Top 10 Cyber Security Checklist for Business Owners

1

Conduct a Cyber Risk Assessment & Regular Audits

- Identify critical assets and vulnerabilities through periodic assessments.
- Perform regular security audits to track evolving threats and compliance.
- Prioritize and remediate identified gaps without delay.

2

Encrypt Data & Maintain Backups

- Encrypt data both at rest and in transit (emails, databases, file storage).
- Schedule frequent, automated backups to off-site or cloud locations.
- Regularly test backup restoration to ensure data integrity.

3

Keep Software & Systems Updated

- Enable automatic updates for operating systems, applications, and firmware.
- Patch newly discovered vulnerabilities promptly.
- Deploy a formal patch management program to stay ahead of emerging threats.

4

Develop an Incident Response Plan

- Outline clear steps to identify, contain, and recover from breaches.
- Assign responsibilities and keep contact lists up-to-date (IT, legal, infosec, etc.).
- Test and revise the plan regularly to handle evolving threats effectively.

5

Implement Multi-Factor Authentication (MFA)

- Require multiple forms of verification (password, device token, biometrics).
- Apply MFA to critical systems (e.g., email, finance, admin dashboards).
- Reduce the risk of password compromise and unauthorized access.

6

Educate & Train Employees

- Conduct frequent security awareness sessions on phishing, social engineering, and password hygiene.
- Encourage a “see something, say something” policy to report suspicious activity.
- Keep staff informed about new scams or attack methods.

7

Enforce Strong Access Controls & Password Policies

- Limit privileged accounts to essential personnel only.
- Review and remove inactive/disabled accounts promptly to reduce entry points.
- Mandate robust passwords (length, complexity) and regular resets.

8

Adopt a Zero Trust Approach

- “Never trust, always verify” each access request, both inside and outside the network.
- Use role-based permissions with continuous authentication checks.
- Limit the lateral movement of attackers through strict segmentation and least-privilege policies.

9

Secure Network Infrastructure

- Use hardware and software firewalls to filter incoming/outgoing traffic.
- Monitor network traffic 24/7 for unusual behavior or unauthorized devices.
- Segment networks (e.g., user, guest, server) to limit lateral movement by attackers.

10

Perform Ongoing Testing & Monitoring

- Schedule regular penetration testing (ethical hacking) to find system weaknesses.
- Continuously audit logs and alerts for anomalous activities (e.g., unauthorized access attempts).
- Adjust security controls as soon as new vulnerabilities or attack patterns are identified.

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com