Zeifmans
Ideas with impact

Protect your business with this Microsoft cyber security checklist

Many businesses have no idea how easy it is to get defrauded, hacked or compromised, especially after companies switched to a remote work model and started using the cloud. They're also likely not to know about Microsoft's threat protection, data protection and device management features.

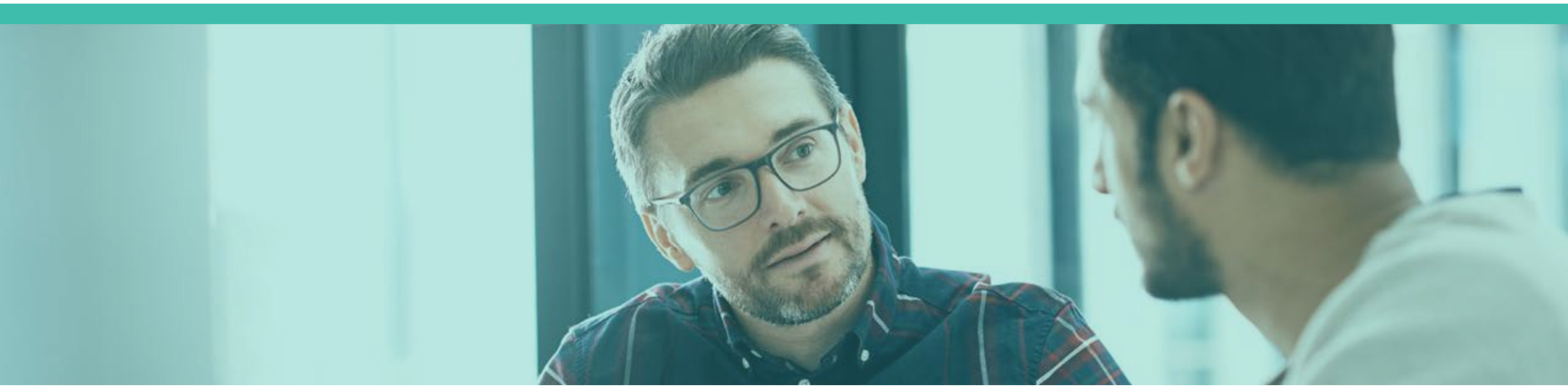
If your company uses Microsoft's 365 Business Premium plan, there are a variety of features you can take advantage of to increase your security and protect your business from any threats.

10 steps to protect your business from cyber security risks:

1 Set up multi-factor authentication:

This is part of the zero-trust security method and adds an essential extra step to the log-in process. It forces users to type in a code from their phones before they're able to log into Microsoft 365. Enabling this extra step will stop hackers even if they have your password. This can also be done for your email account.

For steps on setting up multi-factor authentication in Microsoft, **click here.**



2 Make sure employees are up to date on cyber security best practices

Educated users are less likely to make security mistakes. Ensure your employees use strong passwords, protect their devices through steps like multi-factor authentication, understand what phishing attacks are and enable security features on Windows or Mac PCs.

It's also important for employees to take measures to protect their personal **Outlook** or **Gmail** accounts.

3 Create dedicated admin accounts

Your Microsoft 365 admin accounts are tempting targets for hackers. Since these accounts have more privileges than regular ones, it's important that they're only used for administration tasks. These accounts should also have multi-factor authentication and admin employees should have regular accounts for any other duties.

When using an administrative account, make sure you've closed any unrelated tabs on your computer and always log out after your task is complete.

4 Protect yourself against malware

Many employers don't know about Microsoft 365's malware protection features. These features can identify file types that are commonly used for malware and can block those attachments.

To enable these features, check out a **tutorial here,** or watch **this video.**

5 Use ransomware protection

Don't let a hacker take your data hostage through ransomware (when someone tries to freeze your computer and demands money, often in cryptocurrency, for access.)

Microsoft 365 allows you to create mail flow rules (which lets users set up certain actions or messages that are sent or enacted when certain qualifications are met).

