Is Your Microsoft 365 Safe?

10-Point Checklist for Small Offices

Squared Away Tech
Veteran-owned · Lakewood Ranch, FL

Check each item. Anything you can't check off, or aren't sure about, is worth a closer look.

- [ ] **1. Multi-factor authentication (MFA) for everyone**
  Every user signs in with a second step, including owners, part-timers and shared mailboxes people log into. One account without MFA is the easy way in.
- [ ] **2. Admin accounts and app permissions kept few**
  Only one or two people hold global admin rights, using separate admin-only accounts that are not used for daily email. Remove admin rights nobody needs. Also review app permissions: limit who can approve (consent to) third-party apps, and remove apps with access to mail or files that nobody can name an owner for. A bad app keeps access even after a password reset.
- [ ] **3. Legacy (basic) authentication turned off**
  Older sign-in methods skip MFA entirely. Confirm they are blocked so old mail apps and scripts cannot be used to get around it.
- [ ] **4. No unexpected forwarding or inbox rules**
  Check every mailbox for rules that forward, delete or hide mail. Attackers use these to watch conversations and redirect invoices. Block automatic forwarding outside the company.
- [ ] **5. SPF, DKIM and DMARC set up for your domain**
  These email records help prove your mail is really from you, cut down on spoofing of your domain, and help keep your messages out of spam folders.
- [ ] **6. Backups of email and files you control**
  Microsoft keeps your service running, but deleted or encrypted data may not come back on its own. Make sure mail, OneDrive and SharePoint are backed up and that a restore has been tested.
- [ ] **7. Company devices managed and encrypted**
  Laptops and phones that open company data are enrolled in device management, kept updated, encrypted, and can be wiped if lost or when someone leaves.
- [ ] **8. Sign-in alerts someone actually reads**
  Alerts for risky sign-ins, new admin roles and suspicious inbox rules go to a person who checks them, not to an unwatched mailbox.
- [ ] **9. Guest and external sharing under control**
  Review who outside the company can see your files and Teams. Remove old guests and limit "anyone with the link" sharing for sensitive folders.
- [ ] **10. Security defaults or conditional access turned on**
  At minimum, security defaults are enabled. Offices that need more control use conditional access policies, for example to block sign-ins from unexpected countries or unmanaged devices.

Not sure where you stand? Get a free 20-minute checkup call.

Greg Mitchell will review your Microsoft 365 sign-in and email forwarding settings with you, at no cost and no obligation. Based in Lakewood Ranch, serving small offices across Florida, and remotely anywhere in the U.S.

greg@squaredawaytechfl.com · (941) 479-1075 · www.squaredawaytechfl.com

© 2026 Squared Away Tech · General information, not legal or insurance advice. Every office's setup is different.