within an hour or so.

To create a secure password, it must be derived from something only you know.

What is NOT something only you know:

1. Dates: anniversaries, birthdays, etc. (Your spouse, kids or friends know these dates. They can post happy birthday or anniversary messages on your wall. Your kids can post their birthdays in one of their social media accounts or post pictures from a birthday party, senior prom, etc.)
2. Favorite sports team
3. Cars you have owned
4. Pets and their names
5. Previous addresses

You get the idea. These items should never be considered for a password or security question. Other people may know them and can inadvertently expose it. With little effort, they can be linked back to you.

There are challenges here though. Many financial institutions use auto loan details or mortgage details to verify that you are who you claim to be.

### SO WHAT SHOULD YOU DO?

The best passwords are 18 to 24 characters (64 is ideal). You can use a password manager like LastPass or PassPortal to manage passwords and generate complex passwords that you don't have to remember. But if you want to create your own, the best practice is to mix upper case, lower case, numbers and special characters. Make the password very obscure but at the same time very familiar and easy to remember for you and only you.

**EXAMPLE:** maybe your fondest childhood memory is of Kermit the Frog. Look for a song by Kermit and take the first letter of each word in the lyric with a few random characters.

> *"It's not that easy being green, having to spend each day the color of leaves when I think it can be nicer."*
>
> !^t3BGh2s3Dtc0Lw1ticB^
>
> ! Used as "I" upper i 1 used as "l" lower L ^ used as "n"
> 3 used as "e"
> 2 used as "to"
> 0 used as "o"

Think of passwords as a secret code. You will find that as you recite the lyrics, you will more easily remember your password as you type it.

Never use the same password twice. Come up with a phrase that you can use that will be easy to remember but still be cryptic.

**Phrase:** Mom likes to get her (***) at Walmart.

So your online passwords could be:

**For Walmart:** Ml2gh(C)@WLMrt
**For Kroger:** Ml2gh(G)@K
**For Walgreens:** Ml2gh(M)@WlGrns

Try not to be too patterned! Reciting common phrases while typing the first letter of each word with a symbol or number that looks like the letter gives you a nice cryptic password and it is a lot easier than it looks. After the first few times, you will get used to it.

Be aware of what financial institutions ask you for security questions. Do not provide a security question that you might have posted about or that somebody else knows.

Don't be afraid of posting high school class year or what high school you went to as long as you don't make it a habit of including that information in any passwords.

In this day and age, we all have to be more diligent. A lot of these password guesses are now built into dictionary files that hackers use in brute force attacks with what's called a Dictionary Crack.

It's not some individual trying to get your information now. It is an automated program probing banks and other websites for your account information. Ask your marketing people how much information is gathered about you every day that is sold to the highest bidder. Well, the bad guys have databases too.

Now that we know how to create secure passwords, here is a list of things you can do today around passwords that will raise the bar even further.

1. Secure passwords as described above.

2. Create a password policy that forces a password change with the correct complexity level every 60 days at least.

3. Train employees to not use yellow stickers for password management. A trick I used at a previous company to help motivate employees was to logon to their computer from the password on the yellow sticky and send an email on their behalf to their colleagues stating that "I'm bringing donuts on Monday!"

4. Clean up! On a regular basis make sure you disable or remove accounts of employees that are no longer working for you.

5. Create a policy for employees stating that accounts are never to be shared and enforce it.

This first step in keeping your small business safe from hackers and other cyber crime can be implemented quickly and at little to no cost. Use these password techniques in your business and in your personal life to keep your information secure!

# CHAPTER 3

## *Ransomware:*
## Don't Let Your Small Business Be Held For Ransom

If you're like most entrepreneurs, your small business is like a member of your family. You love it, you work hard for it, and you want to protect it. Unfortunately, hackers love the idea of entrepreneurship too, and they would love nothing more than to hold your small business hostage.

In this chapter, we are going to answer small business owners' most commonly asked questions about ransomware.

