londonist
DMC

Londonist **IT** Guide

Welcome to the IT Guide,

This guide is designed to help you understand and effectively use the IT tools, applications, and security practices provided by Londonist. Our goal is to ensure secure, efficient, and smooth daily operations for everyone.

Before contacting the IT team, please review this guide. If you cannot find the answer you are looking for, the IT team will be happy to assist you.

Table of Contents

1- Email Security & Spam Awareness

1.1 - Non-domain Emails
1.2-Copied or Imitated Email Addresses
1.3-Spam & Phishing Reports

2- DefensX (Web & Network Security)

3- Computer Permissions & Software Installation

4- Two-Factor Authentication (2FA)

5- AnyDesk (Remote Support)

6- DeskTime (Time Tracking)

7- Jira Help Center (IT Support Requests)

8- Layer Zero Security (Basic Security Rules)

9- AI Usage & Acceptable Use Policy

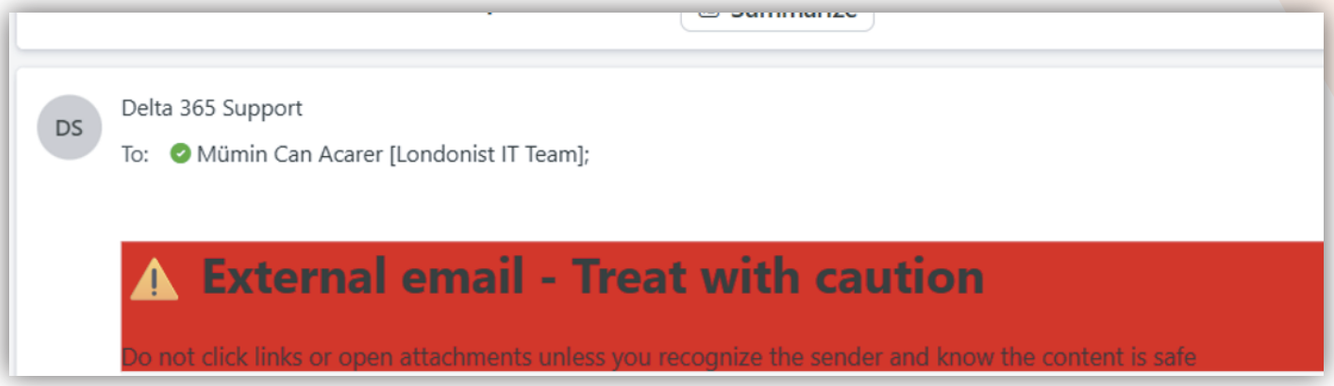
10- Out of Office & Away Message

1-Email Security & Spam Awareness

Email is one of the most common attack vectors in cybersecurity.
Please read this section carefully.

1.1-Non-domain Emails

We should always be careful with emails from outside our domains. Email from unverified domains may contain threats. Non-domain emails are marked as red external emails.



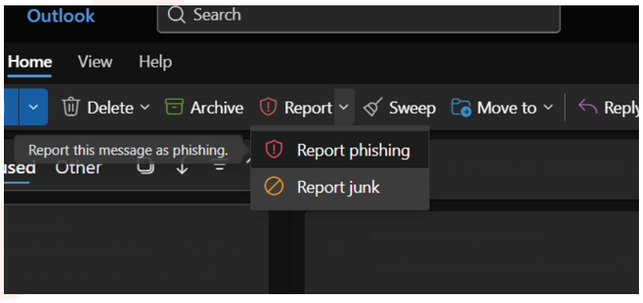
1.2-Copied or Imitated Email Addresses

As can be seen in the example, a spam domain could send emails from a copied name. Check the domain name. It might be a scam with some letter changes.



1.3-Spam & Phishing Reports

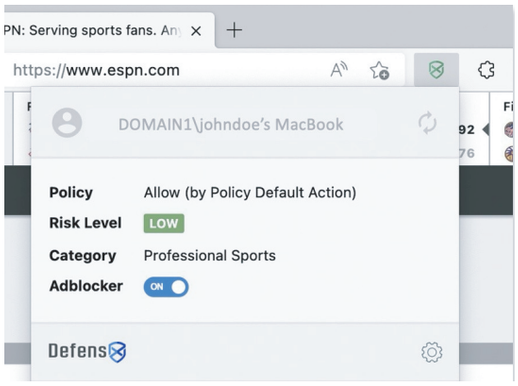
When you receive a suspicious or threatening email, do not click on the incoming links and do not send any reply. Report the issue to the IT team immediately. You can mark the email as spam and have the system automatically block the upcoming emails.

