At Fidelity Bank, we are very concerned about your online security. In order to enhance security and help protect against possible risks, we will be unable to support service to older web browsers with outdated security settings starting **Monday, April 9, 2018**. To maintain the highest level of data security and to align with industry best practices, access to the bank's website and online banking will be denied for browsers that are not TLS 1.2 enabled.

What does this mean?

Transport Layer Security (TLS) is a protocol that provides privacy and data security between two communicating applications, like web browsers and servers. TLS 1.2 is the most current version and is considered to be the most secure. TLS 1.0 and 1.1 are outdated protocols that are being phased out nationwide due to security vulnerabilities.

All modern operating systems and browsers currently allow for TLS 1.1 and 1.2 as shown in the table below:

Browsers and Operating Systems	TLS 1.2 Compatibility Note
Microsoft Edge	Compatible by default
Microsoft IE Desktop and mobile version 11	Compatible by default
Microsoft IE versions 9 and 10	Capable when run in Windows 7 or newer, but not enabled by default
Firefox 27 and higher	Compatible by default
Google Chrome 38 and higher	Compatible by default
Oracle Java version 1.7 and higher	Compatible by default
Mobile Safari versions 5 and higher	Compatible by default
Microsoft Windows Server 2008 R2 and higher	Compatible by default
Microsoft Windows Server 2008 and below	NOT compatible with TLS 1.2
Microsoft Windows 7, 8.0, 8.1 and 10	Compatible by default
Microsoft XP/Vista and below	NOT compatible with TLS 1.2

For TLS 1.2 to work on your device, both your operating system and web browser must support it.

Outdated operating systems no longer supported by their developer (ex. Microsoft XP and Vista) cannot be upgraded to TLS 1.1 and 1.2 and will require new software be installed on your device(s) to gain access to the bank's websites and applications. We encourage you to upgrade your computer software as soon as possible. Continuing to use an operating system or browser that is no longer supported by its developer exposes you and your device to a significant number

of risks and vulnerabilities, since your device no longer receives regular updates and security patches that protect you from malware.

How do I enable TLS 1.2?

Each different browser will have a different navigation to set the security option. Below are a few of the most common browser Navigations:

Microsoft Internet Explorer

- Open Internet Explorer
- From the menu bar, click Tools > Internet Options > Advanced tab
- Scroll down to the Security section and tick the checkboxes Use TLS 1.1 and Use TLS 1.2
- Click OK
- Close your browser and restart Internet Explorer.

Google Chrome

- Open Google Chrome
- Click Alt F and select Settings
- Scroll down and select Advanced
- Scroll down to the System section and click on Open proxy settings
- Select the Advanced tab
- Scroll down to the Security section and tick the checkboxes Use TLS 1.1 and Use TLS 1.2
- Click OK
- Close your browser and restart Google Chrome

Mozilla Firefox

- Open Firefox
- In the address bar, type about:config and press Enter
- In the Search field, enter tls. Find and double-click the entry for security.tls.version.min
- Set the integer value to 3 to force protocol of TLS 1.3
- Click OK
- Close your browser and restart Mozilla Firefox

If you are unable to upgrade, you will get a connection error on and after Monday, April 9, 2018 when attempting to access our website. Please reach out to your IT department or an IT professional and verify your browser is capable of supporting TLS 1.2.