Ransomware

What you Need to Know to Protect your Business.
Understanding and Preventing Ransomware Threats.

direct MSP
IT SERVICES AND SECURITY

☎ 1-866-807-9832
✉ directmsp@directdial.com
🌐 www.directmsp.ca

What is Ransomware?

Ransomware is a constantly evolving form of malware designed to encrypt files on a device, making them and the systems that rely on them unusable. Cybercriminals then demand ransom in exchange for decryption. The most recent strains of ransomware steal data before decrypting, the technique called double-extortion. Cybercriminals often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among government entities and critical infrastructure organizations.

The Rise of Ransomware Attacks.

If you think ransomware is declining, think again. Here are some alarming statistics:

493M

In 2022 alone, organizations all around the world detected 493.33 million ransomware attacks.

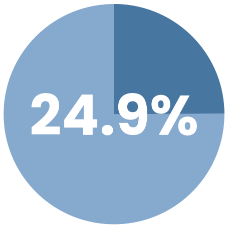
+85%

There has been an 85% increase in ransomware attacks since 2022.

4th

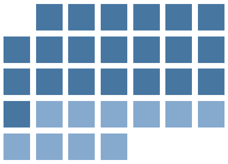
Manufacturing is the 4th most attacked industry by ransomware, following education, government and healthcare.

> Ransomware is unique among cybercrime because for the attack to be successful, it requires the victim to become a willing accomplice after the fact.
>
> - James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology.

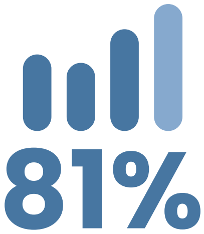


Almost a quarter of all ransomware attacks target professional services firms, especially small and midsize law firms.

This year, there will be a victim of a ransomware attack every 11 seconds.



On average, it takes 21 days to identify and remediate ransomware attack.



81% of cybersecurity experts forecast a record number of ransomware attacks in 2024.

7 Financial Impacts of a Ransomware Attack.

In 2024, the financial impact of ransomware is expected to reach $42 billion, when factoring in the cost of downtime and lost business opportunities. Understanding these factors is crucial for preparing and protecting your organization against such a costly threat.

1

The Ransom

The average ransom payment in 2023 was $812,360 USD, according to the FBI. While paying the ransom may seem like a quick solution, it's important to understand there's no guarantee you'll recover your data. Moreover, paying can encourage further attacks with 36% of businesses that pay the ransom falling victim to ransomware attacks for a second time.

2

Cost of Downtime

Downtime paralyzes operations, preventing client service and product production, with impacts measured in minutes rather than hours.

3

Labour Costs

While your IT resources are focused on restoring your systems, most other employees are dependent on access to data, resulting in a backlog of work throughout your organization.

4

Legal Expenses

Legal requirements mandate informing clients about data breaches, which can also result in fines in certain industries.

Subway Investigates Possible Ransomware Gang Attack
PCMAG, 2024

Huntsville, Ontario, Confirms Details of Cybersecurity Incident
Town of Huntsville, 2024

Toronto Zoo latest public body to be hit by cybersecurity attack
CBC, 2024

5

Data Loss

Even if you can restore from your backup, there is a risk that not all your files were backed up correctly, meaning you might have forever lost valuable data.

6

Collateral Damage

Hacker's trade stolen data and credentials and have become highly organized. After having resolved an incident there is still a risk that your company data could be exploited in future attacks.

7

Brand Reputation

While data can be restored, a damaged reputation is much harder to repair, affecting customers, employees, investors, and other stakeholders.

Phishing emails are responsible for about **62%** of ransomware attacks.

Leading Causes of Ransomware Attacks

Main causes of ransomware attacks reported in 2022 by Managed Service Providers:

Phishing Emails
Cybercriminals often use deceptive emails to trick users into revealing sensitive information or downloading malicious software.

Poor User Practices
Mistakes like clicking on unknown links or trusting unverified sources can inadvertently lead to ransomware infections.

Lack of Cybersecurity Training
Without proper education on cybersecurity best practices, users are more vulnerable to falling for cyber threats.

Weak Passwords/Access Management
Using easily guessable passwords or poor management of access controls can provide cybercriminals easy entry points.

Open Remote Desktop Protocol (RDP) Access
Leaving RDP ports open can allow unauthorized access, making systems more susceptible to attacks.

Clickbait
Enticing but deceptive online content can lure users into clicking on malicious links, leading to ransomware downloads.

Malicious Websites
Visiting compromised or malicious websites can result in the inadvertent download of ransomware.

Lost/Stolen User Credentials
If user credentials are lost or stolen, they can be used by attackers to gain unauthorized access to systems and deploy ransomware.

Understanding these causes is crucial in developing effective strategies to prevent ransomware attacks and protect sensitive data.

Ransomware Prevention Best Practices

Preventing ransomware attacks is possible with the right strategies. Here are some best practices:

Set Up a Strong Firewall with Management
Ensure your firewall is robust and properly managed.

Backup Regularly
Maintain multiple backups of your data.

Adopt a Zero-Trust Security Model
Assume no entity inside or outside your network is trustworthy by default.

Invest in Security AI and Automation
Use advanced technologies to detect and respond to threats.

Network Segmentation
Divide your network into segments to contain breaches.

Staff Awareness
Educate your staff on cybersecurity best practices.

Application Whitelisting
Only allow approved applications to run on your systems.

Comprehensive and Regular Security Tests
Regularly test your security systems to find and fix vulnerabilities.

Password Security
Implement strong password policies and use multi-factor authentication.

Software Patches
Keep all software up-to-date with the latest patches.

> People ask me all the time, “What keeps you up at night?” And I say, “Spicy Mexican food, weapons of mass destruction and cyberattacks.”
>
> - Dutch Ruppersberger

Reduce your Risk, Strengthen your Security Posture

While ransomware statistics can be alarming, you don't have to face the threat alone. Our comprehensive cybersecurity services can protect your business from evolving threats. With multi-layered defenses and advanced technology, you can trust us to safeguard your organization, allowing you to focus on growing your business.

Endpoint Detection and Response	Prevents threats at faster speed, greater scale, and higher accuracy than humanly possible.
Mail Security	Suite of email security, backup, archiving, management, and marketing solutions.
User Defence Training	Tailored to empower your employees to become the first line of defence against cyber attacks.

Explore our Cybersecurity Services

Get the Peace of Mind you Deserve, **Contact our Security Experts today**.

☎ 1-866-807-9832 ✉ directmsp@directdial.com www.directmsp.ca

About directMSP

IT SERVICES AND SECURITY

At directMSP, our mission is to empower businesses to drive better outcomes through strategic technology solutions. We partner with our clients to ensure their technology investments enhance performance, improve profitability, and reduce risks. From proactive IT management to cutting-edge cybersecurity, we help businesses stay resilient in the face of evolving threats. Learn how we can help safeguard your technology and optimize your business success.

10+ Years
Average Account Manager Tenure

25+ Years
In Business

200+ Partners
Including

FORTINET SentinelOne QUALYS Jolera

TOP 100 SOLUTION PROVIDER
TOP100 SOLUTION PROVIDERS
2023

BBB ACCREDITED BUSINESS
BBB Rating: A+