

## Phishing

Phishing is a method attackers use to get access to your personal information, using deceptive emails and websites. They try to trick you by pretending to be an entity you trust (like your bank, for example) and attempt either to make you download an attachment that can hurt your computer or steal information from it, or get you to enter personal information.

For example, imagine receiving an email from what you think is your bank, asking you to change your password for security reasons. To do so, they provide you with a direct link to what you think is your bank's website, designed to look exactly like your bank's, and with a URL which is similar enough. You enter your account number and password, set up a new one, and afterwards you think you've changed your password, but what you've done is give that fraudulent website your account number and password. With that information, they can easily transfer money from your account to one of theirs.

## Malware

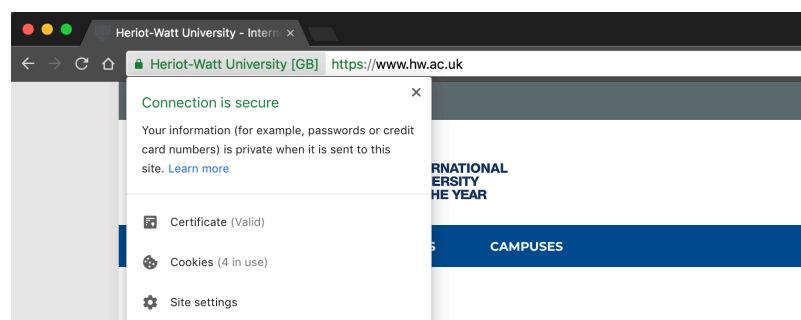
Malware stands for "malicious software". It regroups any kind of software that was written with the intent to damage your computer or act against the best interests of the user. To give a couple of examples:

- There are viruses, which, once in your computer, replicate uncontrollably and delete or corrupt files.
- Spyware is, like its name indicates, malware that is designed to spy on you. It gathers information on what you do online, including passwords, credit card numbers, surfing habits etc.
- Ransomware locks down your computer and threatens to erase all your data unless you pay a ransom to the attacker.

## SSL certificate





SSL (Secure Sockets Layer) certificates are a way to secure the transfer of information between the web server and the browser on the user's computer. When installed on a webserver, it activates the padlock icon and the https (HTTP Secure) protocol, ensuring a secure connection. It's mostly used to secure login pages, data transfers and credit card transactions.

For example, the Heriot Watt website uses an SSL certificate.



## Different kinds of security warnings

During this experiment, we'll focus on Chrome security warnings, and more specifically the ones in the status bar.

-  Like explained previously, this means that the website has a verified SSL certificate, and the connection is secure.
-  This means that the website has an invalid certificate, and your connection isn't private. An attacker could be trying to steal your information.
-  This means that the website doesn't have a certificate, it uses the http protocol, not https. The connection is therefore not secure and someone could steal your data.
-  This means the website uses mixed content. Mixed content is when the code of the page is loaded over a secure https connection, but other resources, like images, videos or scripts are loaded over an insecure http connection. This means the connection isn't fully secured.