### WHAT IS RANSOMWARE?

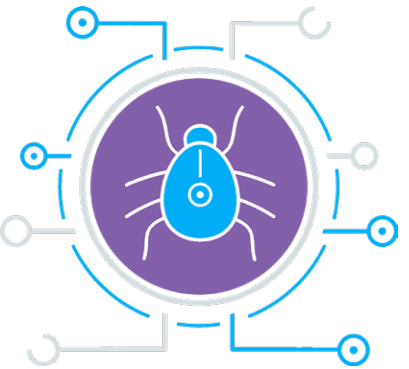
It's a malware that encrypts your company files. In order to get access to your information again, hackers ask for a fee in return for a key code that unlocks the stolen information.

### HOW MUCH CAN RANSOMWARE COST A SMALL BUSINESS?

It can cost a small business anywhere from hundreds to tens of thousands of dollars.

### DO CRIMINALS ACCEPT CREDIT CARD PAYMENTS?

No, but they do accept bitcoin.



### HOW EXACTLY DOES RANSOMWARE WORK?

There are a number of ways that ransomware can hit your computer, but these are a few common ways:

- **Phishing** - A file or link is sent to your email that looks like a something you can trust.
- **Social Engineering** - Bad actors use various types of communication such as email or phone calls to convince a computer user into providing access to their system.
- **Malware** - No tricking necessary with this software - it just needs weak security features on a computer to install itself.
- **Doxware** - A ransomware software that holds sensitive data hostage. The bad actors threaten to release sensitive data, photos or conversations unless the ransom is paid. Basically it is electronic blackmail.

### HOW WILL YOU KNOW IF YOU HAVE A COMPUTER THAT HAS BEEN ATTACKED BY RANSOMWARE?

Usually, the end-user gets a pop-up message when they open an encrypted file on their screen, which states that the mathematical key won't be released until they send untraceable bitcoin.

### WHY WOULD THEY CHOOSE YOUR SMALL BUSINESS TO ATTACK?

The short answer: opportunity.

- **Small Security Teams** - Hackers look for small businesses that either can't afford or refuse to pay for "big" security.
- **Quick payment** - Depending on the field you are in, you may not want sensitive data out there long, or you can not do your work without the data. Either way, you are more of a target.
- **Opportunity** - Ransomware can be automated. Many hackers bide their time until their programs find a company with low security and are able to break in without manual intervention.

It is important to understand that paying the ransom does not always result in the safe un-encryption or return of your data. The FBI estimates that 50% of the time, the hackers just take their money and disappear. For that and many more reasons, it is always better (and cheaper) to prevent an attack than it is to pick up the pieces afterwards.

So how do we prevent ransomware? There are a lot of ways and most do cost money. This is not an exhaustive list, but they are the low hanging fruit in fighting ransomware attacks.

1. Antivirus and anti-malware subscriptions. Get the licensed versions from a reputable provider. Forgetting to download the latest signature files in the free version is a common reason for infection.

2. A good next generation firewall that is configured properly. Don't use consumer grade firewalls and wireless routers here. Security is not as good and updates are slow to come by. Also, have it professionally configured. No sense in spending the money on a good firewall and then poke holes in it with improper setup.

3. A good backup and disaster recovery solution. There are several out there that can take snapshots of your data as frequently as every 15 minutes. In the event of an infection, you can recover the encrypted files from a backup that occurred prior to the infection. Some of these solutions will allow you to actually run your entire server on the backup device if the computer is destroyed because of the infection. Again, it is important to have this properly configured as many ransomware also try to locate and infect the backup files too. Consult an expert to help you select the best solution for your needs. There are a lot of backup technologies out there and they all do not function the same way.

# FINAL THOUGHTS

In today's technology-driven world, it can seem overwhelming to keep track of all the ways you need to keep your small business safe from cyber threats. Here at CloudNexus, we are committed to helping small business owners like you focus on your business and not on IT. We offer the tools and services you need to keep your small business safe from cyber threats (seen and unseen) that come your way.

If you think your business is at risk of a cyber threat, contact us for a FREE cyber-security analysis. We will walk you through any potential threats and help you address them. It could be the difference between keeping your business open for years or closing because your business was vulnerable to a cyber threat.

For a **FREE** cyber-security analysis,
call us at **502-440-1380** or visit
our website at **www.CloudNexusIT.com**.