Introduction

Safe Links and Safe Attachments will be activated within the Office 365 single tenancy on December 14, 2018. This guide covers some of the common questions that you may receive when providing support services to your users. Please contact the system office security team if you have any questions about this guide, or if you receive additional frequent questions that should be added to this guide.

- What is Safe Links and Safe Attachments Service?
  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 services will mostly be invisible to users because it works in the background, at the network level.

  A FAQ is available to all students, faculty and staff:

- Does Safe Links and Safe Attachments protect users when they use SharePoint, OneDrive or Microsoft Teams?
  Yes. These services search SharePoint sites, OneDrive and Microsoft Teams to identify if any emails, documents, or other content contain phishing links or malicious software.

- Does Safe Links and Safe Attachments protect the user anywhere they go or just on campus?
  The service protects the user anywhere they are, as long as they are logged into and working with content that is stored in the Minnesota State shared Office 365 tenant.

- Is there a delay in the time it takes for an email to be received when it contains a large attachment?
  Since the Safe Attachment service has to scan any attachment before it is delivered, the receiver of an email may experience a small delay if the email contains a large attachment. This delay will typically not take longer than a few minutes. If the email delay is consistently taking a lot longer than a few minutes, then a Cherwell ticket could be submitted to the Office 365 Core team.

- What is the process for “black listing” malicious links?
  There may be instances where IT staff or others have identified malicious links or files that currently are not being blocked by Safe Links or Safe Attachments. In these instances, we ask that you forward the email as an attachment to [phish@minnstate.edu](mailto:phish@minnstate.edu). The Information Security, Risk, and Compliance Team will evaluate each request.

- What is the process for “white listing” malicious links?
  There may be instances where IT staff or others have identified links or files that appear “safe” but are currently being blocked by Safe Links or Safe Attachments. In these instances, we ask that you forward the email as an attachment to [phish@minnstate.edu](mailto:phish@minnstate.edu). The
Information Security, Risk, and Compliance Team will evaluate each request and advise how to proceed.

- If I get a request to recover an attachment that was removed/deleted by Safe Attachments, what options are there to recover the document?
  We ask that you submit a Cherwell ticket to the system office security team. The system office security team will investigate each of these instances and advise on how to proceed.

- If a user reports that a link looks ‘funny’, how can I tell if this is a phishing attempt or a Safe Link?
  All links that have been analyzed by Safe Links 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 and no action is required. However, continue to report all suspected phishing emails to phish@minnstate.edu

- Does Safe Links protect users from malicious sites when they are surfing the web using a web browser?
  No. Safe Links examines URLs that appear in email, SharePoint, OneDrive and Microsoft Teams, identifying phishing links and links to web sites that are malicious. However, our companion system wide service, Internet Guardian, does protect users when they are surfing the web via a browser (i.e. Internet Explorer, Chrome, Firefox, etc.) as long as the user is on a campus network.

- Will the URLs that Safe Links creates protect users outside of the shared Minnesota State tenant?
  Yes. These protected URL links will continue to work and protect any user who clicks on them. The new URLs that Safe Links creates (https://na01.safelinks.protection.outlook.com/...) will stay in the email or document even if it is sent to users outside of our shared Minnesota State O365 tenant. It will also work if the user copies and pastes the Safe Links URL into a browser.

- Why doesn’t the link in a Word document that is stored on my workstation have the Safe Links URL format?
  For an Office 365 document (e.g. Word, Excel, Power Point, etc.) to have the Safe Links URL format, it has to be located in the Office 365 environment (SharePoint, Teams, Outlook, etc.). A document that is stored in other locations (local disk, shared drives, Cherwell, etc.) will not have been processed by Safe Links to verify any URLs in the documents.