Online Security Best Practices

1. **Keep your computer updated.**
   - When you receive system updates, say "yes." Keep in mind, these updates ***DO NOT*** come through email.

2. **Install anti-virus, anti-spyware software.**
   - In addition, make sure that the software is running and updated regularly (your software subscription is active). A best practice is to install an internet security suite of products that includes a firewall, anti-spyware, anti-virus and email scan products.

3. **Secure your wireless network (if applicable).**
   - This includes changing the default passwords and following all security prompts.

4. **Secure your router.**
   - This includes changing the default passwords on the equipment.

5. **Keep your passwords and tokens (if applicable) in a safe place.**
   - i.e., do not write your passwords on a sticky note and attach it to your monitor.

6. **Rather than a simple password, use complex passphrases.**
   - i.e., a phrase that includes capital and lower case letters, numbers and special characters.

7. **Follow the procedures outlined in the online banking agreement.**

8. **When finished with online banking, be sure to log out.**
   - Closing out (i.e., hitting the "X" in the upper right corner) is not enough.

9. **Install and activate a firewall.**
   - This can include the Windows firewall built into the Windows operating system.

10. **Be mindful of current scams, including vishing (telephone scams), phishing (email scams) and smishing (text message scams).**
    - Delete email from unknown sources and do not open attachments within email messages from unknown sources. Never provide personal or financial information in response to an unsolicited phone call, fax or email.

For more information, please contact:
Mechanics Bank Information Security Department @ 419-524-0831