Ultimate SMB Cybersecurity Checklist

"Lost files, compromised email, payroll fraud, ransomware... these problems hit small businesses the hardest because they often don't have an IT team watching their back."

Running a business is hard enough without stressing over hackers or phishing scams. For small companies, one incident can shut everything down. This guide offers a simple checklist to see if your business is protected—and when it's time to bring in a Managed Service Provider (MSP) like GTS to take that burden off your plate.

Start Here - A 5-Minute Cyber Risk "Gut Check"

If you answer "No" or "Not Sure" to more than 3, your business is at risk.

- ☐ Do you know who is in charge of your IT and cybersecurity (by name)?
- ☐ Is multi-factor authentication (MFA) enabled for email, banking, etc.?
- ☐ Are all company computers encrypted (so data is protected if stolen)?
- ☐ Do you have automatic backups of company files stored in the cloud?
- ☐ Have you tested restoring something from backup in the last 6–12 months?
- ☐ Do your employees get regular phishing/security training?
- ☐ Are security notifications monitored daily—not just "when there's time"?
- ☐ Do you have a plan for what to do if you're hacked or hit with ransomware?
- ☐ Are your computers, servers, and firewalls automatically updated/patched?
- ☐ If a key employee left today, could you instantly turn off all their access?

For most small businesses, this gut check alone reveals the gaps, but move on to check what your business should have in place for cyber protection.

Ultimate SMB Cybersecurity Checklist

"You don't need to understand cybersecurity — you just need someone who does."

People, Passwords & Identity

- □ Strong, unique passwords
- □ Company-wide password manager
- □ MFA on email, remote access, finance
- □ No shared logins
- □ Standardized onboarding/offboarding

Devices

- □ Supported OS versions
- □ Automatic updates/patching
- □ Business-grade security (EDR)
- □ Device encryption
- □ Standard setup for new devices
- □ Remote-wipe plan

Email & Phishing

- □ Advanced email filtering
- □ Annual phishing training
- □ Verify money requests by phone
- □ "Report Phish" button
- □ External email warnings

Backups & Recovery

- □ All key data backed up
- □ 3-2-1 backup rule
- □ Ransomware-resistant backups
- □ Know restore times
- □ Annual test restore

Access & Vendors

- □ Least-privilege access
- □ Separate admin accounts
- □ Annual access review
- □ Unique vendor accounts

Network & Remote Work

- □ Managed business firewall
- □ VPN + MFA for remote access
- □ Guest Wi-Fi separate
- □ Default network passwords changed
- □ Basic home-network rules

Policies & Insurance

- □ Simple IT/security policies
- □ Know applicable regulations
- □ Cyber liability insurance
- □ Clear incident-response roles

Monitoring & Response

- □ 24/7 monitoring
- □ Alerts reviewed daily
- □ Plans for ransomware, email compromise
- □ Logs kept long-term

Call for a Free No-Pressure Consultation

(904) 606-6011