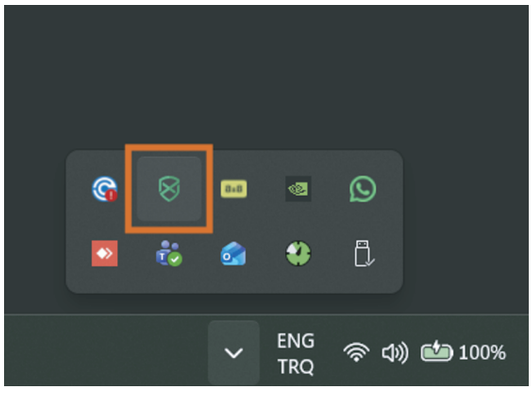


2-DefensX (Web & Network Security)

DefensX is used to protect company devices from malicious websites and unsafe network traffic.

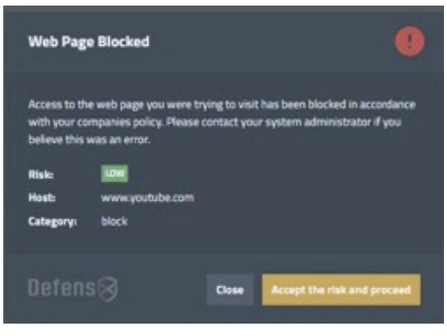
•DefensX runs on both your browser and computer
•It may block access to dangerous or policy-restricted websites



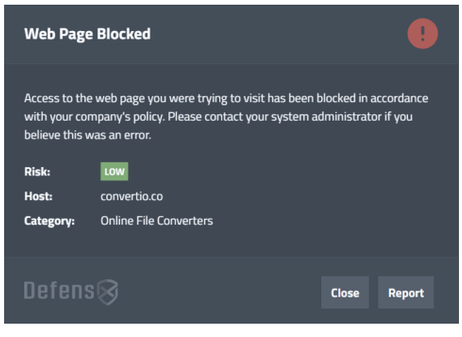


Blocked Pages

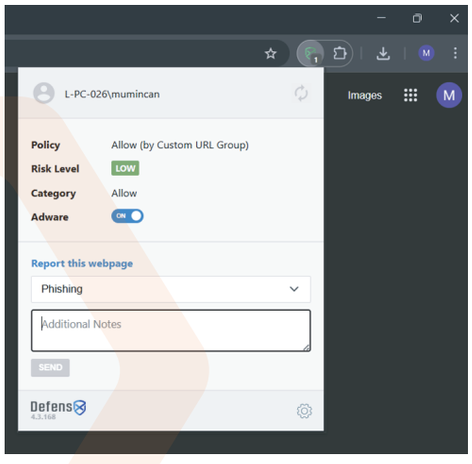
You may encounter different block screens:



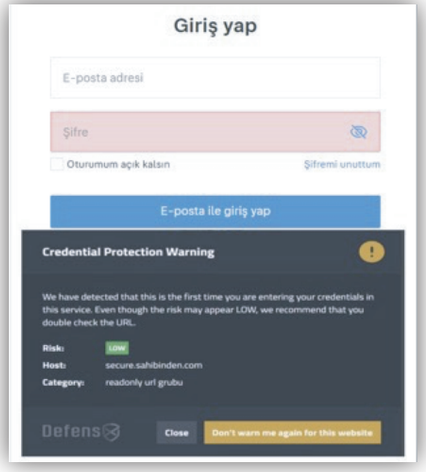
If you believe the block is incorrect, you may proceed and inform the IT team



If the page looks suspicious, report it using the DefensX report button.



