

YOUR RANSOMWARE

SURVIVAL GUIDE



TABLE OF CONTENTS

What is Ransomware?

PAGE 1

Most Popular Ransomware Entry Points

PAGE 2

Emerging Ransomware Trends

PAGE 3

The Impact of a Ransomware Attack

PAGE 4

**Best Practices to Protect Your Business from
Ransomware**

PAGE 5

How To Respond to a Ransomware Attack

PAGE 6



What Is Ransomware?

Ransomware is a type of malware that locks or encrypts a victim's data, rendering it inaccessible. Cybercriminals then demand a ransom, usually in cryptocurrency, to restore access. Refusing to pay doesn't guarantee safety—attackers might delete or publish the data, further compounding the damage.

These attacks are rising at an alarming rate, generating massive profits for cybercriminals while causing severe disruption to businesses and government agencies alike. Ransomware groups are constantly evolving their tactics, finding new methods to extort victims. As long as organizations continue to pay, these attacks will only grow. To defend against this threat, businesses need a strong cybersecurity strategy that reduces risk, limits damage, and ensures a swift recovery if systems are compromised.



Most Popular Ransomware Entry Points

Understanding how ransomware attacks work—and the methods cybercriminals use to deliver them—can help reduce your risk of becoming a target. Below are some of the most common attack vectors used to spread ransomware:

Email Phishing: Phishing emails use social engineering to trick recipients into clicking malicious links or attachments. Once clicked, attackers can gain access to networks, steal login credentials, harvest sensitive data like PII, or compromise trade secrets.

Unsecured RDP Ports: Remote Desktop Protocol (RDP) ports left exposed are a goldmine for hackers. By scanning networks for open ports, attackers can infiltrate servers, take control of systems, steal credentials, or deploy malware directly.

Software & Patch Vulnerabilities: Outdated or unpatched software often contains flaws that criminals exploit to infiltrate systems. A single vulnerability can lead to data breaches, operational shutdowns, and costly recovery efforts.

Malicious Websites: Fraudulent websites are designed to look legitimate but deliver ransomware or steal sensitive information. Cybercriminals often pair these fake sites with phishing emails to lure victims into clicking.

Pop-Ups & Malvertising: Adware or malicious ads can trigger pop-ups that infect devices when clicked. These threats often sneak in through compromised email attachments or hidden links, opening the door to further attacks.



Emerging Ransomware Trends

Ransomware groups are constantly evolving their tactics, adapting to new technologies and stronger defenses. Below are some of the most prominent methods cybercriminals and their affiliates are currently using:

Supply Chain Attacks

Instead of targeting a single company, attackers exploit weak points in the supply chain, allowing them to compromise an entire network of partners, vendors, and customers at once.

Double Extortion

Cybercriminals don't just encrypt files—they also steal sensitive data and threaten to release it publicly if the ransom isn't paid, putting additional pressure on victims.

Ransomware-as-a-Service (RaaS)

With RaaS, hackers can “rent” ransomware through subscription-based platforms that provide ready-to-use attack tools, lowering the barrier to entry for less skilled criminals.

Targeting Small and Midsize Businesses

To avoid law enforcement crackdowns tied to high-profile cases, many cyber gangs are shifting focus to SMBs, seeing them as easier, less conspicuous targets.



The Impact of a Ransomware Attack

A successful ransomware attack can have severe and far-reaching consequences for your business, including;

Extended Downtime

Whether or not you pay the ransom, ransomware can halt operations for hours, days, or even weeks. This downtime often leads to missed revenue opportunities, production delays, and service interruptions.

Data and Resource Loss

Without reliable backups, critical files may be lost permanently. On top of that, businesses often face costs from lost employee productivity and the need to wipe and rebuild compromised devices like laptops, desktops, and servers.

Additional Recovery Costs

From IT labor to data recovery services and hardware replacements, the expenses of restoring operations after an attack can quickly escalate.

Reputation Damage & Customer Loss

A breach can erode customer trust and harm your brand's reputation. If sensitive client data is exposed, it can be even harder to retain existing customers or attract new ones.

Regulatory Fines & Legal Liabilities

If customer data is compromised, your business may face hefty fines or be required to compensate affected clients, resulting in substantial financial strain.



Best Practices to Protect Your Business from Ransomware

The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following steps to help safeguard against today's evolving ransomware threats:

Keep Systems Updated

Outdated software and operating systems leave openings for attackers. Regularly apply patches and updates to close vulnerabilities before hackers can exploit them.

Be Wary of Phishing Emails

Phishing remains one of the most common ransomware delivery methods. Avoid clicking links or opening attachments in unsolicited or suspicious emails.

Secure Your Backups

Store backups offline and verify they are free of malware. This ensures you can restore your data quickly if systems are compromised.

Train Employees on Cyber Hygiene

Employees are your first line of defense. Educate them on safe browsing habits, secure remote connections, and best practices to reduce risks.



How To Respond to a Ransomware Attack

With ransomware attacks becoming more frequent and more damaging, it's critical to have a clear response plan in place. According to the U.S. Secret Service, here are key best practices to follow if your business falls victim to an attack:

Identify Compromised Systems:

- » Determine which systems have been affected and the attack vector used to gain access.

Assess the Infection: Document the infection status, your network topology, and note any virtual currency addresses provided for ransom payment.

- »

Do Not Power Down Systems: Avoid shutting down infected devices, as this may destroy valuable forensic evidence.

- »

Isolate the Threat: Disconnect the infected devices and compromised areas of the network immediately to prevent further spread.

- »

Check for Dropped Files or Memory Captures:

- » Investigate whether any suspicious files were left behind or memory captures were taken that could indicate deeper compromise.

Secure Accounts & Logs: Change online account and network passwords right away. Collect all available log information for analysis.

- »

Review Network Activity: Check for any domains or IP addresses that were contacted before the attack began.

- »

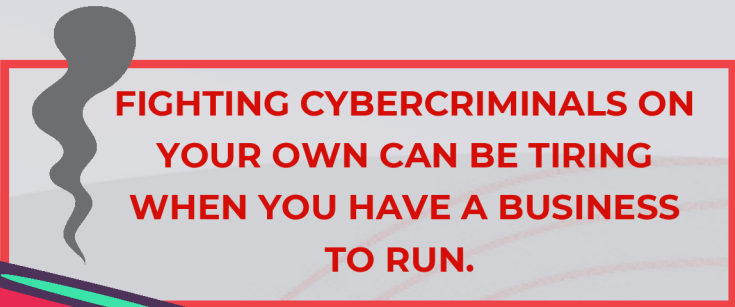
Recover Data Safely: Use the oldest clean backup to restore files and ensure it is free from malware before redeployment.

- »

Use Out-of-Band Communication: Rely on secure, external communication channels rather than the potentially compromised internal network.

- »

Every business is equally at risk of ransomware. The real question is: if it happens to you, will you be able to recover?



FIGHTING CYBERCRIMINALS ON YOUR OWN CAN BE TIRING WHEN YOU HAVE A BUSINESS TO RUN.





Let's Stay in Touch 🚀

Follow us on social media (@tekiegeek) for updates, insights, and tips on staying safe online.



Learn how ransomware works and how to protect your business—contact us today!

📞 **Phone: 347-830-7322**

4218 Amboy Road Staten Island, NY 10308