Title

EMAIL SOLUTION AND THREAT PROTECTION IN MICROSOFT 365

Smart Technologies (BD) Ltd.

Jahir Smart Tower 205/1 & 205/1/A,

West Kafrul, Taltola, Dhaka-1207.

+8802-58157002, +8802-58153040.

Info@Smartbd.Com

https://smartbd.com/

https://smart-bd.com/

Microsoft 365 Email Solution: Exchange Online

Overview of Exchange Online

Features	Description
Email Hosting	Exchange Online is a cloud-based email server, that hosts business email accounts and enables users to send and receive emails.
Calendaring	Users can manage and share calendars, schedule appointments, and set reminders. Calendar events can be accessed across various devices.
Contacts and Address Book	Exchange Online includes a shared address book and contact management system, making managing and sharing contact information within the organization easy.
Tasks and To-Do Lists	Users can create tasks and to-do lists, helping them stay organized and manage their workload efficiently.
Web-Based Access (Outlook Web App)	Access your emails, calendar, and contacts through a web browser using Outlook on the Web (formerly known as Outlook Web App), providing flexibility in accessing email from any device with internet access.
Mobile Device Support	Exchange Online is compatible with a variety of mobile devices, allowing users to access their email, calendar, and contacts on smartphones and tablets.
Security and Compliance	Exchange Online incorporates robust security features, including antivirus and anti-spam filtering. It also supports data loss prevention (DLP) policies to protect sensitive information.
Archiving and Retention	Automatic archiving and retention policies help manage mailbox sizes, ensuring that important emails are retained and accessible while maintaining optimal performance.

Integration with Office Apps	Tight integration with other Microsoft 365 apps such as Word, Excel, PowerPoint, and SharePoint, facilitating seamless collaboration and communication.
Unified Messaging	Exchange Online offers unified messaging capabilities, integrating voicemail and email into a single inbox for users.
Resource Mailboxes	Resource mailboxes, such as conference rooms or equipment mailboxes, can be created and managed for efficient scheduling of resources.
Hybrid Deployments	Exchange Online supports hybrid deployments, allowing organizations to integrate their on-premises Exchange Server with the cloud-based Exchange Online.
Advanced Threat Protection	Additional security features, including Advanced Threat Protection (ATP), help protect against advanced security threats and phishing attacks.
Compliance Center:	Compliance features enable organizations to meet regulatory requirements by providing tools for eDiscovery, retention policies, and legal hold.

Use Case: Email Communication Security

Scenario:

For example, an organization regularly exchanges sensitive documents and information via email. Employees collaborate on projects, sharing files and links to enhance productivity. The use case involves securing this email communication to mitigate risks associated with malware, unauthorized access, and phishing attacks.

Email Security Assessment

- Are user accounts configured securely?
- Is multi-factor authentication (MFA) enabled for all users?
- Are domain settings configured to prevent spoofing and phishing?
- Is email content encrypted for sensitive information?
- Are policies scanning and filtering attachments for malware?
- Is link protection activated to block malicious URLs?
- Are spam filtering measures and policies up to date?

Recommendations

Enhance Attachment Security:

- Implement advanced attachment filtering.
- Enable real-time scanning of email attachments.

Reinforce Link Protection:

- Conduct user training on recognizing and reporting phishing attempts.
- Review and strengthen link protection policies.

Optimize Spam Mail Control:

- Regularly update and customize spam control policies.
- Leverage machine learning capabilities for adaptive filtering.