If you believe the block is incorrect, you may proceed and inform the IT team



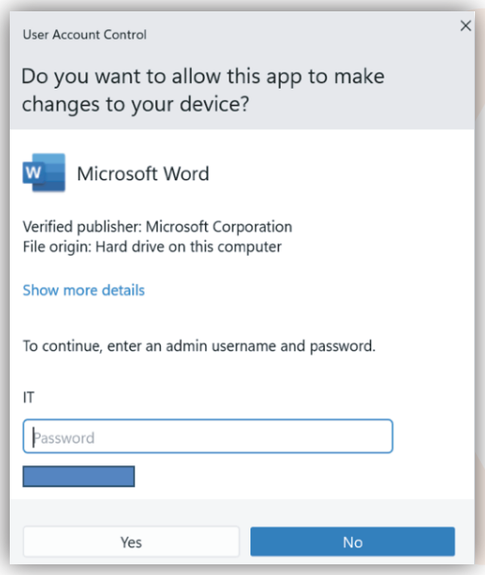
If the page looks suspicious, report it using the DefensX report button.

3-Computer Permissions & Software Installation

Company computers are pre-configured according to security policies.

- Software installation requires administrator permission
- Do not install unauthorized applications
- Contact IT for any required changes or new tools

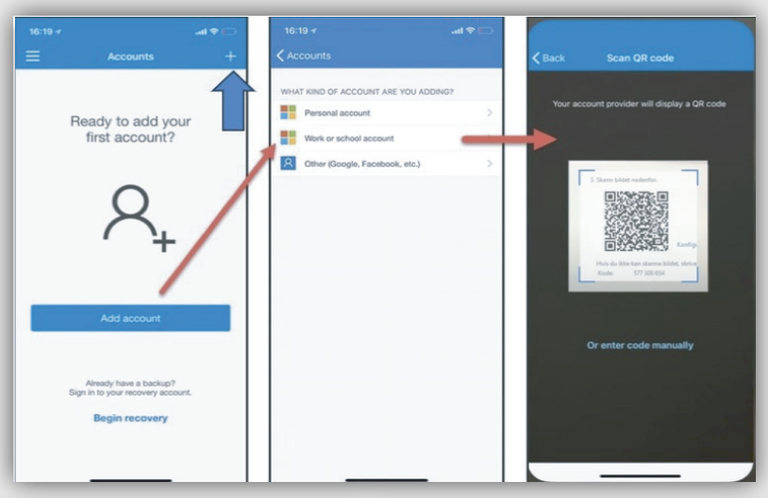
This ensures system stability and data security.

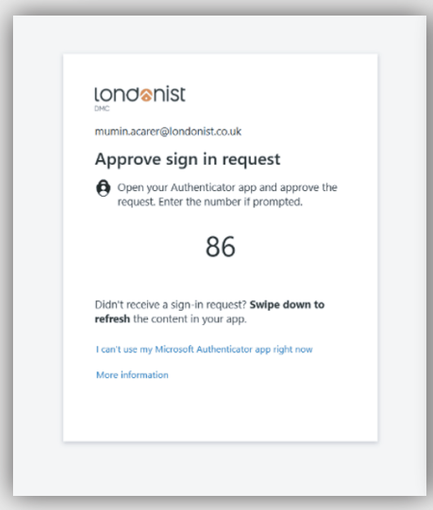


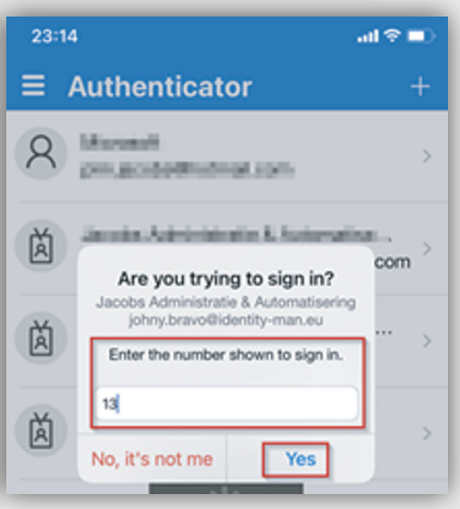
4-Two-Factor Authentication (2FA).

To enhance account security, two-factor authentication (2FA) is mandatory.
•The Microsoft Authenticator app is pre-installed on company mobile phones.
•Login requests must be approved via the Microsoft Authenticator app.

