Simple Ransomware Protection Guide

Five Practical Steps to Reduce Ransomware Risk

By: Shawn Awan, SkySec Founder & Lead Assessor

What is Ransomware?

Ransomware is when attackers lock access to your systems or data and demand payment—often in cryptocurrency—to restore it.

How it Works?

Attackers most often start by phishing users to steal credentials.

They may spend weeks—or months—inside an environment quietly preparing before encrypting systems and demanding payment.

Once access is established, attackers lock critical assets and threaten permanent data loss if demands are not met.

Why this Matters? (Impact)

Most ransomware doesn't come from the malware itself – it's usually due to failing to prepare, unclear ownership, and false confidence in tools or reports.

Actions to Take Today (Checklist)

1. *Enforce MFA on **ALL** external access (especially email and VPN)*
2. *Patch and update any and all system when possible*
3. *Maintain offline, tested backups – this takes power and leverage away from hackers*
4. *Limit admin privileges*
5. *Ensure browser cookies and cache are set to clear every time you close your web browser*

Common Mistakes (Reason for Failures)

- *Assuming tools will address all issues*
- *Failing to verify changes persisted*
- *Lacking proper incident response plans*

SkySec finds gaps focused on real-world attack paths – not compliance theater.
Contact us www.skysecsecurity.com