Setting Up Email Communication in Microsoft 365

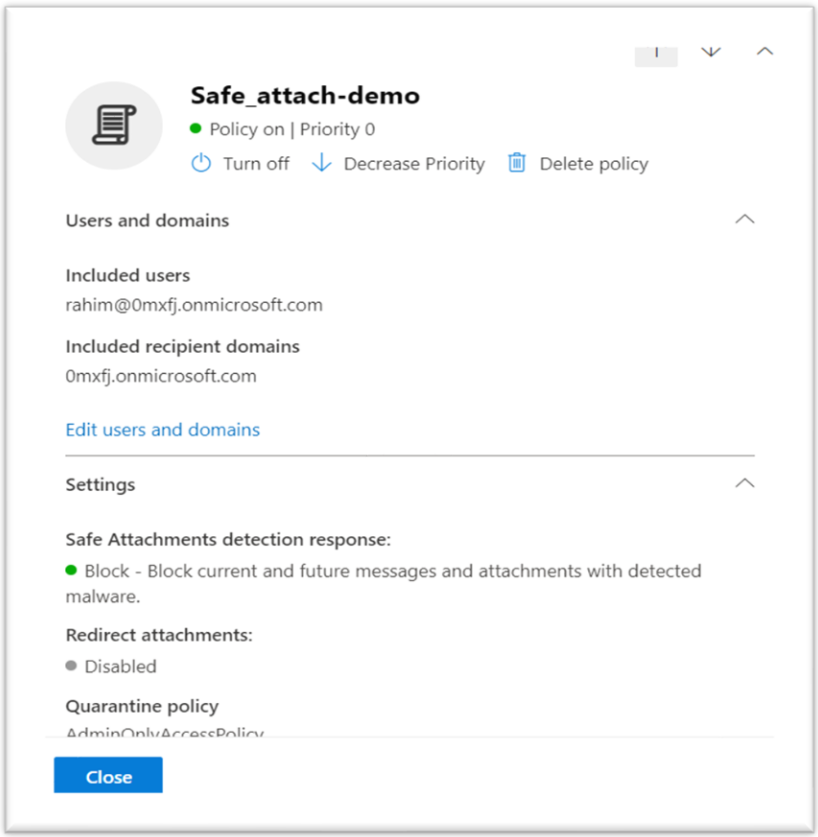
Steps Taken

- ✓ User account creation and management within Microsoft 365.
- ✓ Implement multi-factor authentication (MFA) for an added layer of security.
- ✓ Configuration of email accounts for seamless communication.
- ✓ Verification of domain settings to prevent spoofing and phishing attempts.

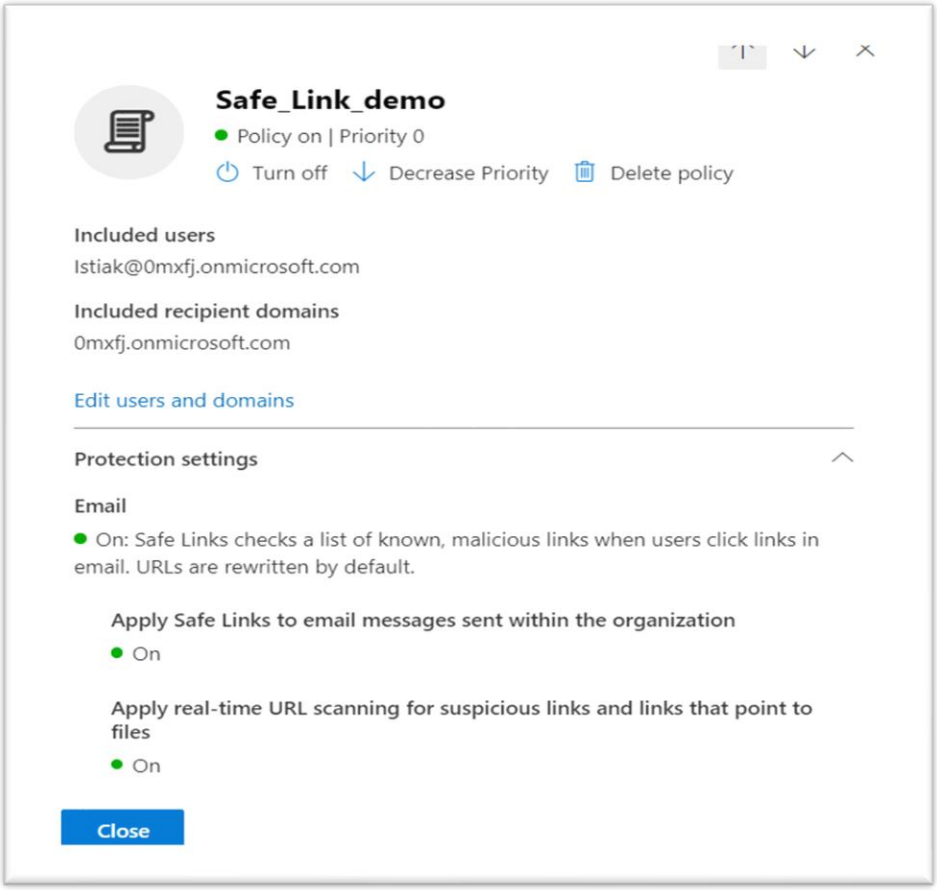
Security Policies in Microsoft Defender for Office 365