Account Setup Steps

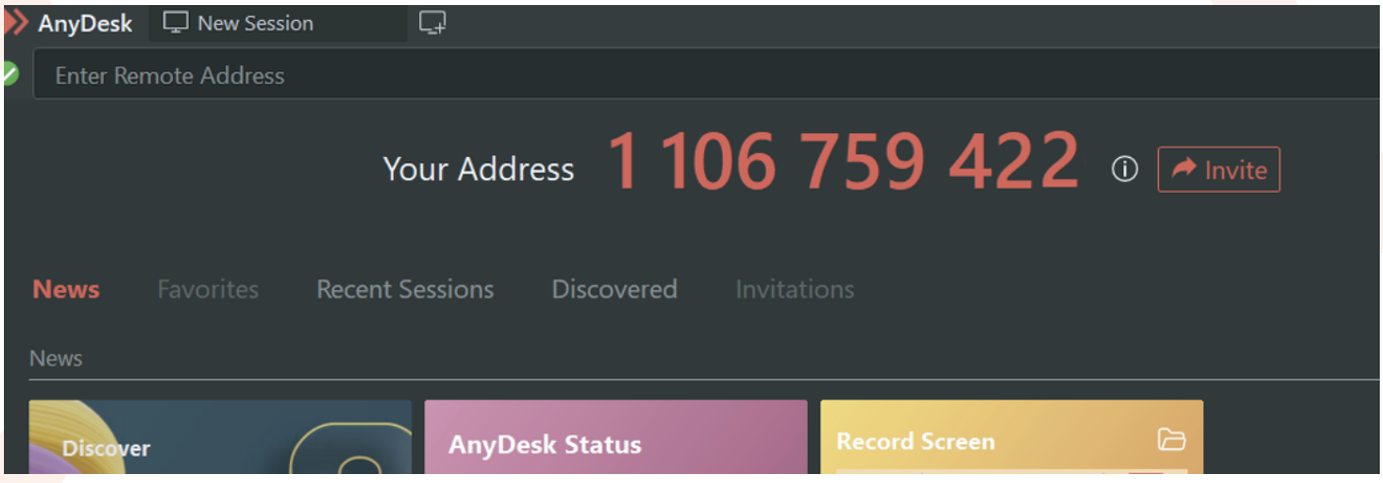




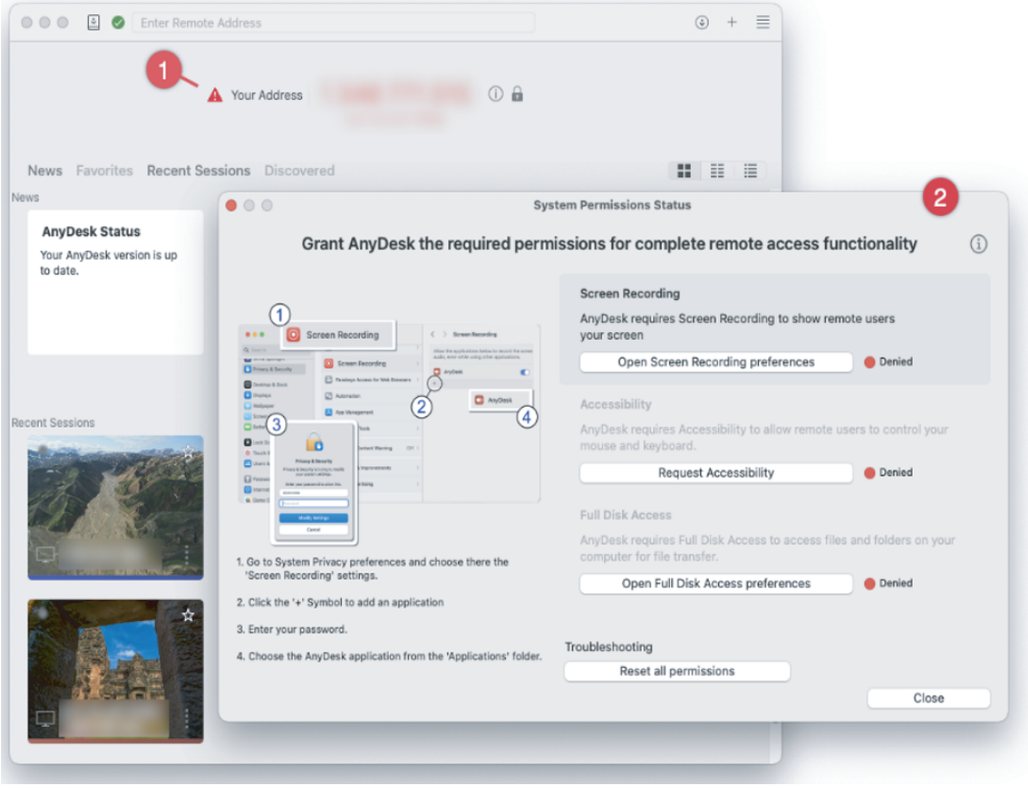


5-AnyDesk (Remote IT Support)

AnyDesk allows IT to provide remote support when needed.
- Share your AnyDesk ID with IT
- Approve the connection request

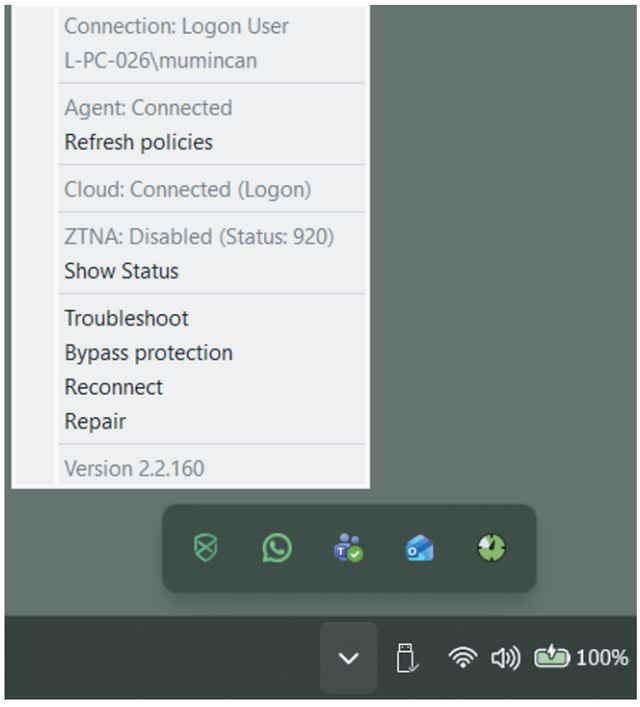


