Frequently Asked Questions

Microsoft Office 365 Strengthening

Updated: 2 November 2022

UNSW is taking steps to improve the resilience of our Microsoft 365 platform and will commence the implementation of additional technical controls to SharePoint, Teams, and Email in line with the University Cyber Security and Acceptable Use of UNSW Information Resources policies.

Strengthening critical controls of our core collaboration tools will minimise the potential for accounts to be compromised and reputational damage. Staff and students will notice alerts in SharePoint, Teams, and Outlook, if suspicious attachments, links, or websites are detected through the new anti-phishing, anti-malware, and anti-spam controls.

For help with Microsoft Office 365 please call **the IT Service Centre on 02 9385 1333**, or alternatively visit the Cyber Security website to access all support materials and information. If your question is not listed below, please email the Cyber Security Resilience Program.

Contents - Click on the question to be taken to the answer.

FAQs

FAQs

1. What is Microsoft Defender for Office 365?

Microsoft Defender for Office365 safeguards the University against malicious threats posed by email messages, links (URLs) and collaboration tools, like SharePoint, Teams and Outlook.

Return to Contents

2. What is malware?

Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorised access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.

Return to Contents

3. What do Safe Links do?

Safe Links are a feature in Defender for Office 365 that provides URL scanning of inbound email messages, and time-of-click verification of URLs and links in email messages and other locations.

Return to Contents

4. What if I am blocked from accessing a legitimate website?

Please contact the IT Service Centre to report any false positives. The Cyber Security Team will assess to help manage URLs that should be whitelisted.

Return to Contents

5. How do Safe Links and Safe Attachments impact my email?

Safe Links and Safe Attachments look for and protect you from email phishing links/websites that are known to contain malicious software, email attachments, and links.

Return to Contents

6. Does that mean Microsoft/UNSW IT are reading my email?

No, neither Microsoft or the University are reading your email. URLs are scanned in incoming emails to see if they are malicious when a user clicks on the URL to access it.

Return to Contents

7. What should I do when I encounter the Safe Links protection page?

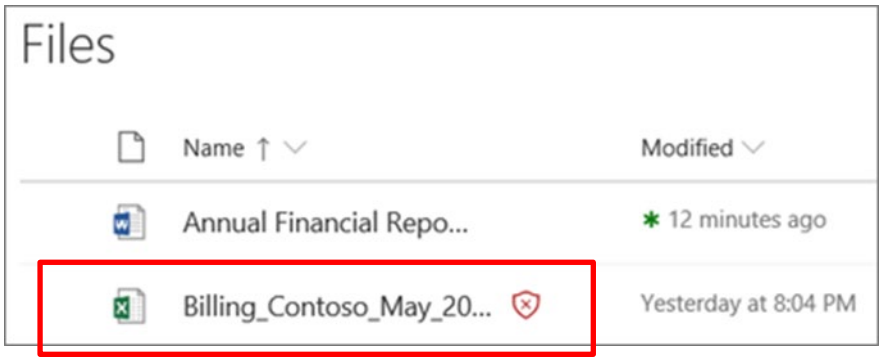
First, you should verify that the site you were trying to access is correct by looking closely at the site named in the browser bar. Sometimes a misspelled word or string of characters in the site name takes you to a website you may not have intended to visit. If you think that this was blocked

in error, and there is a business or academic reason to get to the site, contact the IT Service Centre.

Return to Contents

8. Do Safe Links and Safe Attachments work when I use SharePoint, Teams or other Office 365 applications?

Safe Links and Safe Attachments search SharePoint, Outlook and Microsoft Teams to identify if any documents contain phishing links or malicious software. If a malicious file is detected, it will be blocked from interaction. A blocked file will appear as in the screenshot below.



Once a file is blocked, you will not be able to interact with it in any way other than delete it.

Return to Contents

9. Is there a delay in the time it takes for my email to be received if I attach a file?

The recipient of an email may experience a small delay if the email contains a large attachment.

Return to Contents

10. What should I do if I think a link or attachment was blocked in error?

If you believe a site or attachment was blocked by mistake or you have a business or academic need to access a site or attachment that was blocked, please contact the IT Service Centre who can assist with recovering it.

Return to Contents

11. If I get the Safe Links protection page, does that mean I was infected with malware?

No, just the opposite. You were prevented from accessing the malware site before you could be impacted.

Return to Contents

12. Does Safe Links protect me from malicious sites when I'm browsing the web?

No. Safe Links only scans your Office 365 email to identify phishing links and links to websites that are malicious.

Return to Contents

13. What happens if a user, or group of users, needs to access a blocked site?

The user or group of users with a legitimate academic or business need can request access to a blocked site by contacting the IT Service Centre. The IT Security Office will evaluate each request.

Return to Contents

14. I didn't receive an email I was expecting, what should I do?

If you are missing an email you are expecting, please check your Junk folder in the first instance.

To find your Junk Email folder:
1. Open the Outlook App.
2. In the left pane, in your folder list, you can find the Junk Email folder.

