SHARTEGA.IT

10 WAYS TO SECURE MICROSOFT 365 FOR BUSINESS

powered by Microsoft

SHARTEGA.COM
(773) 305-3535

Security Tasks To Complete

If you are a small or medium-size organization using one of Microsoft's business plans, you can use the guidance in this document to increase the security of your organization.

01

Set up multi-factor authentication

Protect against lost or stolen passwords by using multifactor authentication (MFA). When multifactor authentication is set up, it requires people to use a code on their phone to sign into Microsoft 365. This extra step can prevent hackers from taking over if they know your password.

02

Train your users

The Harvard Kennedy School Cybersecurity Campaign Handbook provides excellent guidance on establishing a strong culture of security awareness within your organization, including training users to identify phishing attacks.

03

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 cyberattackers. 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.

04

Protect against malware

Your Microsoft 365 environment includes protection against malware. You can increase your malware protection by:

- Blocking attachments with certain file types
- Using antivirus/antimalware protection on your devices

05

Protect against ransomware

You can protect against ransomware by creating one or more mail flow rules to block file extensions that are commonly used for ransomware, or to warn users who receive these attachments in email.

06

Stop auto-forwarding in 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.

07

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.

08

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.

09

Protect against malicious attachments, files, and URLs

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.

10

Increase protection for your organization's devices

Microsoft Defender Antivirus is built into the Windows operating system and provides good protection against viruses and malware. However, you can increase protection for your organization's devices by onboarding them to Microsoft Defender for Business, a new offering for small and medium-sized businesses like yours. **Beginning March 1, 2022, Microsoft Defender for Business capabilities are being added to Microsoft 365 Business Premium.**