Policies Implemented

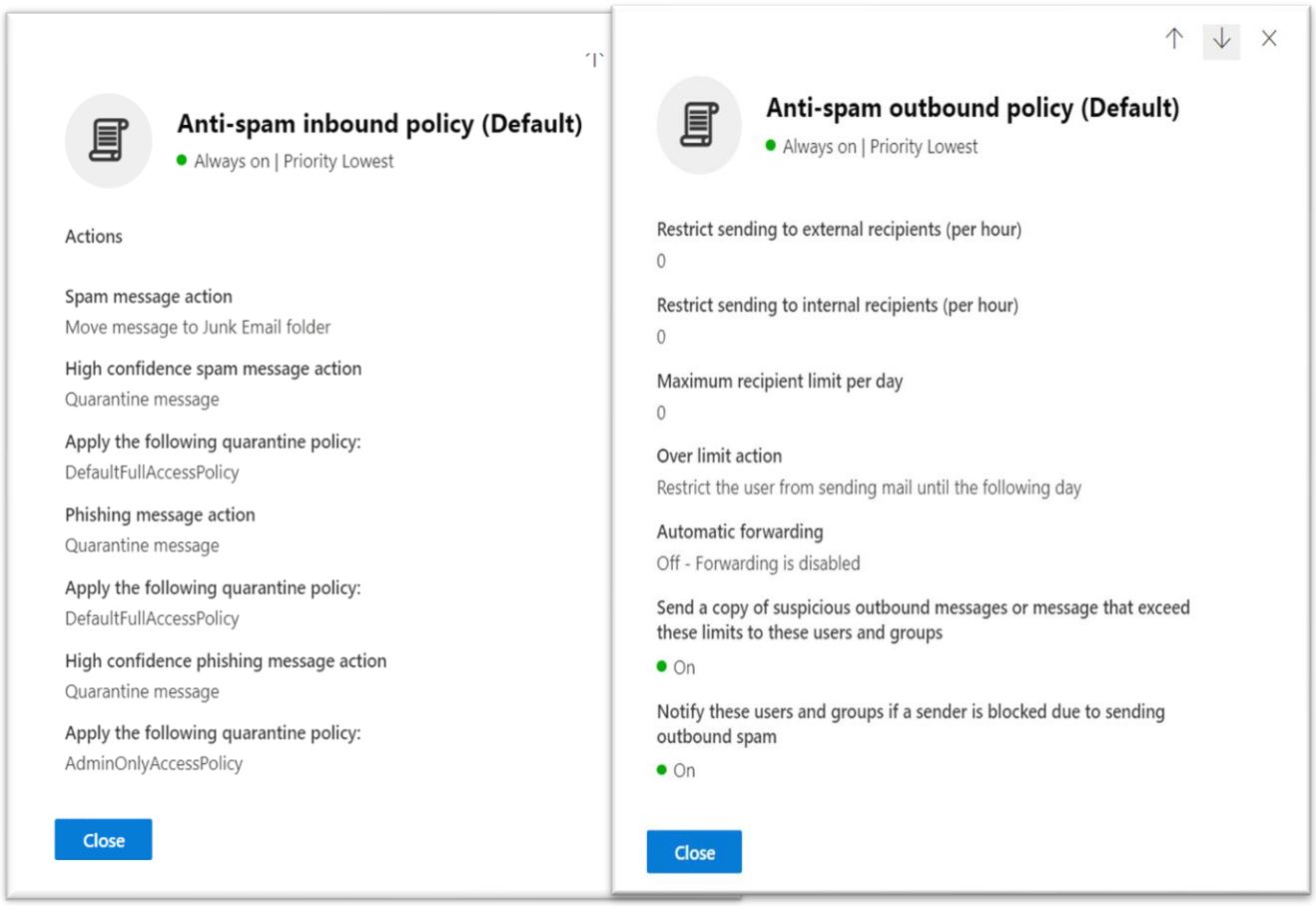
Safe Email Attachments	• Implementation of policies to scan and filter email attachments for malware. • Configuration of attachment restrictions to prevent the transmission of potentially harmful files.