If the email is not in the Junk folder, please contact the IT Service Centre for assistance.

Return to Contents

15. What do the anti-phishing warning messages look like?

First Contact Safety Tip

The safety tips are shown to recipients in the following scenarios.

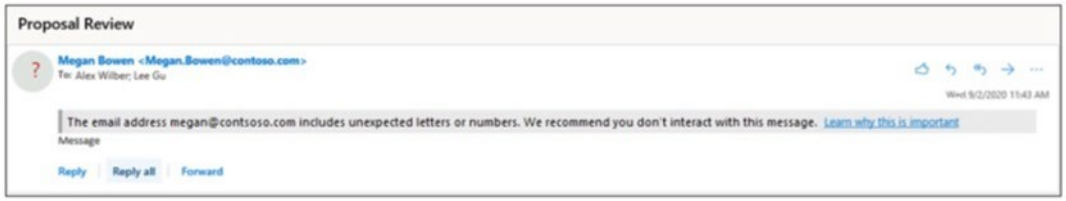
The first time they get a message from a sender:
"You don't often get email from Megan.Bowen@contoso.com"

They don't often get messages from the sender:
"Some people who received this message don't often get an email from Megan.Bowen@contoso.com."

User Impersonation Unusual Characters Tip

This tip is shown to recipients in messages where the sender's name or email address contains characters that aren't typically used together (for example, a mix of mathematical symbols and plain text or a mix of uppercase and lowercase letters).

"The email address megan@contsoso.com includes unexpected letters or numbers. We recommend you don't interact with this message."



Show (?) for Unauthenticated Senders for Spoof

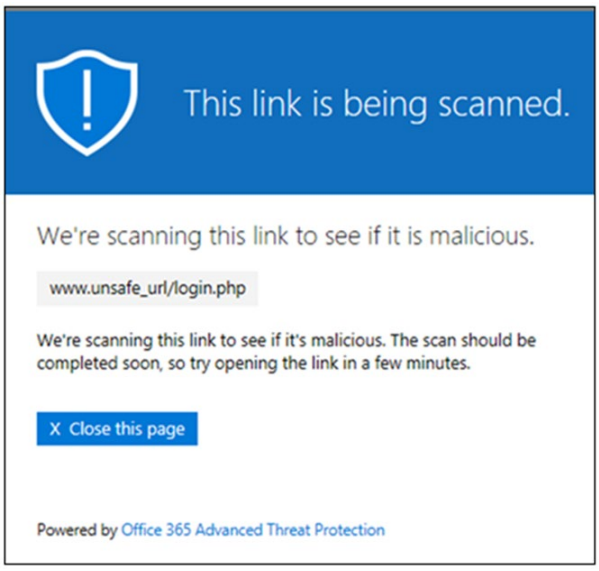
This helps you distinguish if the sender is actually who they say they are through a visual cue.

Return to Contents

16. What do the Safe Links warning messages look like?

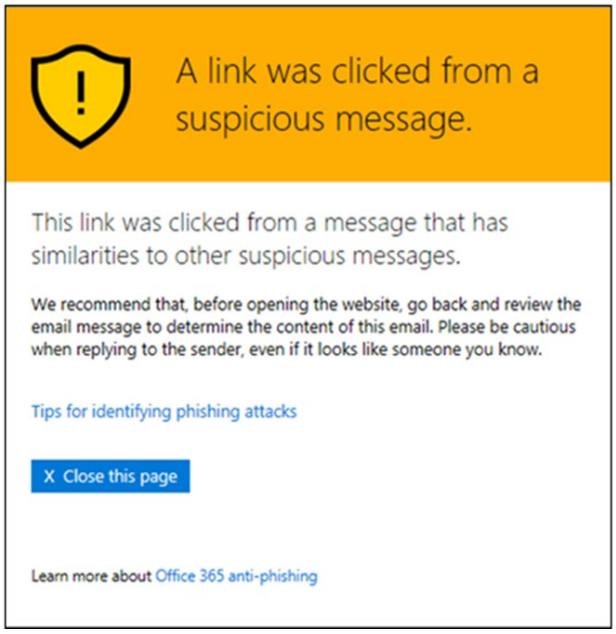
Scan in progress notification

The clicked URL is being scanned by Safe Links. You might need to wait a few moments before trying the link again.



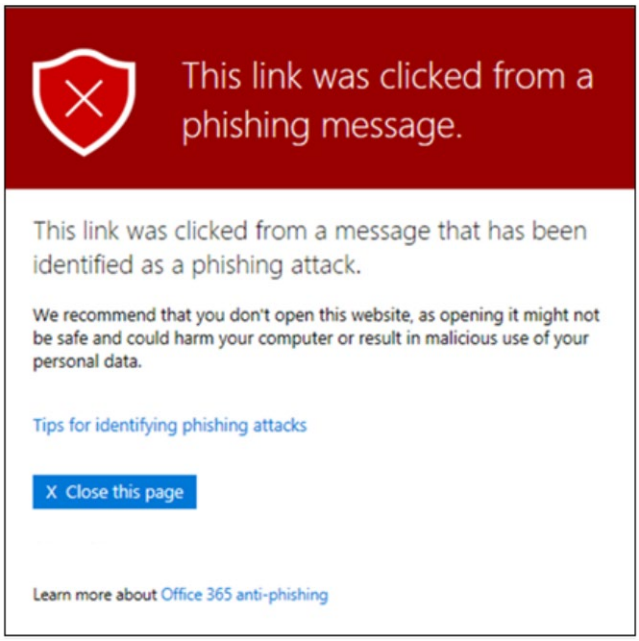
Suspicious message warning

The clicked URL was in an email message that's like other suspicious messages. We recommend that you double-check the email message before proceeding to the site.



