A new security patch will be implemented into the network for credit card processing. This patch is required to guard against any network vulnerabilities and better protect the PCI network and credit card processing.

There has been a serious vulnerability disclosed in version 3.0 of SSL protocol. It is no longer considered to be safe to use. So, to ensure secure payments, our payments page is updated to support TLS protocol versions 1.1 and 1.2. Your browser needs to be configured to support these protocol versions to be able to make payments on our website. If you have problems to see the payments page,

Once this patch is implemented, anyone using Internet Explorer or Google Chrome must verify that their security settings are correct or the payment page will not be accessible. To verify the settings, users should do the following:

**Internet Explorer**
Google Chrome

Network

Google Chrome is using your computer’s system proxy settings to connect to the network.

Change proxy settings...
Select both options

Internet Properties

Settings

- Enable DOM Storage
- Enable Integrated Windows Authentication
- Enable memory protection to help mitigate online attacks
- Enable native XMLHttpRequest support
- Enable SmartScreen Filter
- Use SSL 2.0
- Use SSL 3.0
- Use TLS 1.0
- Use TLS 1.1
- Use TLS 1.2
- Warn about certificate address mismatch
- Warn if changing between secure and not secure mode
- Warn if POST submission is redirected to a zone that does not match

*Take effect after you restart Internet Explorer

Restore advanced settings

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Some settings are managed by your system administrator.

OK Cancel Apply