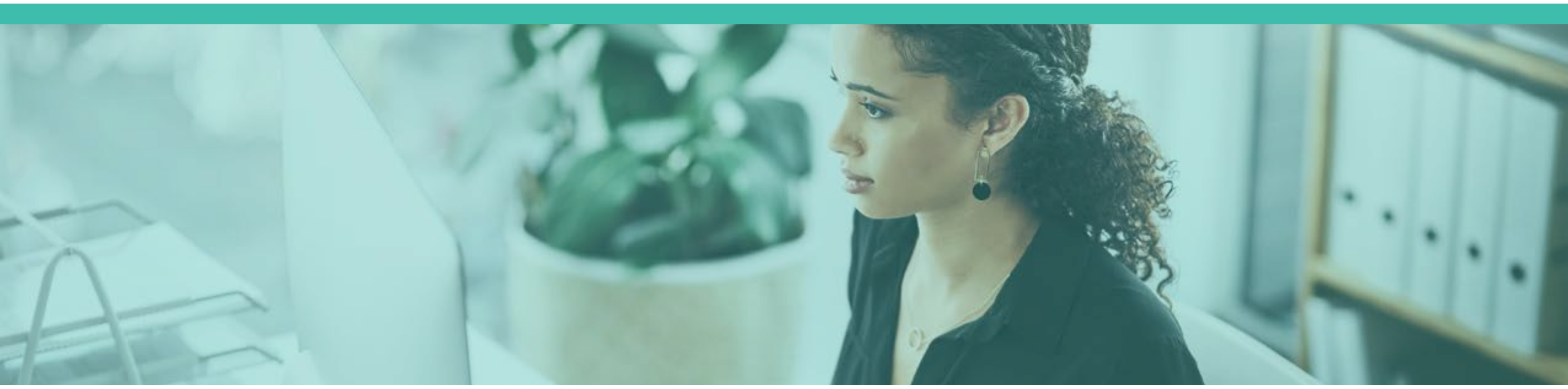
Create a mail flow rule that will block ransomware file extensions and/or warn users who get these attachments.

To do this, check out a **training video** or **click here** for a step-by-step tutorial.

6 Don't allow email auto-forwarding

If a hacker is able to hack your mailbox, they can use auto-forwarding to gain access to all your email without you knowing.

To prevent this, Microsoft 365 lets you create a mail flow rule that stops auto-forwarding. For a tutorial, **click here.**



7 Start using your Office Message Encryption

Your Microsoft 365 account already has Office Message Encryption set up. This feature allows you to safely send messages to other accounts outside your business. Only the intended recipient will be able to view your message.

Message encryption includes two options: Do not forward and Encrypt, though it's possible to create more options, such as Confidential Mail

Microsoft's encryption works with Outlook, Yahoo, Gmail and a variety of other services.

To send or receive encrypted mail, check out this simple **tutorial.**

8 Prevent phishing attacks

Office 365's Microsoft Defender allows users to configure targeted anti-phishing protection.

Your business can create anti-phishing policies that specifically protect certain users and your domain. For steps on how to do this, check out this **video** or this **tutorial.**

9 Use Microsoft's Safe Attachments feature

Microsoft Defender includes a Safe Attachment feature, which protects users from accidentally sending suspicious email attachments.

It uses a virtual environment to inspect inbound email attachments after anti-malware protection has scanned them but before they've been delivered.

Configure this feature through this simple **tutorial,** or watch a video **here.**

10 Use Safe Links for added phishing protection

Microsoft Defender has a Safe Links feature which provides time-of-click verification for URLs in Office docs or emails. This helps protect against malicious links hidden in these files or emails.

To set this feature up, check out this **tutorial** or watch this **video.**

The strategies, advice and technical content in this publication are provided for general information only. This publication is not intended to provide specific financial, tax, accounting or other advice for you, and should not be relied upon in that regard. Readers should consult with their professional advisor when planning to implement a strategy to ensure that individual circumstances have been considered properly and it is based on the latest available information.

Zeifmans LLP is a member of Nexia International, a worldwide network of independent accounting and consulting firms. Nexia International Limited does not deliver services in its own name or otherwise. Nexia International Limited and the member firms of the Nexia International network (including those members which trade under a name which includes the word NEXIA) are not part of a worldwide partnership. Nexia International Limited does not accept any responsibility for the commission of any act, or omission to act by, or the liabilities of, any of its members. Each member firm within the Nexia International network is a separate legal entity.