Warning: Computer & Smarttphone Users

By Information Technology Commission March 13, 2015

Several months ago, ITC reported concerns about the discontinuation of Microsoft support for Windows 7 and previous versions and its vulnerabilities to malicious attacks by hackers. As anticipated, several Microsoft and Apple products have been recently attacked through a major security flaw, dubbed FREAK, that jeopardizes secure web connections and could potentially expose sensitive information.

The FREAK flaw allows a third party to interrupt a secure connection and intervene between your computer or smartphone browser and the websites you share data. When a susceptible device connects to a vulnerable HTTPS-protected site, a flaw in the encryption allows an attacker to penetrate and seize the data going back and forth between the web session. This security weakness permits access to personal information, passwords, and pretty much anything else stored on your computer.

Some of the highest-traffic domains that are affected include Business Insider, American Express, Groupon, Bloomberg, NPR, Kohls, and MIT. A number of very high-profile government sites were also affected, including the NSA, the FBI, and the White House's sites, as well as the site (USAJobs) that all applicants for any federal job must use.

The browsers and platforms known to be vulnerable include:

- Android: stock browser
- Android: Chrome
- Blackberry: stock browser
- iOS (iPhone/iPad): Safari
- Linux: Opera
- Mac OS: Chrome
- Mac OS: Opera
- Mac OS: Safari
- Windows: Internet Explorer

The best course of action to take for the computers using the previously mentioned operating systems should consider the following recommendations:

1. Maintain an external backup of all important documents, images and photos
2. Implement the latest updates or service pack for the version of the operating system installed on the church or home PC. If the patch is not available, use the Firefox browser until patches are available for the above affected browsers, you may want to use Firefox on iOS, Android, and Mac OS to securely browse the web and connect to your online accounts.
3. Seriously consider upgrading to the newer technology (i.e., tablets, laptops, smartphones)
4. Though it's unlikely that you were attacked, as devices and websites are patched it may be a good time to change the passwords to any accounts accessed on any of your devices shown to be vulnerable. It's important to use a different, strong password on

every website, so that a password stolen from one website can’t be used to login to any of your other accounts.

If you have any questions or require additional information, feel free to contact us at itc@nationalcapitalbaptist.org.