Customer Education & Awareness for Consumer Internet Banking, Business Internet Banking, ACH, RDC

Due to the increase of cybercrime and exposure to fraud, Wayne Bank would like to take this opportunity to present our customers with materials on how to prevent cybercrime and reduce your exposure to fraud. Whether you are a consumer or business, these guidelines and best practices can assist you in banking safely while utilizing the latest technology.

Wayne Bank will never contact our customers and ask for passwords, online banking credentials, account numbers or social security numbers. Please visit wayne.bank to review our Privacy Policy and Terms of Use. We also offer helpful resources and links to keep customers well informed and help protect against fraud. If you are concerned, your accounts have been compromised or have any questions related to this information please contact a representative at (800) 598-5002.

Password Security- Only the user and the system being authenticated should know a password. The system cannot differentiate the real user from another user who knows your password. For this reason, it is imperative that you keep your passwords private. Never write your password down where someone may be able to find it and use it.

Below is a list of password parameters using Wayne Bank's online banking criteria:

- Password should be between 9-17 characters in length
- Use at least one capital letter, lowercase letter, numeric digit and special character
- Can be easily remembered but hard to guess
- Change your password often, we recommend at least every 120 days
- Not based on a word in the dictionary

Below is a list of some common password choices to avoid:

- Your name, family member or pet's name
- Social security, account or telephone numbers
- Birth dates
- A password used on another website
- Any of the above spelled backwards
- Sequences such as 1234567, 55555555, abcdefgh, abc123

Other Important Considerations

- Never share user IDs, passwords, PINs, tokens, secret questions and answers with anyone. Do not leave them in an unsecure area.
- Do not use the same login or password on multiple sites or programs.
- Install antivirus, antimalware and antispyware software on all computers and keep up to date. Run virus scans often.
- Install a firewall and ensure it is automatically updated or take steps necessary to keep it up to date. Password protect wireless access so unauthorized persons cannot utilize your wireless connectivity.
- Limit unnecessary web surfing and email activity by employees, including personal activity on work computers used for online banking.
- Educate all personnel on cyber security practices.
- Verify use of secure sessions (https:// not http://).
- Avoid saving passwords on computers. If saving a list of passwords use an encrypted password

database program to store them on the computer's hard drive.

- Never leave a computer unattended while logged into an online banking session. Always lock computers when stepping away.
- Do not access financial institution websites for online banking from a public computer access such as a library, coffee shop or other public access point. Treat all public WI-FI networks as a security risk.
- If Adobe Acrobat and Java are installed on a computer, these programs should be updated. You can set programs to automatically update or go to the vendor's website for updated versions.
- Shred all personal and business mail rather than disposing of it in the trash.
- Promptly review your bank statements and report any errors to the bank.
- If using a smartphone for banking transactions make sure no one watches over your shoulder when in public. The smartphone should be encrypted and have strong password protection.

Wired Access by Computer: Needs a current anti-virus/anti-spyware scanning program, a current patched operating system, and a secure, patched browser program. Internet Explorer 8 and 9 have security capabilities written into them. Firefox also has secure browser programs.

Access by Wireless Network: Needs all of the security measures applicable to the wired home computers plus the wireless router should have strong password protection, and it is recommended the wireless network have at least WPA or WPA-2 encryption rather than WEP encryption. The strongest wireless encryption, outside of military grade wireless encryption, is WPA-2 PSK.

Secure your Wi-Fi networks

If you have a Wi-Fi network for your home or workplace, make sure it is secure and hidden. To hide your Wi-Fi network, set-up your wireless access point or router so it does not broadcast the network name also known as the Service Set Identifier (SSID). In addition, make sure to turn on the encryption so that passwords are required for access. Lastly, it is critical to change the administrative password that was on the device when it was first purchased.

Glossary of commonly used terms

- Virus- A computer program that can replicate itself and spread from one computer to another. It may infect more files or perform an action such as wiping out a hard drive.
- Malware- software created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
- Trojan- A type of malware, which appears to perform a desirable function but instead facilitates unauthorized access to the computer's system. Trojans do not attempt to inject themselves into other files like a virus. Trojan horses may steal information or harm their host computer systems by installing an online games or internet-driven applications in order to reach target computers.
- Spyware- Software that gathers information about a person or organization without their knowledge and may send such information to another entity without consent
- Phishing- The act of attempting to acquire information such as usernames, passwords, credit cards by masquerading as a trustworthy entity in an electronic communication such as an email.
- Key logger- The action of recording or logging the key struck on a keyboard in a covert manner so the person using the keyboard is unaware.
- Adware- Any software that automatically renders advertisements in order to generate revenue for the creator.