2025 SMALL BUSINESS CYBERSECURITY CHECKLIST

SIMPLE STEPS TO STAY SAFE ONLINE

GLOBAL CREATIVE SERVICES

A COMPLETE CHECKLIST TO PROTECT YOUR BUSINESS FROM COMMON CYBER THREATS.

1. Strengthen All Passwords □
Create long, unique passwords (12–16 characters) for every account.

2. Turn On Multi-Factor Authentication (MFA) □
Enable MFA on email, banking, cloud tools, and any system with sensitive data.

3. Update All Devices & Software □
Install updates on computers, mobile devices, routers, and business apps.

4. Update All Devices & Software □
Use a strong password and separate guest Wi-Fi from internal systems.

5. Install Antivirus & Anti-Malware Protection □
Use trusted security software on every company device.

6. Back Up All Data Regularly □
Use automated cloud backups and keep at least one offline copy.

7. Train Your Team to Spot Phishing □
Teach employees to recognize suspicious links, emails, and attachments.

8. Protect Business Email Accounts □
Use spam filters and security settings to block fraudulent messages.

9. Limit Employee Access to Data □
Give access only to the tools and information each role requires.

10. Secure Company Mobile Devices □
Require screen locks, encryption, and remote-wipe options.

11. Review Vendor & Software Security □
Use trusted tools and confirm that partners follow strong security practices.

12. Create an Incident Response Plan □
Use automated cloud backups and keep at least one offline copy.

13. Regularly Delete Old Users & Devices □
Remove accounts of former employees and disconnect unused devices from company systems.

14. Don’t Click Unknown Links □
Avoid clicking links in emails, texts, or pop-ups unless you trust the sender.

15. Don’t Download Files From Untrusted Sources□
Only download apps, PDFs, tools, or software from official websites or app stores.

16. Avoid Public Wi-Fi Without a VPN □
Public Wi-Fi in cafes, malls, airports, etc., is unsafe for business activities.

17. Verify the Sender Before Responding □
If an email looks suspicious, call the person or business to confirm.

18. Use Secure Websites Only □
Make sure the URL begins with https://
(“s” = secure)

19. Avoid Reusing the Same Password □
Use a different password for email, banking, social media, and business tools.

20. Log Out from Shared or Public Devices □
Especially after using email, banking, or work accounts.