You may need to change some additional settings on MacBook computers before connecting the IT staff.

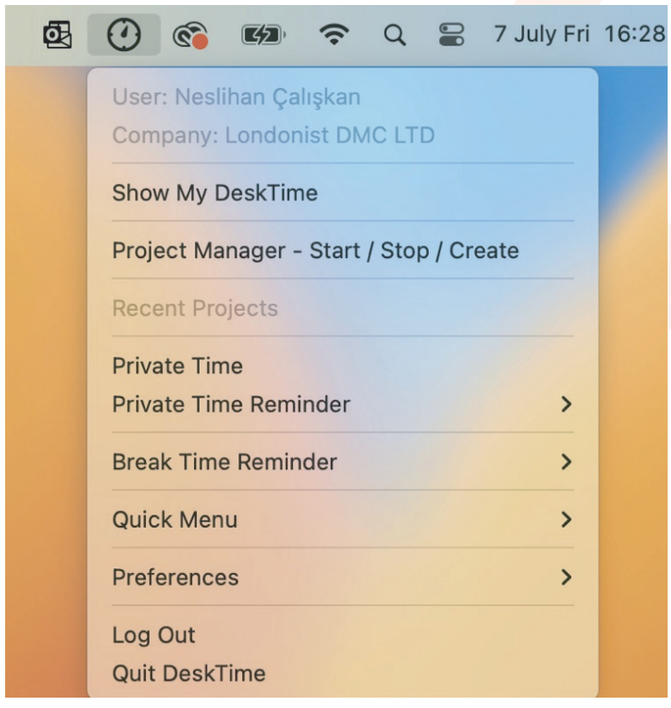


6-DeskTime (Time Tracking)

We are tracking your activities during the working hours. Shortcuts allow you to manage the login, logout, and project time sections.

