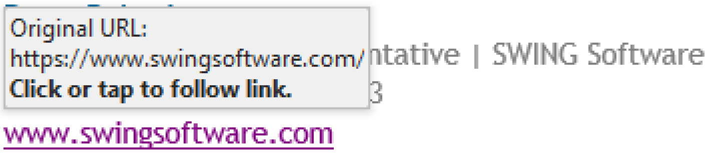
Microsoft Safe Links and Safe Attachments

What is Safe Links and Safe Attachments?

The Safe Links and Safe Attachments service are part of Microsoft's Office 365 Advanced Threat Protection (ATP) for enterprise organisations. Safe Links and Safe Attachments are designed to protect staff from email phishing attempts, and links/web sites or email attachments that contain malicious software. The service will mostly be invisible to you because it works behind the scenes to protect you.

How do I know I am protected by Safe Links?

You can verify that Safe Links is working by opening in the Web URL link in a browser, for a short period of time it will display something like: " https://eur01.safelinks.protection.outlook.com/?url=https.." before being redirect to the original website. If you hover above the original web URL link in the email it should display the original URL. See below:

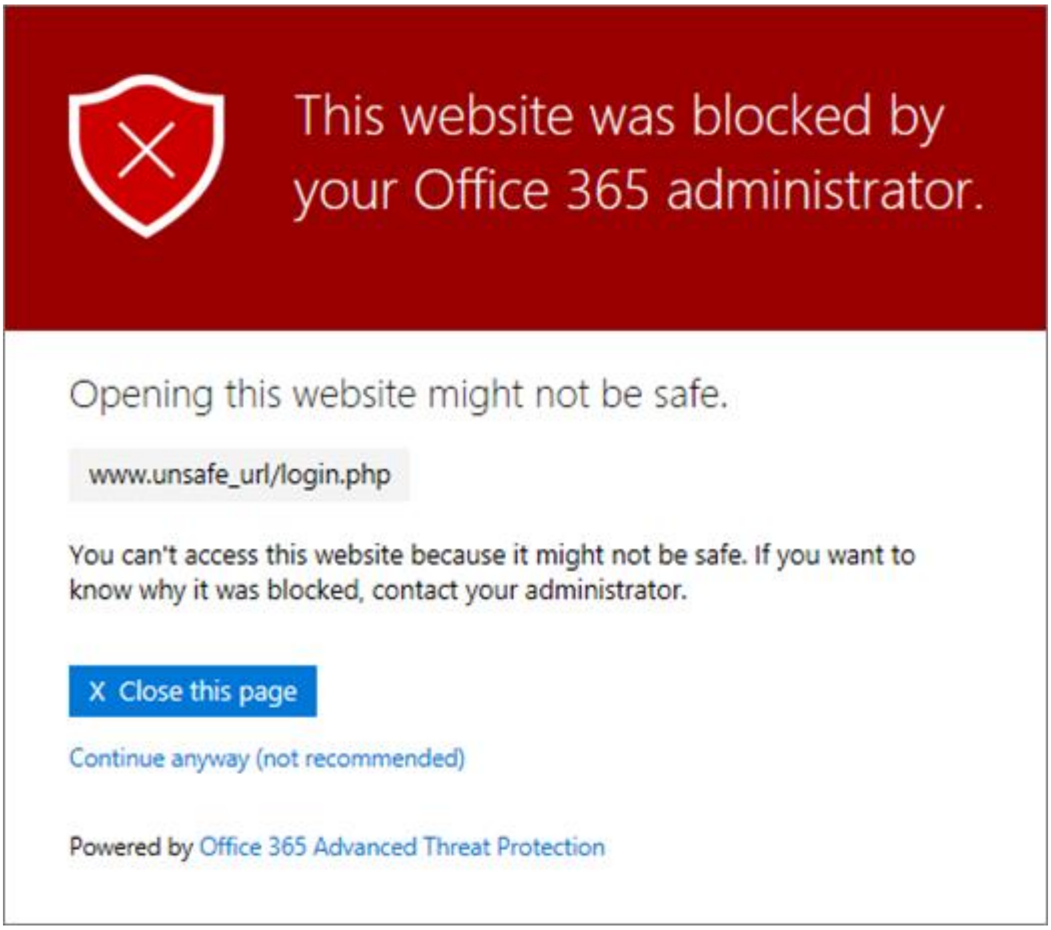


Original URL:
https://www.swingsoftware.com/
Click or tap to follow link.

