

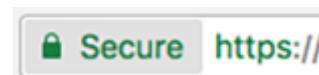
What is TLS 1.0?

Transmission Layer Security (TLS) is a protocol that encrypts information across networks, including the Internet.

Definition

Encryption	A method for disguising (or enciphering) information with a series of instructions
------------	--

When you visit a secure website, using Internet banking services or are looking to purchase something online your Internet browser should display the secure padlock.



When your device talks to a web server, for example Amazon, both sending and receiving devices find a common way of communicating starting with the most secure method it can try (*currently TLS 1.3*). If both devices can't use this, it tries the next best option (*TLS 1.2*) and so on until it can communicate.

What's changing?

On **Monday 5th June 2017**, TLS 1.0 will be removed from University services, such as the Digital Learning Environment (DLE), the University website and Employee Self Service etc.

How may this affect me?

You will no longer be able to access University services from a computer if you are using Windows XP, Windows Vista or it has an unsupported Internet browsers (e.g. Internet Explorer less than version 10), mobiles or tablets if they cannot support newer protocols than TLS 1.0.

If you are using a supported operating system, there may be some websites you may visit that do not support the latest TLS protocols, for these sites you will receive an error and the content will not be displayed.

Why is this changing?

The National Institute of Standards and Technology (NIST) and the Payment Card Industry Security Standards Council (PCI SSC), have declared TLS 1.0 to be insecure; this means that the encryption can be broken and the information being sent can be exposed in plain text.

The University has already undertaken a piece of work to secure the services you connect to, with the modern and supported versions of TLS to protect your information.

Is there any additional advice or guidance?

There is guidance (in [SEC-GDL-001 – Secure Online Browsing Guidelines](#)) available on how to configure your personal computer to support the most modern and secure encryption protocols.