Identity Theft Business – Southern First Bank

Hackers, backed by professional criminal organizations, are targeting small and medium businesses to obtain access to their web banking credentials or remote control of their computers. These hackers will then drain the deposit and credit lines of the compromised bank accounts, funneling the funds through mules that quickly redirect the monies overseas into hackers' accounts. As a business owner, you need an understanding of how to take proactive steps and avoid, or at least minimize, most threats.

- Use a dedicated computer for financial transactional activity. DO NOT use this computer for general web browsing and email.
- Apply operating system and application updates (patches) regularly.
- Ensure that anti-virus/spyware software is installed, functional and is updated with the most current version.
- Have host-based firewall software installed on computers.
- Use latest versions of Internet browsers, such as Explorer, Firefox or Google Chrome with "pop-up" blockers and keep patches up to date.
- Turn off your computer when not in use.
- Do not batch approve transactions; be sure to review and approve each one individually.
- Review your banking transactions daily and your credit report regularly.
- Contact your Information Technology provider to determine the best way to safeguard the security of your computers and networks.
- Contact your Client Officer should you suspect your account has been compromised. If your checks or debit cards have been lost or stolen, please report the fraud.

Additional resources to assist you with a compromise are the FTC's

Protecting Personal Information – A Guide for Businesses.