This indicates that Safe Links has analysed the link and is protecting you in the event the site is malicious.

The protection service is handled within Office 365 so it will most likely be transparent to you. If you click on a link in an email that takes you to a site that does not contain malicious software, you will be allowed access to the site and proceed normally. However, if a link is identified as malicious, or a link is determined to be a phishing link, after clicking on the link a Safe Links screen will appear indicating the web site cannot be accessed. This protects you, and your workstation from infection.

The protection page may look like this:



This website was blocked by your Office 365 administrator.

Opening this website might not be safe.

www.unsafe_url/login.php

You can't access this website because it might not be safe. If you want to know why it was blocked, contact your administrator.

Powered by Office 365 Advanced Threat Protection

For more information about other different warning messages please click here.

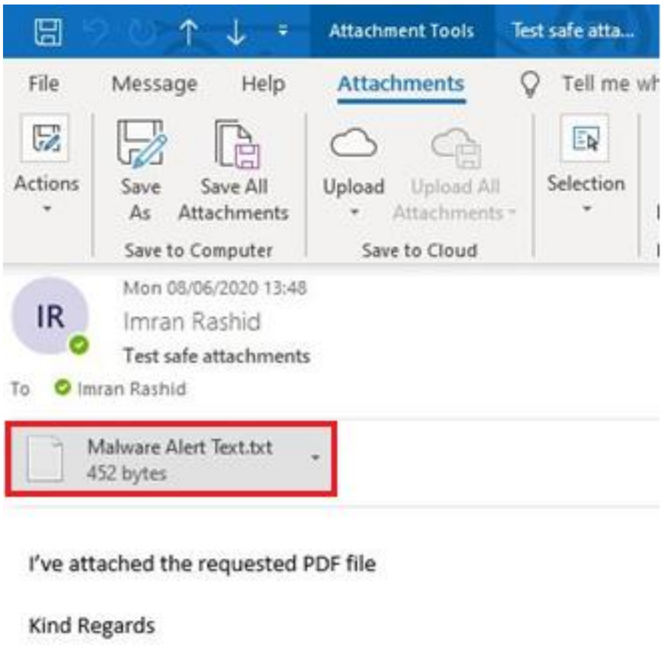
What happens if you need to access a blocked web site?

Please contact the following mailbox network.security.team@birmingham.gov.uk

How do I know I am protected by Safe Attachments?

The Safe Attachments service only scans email attachments to detect if the attachment contains any malicious code. If none is found, the attachment is sent as normal. If malicious code is found, only the bad attachment will be removed and the rest of the email will be sent to the recipient with a notice that the attachment was identified as containing malware and has been removed.

Below is an example of the replacement attachment that would show up in an email that contained an infected attachment.



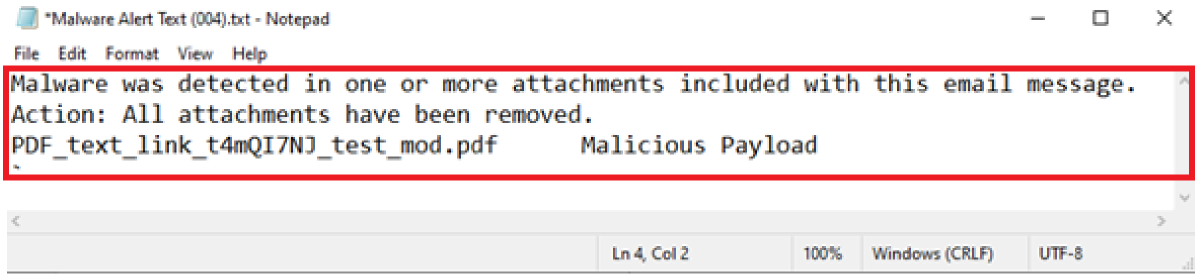
Mon 08/06/2020 13:48
Imran Rashid
Test safe attachments
To Imran Rashid

Malware Alert Text.txt
452 bytes

I've attached the requested PDF file

Kind Regards

If you attempt to open the replaced attachment, the following message example would be displayed.



```
Malware was detected in one or more attachments included with this email message.
Action: All attachments have been removed.
PDF_text_link_t4mQI7NJ_test_mod.pdf      Malicious Payload
```

What happens if you need to access a blocked attachment?

Please contact the following mailbox network.security.team@birmingham.gov.uk