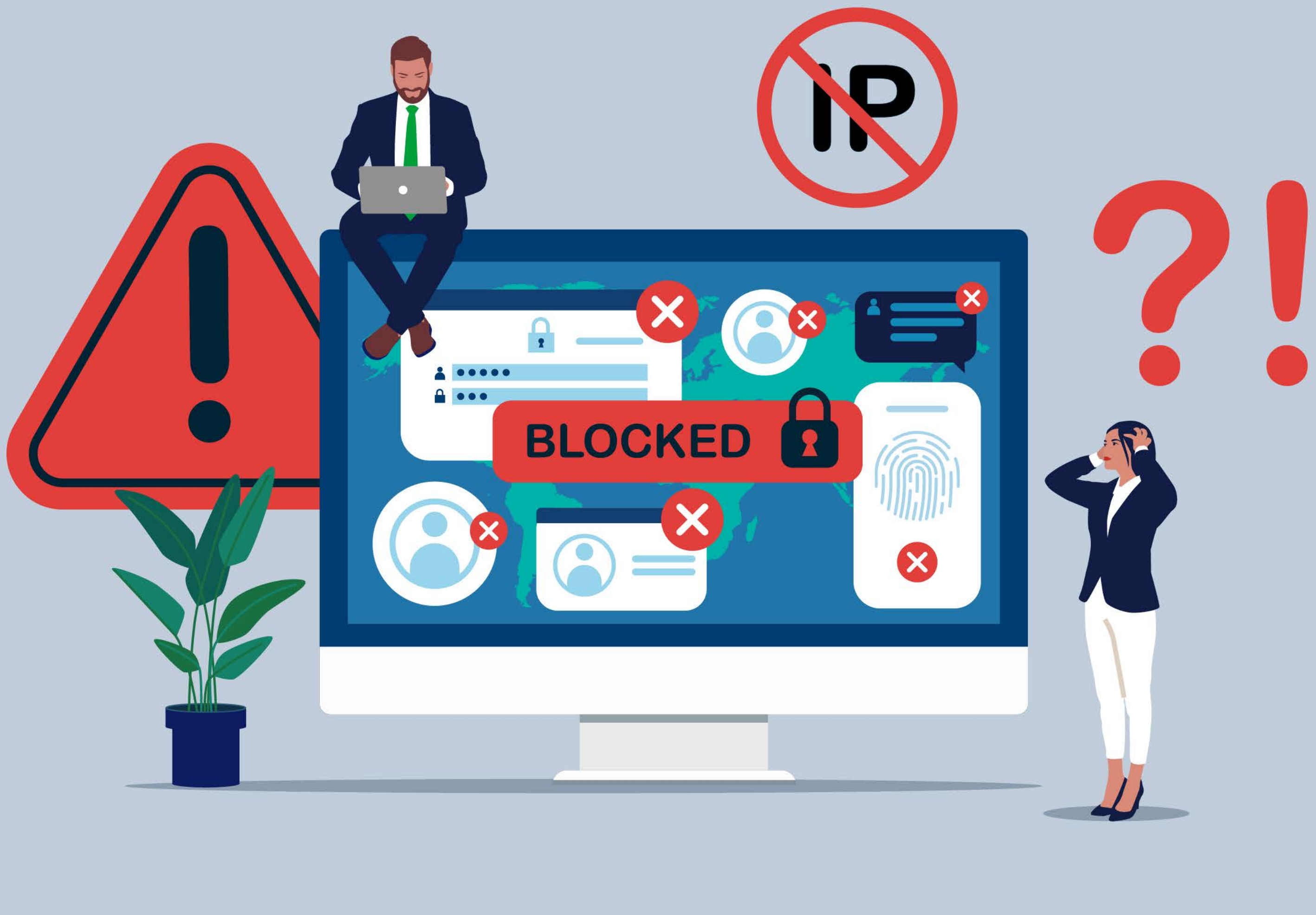
RANSOMWARE

A Proactive Preparation Guide



teal

RANSOMWARE

A Proactive Preparation Guide

Table of Contents

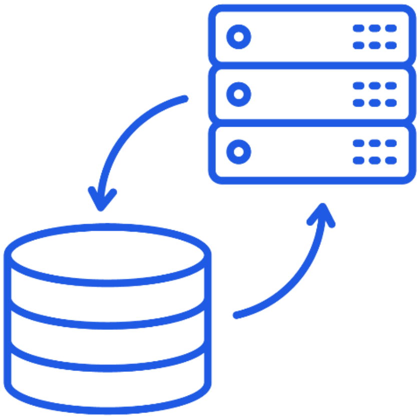
Our highly trained cybersecurity experts have many years of experience and offer their insights to help you safeguard your organization against rising ransomware threats.

