SENDMARC

Ransomware Readiness Checklist

As the **fastest-growing** type of cybercrime, ransomware is an immediate concern for businesses of every size. Attacks are increasing in numbers and sophistication, impacting all industries and causing serious financial and reputational damage. This means it's critical to understand your company's vulnerability and prepare a resilient, layered defense.

This checklist will help you assess if your company is prepared to proactively defend against and effectively recover from a ransomware attack.

Ransomware is expected to cost victims $265B annually by 2031

72%+

Over 72% of businesses were affected by ransomware attacks in 2023 – the highest figure reported yet

A ransomware attack will take place every 2 seconds by 2031

1 Identify potential entry points

Understand where ransomware might get in.

- [ ] Do you have visibility of all inbound email sources?
- [ ] Are your email domains protected from phishing, spoofing, & impersonation?
- [ ] Are remote access points secured and monitored?
- [ ] Are third-party/vendor integrations regularly reviewed?
- [ ] Are regular security audits performed for cloud configurations?

2 Prevention readiness

Evaluate if your existing defenses stop attacks before they spread.

- [ ] Is DMARC implemented and enforced with a p=reject policy?
- [ ] Are SPF and DKIM configured and monitored?
- [ ] Do you have proactive reporting measures in place?
- [ ] Is MFA enabled for critical systems and accounts?
- [ ] Are patches and software updates applied regularly?
- [ ] Do employees get phishing awareness and cybersecurity training?

3 Response readiness

Can your business act fast and effectively if a ransomware attack hits you?

- [ ] Is there a tested incident response plan?
- [ ] Do you have a ransomware-specific playbook?
- [ ] Are secure, offline, and unchangeable backups in place?
- [ ] Have external response partners (legal, forensic, communication) been identified for rapid response?

4 Recovery & resilience

What happens after the breach?

- [ ] Can you restore systems from clean backups quickly?
- [ ] Is there a documented business continuity plan?
- [ ] Do you review incidents and apply learnings?
- [ ] Are future security improvements budgeted and prioritized?

5 Implementing proactive defenses

- [ ] 95% of businesses have increased their 2025 recovery budget for prevention. **Has yours?**

By enforcing Domain-based Message Authentication, Reporting, and Conformance (DMARC) with a p=reject policy, you can stop your organization from falling victim to a ransomware attack by cutting off a key delivery method – email impersonation.

DMARC benefits include:

Trust

Stop fake emails being sent from your domain and ensure that all recipients can trust the emails they receive from you.

Visibility

Our DMARC reports collect data from servers worldwide, turning it into actionable insights, and give you visibility of who is sending emails from your domain.

Delivery

Strong DMARC compliance and policies ensure that all legitimate emails with your name reach the intended inbox, not Spam or Junk folders.

Compliance

Sendmarc ensures compliance with global regulatory standards, providing compliance to every email service used by every department.

Ready to strengthen your defenses against ransomware?

Let's make sure your email ecosystem isn't your weakest link:

Book a demo | Test your domain | Free trial