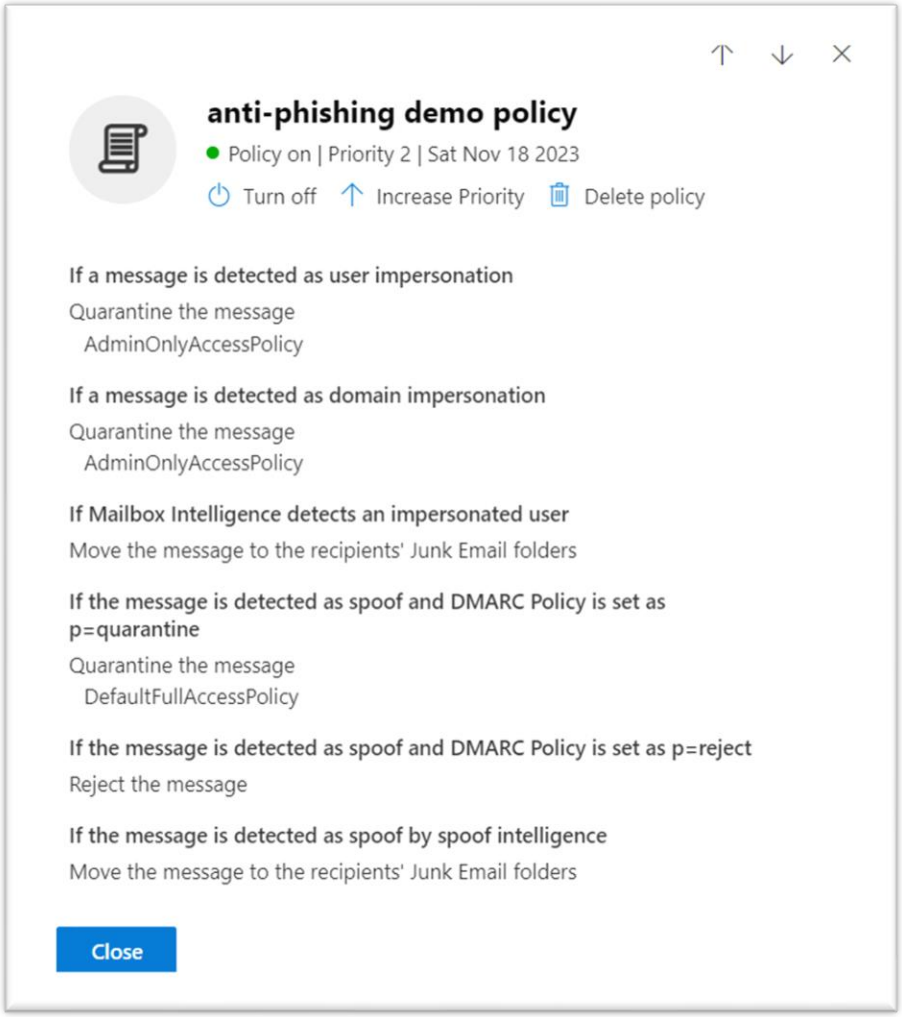
Link Protection	• Activation of link protection to identify and block malicious URLs. • Real-time scanning of links within emails to mitigate the risk of phishing attacks.



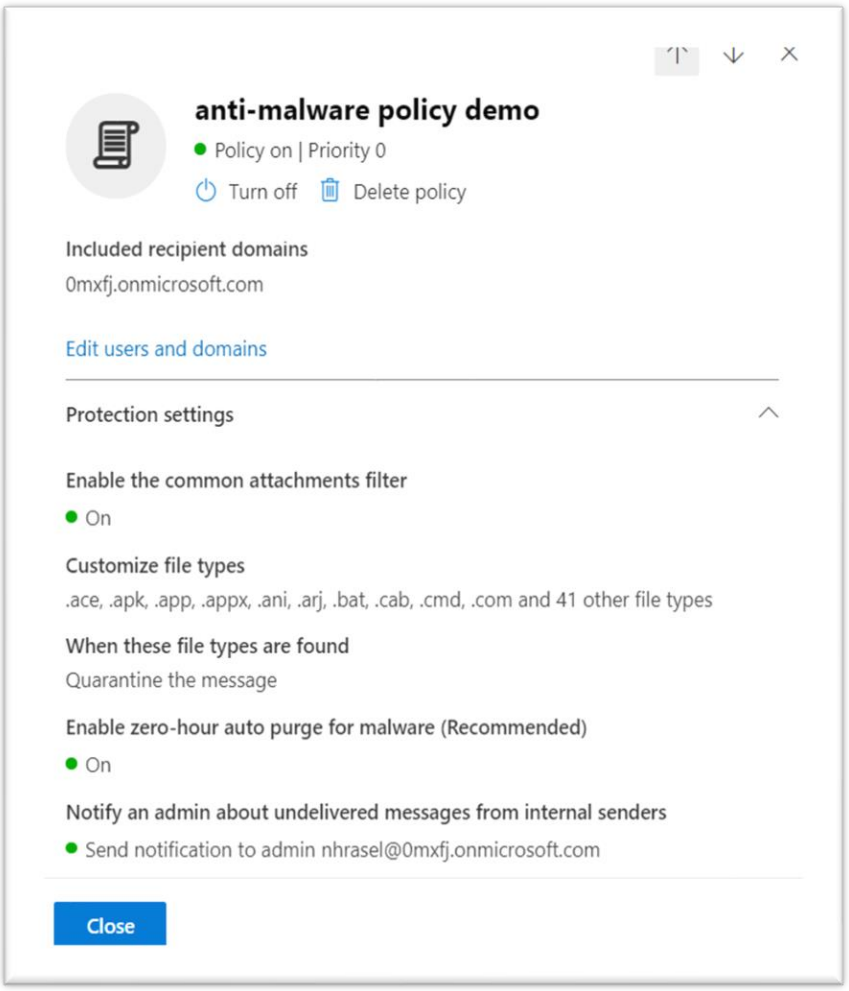
Spam Mail Control	• Implementation of advanced spam filtering to reduce the likelihood of unwanted emails. • Regular updates and customization of spam control policies to adapt to new threats.



