16 MICROSOFT OUTLOOK SECURITY & OPTIMIZATION TIPS

This article provides advice on how to increase Outlook productivity, improve security, and get the most out of this critical program. We can assist you in protecting your account if you receive a link in an email that appears to be from your bank but isn't fake notifications from social networking sites or malicious advertisements. We stay up to date on the latest scams, so you don't have to. Though we protect your account from a variety of threats, there are several steps you can take to keep your account and personal information safe.

OUTLOOK SECURITY TIPS

1. Outlook User Email Security Tips

- If you see a yellow safety bar at the top of your message, then the message contains blocked attachments, pictures, or links to websites. Ensure you trust the sender before downloading any attachments or images or clicking any links. Emailing the sender to verify they intended to send you an attachment is also a good practice for any attachments you're not expecting.
- A red safety bar means that the message you received contains something that might be unsafe and has been blocked by Outlook.com. We recommend that you don't open those email messages and delete them from your inbox.
- When you add an address to your Outlook safe sender’s list, all messages you receive from that address go right to your inbox. Adding a sender to your blocked sender’s list sends messages from that address to your Junk email folder.
- If the URL that appears in the address bar when you sign in doesn't include login.microsoftonline.com or login.live.com, you could be on a phishing site. Don't enter your password. Try to restart your browser and navigate to login.microsoftonline.com or Outlook.com again. If the problem continues, check your computer for viruses.

2. Use Multi-Factor Authentication.

- Multi-factor authentication (MFA) also known as two-step verification, requires people to use a code or authentication app on their phone to sign into Outlook and Microsoft 365,

and is a critical first step to protecting your business data. Using MFA can prevent hackers from taking over if they know your password.

3. Protect Your Administrator Accounts.

- Administrator accounts (also called admins) have elevated privileges, making these accounts more susceptible to cyberattacks. You'll need to set up and manage the right number of admin and user accounts for your business. We also recommend adhering to the information security principle of least privilege, which means that users and applications should be granted access only to the data and operations they require to perform their jobs.

4. Use Preset Security Policies.

- Your subscription includes preset security policies that use recommended settings for anti-spam, anti-malware, and anti-phishing protection.

5. Protect All Devices.

- Every device is a possible attack avenue into your network and must be configured properly, even those devices that are personally owned but used for work.
    - Help users set up MFA on their devices
    - Protect unmanaged Windows and Mac computers
    - Set up managed devices (requires Microsoft 365 Business Premium or Microsoft Defender for Business)

6. Train Everyone On Email Best Practices.

- Email can contain malicious attacks cloaked as harmless communications. Email systems are especially vulnerable because everyone in the organization handles email, and safety relies on humans making consistently good decisions with those communications. Train everyone to know what to watch for spam or junk mail, phishing attempts, spoofing, and malware in their email.

7. Use Microsoft Teams For Collaboration And Sharing.

- The best way to collaborate and share securely is to use Microsoft Teams. With Microsoft Teams, all your files and communications are in a protected environment and aren't being stored in unsafe ways outside of it.

- Use Microsoft Teams for collaboration.
- Set up meetings with Microsoft Teams
- Share files and videos in a safe environment

8. Set Sharing Settings For SharePoint And OneDrive Files And Folders.

- Your default sharing levels for SharePoint and OneDrive might be set to a more permissive level than you should use. We recommend reviewing and if necessary, changing the default settings to better protect your business. Grant people only the access they need to do their jobs.

9. Use Microsoft 365 Apps On Devices.

- Outlook and Microsoft 365 Apps (also referred to as Office apps) enable people to work productively and more securely across devices. Whether you're using the web or desktop version of an app, you can start a document on one device and pick it up later on another device. Instead of sending files as email attachments, you can share links to documents that are stored in SharePoint or OneDrive.

10. Manage Calendar Sharing For Your Business.

- You can help people in your organization share their calendars appropriately for better collaboration. You can manage what level of detail they can share, such as by limiting the details that are shared to free/busy times only.

11. Maintain Your Environment.

- After your initial setup and configuration of Microsoft 365 for business is complete, your organization needs a maintenance and operations plan. As employees come and go, you'll need to add or remove users, reset passwords, and maybe even reset devices to factory settings. You'll also want to ensure people have only the access they need to do their jobs.

TOP 10 MICROSOFT OUTLOOK TIPS TO BOOST PRODUCTIVITY

12. Create Folders To Organize Your Emails.

- This is the apparent first step if you want to simplify how you use email. However, it may also be the most difficult, particularly if your inbox is overloaded. Even so, it makes the most sense to organize your emails into a user-friendly folder system so that you won't have to spend hours sifting through hundreds of emails in search of the one you're looking for. An easy-to-use folder system will also encourage you to respond to each email as it comes in rather than putting it off till later all the time.

13. Utilize The Simple Email Templates Provided By Outlook.

- Save one of the emails as a template if you frequently write the same type of message so that you may conveniently access it in the future when you're ready to use that previously saved form.

14. Accept The Web-Based Future Of Outlook.

- Most of the email, calendar, and contact infrastructure is moved to a web-based view in Outlook Office 365, and other recent versions of the program so that it can be accessed on any device. Even sending brief notes amongst coworkers is straightforward with Microsoft's Send email software for cellphones, which also enters all the communications into your Microsoft Outlook history for convenient archiving and access.

15. Adjust Desktop Notifications So That You Only Receive Critical Messages.

- If you get a notification every time a message arrives in your inbox, you'll be distracted. But you don't want to miss important emails, so disable desktop alerts in File > Options > Mail Options, then create a custom rule to only display alerts for messages sent to you by specific contacts.

16. Make A Folder For Frequently Used Searches.

- Looking for a specific folder among a hundred can be time-consuming if you still do so by typing words or phrases into the search field above the message list. You can, however, make the job easier by creating a "Search" folder for frequently searched terms.
- To make one, go to the "Folder" tab and right-click on "Search Folder.

Read more