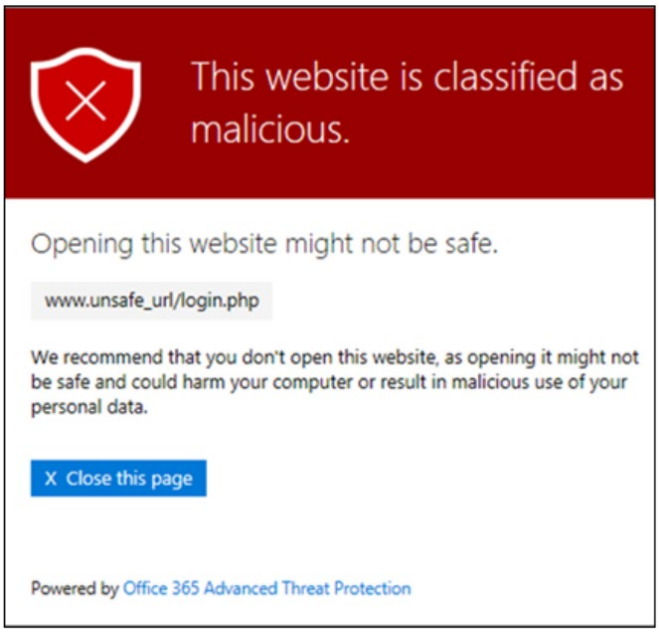
Phishing attempt warning

The clicked URL was in an email message that has been identified as a phishing attack. As a result, all URLs in the email message are blocked. We recommend that you do not proceed to the site.



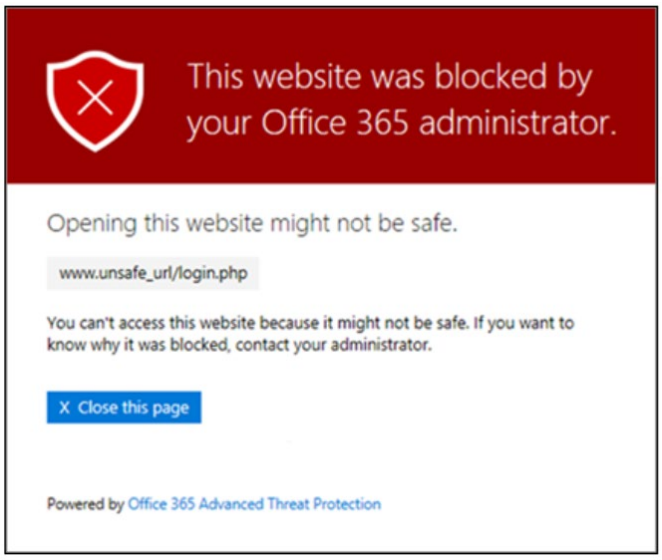
Malicious website warning

The clicked URL points to a site that has been identified as malicious. We recommend that you do not proceed to the site.



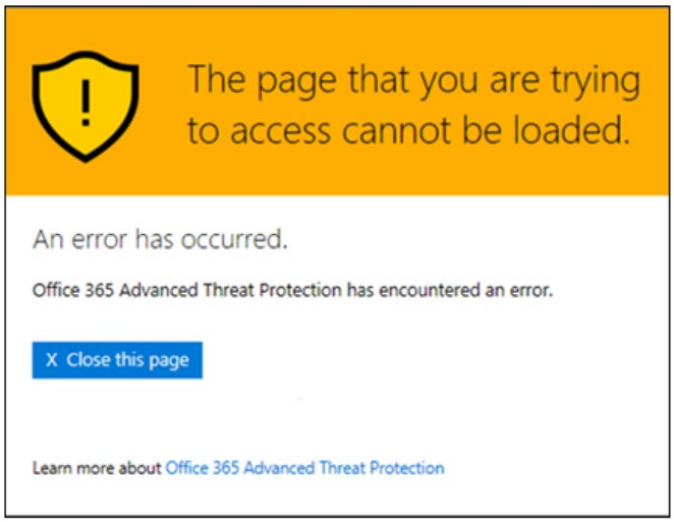
Blocked URLs

The clicked URL has been manually blocked by UNSW. The link was not scanned by Safe Links because it was manually blocked.



Error warning

Some kind of error has occurred, and the URL can't be opened



Return to Contents

END