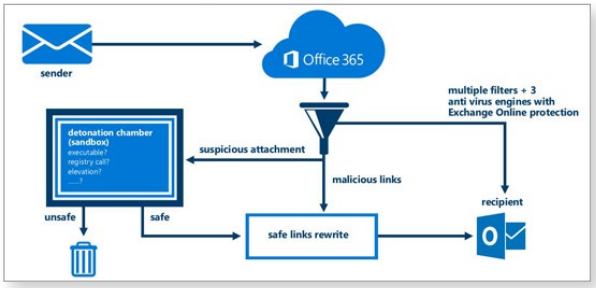
OFFICE 365

Advanced Threat Protection

Protect your email, files, and Office 365 applications against unknown and sophisticated attacks.

Office 365 Advanced Threat Protection (ATP) helps to protect your organization from malicious attacks by:

- Scanning email attachments for malware with ATP Safe Attachments
- Scanning web addresses (URLs) in email messages and Office documents with ATP Safe Links
- Checking email messages for unauthorized spoofing with spoof intelligence
- Detecting when someone attempts to impersonate your users and your organization's custom domains with ATP anti-phishing capabilities in Office 365
- Identifying and blocking malicious files in online libraries with ATP for SharePoint, OneDrive, and Microsoft Teams

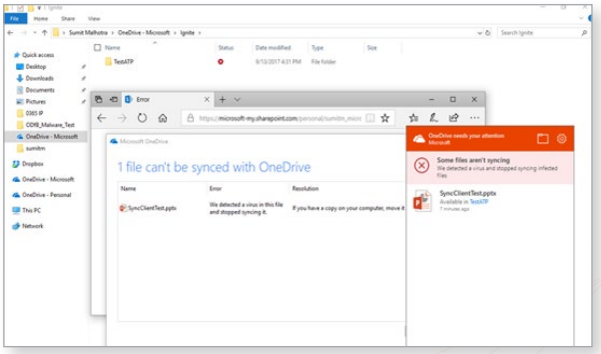


Secure your mailboxes against advanced threats

New malware campaigns are being launched every day. Office 365 Advanced Threat Protection can help protect your mailboxes, files, online storage, and applications against new, sophisticated attacks in real time. By protecting against unsafe attachments and expanding protection against malicious links, it provides better zero-day protection.

Protect against unsafe attachments

With Safe Attachments, you can prevent malicious attachments from impacting your messaging environment. All suspicious content goes through a real-time behavioral malware analysis that uses machine learning techniques to evaluate the content for suspicious activity. Unsafe attachments are sandboxed in a detonation chamber before being sent to recipients. The advantage is a malware free and cleaner inbox.

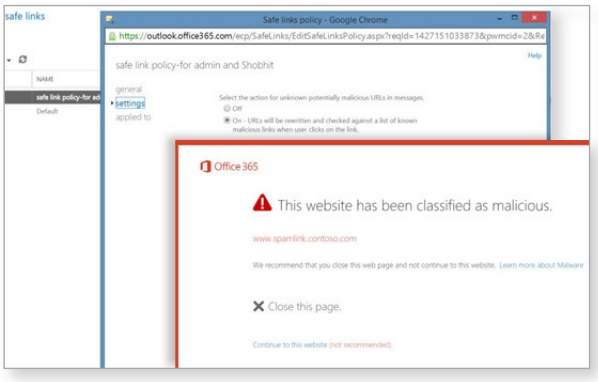


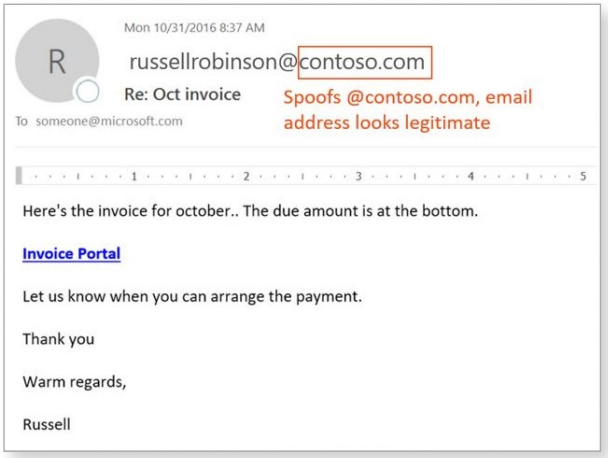
9 Slack Rd. 2nd Floor Ottawa, ON, K2G 0B7 | GradeA.ca | Tel: 613-721-3331

GRADE·A

Protect your environment when users click malicious links

Exchange Online Protection provides protection against malicious links by scanning content. Safe Links expands on this by protecting your environment when users click a link. While the content is being scanned, the URLs are rewritten to go through Office 365. The URLs are examined in real time, at the time a user clicks them. If a link is unsafe, the user is warned not to visit the site or informed that the site has been blocked.



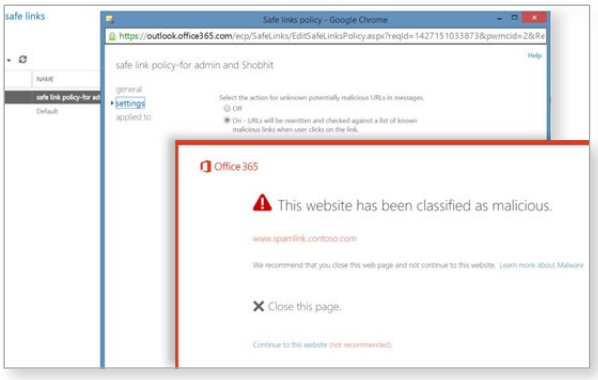


Anti-spoofing protection in Office 365

When it comes to protecting its users, Microsoft takes the threat of phishing seriously. One of the techniques that spammers and phishers commonly use is spoofing, which is when the sender is forged, and a message appears to originate from someone or somewhere other than the actual source. Microsoft's Anti-spoof technology specifically examines forgery of the 'From: header' which is the one that shows up in an email client like Outlook. When Microsoft has high confidence that the From: header is spoofed, it identifies the message as a spoof.

Use machine learning to protect against incoming phishing attacks

ATP anti-phishing applies a set of machine learning models together with impersonation detection algorithms to incoming messages to provide protection for commodity and spear phishing attacks. All messages are subject to an extensive set of machine learning models trained to detect phishing messages, together with a set of advanced algorithms used to protect against various user and domain impersonation attacks.



Contact us to learn more about how implementing Microsoft's Advanced Threat Protection will secure your users and protect your business data.

9 Slack Rd. 2nd Floor Ottawa, ON, K2G 0B7 | GradeA.ca | Tel: 613-721-3331