Ransomware Prevention Guide

A straightforward guide to help businesses reduce ransomware risk before an attack occurs.

Your IT Department. Your Cybersecurity Team. Your Technology Partner.

Network Solutionist, LLC

Serving Wilmington, Newark, Middletown, Dover, Rehoboth Beach, and businesses across Delaware.

What Ransomware Does

Ransomware is malicious software that can encrypt files, disrupt operations, and pressure a business into paying for access to its own data. Prevention focuses on reducing entry points, limiting spread, and maintaining recoverable backups.

Prevention Priorities

- Enable MFA for email, remote access, admin portals, and financial applications.
- Patch internet-facing systems quickly, including firewalls, VPNs, servers, and remote access tools.
- Use managed endpoint protection with centralized alerts and reporting.
- Block or restrict legacy authentication and outdated protocols where possible.
- Limit local administrator rights on workstations.
- Segment critical systems so one compromised device cannot reach everything.
- Maintain backup copies that are protected from ordinary user access.
- Test restores using real files, databases, and line-of-business applications.
- Train employees to report suspicious emails and unusual prompts immediately.
- Document who makes legal, financial, operational, and communication decisions during an incident.

If You Suspect Ransomware

Done	Security Item	Why It Matters
[ ]	Disconnect affected machines from the network.	Containment can reduce spread to shared drives or servers.
[ ]	Do not wipe systems before evidence is reviewed.	Logs and artifacts may be needed for investigation and insurance.
[ ]	Notify leadership and your IT/security contact.	Fast escalation improves containment and recovery decisions.
[ ]	Preserve backups and avoid overwriting restore points.	Backup integrity is critical to recovery.
[ ]	Document timelines, affected systems, and user reports.	Written detail helps with insurance, legal, and remediation work.

Helpful Reference Points

- CISA small business guidance recommends incident response planning and prioritizing actions aligned to how attacks actually happen.

- FTC cybersecurity basics include updating software, backing up files, strong passwords, encryption, and MFA.

Disclaimer

This guide is for general educational purposes and does not replace a formal cybersecurity assessment, compliance review, or incident response engagement.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, monitor, and support your business technology environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com