Safe Links and Safe Attachments FAQ

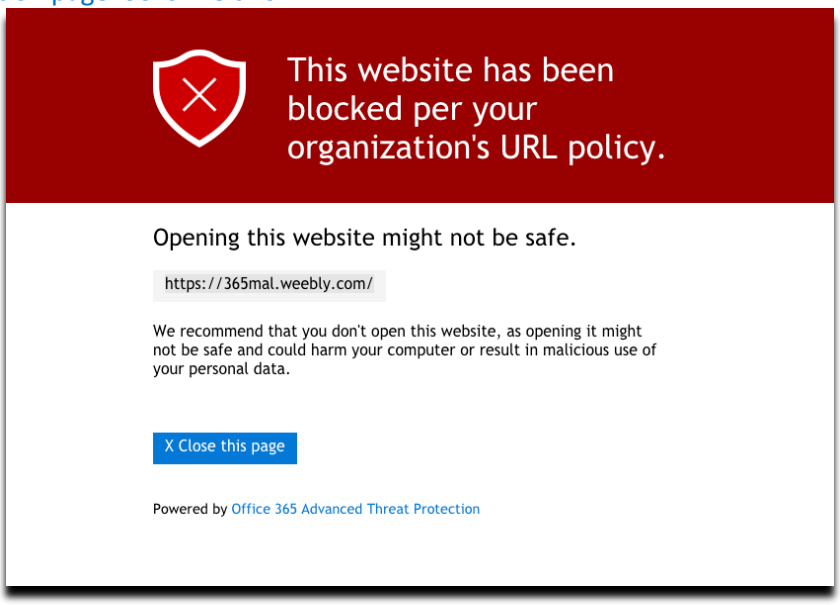
- What is Safe Links and Safe Attachments?

  The Safe Links and Safe Attachments service are part of Microsoft's Office 365 Advanced Threat Protection for enterprise organizations. Safe Links and Safe Attachments are designed to protect students, faculty, and 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?

  The protection service is handled within Office 365 so it will most likely be transparent to you, the end user. If you click on a link in an email, SharePoint, OneDrive or Microsoft Teams 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 looks like this:



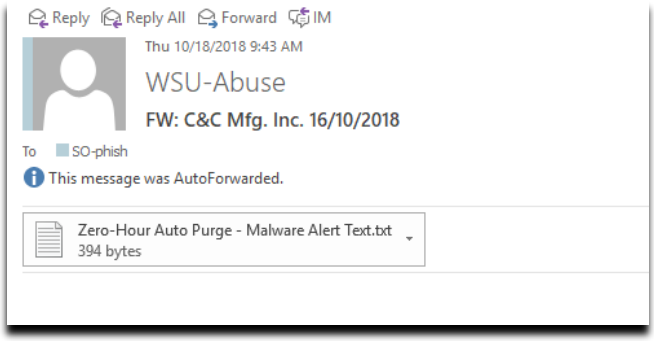
  You can verify that Safe Links is working by hovering your mouse pointer over any link that you have in an email, SharePoint, OneDrive, etc. If you look at the URL that is displayed, it will begin with *https://na01.safelinks.protection.outlook.com*. This indicates that Safe Links has analyzed the link and is protecting you in the event the site is malicious.

- How do I know I am protected by Safe Attachments?

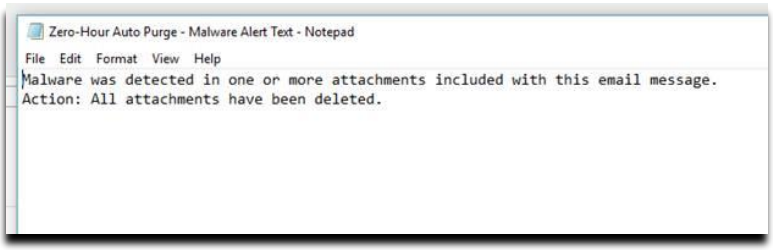
  The Safe Attachments service scans email attachments to detect if the attachment contains any malicious software. If none is found, the attachment is sent as normal. If malicious software is found, the bad attachment will be removed and the email sent to the receiver

will contain a notice that the attachment was identified as containing malware and the attachment will have been deleted. An “un-delete” process is in place if the need arises. Please contact your local campus service/ help desk for assistance.

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



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



- Does Safe Links and Safe Attachments impact my email or Office 365?

  Typically no. Safe Links and Safe Attachments only look for, and protect you from email phishing links/web sites that are known to contain malicious software, email attachments, and ‘bad’ links in SharePoint, OneDrive and Microsoft Teams. ***These services do not monitor which web sites you visit.*** They only protect you from accessing a site or attachment that is known to be bad. If nothing malicious is found, your web access and email experiences are normal.

- 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 web site 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 your local campus service/help desk.

- Does Safe Links and Safe Attachments protect me when I use SharePoint, OneDrive or Microsoft Teams?

  Yes. These services search SharePoint sites, OneDrive and Microsoft Teams to identify if any documents contain phishing links or malicious software.

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

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

- Are my emails or attachments being viewed by the college/university or the system office?
  No. This is an automated service provided by Microsoft to protect you and your device(s). No college/university or system office personnel will monitor web sites you visit or emails and attachments you send.

- What should I do if I think the protection event is in error?
  If you have a business or academic need to access a site that has been protected/blocked, you may submit an inquiry by contacting your local campus service/help desk for assistance.

- 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 infected.

- Does Safe Links protect me from malicious sites when I'm surfing the web using a browser?
  No. Safe Links only scans email, SharePoint, OneDrive and Microsoft Teams to identify phishing links and links to web sites that are malicious. However, Minnesota State has implemented Internet Guardian which does protect you when you are surfing the web via a browser (i.e. Internet Explorer, Chrome, Firefox, etc.) as long as you are on a campus/Minnesota State network.

- Does Safe Links or Safe Attachments identify and protect me from malicious links or software in files that I store locally on my PC, or that I store on my campus network (i.e. H: drive, shared drives, etc.)?
  No. Safe Links and Safe Attachments only works on files that are attached to emails or uploaded to SharePoint, OneDrive or Microsoft Teams.

- 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 your local campus service/help desk. The system office security team will evaluate each request.

- What if I have further questions about Safe Links or Safe Attachments?
  Contact your local campus service/help desk if you have any questions or issues with Safe Links or Safe Attachments.

Important: Safe Links and Safe Attachments acts like an additional safety net in protecting you and your information assets. However, no technology is perfect and practicing safe computing habits is still extremely important in our day to day use of technology – at school, work, home, or at play. Everyone still needs to be alert and diligent in their safe computing practices.