This guide will provide you with actionable steps to help protect your business from the damaging effects of a ransomware attack. It contains best practices for employee training, data backup strategies, and cybersecurity measures to implement on business devices and networks.

At the end, you can develop a plan to prevent, detect, and respond to ransomware attacks – helping you protect your data and systems from harm.

Step 1. Regularly Back Up Important Data

Ransomware attacks are so effective and frightening because you can't afford to lose your data. That's why backups are a vital component in protecting against them.



Possessing recent backups of your data gives you the ability to restore your systems and data without having to pay a ransom. It also helps your business avoid the loss of critical information. For example, suppose you lose customer data or financial records due to a ransomware attack. In that case, you can recover that data with recent backups.

Implement a backup strategy that includes regular backups and storing them securely, preferably offsite or in the cloud. Ensure employees understand that it's essential to maintain at least one extra copy of important files stored in a different location. Cloud backup services are excellent for this because they are cost-effective, easy to deploy, and familiar to most employees.

Additionally, test backups regularly to ensure they are working so they are in place should you experience an attack. Regularly backing up your data can significantly minimize the impact of a ransomware attack and protect your critical information.

Step 2. Control User Access

Small organizations where everyone knows everyone else often hand out administrator privileges like candy on Halloween. That should not be the case because it dramatically increases the risk of attackers gaining access to critical systems and sensitive data.

Instead, organizations should give users the minimum privileges needed to do their jobs and raise them only when necessary. Consider these user access controls to help protect your business against ransomware attacks:

Restricting administrative access: Limiting administrative access can help prevent ransomware from spreading throughout a business's network. If a user's account is compromised, limiting their permissions can prevent the attacker from accessing and encrypting critical files and systems.

Implementing least privilege: Implementing the principle of least privilege, which means granting users the minimum level of access necessary to perform their job functions, can help limit the spread of ransomware. If a user cannot access a critical file or system, the ransomware cannot encrypt it.

Using multi-factor authentication (MFA): MFA can help prevent unauthorized access to a user's account, making it more difficult for attackers to compromise their account and spread ransomware.

Educating employees: Educating employees on how to recognize and avoid phishing emails and suspicious websites can help prevent the initial ransomware infection. Employees should also know how to report suspicious activity to their IT department.

By limiting user permissions and implementing multi-factor authentication, businesses can prevent the spread of ransomware and minimize the impact of an attack.

Step 3. Use Email Spam Filtering

Ransomware attacks typically start with spam messages because they make it possible for cybercriminals to target thousands of unsuspecting victims with minimal effort. Carefully crafted spam messages that target a specific victim are challenging to catch; however, most can be blocked using an email spam filter.

Email spam filtering analyzes incoming emails and blocks identified spam or phishing attempts. This filtering can help prevent ransomware attacks from ever reaching a user's inbox, reducing the risk of infection.

The following are some of the ways email spam filtering can help protect against ransomware attacks:

Identifying malicious emails: Email spam filtering can help identify and block emails that contain malicious links or attachments, commonly used to deliver ransomware.

Enhancing email security: Spam filtering can help improve email security by preventing unauthorized access to email accounts and reducing the risk of phishing attacks.

Reducing the attack surface: Email spam filtering can reduce the attack surface of a business by preventing malicious emails from reaching users, which can help prevent the spread of ransomware throughout a business's network.

Using spam filtering is an essential step in protecting against ransomware attacks. Such filters are available from many different vendors and serve as an excellent first line of defense against ransomware.

Step 4. Cybersecurity Training

One of the most important things any organization can do to protect its employees against ransomware is to teach them about cybersecurity. This training is important because employees are often the first line of defense against cyber threats. Ransomware attacks often rely on human error, such as clicking on a malicious link or downloading an infected attachment, to infect a computer or network. By educating employees on best cybersecurity practices, businesses can:

Reduce the Risk of Infection

By teaching employees about the dangers of phishing emails, and other types of cyber threats, businesses can reduce the risk of a successful ransomware attack. Employees trained to recognize and avoid suspicious emails and websites are less likely to inadvertently infect their computers or network with ransomware. Employees should understand how strong passwords, timely patching, regular backups, cautious web browsing/emailing, and other best practices help protect against them.

