DAVETHAN
TECHNOLOGIES

Table of Contents

Introduction

In today's digital landscape, businesses face an increasing number of cyber threats, from phishing scams to data breaches. Without proper security measures, companies risk losing sensitive information, financial stability, and customer trust.

At Davethan Technologies, we are committed to providing cutting-edge cybersecurity solutions that help businesses stay protected. This checklist highlights 10 essential steps to safeguard your business and ensure a resilient, secure digital environment.

Message From The Team At Davethan Technologies

At Davethan Technologies, cybersecurity is not just a service—it's a commitment. As a leading provider of IT security and digital transformation solutions, we help businesses stay ahead of cyber threats with innovative, scalable, and data-driven security strategies.

"Our goal is to make cybersecurity simple and effective for businesses of all sizes. Whether you're a startup or an enterprise, we believe that security should never be an afterthought—it should be a priority."

Stay protected, stay secure, and let Davethan Technologies handle your cybersecurity needs!

DAVETHAN
TECHNOLOGIES

Cybersecurity Checklist

1. Secure Your Password

- Use strong passwords (12+ characters with symbols and numbers).
- Enable two-factor authentication (2FA) on all accounts.
- Change passwords every 3-6 months.

2. Update and patch your software

- Keep operating systems, software, and applications updated.
- Enable automatic updates to fix vulnerabilities.

3. Install firewalls And Antivirus

- Set up firewalls to block unauthorized access.
- Install and update antivirus and anti-malware software.

4. Protect your WiFi Network

- Change default router login credentials.
- Use WPA3 encryption for better security.
- Hide your SSID (Wi-Fi name) to prevent easy detection.

5. Backup Your Data Regularly

- Implement automatic cloud and offline backups.
- Store backups in a secure location, separate from primary systems.

6. Train Employees On Cybersecurity Best Practices

- Educate staff on phishing attacks and cyber scams.
- Conduct regular cybersecurity training sessions.
- Encourage employees to report suspicious activities immediately.

7. Restrict Access to Sensitive Information

- Use role-based access control (RBAC) to limit employee access.
- Monitor and log who accesses critical data and when.

8. Secure Mobile Devices

- Enable remote wipe for lost or stolen devices.
- Require device encryption and strong passwords for work devices.

9. Monitor Network Activity

- Use intrusion detection systems (IDS) to identify suspicious activity.
- Review system logs regularly for unusual access patterns.

10. Develop an Incident Response Plan

- Prepare a clear action plan for cybersecurity breaches.
- Assign a dedicated response team and conduct security drills.
- Regularly update and test the plan to stay ahead of threats.

Conclusion

Cyber threats are evolving, and businesses must stay proactive in their security efforts. Implementing these 10 cybersecurity best practices can protect your organization from cyber risks, ensuring data privacy, operational efficiency, and customer trust.

Take action today—because in the digital world, prevention is always better than cure.

CONTACT US

+234 812 279 8051

info.ng@davethantech.com

104, Emmanuel Adiele, Off Mike

Akhigbe Way, Jabi, Abuja, Nigeria

+44 02080580860

info@davethantech.com

Halford House, 2Coval Ln,Chelmsford,United Kingdom