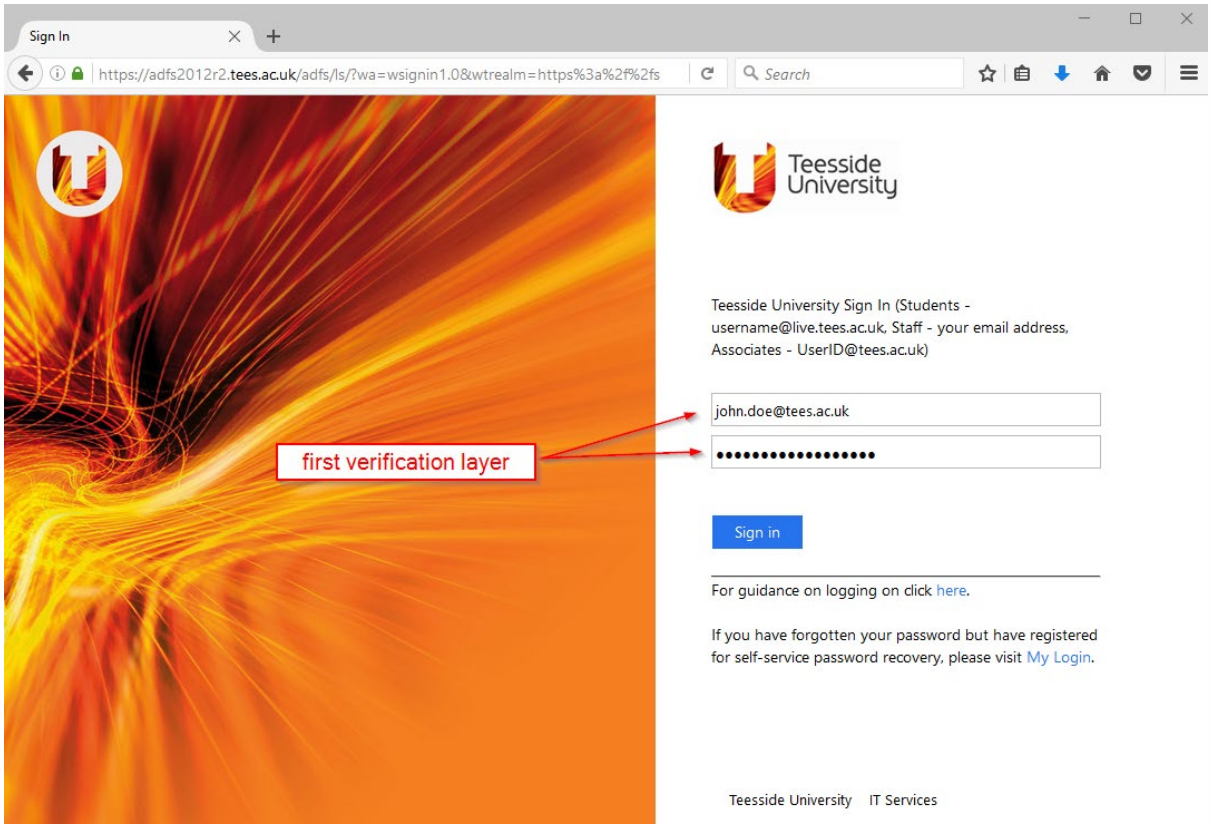
So, what exactly ***is*** Two-Factor Authentication?

Two-factor authentication, also called multiple-factor or multiple-step verification, is an authentication mechanism to double check that your identity is legitimate. It increases security by using “something you know” – your password, and also “something you have” a mobile phone.

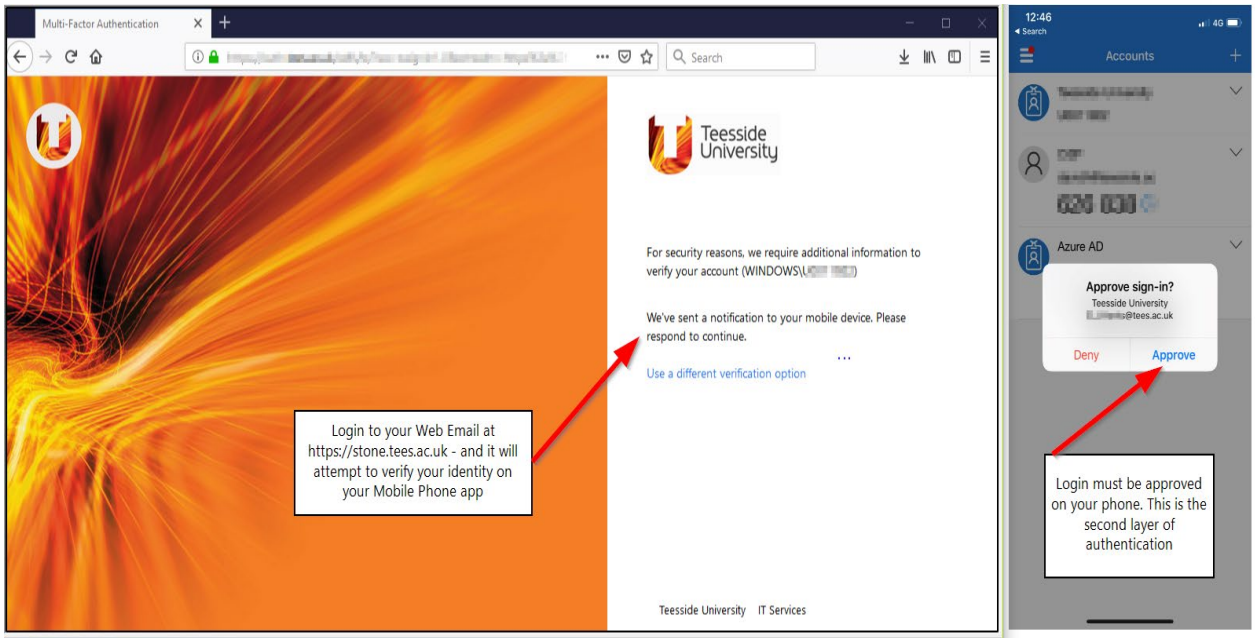
We have implemented two-factor authentication across several systems at Teesside, including email (Outlook Web Access at http://stone.tees.ac.uk)

How does Two-Factor Authentication work at Teesside?

When you want to sign into your account, you are prompted to authenticate with a username and a password – that is the first verification layer. (Something you know)



Two-factor authentication works as an extra step in the process, **a second security layer**, which will reconfirm your identity.



At Teesside we use Microsoft's Authenticator app. Once you have enrolled your device, you must approve each login to the email gateway at http://stone.tees.ac.uk with the mobile phone app. You can enrol your device by following the guide available from the IT Helpdesk

Its purpose is to make attackers' life harder and reduce fraud risks. If you already follow basic password security measures, two-factor authentication will make it even more difficult for cyber criminals to breach your account.

Why are we implementing this?

On the 25th May 2018, the EU GDPR (General Data Protection Regulation) is due to come into effect

The GDPR will cover all countries that process or hold the personal data of EU citizens, whether that country is a part of the EU or not. This means that Britain will still have to abide by the laws of the GDPR despite the result of the EU referendum at the end of June.

The fines for not complying with the laws can reach a maximum of 4% of the businesses global annual turnover or up to €20,000,000.

We must therefore implement robust, technical controls to protect personal data that may be included in staff member email inboxes. You must carefully consider the types of information that you store in your email inbox, by referring to the Information classification scheme in the University Information Security Policy.