Internet Explorer

1. Left-click the gear icon:

2. Select “Internet options” from the dropdown menu:

3. Click the “Advanced” tab, scroll down and deselect “SSL 3.0” and “TLS 1.0”.

4. Click “OK” to accept your changes, which should take effect immediately. (You may need to refresh your browser.)
Firefox

1. In the address bar, type “about:config” and hit enter.

2. In the “Search” field, enter “tls”. Find and double-click the entry for “security.tls.version.min”.

3. Set the integer value to “2” to force a minimum protocol of TLS 1.1 (entering “3” would force TLS 1.2).

4. This configuration will now show the new value and will take effect immediately (don’t forget to clear your cache).
Chrome

Unlike IE and Firefox, Chrome can only be made to use TLS 1.1/1.2 by a command-line switch – an argument added to the string that fires up the browser. This can be implemented by setting up a shortcut as we will show you below, but note that ONLY starting Chrome from this shortcut will prevent use of insecure protocols.

To create a secure shortcut:

1. Right-click on your desktop and select “New”, then “Shortcut”.

2. In the “Create Shortcut” panel, browse to the location of your Chrome installation and select the Chrome icon – the default location is:
3. Add the following command line switch `--ssl-version-min=tlsv1.1` after the item location (i.e., after the ending quote) to appear thus:

```
"C:\Program Files (x86)GoogleChromeApplication\chrome.exe" --ssl-version-min=tlsv1.1
```

Make sure and separate the switch from the location with a space.
4. Name the shortcut (SSL.com suggests giving it a unique name which will remind you that this shortcut is secure) and click “Finish”.

5. Again, the only way to be certain that your Chrome session is secure will be using your new shortcut.