Microsoft 365 Business Premium Security Recommendations

1. Set up multi-factor authentication

Using multifactor authentication is one of the easiest and most effective ways to increase the security of your organization. It's easier than it sounds - when you log in, multifactor authentication means you'll type a code from your phone to get access to Microsoft 365. This extra step can prevent hackers from taking over if they know your password. Multifactor authentication is also called 2-step verification.

2. Use dedicated admin accounts

The administrative accounts you use to administer your Microsoft 365 environment include elevated privileges. These are valuable targets for hackers and cybercriminals. Use admin accounts only for administration. Admins should have a separate user account for regular, non-administrative use and only use their administrative account when necessary to complete a task associated with their job function. Additional recommendations:

- Be sure admin accounts are also set up for multi-factor authentication.
- After completing admin tasks, be sure to log out of the browser session.
- Try to have as few global admins within the tenant to lower attack surfaces

3. Raise the level of protection against malware in mail

Your Microsoft 365 environment includes protection against malware, but you can increase this protection by blocking attachments with file types that are commonly used for malware.

4. Protect against ransomware

Ransomware restricts access to data by encrypting files or locking computer screens. It then attempts to extort money from victims by asking for "ransom," usually in form of cryptocurrencies like bitcoin to retrieve the lost data.

You can protect against ransomware by creating one or more mail flow rules to warn users who receive these attachments in email as office 365 defender is already configured to block most file types.

Warn users before opening office file attachments that include macros. Ransomware can be hidden inside macros, so we'll warn users to not open these files from people they do not know.

5. Stop auto-forwarding for email

Hackers who gain access to a user's mailbox can exfiltrate mail by configuring the mailbox to automatically forward email. This issue can happen even without the user's awareness. You can prevent this from happening by configuring a mail flow rule.

6. Use office message encryption

Office message encryption is included with Microsoft 365. It's already set up. With office message encryption, your organization can send and receive encrypted email messages between people inside and outside your organization. Office 365 message encryption works with outlook.Com, yahoo!, Gmail, and other email services. Email message encryption helps ensure that only intended recipients can view message content.

7. Protect your email from phishing attacks

If you've configured one or more custom domains for your Microsoft 365 environment, you can configure targeted anti-phishing protection. Anti-phishing protection, a part of Microsoft defender for office 365, can help protect your organization from malicious impersonation-based phishing attacks and other phishing attacks. If you haven't configured a custom domain, you do not need to do this.

8. Protect against malicious attachments and files with safe attachments

People regularly send, receive, and share attachments, such as documents, presentations, spreadsheets, and more. It's not always easy to tell whether an attachment is safe or malicious just by looking at an email message. Microsoft defender for office 365 includes safe attachment protection, but this protection is not turned on by default. We recommend that you create a new rule to begin using this protection. This protection extends to files in sharepoint, onedrive, and Microsoft teams.

9. Protect against phishing attacks with safe links

Hackers sometimes hide malicious websites in links in email or other files. Safe links, part of Microsoft defender for office 365, can help protect your organization by providing time-of-click verification of web addresses (urls) in email messages and office documents. Protection is defined through safe links policies.

10. Enable unified audit log (ual)

O365 has a logging capability called the unified audit log that contains events from exchange online, sharepoint online, onedrive, azure ad, Microsoft teams, powerbi, and other o365 services.[4] An administrator must enable the unified audit log in the security and compliance center before queries can be run. Enabling ual allows administrators the ability to investigate and search for actions within o365 that could be potentially malicious or not within organizational policy.

11. Disable legacy protocol authentication when appropriate

Azure ad is the authentication method that o365 uses to authenticate with exchange online, which provides email services. There are a number of legacy protocols associated with exchange online that do not support mfa features. These protocols include post office protocol (pop3), internet message access protocol (imap), and simple mail transport protocol (smtp). Legacy protocols are often used with older email clients, which do not support modern authentication. Legacy protocols can be disabled at the tenant level or at the user level. However, should an organization require older email clients as a business necessity, these protocols will presumably not be disabled. This leaves email accounts accessible through the internet with only the username and password as the primary authentication method. One approach to mitigate this issue is to inventory users who still require the use of a legacy email client and legacy email protocols and only grant access to those protocols for those select users

12. Enable alerts for suspicious activity

Enabling logging of activity within an azure/0365 environment can greatly increase the owner's effectiveness of identifying malicious activity occurring within their environment and enabling alerts will serve to enhance that. Creating and enabling alerts within the security and compliance center to notify administrators of abnormal events will reduce the time needed to effectively identify and mitigate malicious activity.[6] At a minimum, cisa recommends enabling alerts for logins from suspicious locations and for accounts exceeding sent email thresholds.

13. Azure conditional access

You can further guard the access to the office 365 tenant by implementing azure ad conditional access functionality. It allows us to safeguard the tenant based on a myriad of conditions like location, ip address, and application usage. When combined with other ad user properties like department, it is easy to block users from, for example, the marketing department to connect to office 365 from a suspicious, non-company location.

14. Azure information protection

In many office 365 deployments, the most critical data is often stored in Microsoft office documents. Azure information protection allows us to protect documents from being shared, and , as well as emails to be forwarded. In essence, it encrypts the document, and only authorized, hand-picked personnel can decrypt its contents.

The following file types are supported:

- Adobe portable document format: .Pdf
- Microsoft project: .Mpp, .Mpt
- Microsoft publisher: .Pub
- Microsoft xps: .Xps .Oxps
- Images: .Jpg, .Jpe, .Jpeg, .Jif, .Jfif, .Jfi. Png, .Tif, .Tiff
- Autodesk design review 2013: .Dwfx
- Adobe photoshop: .Psd
- Digital negative: .Dng
- Microsoft office

15. Sharing links

On top of external sharing controls, it is crucial to configure the types of sharing links that your users can generate by default. The best practice would be to stick to the option "specific people (only the people the user specifies)." With this option selected, even if a user forwards a link to someone else in your organization, this user would not be able to open the document.Properties like department, it is easy to block users from, for example, the marketing department to connect to office 365 from a suspicious, non-company location.

16. Train your users

The final step is to train your users. Follow the link for some excellent Microsoft resources.