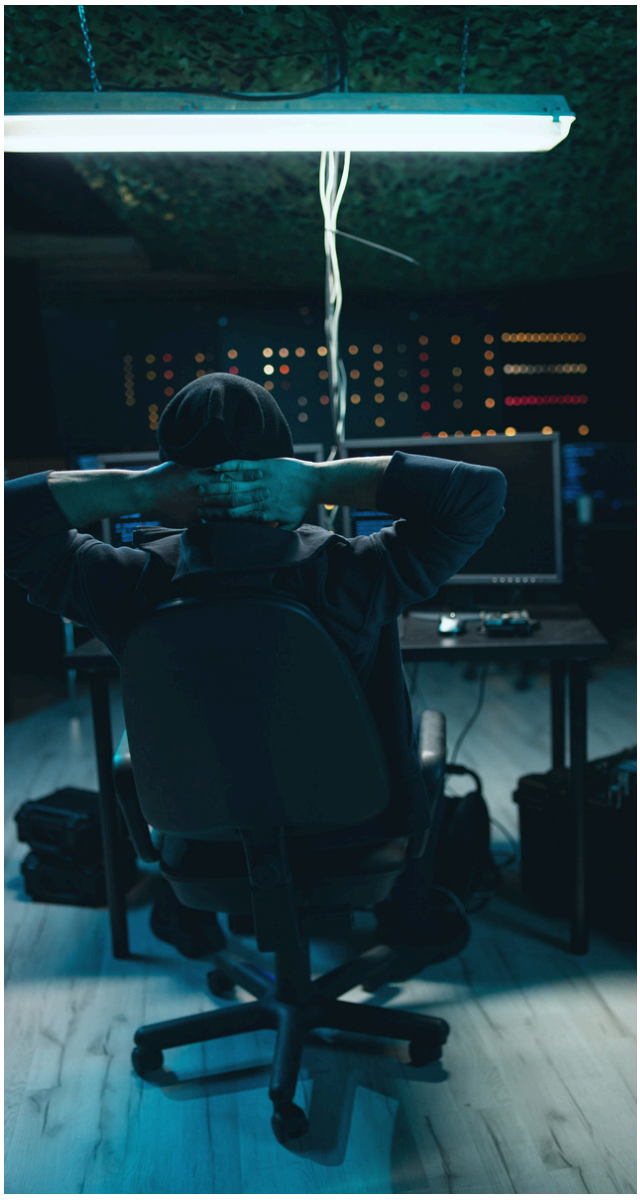
Ransomware by the Numbers

MSP CORP

National Reach
with a **Local Focus**

What is Ransomware



Ransomware is one of the biggest security problems for organizations, businesses, and individuals. Criminals are taking advantage of the weakness of those IT departments.

Ransomware is a type of malware the infects the computer systems of users and manipulates it and prevents or limits users from accessing their system, either by locking the system's screen or locking users files unless a ransom is paid.

The victim usually shortly after receives blackmail note by pop-up, pressing the victim to pay the ransom through certain online payment methods to regain full access to system and files.

It is important to learn about ransomware, how it works and how to prevent it.

Facts

- In 2024 there has been a 56% increase in active ransomware groups.
- In just the first half of year 2025 there have been 2,321 attacks globally.
- The average ransom in 2024 was $2.73 million, an increase of almost $1 million from 2023.
- The average downtime a company experiences after a ransomware attack is 24 days.
- On average, victims permanently lose 43% of the data affected by an attack
- Financial services, healthcare, manufacturing, and professional services were among the most targeted industries.
- Email phishing campaigns, RDP vulnerabilities, and software vulnerabilities were the most common attack vectors.

How Do You Get Infected?

60% Phishing Emails: the most common vector, ransomware is often delivered through malicious email attachments or links.

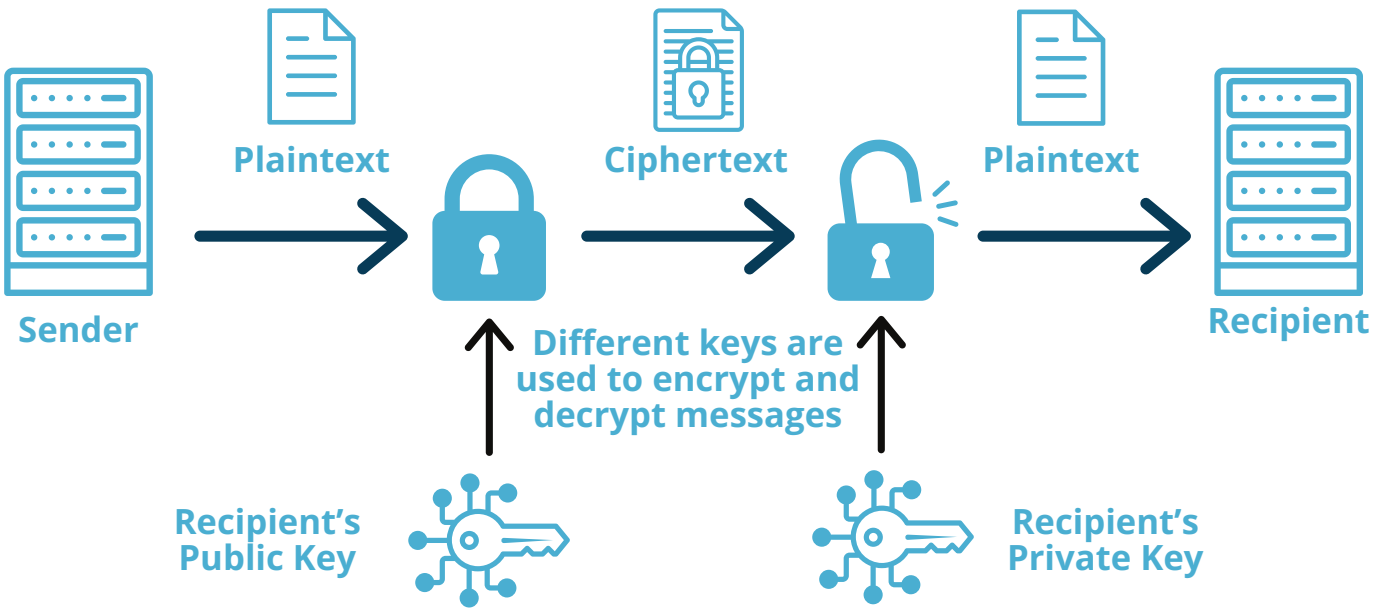
20% Compromised Websites: malicious websites or legitimate sites infected with exploit kits can drop ransomware onto a victim's machine.

15% Malicious File Downloads: users downloading pirated software, fake security updates, or infected installers may inadvertently install ransomware.

10% Brute Force Attacks: 15% Attackers gain unauthorized access to systems by brute-forcing weak credentials, particularly Remote Desktop Protocol (RDP) and VPN services.

5% Other: includes USBs, supply chain attacks, exploit kits, insider threats, etc.

How Do They Take Your Data?



How to Prevent It

Preventing ransomware attacks requires a proactive approach that combines technology, user awareness, and strong security policies. Cybercriminals often exploit human error and system vulnerabilities to infiltrate networks, making it essential to implement multiple layers of defense.

By following these best practices, organizations and individuals can significantly reduce the risk of falling victim to ransomware:

- **Create a human firewall through training**
- **Restrict access to unneeded websites**
- **Have a working backup solution**
- **Keep your anti-virus and MDR solution updated**
- **Use a firewall with Intrusion Prevention (IPS)**
- **Use long passwords, minimum 11 characters**