INTERNET EXPLORER VULNERABILITY

The Department of Homeland Security and Microsoft are warning computer users about a serious security hole in the Internet Explorer (IE) web browser. The vulnerability in IE is triggered when users click on a link or visit a website that has been constructed to exploit this issue, so careful browsing is important.

Please review the following suggestions and information as interim considerations while Microsoft works on a more permanent and complex fix for this issue:

1. Limit your browsing using Internet Explorer to known, good-reputation business websites.
2. Do not follow advertising links or "pop-up" ads/content.
3. Never click on links on a website or in an e-mail that take you to a place with which you aren't familiar.
4. Avoid sites with "Flash" content.

On a more technical note:

1. The Department of Homeland Security has recommended that firms reduce or eliminate their use of IE until a permanent fix is released. This is an appropriate consideration, but requires validation to ensure that business applications and processes can continue without issue using another browser.
2. Where available, work with your internal technology team to implement Microsoft-provided suggestions to reduce risk. (see: https://technet.microsoft.com/en-us/library/security/2963983.aspx)
3. Update Flash plugins to the more recent versions. (see: http://helpx.adobe.com/security/products/flash-player/apsb14-07.html)
4. Work with your Anti-Virus, Intrusion Prevention System (IPS), Firewall, and Content Filtering technology providers to implement their recommendations for detecting and preventing exposure.

This information is provided as a guide only and does not prevent issues or guarantee your systems will not be compromised. Please use this information to consult with your information technology advisors.