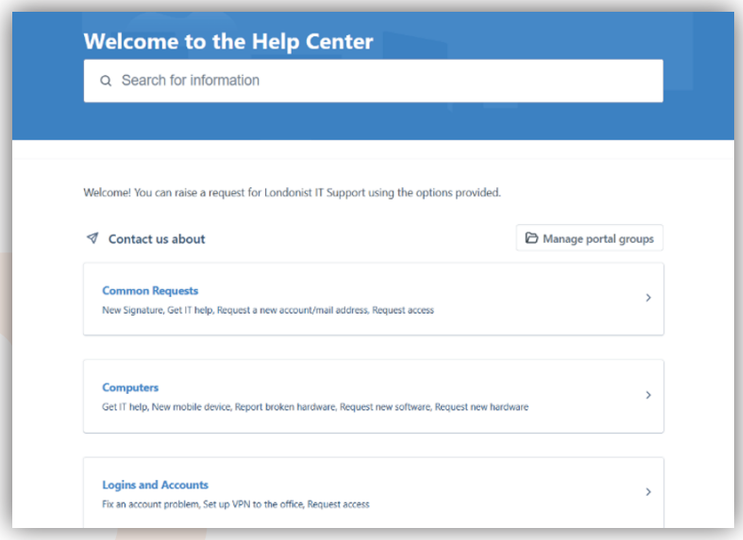


Windows



MacOS

7-Jira Help Center (IT Support Reques



1. Select the correct request category
2. Provide clear and detailed descriptions
3. Add screenshots if possible

All IT-related requests must be submitted through the Jira Help Center:
https://londonistdmc.atlassian.net/servicedesk/customer/portal/

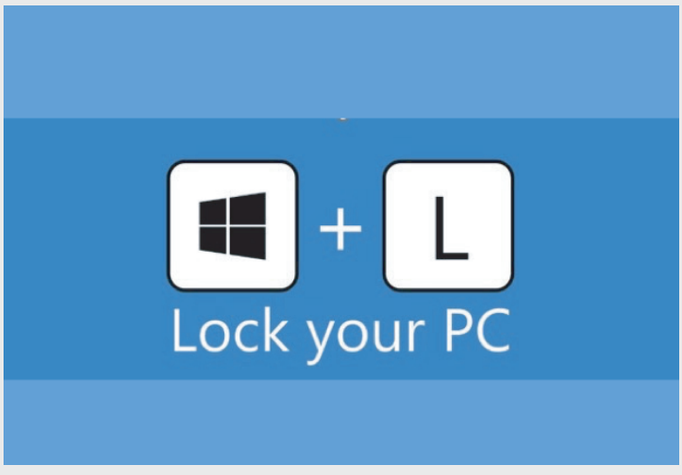
Marketing-related requests are handled via a separate form:
https://forms.monday.com/forms/952c522323160e6a779147df08607d04

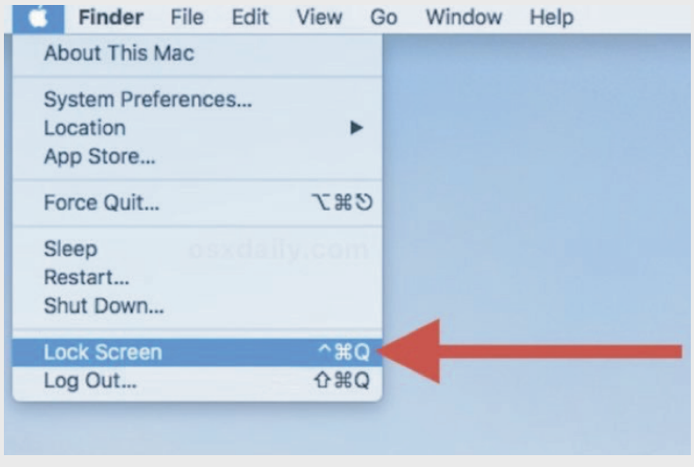
7-Layer Zero Security (Basic Rules)

These are fundamental rules everyone must follow:

Never connect company devices to public or unsecured Wi-Fi networks
Examples: cafes, restaurants, shopping malls. Passwords must never be shared with colleagues, managers, or third parties. Always use a password on company devices







Lock your screen during breaks

Security starts with individual responsibility.

