***NOTICE****: The following has been provided by WBA committee and section volunteers for use by member banks.
It should be reviewed and revised as appropriate to the user-bank’s own policies, procedures, and practices.*

**What is the Difference Between Pharming & Phishing?**

For those of us who are not IT wizards and don’t understand all of the in’s and out’s, I found this short article to help us understand this potentially serious crime.

**Answer:**Pharming is the hijacking of an official website's address, usually by hacking a Domain Name System server and altering the legitimate website's IP address so that users who enter the correct Web address (for example, www.bankersonline.com) are directed instead to a 'knock of' of the correct page, where user names, passwords and perhaps additional personal information is collected for later illegal use.

Phishing omits the step of hacking into a DNS server, and instead sends illicit email messages that appear to come from a legitimate source. The emails attempt to lure the reader into clicking a link that appears to go to a legitimate web address, but the actual link is to a fraudulent, look-alike site, again designed to trick the user into providing personal information. Phishing and pharming are two slightly different strategies to the same illicit end.