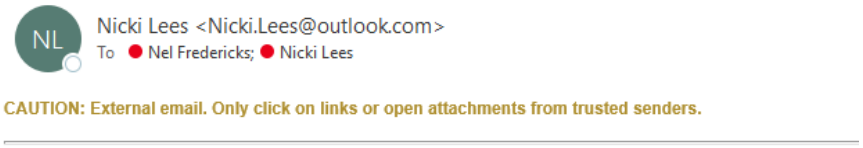
Enhanced Email Security

Additional Mimecast email protection will soon be added. Mimecast scans all emails sent to or from the University to detect spam, viruses, malware, and other threats.

We're keeping your email and systems safer

As part of our ongoing security focus, we have enabled two new features in our email security platform from Mimecast that occasionally requires your engagement. The aim is to increase your awareness as a user of potentially harmful content embedded in email, and malicious links found in attachments.

Feature 1: external email warning

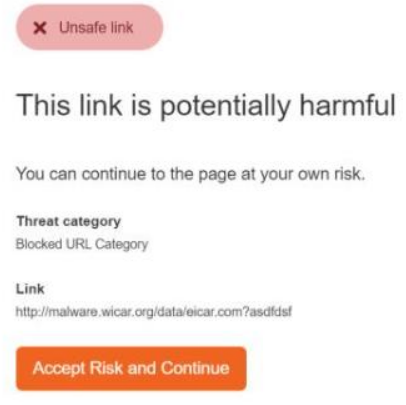


If you see this on top of your email, it means it came from outside the University of Adelaide. When clicking on links or opening attachments, please be extra careful. Only click on links or open attachment if you trust the sender and the nature of the email.

Sophisticated cyber criminals attempt to feign emails to appear as if it is internal and official, often impersonating IT or HR staff. Mimecast will highlight when an email is sent from outside the University.

Feature 2: URL link protection

Malicious parties often attempt to entice users to click on links in emails that may cause harm to your computer and the organisation. They may lead you to a fake login site, or force downloading and running of a malicious file. Mimecast performs a pre-scan of the URL to determine whether it could be dangerous. If the link is determined to be safe, it will silently redirect you to the original link.



If the link is determined to be potentially harmful, you'll be asked to decide if you're happy to continue to the website, or if you want to change your mind.

By prompting you to think before you click, you can help to strengthen our defences.

FAQ

Why was an internal email tagged as “external”?

> While Mimecast can automatically determine whether an email originated internally, there could be instances where system-generated emails from a cloud system is falsely categorised as “external”. An example of this is official University emails that are sent through Campaign Manager. Please complete send a request to the Service Desk with email address you wish to be excluded from being tagged as external.

What email addresses can we exclude from being tagged as external?

- Email addresses that end with *@adelaide.edu.au*
- Are not personal email addresses such as *firstname.lastname@adelaide.edu.au*
- Are used to send emails to staff

I have a trusted external partner, can emails from them be excluded from the external email warning?

> In most cases, the answer is no. We still want to warn people of external emails – it helps increase protection in the case that a trusted sources security is compromised. However, we have excluded some system generated emails (like jira/atlassian).

Can I still “hover” over a link to determine the destination link?

> Yes, when you hover over the link, the link will appear like this, where domain=xxx portion indicates the original link domain.
>
> e.g. https://protect-au.mimecast.com/s/dizbc1wlan?domain=abc.net.au

Can I still send and receive links via email?

> Yes, links that are in indeed in the body of an email will still be received and appear as normal. It is only if you hover over the link that the URL will change.

What do I do if I am presented with the “This link is potentially harmful” page?

> Examine the link, and if you believe it is safe, go ahead and lick on [Accept Risk and Continue]. If you are not sure, please call Service Desk and seek advice.

What do I find a dangerous link that is not blocked by Mimecast?

> Please forward the details to Service Desk so that the link can be blocked on the system for everyone else.

Do “Safe Links” ever expire?

> No, safe links are maintained indefinitely within Mimecast

Do students have this feature turned on in their email?

> No, these new security features are only for staff and HDR student emails currently.

Support is available

For assistance, please contact the ITDS Service Desk on +61 8 313 3000 or servicedesk@adelaide.edu.au