Improve Incident Response

Employees trained in incident response procedures can help minimize the impact of a ransomware attack. They can quickly report any suspicious activity to their IT department, which can help contain the attack and prevent it from spreading.

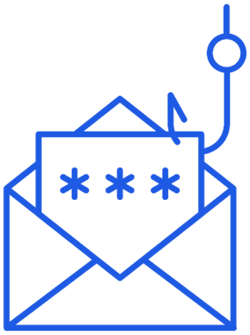
Enhance Overall Cybersecurity

By educating employees on best cybersecurity practices, businesses can create a culture of cybersecurity awareness. This practice can promote good cybersecurity habits among employees and enhance overall cybersecurity.

Meet Compliance Requirements

Many industries have compliance requirements related to cybersecurity training. By educating employees on cybersecurity best practices, businesses can meet these requirements and avoid potential fines or penalties.

Step 5. Simulated Phishing Attacks



Teal believes employee training should combine theory with practice through simulated phishing attacks. Simulated phishing attacks involve sending fake phishing emails to employees to see how they respond. These emails are designed to look like real phishing emails. However, instead of leading to a malicious website or downloading malware, they lead to a landing page that educates the employee on recognizing and avoiding phishing emails.

Such attacks serve two different but equally important purposes. First, they provide valuable feedback about the effectiveness of employee training and identify areas for improvement. Second, they allow employees to experience life-like threats without suffering real consequences.

Simulated phishing attacks are a vital tool in reducing the risk of a successful ransomware attack and minimizing the impact of an attack if it does occur.

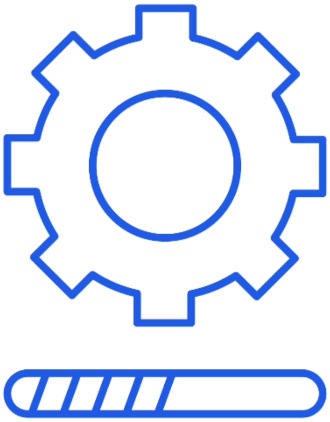
Step 6. Keep Software Up to Date

Cybercriminals are constantly trying to exploit software vulnerabilities to distribute ransomware. Businesses need to understand the importance of timely patching and avoid having outdated software on their work devices.

Software vulnerabilities are flaws or weaknesses in software code that cybercriminals can exploit to gain unauthorized access to a system or network. Ransomware attacks often rely on these vulnerabilities to infect devices and encrypt files, making them inaccessible to the business.

Patching is critical regarding security software because over 350,000 new malicious programs and potentially unwanted applications are registered daily.

By keeping software on business devices up to date, you can reduce the risk of a successful ransomware attack and minimize the impact of an attack should one occur.



Step 7. Disable Commonly Exploited Features

There are several features commonly exploited by ransomware creators to infect devices that most employees don't need, at least not regularly. Such features include Microsoft Office macros, Remote Desktop Protocol (RDP), or autorun.

Disabling these features won't negatively impact employee productivity and will go a long way in keeping ransomware at bay.

Step 8. Monitor User Activity

User activity monitoring software is highly effective for stopping insider threats, whether unintentional or with malicious intent. Ransomware attacks often rely on the actions of users to spread throughout a network.

For example, an employee may unknowingly download a malicious file or click on a phishing email, which can then infect the device and spread the ransomware to other devices on the network.

Monitoring can detect:

- Risky behavior that could potentially open the door to a ransomware attack.
- Compromised devices that can be isolated before they cause significant damage.
- The origin of an attack to fix the vulnerability that made it possible.

Monitoring user activity can help businesses enhance their incident response capabilities. By better understanding how ransomware attacks occur, companies can develop more effective incident response plans to respond quickly and effectively to ransomware attacks.

Don’t Pay the Ransom

Our experts recommend that you speak to your legal counsel and insurance company before paying a ransom. Sometimes, insurance companies will pay the ransom for you as a remediation step or hire negotiators to handle ransom payments.

The best action is not to pay the ransom, turn infected machines off, and contact legal counsel. However, if the infected machine is a server, contact an information security professional immediately before taking any action. Keep these three things when considering a ransom:

Encouraging Law Enforcement Action

By not paying a ransom, businesses can encourage law enforcement to investigate the attack and act against the criminals.

