

*A quick guide to*

# SECURITY PROTECTION FOR SMBs



**VISUAL  
EDGE IT™**  

---

**SECURE TECHNOLOGY SOLUTIONS**

*See what your technology can do.*

[www.visualedgeit.com](http://www.visualedgeit.com)

# Introduction

Protecting your assets is one of your key responsibilities as a business owner or manager. Threats exist in many different forms, so taking the measures necessary to protect your interests is a good practice. It's not about living in fear or assuming everything will go wrong. Rather, it's about logically identifying potential threats and taking steps to reduce or eliminate the risk associated with those threats.

This concept applies perfectly to the matter of ransomware. Any business that has an online presence—which is nearly every business at this point—needs to consider the importance of cybersecurity. Taking some basic steps toward securing your online operations will go a long way toward avoiding an expensive and frustrating event in the future.

While this topic is important for the health of your business, it should not dominate your thoughts each day. Instead, take the time to create a plan that makes sense for your needs, and then move on with confidence. The information below should help you understand what threats exist and how they can be effectively mitigated. This white paper will answer the following questions:

- **What Is Ransomware?**
- **Why Is It a Threat?**
- **How Do Ransomware Attacks Work?**
- **Why Is Cybersecurity More Important Than Ever?**
- **What Are Some Cybersecurity Best Practices for Businesses?**
- **Why Should You Work with a Data Security Provider?**



# What Is Ransomware?

Before we dive too far into the protection side of things, let's back up for a moment and talk about ransomware. If you are fortunate enough to have avoided a cybersecurity attack to this point, you might not know exactly what ransomware is and why it is a threat to businesses.

As the name would suggest, ransomware is software that is used with the goal of extracting a ransom payment from the targeted business (or individual). While the details can get very technical, the basic concept is that unwanted software is placed on your computer to lock everything up and render the system unusable. Then, a request for payment is made, with the promise of removing the ransomware once the money is paid.



Ransomware can take many different forms, and the threats that are made will vary from case to case. If an individual is targeted, the criminal may threaten to publish important or embarrassing personal information. In the case of a business, the approach is usually to hold the system and data hostage to bring operations to a halt.

*More than  
300 million  
ransomware  
attacks were  
attempted  
in 2020.*

**SOURCE: STATISTA**

## **Is this a real threat?**

While the idea of some far-off hacker infiltrating your computer system might seem like something out of a movie, it is a real threat that every business should address. In 2020 alone, it is estimated that more than 300 million ransomware attacks were attempted. Given the scale of this threat, it is worth your time and attention to establish a proactive plan for prevention.

Targets for a ransomware attack are sometimes chosen intentionally, while in other cases the targeting is random. Whether your specific industry is identified as one that often has cybersecurity weaknesses, or you just so happen to become a victim as a result of a bulk phishing effort, the result is the same—you'll need to have a plan in place to fend off the attack or recover from it.

# Is It a Threat to Your Business?

While it's important to understand the harsh truth that ransomware attacks do happen to businesses of all kinds, we want to assure you that your business isn't destined for an attack. But it's always in your company's best interest to stay ahead of the game and proactively protect your data. Think of it like changing the oil in your car. Taking a small step every 5,000 miles helps you avoid much larger, more costly fixes in the future. But as small of a step as it is, it's something that, if ignored, can wreak havoc on your engine.

Answering these questions will give you a quick idea of whether or not your data is secure or in need of some protection updates.

Are you...

- Securing your remote workforce properly?
- Following cybersecurity best practices and maintaining compliance?
- Improving your company's cyber resilience with layered security?
- Running phishing simulation training at least quarterly?
- Making security awareness training mandatory?
- Reducing your access points with single sign-on (SSO)?
- Using multi-factor authentication to keep hackers out?
- Utilizing secure and shared password vaults for sensitive credentials?
- Watching for dark web credential compromise surprises?

Answering these questions will give you a quick idea of whether or not your data is secure or in need of some protection updates.

## Cyber security in a post-pandemic world

The COVID-19 pandemic has seemingly encouraged an uptick in ransomware attacks. In fact, tech experts are calling this swift increase in cyber attacks a pandemic in its own right. VMware Carbon Black saw a 148% increase in ransomware attacks in March 2020 over baseline levels in February 2020. Sources suggest that at the start of the pandemic, hackers were taking advantage of a very vulnerable and unsettled population of people hungry for news updates on COVID-19.

