



Online Security Best Practices

- **Be mindful of current scams, including phishing (email scams) and telephone scams.**
 - Delete email from unknown senders and *do not open* attachments or click on links within email messages from unknown senders. Never provide personal or financial information in response to an unsolicited phone call or email.
- **Keep your passwords and tokens (if applicable) safe.**
 - Never share your password (or user name) with unknown individuals, *especially* if this information is requested via an unsolicited phone call or email.
- **Keep your computer updated.**
 - When you receive system updates, install them. Keep in mind, these updates **DO NOT** come through email.
- **Rather than a simple password, use a passphrase.**
 - Think of a phrase or sentence you might use that includes capital and lower-case letters, numbers, and special characters. A longer password is a stronger password!
- **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.
- **Install and activate a firewall.**
 - This can include the Windows firewall built into the Windows operating system.
- **Install anti-virus, anti-spyware software.**
 - In addition, make sure that the software is running and updated regularly (i.e., 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.
- **Secure your wireless network (if applicable).**
 - This includes changing the default password and following all security prompts.
- **Secure your router.**
 - This includes changing the default password on the equipment.

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