# How to Avoid Ransomware

**Ransomware attacks happen constantly** and to all types of agencies, businesses, governments, organizations, and school systems. These nine security practices provide guidance for preventing an expensive and harmful ransomware attack from happening to you.

**Not sure what to do next?** **Reach out to us and we'll help get you started!**

## 1 Email Filtering & Anti-Phishing Training

Emails should be filtered to **block spam and malicious attachments/links** from reaching users.

It is critical that employees are aware of network security obligations and are **regularly trained** on phishing, which includes how to spot, avoid, and report attempts.

Companies should also conduct **periodic phishing exercises** to test if employees will click on attachments and embedded links in fake emails, and provide additional training as needed.

## 2 Vulnerability & Patch Management

Companies should have a documented program to identify, assess, track, and remediate vulnerabilities on all enterprise assets within their infrastructure. The program should include **periodic penetration testing**.

Timely remediation of vulnerabilities is essential and requires strong governance, including assignment and tracking of responsibilities. Vulnerability management should include requirements for **timely application of security patches & updates**. Regulated companies should enable automatic updates wherever possible.

## 3 Multi-Factor Authentication (MFA)

MFA protects user accounts and can **prevent hackers from obtaining access to the network** and from escalating privileges once inside the network. MFA should be a requirement by all companies for remote access to the network and for all externally exposed enterprise and third-party applications.

All logins to privileged accounts, whether remote or internal, should **require MFA**, as this is a highly effective way of blocking privilege escalation via password cracking.

## 4 Password Management

Companies should ensure that **strong, unique passwords** are used. Privileged user accounts should require passwords of at least 16 characters and ban commonly used passwords.

Larger organizations with dozens or hundreds of privileged user and service accounts should strongly consider a **password vaulting PAM** (Privileged Access Management) solution, which requires employees to request and checkout passwords. Password caching should be turned off wherever possible.

DSI TECH

571-707-3636 • sales@dsitech.com

@ITbyDSI

CONTINUE

# How to Avoid Ransomware

## 5 Disable RDP Access

Companies should **disable RDP access from the internet** wherever possible. After assessing the risk, if RDP access is deemed necessary, then access should be restricted to only approved (whitelisted) originating sources and require MFA as well as strong passwords.

## 6 Privileged Access Management

Companies should implement the principle of **least privileged access**, where each user or service account should be given the minimum level of access necessary to perform the job. Privileged accounts should be carefully protected and universally require MFA and strong passwords.

Companies should also maintain and periodically **audit an inventory of all privileged accounts**. These accounts should be used only for tasks requiring elevated privileges, and administrators should have a second non-privileged account for all other tasks such as logging into their workstation, email, drafting documents, etc. Privileged service accounts are a **frequent source of compromise** and should not be overlooked. Service accounts should have the same or more restrictive access controls as equivalent user accounts.

## 7 Segregated & Tested Backups

Companies should maintain comprehensive, segregated backups that will allow **recovery in the event of a Ransomware attack**. To prevent hackers from deleting or encrypting backups, at least one set of backups should be segregated from the network and offline.

It is important to periodically test backups by actually **restoring critical systems from backups**. This is the only way to be sure that the backups will actually work when needed.

## 8 Monitoring & Response

Companies must have a way to monitor their systems for intruders and respond to alerts of suspicious activity. Regulated companies should implement an **Endpoint Detection and Response (EDR)** solution, which monitors for anomalous activity. Advanced EDR can quarantine infected systems, potentially stopping Ransomware from executing before it can encrypt the endpoint. EDR can also facilitate incident response.

Companies with larger and more complex networks should also have lateral movement detection and a **Security Information and Event Management (SIEM)** solution that centralizes logging and security event alerting.

## 9 Incident Response Plan

Companies should have an incident response plan that **explicitly addresses Ransomware attacks**. The plan should be tested, and the testing should include senior leadership. Decision makers like the CEO should not be testing the incident response plan for the first time during a real Ransomware incident. Any successful deployment of Ransomware on a company's internal network should be **reported as promptly as possible** and within 72 hours at the latest. We recommend that any intrusion where hackers gain access to privileged accounts should be reported.

**Let us protect you!** Contact DSI Tech for a Network Security Assessment, Product Demos, and Expert Advice:

DSI TECH

571-707-3636 • sales@dsitech.com