**What is User Awareness?**

As part of our ongoing security focus, we’ve enabled a new feature 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.

**What will I see?**

What you’ll see depends on the configuration made by your Administrator. For a small percentage of links that you click on in emails, you’ll be shown a page with information about the website you’re trying to access.

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. Look out for useful Safety Tips shown throughout these pages, and click the *Previous* or *Next* links to view more.


If malicious content is found in the website you’re trying to access, you’ll be shown the page below. This lets you know that access has been blocked and you’ll need to close the browser. Click on the *Show More* link, or contact your Administrator, to find out more information.



**What do I need to do?**

The next time you click a link in an email, or request the release of an original email attachment, you’ll be asked to enroll your device to continue.

When prompted in the browser, enter your work email address and click *Get Authentication Code*. You’ll receive a one-time code by email to enter into your browser where indicated.

You’ll be asked to enroll once on each device that you use your work email to access (e.g. laptop and mobile). Bear in mind, you’ll need to enroll any new devices, or if you delete your browser cookies.



If you have any questions or need further help, please contact your IT help desk.