Mirazon®

CHECKLIST

From Default to Defended: A Microsoft 365 Checklist

Turning Built-In Features Into Real Protection

www.mirazon.com
(502) 240-0404
info@mirazon.com

From Default Settings to Real Protection

Let's be real: Microsoft 365 security can feel overwhelming. There are a lot of settings, a lot of opinions, and not a lot of clarity on what actually needs to be done *right now*. Most teams aren't ignoring security—they're just busy keeping the business running.

This checklist is here to help. It breaks Microsoft 365 security into clear, manageable steps so you can spot gaps, make smart improvements, and move forward with confidence—without trying to do everything at once.

Phase #1 Identity & Access Control

Because identity is still the front door attackers try first.

- [ ] **Turn on Multi-Factor Authentication (MFA) for everyone**

  Make MFA non-negotiable. Where possible, prioritize phishing-resistant options (like FIDO2 or Microsoft Authenticator) to stop credential theft before it starts.

- [ ] **Harden administrative accounts**

  Admins shouldn't use their elevated accounts for day-to-day work. Enforce separate, non-daily-driver admin accounts—and keep at least one locked-down "break-glass" account secured for true emergencies.

- [ ] **Apply least privilege (and mean it)**

  Admins should only have access when they need it—and only to what they need. Use Privileged Identity Management (PIM) and Just-In-Time access where licensing allows.

- [ ] **Go beyond Security Defaults with Conditional Access**

  Security Defaults are meant to protect you—but many organizations turn them off as one of the first admin actions, leaving accounts exposed. If you're not using Security Defaults **or** Conditional Access, that's a major risk. When building Conditional Access policies, make sure to factor in location, device compliance, and user risk to reduce exposure without slowing people down.

Phase #2 Data & Application Governance

This is where "helpful tools" quietly turn into risk.

- [ ] **Lock down app registrations and third-party access**

  Require administrator approval for all third-party app consent. This prevents shadow apps from quietly accessing email, files, or user data.

- [ ] **Audit external sharing in SharePoint & Teams**

  Review who has access to what—especially externally. Sensitive sites should be private, and sharing should be limited to approved domains only.

- [ ] **Enable unified audit logging**

  Make sure Microsoft's unified audit log is enabled and retention aligns with your business needs. When something goes wrong, this log is often the difference between clarity and chaos. Learn More >>

- [ ] **Set idle session timeouts**

  Protect against walk-away risk by configuring session controls for web access—especially on unmanaged or shared devices.

Phase #3 Threat Protection & Resiliency

Because prevention is great—but recovery matters too.

- [ ] **Optimize email security settings**

  Email is still the #1 attack vector. Ensure baseline or advanced Defender for Office 365 policies are enabled for anti-phishing, anti-spam, and impersonation protection.

- [ ] **Implement independent Microsoft 365 backups**

  Microsoft handles availability—but not traditional, point-in-time backups. A third-party solution (like Veeam) ensures you can recover data when users delete it, attackers encrypt it, or retention runs out.

- [ ] **Monitor your Microsoft Secure Score regularly**

  Secure Score isn't about chasing 100%. It's about visibility. Review it routinely to spot new risks and prioritize improvements. Learn More >>

- [ ] **Configure alerts for high-risk activity**

  Set automated alerts for things that shouldn't happen quietly—like admin role changes, new mailbox rules, or password resets.

Security Shouldn't Feel Overwhelming. It Should Feel Intentional.

If we're being honest, most organizations already have solid Microsoft 365 security tools in place—they're just not always turned on, fully configured, or reviewed regularly. And that's completely understandable. Microsoft 365 is powerful, but it's not exactly simple.

The good news? You don't have to figure it all out alone. A focused Microsoft 365 security assessment can help you see what's working, what's missing, and where a few smart changes can meaningfully reduce risk—without disrupting your day-to-day operations.

If you'd like a second set of eyes, have questions about your setup, or just want to sanity-check your security posture, reach out to us. We're happy to help you cut through the noise and make Microsoft 365 security feel a lot more manageable.

Contact Us

Mirazon®

www.mirazon.com
(502) 240-0404
info@mirazon.com
1640 Lyndon Farm Ct., Suite 102
Louisville, KY 40223