*The pandemic has seemingly encouraged an uptick in ransomware attacks—a 148% increase in March 2020 over February 2020.*

SOURCE: TECHTARGET

While that specific kind of vulnerability may be behind us, new work-from-home environments could open up your team to the possibility of a cyber attack. When you can't ensure all team members have a private, secure network at home, you can ensure that your entire office has expert ransomware protection and proper cybersecurity measures in place.

# How Do Ransomware Attacks Gain Access to Your Computers?

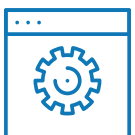
Running a business in the 21st century requires a sufficient level of technical acumen. You likely have a website for your business, use various software products to manage your operations, and more. However, most business owners and managers aren't knowledgeable enough in the tech world to fully understand how cyberattacks work and what it is that makes a system vulnerable.

One of the best ways to keep your systems secure is to have a basic understanding of what hackers are looking for when trying to execute a ransomware attack. It's not necessary to become an IT expert just to keep your system safe but knowing how this form of extortion works is a big help.



## Email links or attachments

Unsolicited emails have long been a common tactic for hackers to gain access to computer systems. An email is sent – usually to a huge list of addresses – that contains either an attachment or a link to a malicious website. If the attachment is downloaded or the link is visited, ransomware may be placed on the computer. These email attacks have gotten more and more sophisticated over the years, using techniques like cloaking the “From” address to make the email appear as though it is coming from someone you know or a business you trust.



## Out-of-date software

In addition to enticing computer users to click on malicious links or attachments, another approach is to target software that hasn't been updated. The updates that are frequently released for pieces of software and for computer operating systems often have to do with security holes. Once a hole is identified, a patch is developed and released to users. If the end-user fails to install that update, the hole remains, and it can be used by hackers for purposes like ransomware. The longer a hole is allowed to exist within a system, the more likely it is that a successful attack will occur.



## Compromised credentials

Sometimes, the easiest way into a computer system for a hacker is through the front door. If the hacker can gain access to a username and password, the system can be accessed directly, and malicious software can quickly and easily be placed. This type of access can be particularly damaging because there will be very little limit to the damage that can be done when using authentic credentials to get in. If usernames are known, the hacker may be able to guess the password using bulk lists of common passwords, or the password may be available on the dark web from a previous data breach

There is no end to the creativity of the criminals who execute ransomware attacks. The evolution of ransomware as a criminal act is sure to continue, so the best thing you can do as a small or medium-sized businesses owner or manager is stay up to date with the best available practices for prevention.

# Cybersecurity Goals & Best Practices for SMBs

## Goals

When it comes to ransomware, there are two main goals for businesses:

**PREVENT.** Prevent the placement of ransomware on the computer system.

**RESTORE.** If ransomware is placed, there should be a way to restore the system without making a payment to the criminals.

Those two goals will guide the decisions you make when establishing a cybersecurity plan for your business. Taking steps to stop hackers from accessing your system in the first place is a good start. Then, for another layer of protection, you'll want to have a way to get back up and running without making a ransom payment.

## Best Practices

Fortunately, by following some cybersecurity best practices for small- and medium-sized businesses, we can greatly reduce the chances that your business will be harmed in any meaningful way by this type of attack.

**KEEP EVERYTHING UP TO DATE.** Running system updates regularly is an essential piece of cybersecurity. This might seem like an easy one, but many people and businesses get into the habit of skipping updates just because they don't want to deal with the few minutes of downtime required to boot up the new version of the operating system or software program.

Get into the habit of automatically running updates when they come out or set your systems to take care of them overnight when they won't be an inconvenience. Simply keeping all business software current will go a long way toward limiting the options hackers have available when trying to get into your system.

**BE WARY OF UNSOLICITED EMAILS.** As mentioned earlier, phishing emails are a classic tool used by criminals to get into your computer. While you might be familiar with this issue, don't assume that everyone in your business knows what to look for or why to be wary. Take the time to educate your entire team on how to deal with emails that come from unknown or suspicious senders.



The best course of action when you aren't sure about an email is simply to delete it. It's better to be safe than sorry in this case. If the message looks like it might come from someone you know, but it still looks suspicious, contact that person through another means (not a reply email) to confirm that they sent the message. Legitimate businesses never ask for personal details like passwords through emails, so always disregard such requests.