9-AI Usage & Acceptable Use Policy

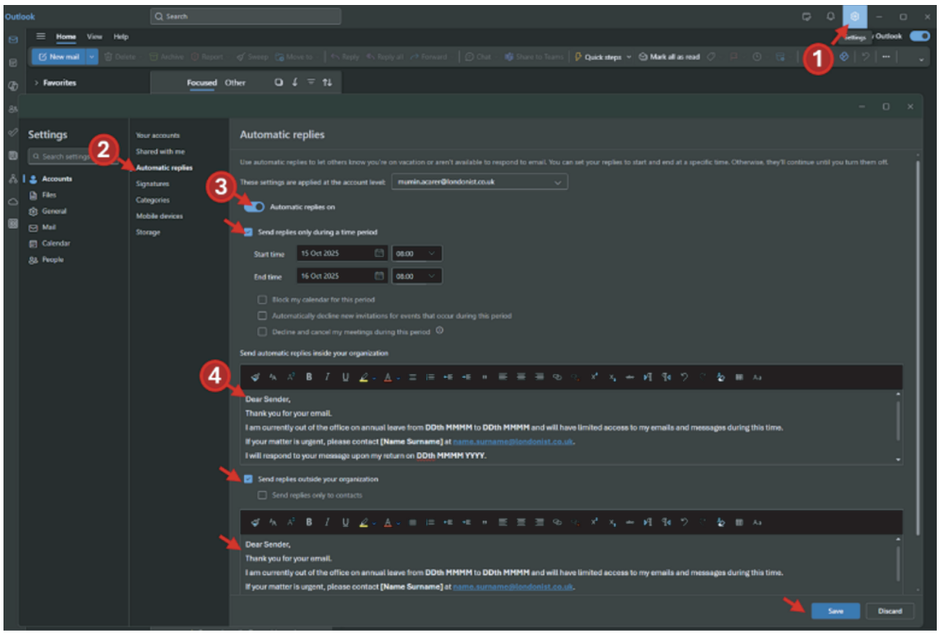
Artificial Intelligence (AI) tools can significantly improve productivity; however, they also introduce data security, confidentiality, and compliance risks. Before using any AI platform for work-related purposes, employees must follow the rules below.

Londonist AI Policy:

https://people.londonistglobal.com/courses/generative-ai-acceptable-use-policy/

10-Out of Office & Away Message Guidelines

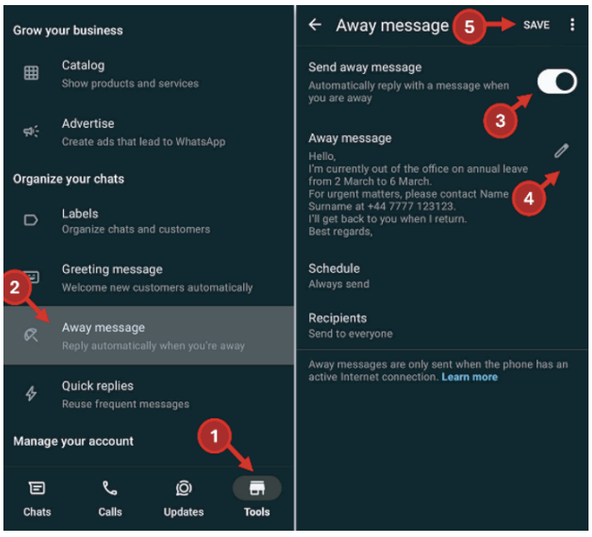
1. Open Outlook (desktop or web)
2. Go to Settings → Automatic Replies (Out of Office)
3. Turn on Send automatic replies and set your leave dates



WhatsApp Business – Away Message

If you use WhatsApp Business for work purposes, please also set an Away Message for the same dates.

- Open WhatsApp Business.
- Go to Settings → Business Tools → Away Message.
- Turn on Send away message and set your leave dates.



Note: WhatsApp Away Messages only work when the phone is powered on and connected to the internet; messages will not be sent if the device is offline.