INFORMATION SECURITY BEST PRACTICES

Computer crime, also known as cybercrime or e-crime, continues to rise. Every day hackers break into networks, computers, and wireless devices. Utilize these key steps to help protect against unauthorized computer access and potential losses:

COMPUTER SECURITY

- Ensure Security Patches for Microsoft and third party applications are up-to-date.
- Keep operating systems up-to-date.
- Use Anti-Virus and Anti-Malware software with up-to-date virus definitions.
- Limit computer access to those who need it. For businesses, physically secure computers and allow only authorized personnel access.

NETWORK SECURITY

- Use Wireless Encryption (WPA/WPA2) for Internet access.
- Use a Network Firewall and NAT internal network devices; ensure client machines aren't routable on the Internet.

PASSWORD MANAGEMENT

- Use strong passwords (8+ characters, upper and lower case, alphanumeric, and at least one special character). Do not use easily guessed passwords such as birthdays or family members.
- Protect passwords. Use different passwords for each application and never share passwords or leave them accessible to others.

EMAIL SECURITY

- Do not open suspicious emails or emails from unknown persons—opening an email may expose a computer or network to malware.
- Never open an e-mail attachment from someone you don't know, and be wary of forwarded attachments from people you do know as they may contain unknown malicious code.
- Do not click on links within unsolicited or suspicious emails. The link can be for an infected website or may download malware.
- Don't respond to unsolicited emails requesting personal information.
- Do not send account numbers or personal information via unencrypted e-mail. If you need to send sensitive information to the Bank, sign-in to Online Banking to send it securely.

ONLINE BANKING TRANSACTIONS

- If possible, use a designated machine for doing strictly Online Banking or Cash Management transactions. Avoid surfing the internet, checking email, etc.
- Close all other applications and browser windows before initiating Online Banking. Look for any strange or foreign changes on the Online Banking website. If you notice something unusual, do not log on—contact us.
- Turn off your computer. Computers that are "always on" are more susceptible. Plus turning the computer off effectively severs an attacker's connection.

EDUCATION

- Be aware of common cyber fraud such as viruses, worms, Trojans, spyware, computer hacking, and phishing (email fraud).
- Educate other users on cyber schemes and how to reduce exposure to such threats.

MONITOR

- Check your accounts regularly. Notify us immediately if you notice any unusual activity.

CONTACT US AT 509-744-6900 IF YOU HAVE ANY QUESTIONS OR TO REPORT ANYTHING UNUSUAL.