

In the past few days, there has been an increased number of reported phishing attempts targeting the Internet Banking solution. The phishing has had these tendencies:

- The login process is modified by adding a Web page stating that computer cannot be identified, and that the user is required to enter credit card information to continue.
- The page that requests the user data does appear to originate from our Internet Banking site with the correct URL and certificate information. However, this page is generated by malware installed on the local computer and not from the Internet Banking site. Fiserv's Internet Banking servers remain secure.
- This malware was most likely installed from an opened e-mail attachment or a compromised website viewed on the infected computers of your bank customers using Internet Banking.

Internet Banking will not ask you to enter personal or account information during the login process or for any Internet Banking pages where the information requested is not relevant to the transaction. Customers should not enter sensitive data if they are prompted to do so. Also, any system accessing Internet Banking should have anti-virus and anti-malware installed and the software definitions kept up-to-date.

If you have any questions please contact the Bookkeeping Department at 608-943-6351.