Anti-Phishing Policies	• Configured and deployed anti-phishing policies to identify and block phishing attempts. • Utilized advanced threat intelligence to recognize and mitigate phishing threats in real time.

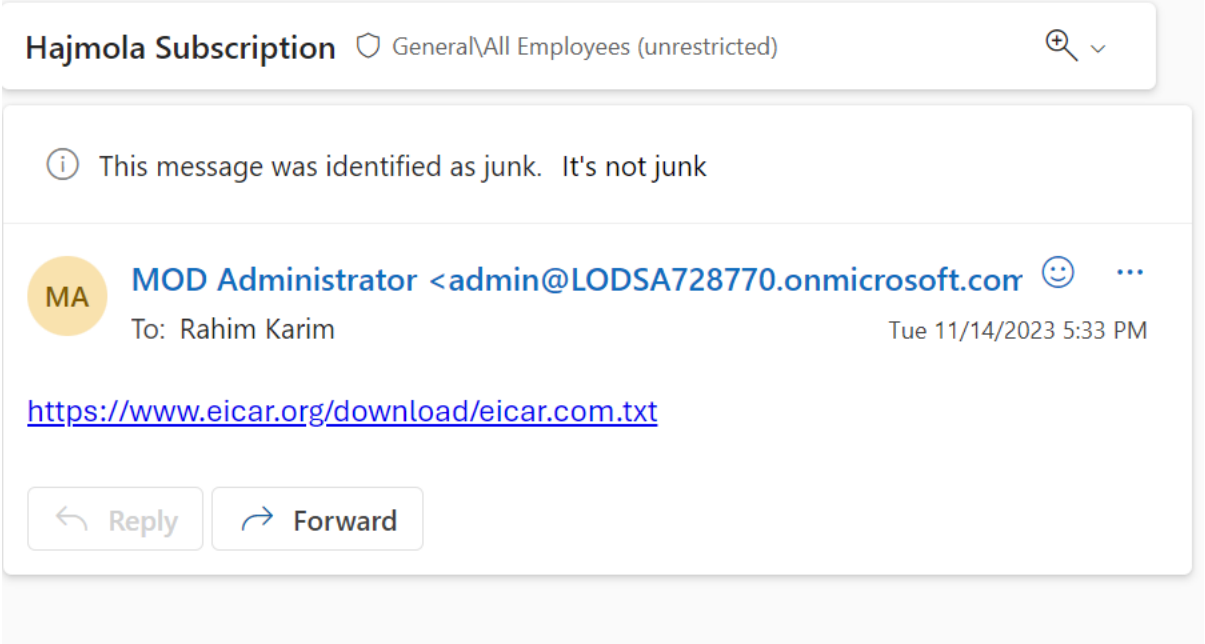


Anti-Malware Policies	• Implemented robust anti-malware policies to scan and block malicious attachments and links. • Regularly updated malware definitions to stay ahead of emerging threats.



Threat Protection System in Email

Some actions of Microsoft Defender are shown after applying the policy.



Secure Score

We regularly assess and enhance our security posture using the Security Score feature in Microsoft Defender for Office 365. The Secure Score provides a comprehensive overview of our security status, highlighting areas of strength and suggesting improvements. This allows us to proactively address vulnerabilities and ensure a robust defense against cyber threats. The dashboard shows the Secure Score.