Discouraging Future Attacks

When businesses refuse to pay, it sends a message to attackers that ransomware attacks are not profitable and will not be successful. This may discourage future ransomware attacks and reduce the overall risk of ransomware for businesses and individuals.

No Guarantee of Data Recovery

Even if a business pays the ransom, there is no guarantee that the attackers will give you what you want – whether that is a decryption key to recover encrypted data or not leaking stolen data. In some cases, paying the ransom may result in losing both the data and the ransom payment.

Your business can't stop attacks from happening, but you can be proactive. Ensure the four critical pathways to your data and systems are blocked to prevent ransomware from taking hold: Phishing, Credentials, Exploiting Vulnerabilities, and Botnets. By establishing a stronghold, you mitigate threats.

Want to see our approach to your cybersecurity firsthand?

Call us today to talk with one of our expert consultants.

We're happy to answer your questions, provide recommendations, and audit your current IT network.

Request your free consultation today!

Phone: 833-FOR-TEAL Email: sales@tealtech.com

TOP CYBERSECURITY COMPANY
Clutch
2023

A 99/100
Security Scorecard

TOP PENETRATION TESTING COMPANY
Clutch
2023

Advanced IT Strategies That Empower Your Team

Business-focused | Sophisticated Cybersecurity | Concierge Service

Leveraging technology to elevate business strategies is more dynamic than ever. From AI assistants to low-code applications, small to mid-sized businesses are taking advantage of more technology opportunities to accelerate growth and improve customer satisfaction.

Innovative business leaders recognize how crucial it is to drive digital transformation today to stay competitive tomorrow. That's why when you invest in a service provider to help you drive your strategies, you need one that recognizes your distinct needs and offers personalized services tailored to your industry.

Why Choose Teal?

The IT landscape can often be shrouded in complexity and confusion. You require IT systems that support your teams and align with your business goals; however, most Managed Service Providers (MSPs) fall short by offering off-the-shelf solutions that don't fit the nuanced requirements of your business.

Your Partner in IT.

Teal is a human-focused IT partner committed to turning every technology and cybersecurity challenge into an opportunity for enhancement. We provide tailored, best-in-class systems that extend beyond standard, off-the-shelf offerings – aligning perfectly with your business goals. Our approach centers on developing a deep understanding of your business, enabling us to make insightful technical decisions to propel your success forward.

160+ Highly Satisfied Partners

98% Average Customer Satisfaction Rate

A Score from SecurityScorecard

We'll Exceed Your Expectations.

Our ambition transcends mere customer satisfaction; we aim for outright elation. Our people, recruited explicitly for their excellent service and communication, are our most significant differentiators. We know the technical stuff inside and out, but our primary focus is creating an exceptional client experience with every interaction. It's not just what we do; it's how we do it.

We surpass your expectations by thoroughly understanding your systems, processes, standards, operations, goals, and teams. Then, we apply that knowledge to adapt your technology to be as effective, efficient, powerful, and protected as possible. Layering this with engineering and support teams who adore people and technology equally, we seek to become indispensable team members – the ones you never have to worry about.

teal

Learn more about Teal at www.tealtech.com
To speak with a qualified expert, call 703-740-8797

Advanced IT Strategies That Empower Your Team

Business-focused | Sophisticated Cybersecurity | Concierge Service

Who We Help

Healthcare	Government & Defense	Nonprofits
Construction & Manufacturing	Finance, Banking, & Wealth Managers	Legal & Professional Services

We’re Specialized, Sophisticated, and Service-focused.

More than just resolving daily technology concerns, we handle the complex stuff that many MSPs don’t. From CMMC, ITAR, and DFARS compliance to managed IT services and IT consulting, we help organizations with all their managed security services. We know what’s worth protecting and ensure you’re future-ready.

Should challenges arise, our diverse team of seasoned specialists stands ready to tackle any problem. We recruit individuals with a profound comprehension of technology and then further equip them to protect your operations from real-world cyber threats. At Teal, we're not just a service provider; we're an essential partner in the digital realm.

We put our clients first, always.

We believe that changing our focus from getting to giving – putting our client’s interests first and continually adding value to their lives – ultimately leads to unexpected and rewarding returns for all. After all, your success is our success.

Teal is Always in Your Corner

Our professionals are highly involved in understanding the nuances of your business so that we can help you make smarter technical decisions that empower your success. No matter your business goals, we're always in your corner.