Network Security Best Practices

Experts recommend that you conduct an initial risk assessment of your online and operating systems. These best practices have been collected from various industry sources. Park Bank makes no recommendation as to which best practices are appropriate for your business. Since every business is unique, Park Bank strongly recommends that you contact your IT professional to evaluate your system and suggest best practices for your business.

- Install updated anti-virus and anti-spyware programs and firewall on all computers annually. Ensure that they are enabled and configured for automatic updates.
- Keep all security programs, along with the operating system and software, up-to-date with the most current patches. If operating system is discontinued, patches may no longer be available. Upgrade to a newer operating system.
- Centrally manage both physical and systems access. Audit system activities, such as successful and failed user logins, file and system access. All operating systems, and most applications such as firewalls, have the ability to audit system activities.
- Back up files incrementally (daily) and fully (weekly). Test restore function to ensure backups are working as intended. Another option is to use an external hard drive or website service to back up. Keep backups off site.
- Consider encryption of sensitive data.
- Conduct an external network penetration test (simulates a targeted attack on your systems via the Internet) to identify vulnerabilities in your organization's systems.
- Conduct 'test' phishing attacks on your employees.
- Perform and maintain a complete asset inventory; take steps to securely dispose of hardware and software.
- Monitor third-party vendors and their products to ensure secure remote access implementations.
- Don't allow company-issued workstations to be used as personal computers. Do not allow employees the ability to install any personal software or downloads (games, file sharing, personal email accounts) from the Internet.
- Prohibit the use of personal USB drives, portable hard drives or other unauthorized devices to be connected to company systems.
- Use multi-factor authentication wherever possible (tokens, PINs, digital certificates, etc.).
- Use mobile or email alerts and notifications for high-risk activities.
- Make sure your card processing systems and hardware are Payment Card Industry compliant.
- Secure data on mobile phones and portable flash drives with password entry.
- Prevent users from sharing login credentials.
- Require strong passwords, having at least eight characters. Incorporate upper and lower case letters, numbers and special characters. Do not use dictionary words.
- Educate employees about social engineering scams in the office, such as fake employment interviews, fake vendors or phony contract bids or rogue media such as USB drives found near the entryway or in a public area.

PARK BANK
first IN LASTING RELATIONSHIPS®

- Be careful what you download, open or click on because this action can circumvent even the most vigilant anti-virus software. Be wary of forwarded attachments from people you do not know.
- Turn off your computer when not in use, which severs an attacker's connection to other company resources.
- Use bookmarks in your Web browser for entities with which you regularly communicate.

Tips from leading experts:

- Use a dedicated PC for conducting online banking activities.
- Restrict remote access users and applications.
- Never give out your password, account number, ID, or credentials via email, the Web, text messages, or telephone. Park Bank will never ask for confidential information via email.
- Retire "end of life" hardware and software that have no security patches available.
- Consider a network firewall with unified threat management capabilities. This will provide another layer of protection from viruses, spam and other targeted attacks on your network.
- Use an authorized, separate administrator account for installing or removing software.
- Know the warning signs of when you may have a problem:
  - Know your computer. If acting strangely (slow response time, excessive pop ups, etc.) check it out.
  - Know when to expect your account statements. Better yet, use online functionality to review activities daily.

Create a security agreement:

- Have all employees sign a security agreement in order to demonstrate that they are taking cyber security seriously and are active participants in helping to maintain a secure online environment.

PARK BANK
first IN LASTING RELATIONSHIPS®