**CUT DOWN ON LEGITIMATE ACCESS.** The more people that have access to your system, the more vulnerable that system will be. Of course, to run a business, you probably have to grant access to most of your employees in one form or another, but make sure they only have access to what they need in order to work. Don't give everyone unrestricted access to your entire system. Instead, put limits on permissions to tighten up your security.

Also, always remember to remove credentials for anyone who is no longer working for your business. Even if that person has no ill intentions, keeping their credentials active serves no purpose and leaves open one more potential hole for criminal access and ransomware.

**REGULAR BACKUPS.** Keeping regular backups of all your digital assets is a huge part of the battle against ransomware. If ransomware is successfully placed on your system, you shouldn't need to pay that ransom to get back up and running. Instead, you can turn to one of your backups to restore the system and get back to business as usual right away.

In addition to serving your business well for ransomware issues, backups are a great idea for many other reasons. Computer systems can fail as the result of technical glitches or other issues, so having data backups is important for that possibility, as well. Setting up a system to take backups and store them off your server is relatively quick and easy, and it's a decision that will pay off in a big way down the line.

The four points above touch on some of the key cornerstones for a ransomware best practices plan. Other points worth considering include limiting the ways your system can be connected to the internet (avoiding public Wi-Fi, for example), using firewalls, and installing scanning software to watch for threats. No cybersecurity plan is 100% foolproof, but taking the basic steps toward security will make you a more difficult target for hackers. They may just move on to the next business instead of working harder to get into your system.

*No cybersecurity plan is 100% foolproof, but taking the basic steps toward security will make you a more difficult target for hackers.*

# Here's Why You Should Work with a Data Security Provider...



Trying to set all of this up on your own can be a big challenge. Even if you are comfortable with technology and know your way around a computer, there are technical details that you want to make sure are set up just right. Also, you have enough on your plate while running a business, so you don't need to take up even more of your time by trying to manage cybersecurity on your own.

A data security provider is going to offer many benefits on this front.

- First, the task will be taken off your plate, and the service will likely cost much less than you may expect.
- It will also be easier to keep your security plan up to date when you have a team of professionals in charge of this part of your business.
- As new threats come into play, your security provider can respond with the appropriate measures to keep everything secure.

## **Avoid downtime & strengthen your recovery plan**

Fortunately, by following some cybersecurity best practices for small- and medium-sized businesses, we can greatly reduce the chances that your business will be harmed in any meaningful way by this type of attack.

“I'll just pay the money; it will probably cost about the same as all the protection you want me to buy.” While we certainly understand this common train of thought, we encourage you to think about the other potential risks and costs involved with a cybersecurity attack on your business:

- Can you ensure your data wasn't corrupted or tampered with?
- Are you confident the attackers didn't make copies of your data?
- Have you taken steps to ensure the attacker doesn't just attack again for another payment?

In reality, the actual ransom payment may be the least of the incident response costs. Protection from Visual Edge IT™ ensures your company's security while reducing the risk of costly downtime and recovery.

# What You Get from Visual Edge IT™

Working with a reliable partner to secure your digital assets is the easiest way to manage this side of your business. There is no need to develop advanced technical knowledge in-house when you can work with the expert team at Visual Edge IT to handle this issue with ease.

Visual Edge IT provides full-service IT management, including 24/7 remote monitoring and administration of networks, service desk, and data backup and restore. Backed by local service and a national network of engineers, Visual Edge IT is uniquely positioned to support managed IT and print services, IT hardware and software, and communication and data needs.

Visual Edge IT ensures your company's security while reducing the risk of costly downtime and recovery. You'll get:



**Antivirus,  
ransomware &  
hacker protection**



**24/7 remote  
monitoring**



**Proactive  
management &  
problem resolution**



**Unlimited (8am–  
5pm) service desk  
remote end user  
support services**

If you are a current print management customer, we will be happy to offer an assessment of your backup system at no cost. We'll even provide some advice on how that system can be strengthened to fortify your digital assets against attack. We look forward to working with you.



# **VISUAL EDGE IT**<sup>TM</sup>

*SECURE TECHNOLOGY SOLUTIONS*

6050 Corporate Way  
Indianapolis, IN 46278  
**(866) 863-2266**

**learnmore@visualedgeit.com**  
**www.visualedgeit.com**  
**@visualedgeit**