

TLS 1.2 Protocol Upgrade Requirement

Davis Trust Company is committed to providing the most secure digital access for our customers. To ensure the highest levels of data protection, our core processing partner, Computer Services Inc. (CSI), will update the minimum security requirements for CSI hosted websites beginning **the** week of February 19, 2018. This update process is expected to be completed on or before June 30, 2018.

This update will affect any of our customers who are using browsers that do not support the Transport Layer Security (TLS) 1.2 protocol. The TLS 1.2 protocol is needed to maintain data security. Customers who use non-supported browsers will lose access to the Davis Trust Company Internet Banking website following the update.

PLEASE NOTE: Since the TLS 1.2 protocol has been supported for a number of years, it is likely that most customers will not be required to update their browsers at this time.

Non-supported browsers are listed below along with instructions for testing the support of your existing browser. This test will enable customers to confirm whether or not their current browser supports the TLS 1.2 protocol.

Why are we making this change?

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS 1.2 protocol helps ensure that no third party can eavesdrop or tamper with any message or data transmission.

Who is making this change?

This is not an action that our core processor is taking alone. This change is happening throughout the industry in response to PCI Security Council mandates and other general operating standards for transmitting sensitive data.

EVERY website that transmits or processes sensitive (secure) data will be making this change. If you are using an unsecure or non-supported browser you will find that all secure websites, including our Internet Banking site, will not be accessible after the update has been completed.

How do I know if I am affected?

Most browsers have supported TLS for at least the last few years. A comprehensive list of supported browsers is available here: <https://www.ssllabs.com/ssltest/clients.html>

Which browsers are unsupported?

The following browsers (or older) **DO NOT** support TLS 1.2 and **will no longer work** after the update.

- Google Chrome 29
- Firefox 26
- Internet Explorer 10
- Safari 8
- iOS 4
- Android 4.2

How do I test support for my browser?

- Visit the following website: <https://www.ssllabs.com/ssltest/viewMyClient.html>

- A message stating, **“Your user agent has good protocol support”** should display. This indicates your browser will continue to work after the security update.
- **If you do not see this message, please update your browser or install a newer supported browser as soon as possible to avoid having any problems accessing your online banking accounts with Davis Trust Company.**
- **If you have any questions, please contact one of account customer support representatives at (304) 636-0991.**