SALISBURY BANK | enriching.

Business Smart

cash management update

Updated March 2012

Computer Security Checklist

Keeping your business accounts secure is most effective if you keep up with what is necessary on a regular basis. Though particular business security procedures may vary somewhat, this checklist will help keep you on track with the most critical tasks for maintaining electronic computer security.

Virus Protection

Viruses can reach your computer in many ways, through floppy disks, CD-roms, thumb drives, email, websites, and downloaded files. Using and regularly updating anti-virus software is a critical element of computer security protection.

□ Install anti-virus software on all computers and workstations.

□ Configure anti-virus software to check all mediums (floppy disks, CD-roms, email, thumb drives, websites, downloaded files) for viruses.

□ Set anti-virus software to automatically scan your computer at least weekly.

□ Create procedures for automatically updating the anti-virus software.

□ Create procedures for handling computer viruses and other infections when they are discovered.

Firewall

A firewall is like a security guard that stands between your computer and the Internet. It examines all traffic routed between your computer and the Internet to see if it meets certain criteria. If it does, it is allowed in. If it doesn't, it is stopped.

□ Install firewall software on all computers and workstations, and at every point where your computer system is connected to other networks, including the Internet.

□ Configure firewall software to protect the required information on all computers and workstations.

□ Install a hardware firewall on your computer network.

Password Management

Strong locks and alarm systems help keep intruders out of your place of business. A password management program with strong passwords that are changed regularly will help protect your computers and your business's confidential information.

□ Require User IDs and passwords for access to all computers and workstations.

□ Instruct staff to choose "strong" passwords (alpha/numeric and special characters) that are not easily duplicated and change passwords regularly.

□ Do not allow staff to write down or share passwords.

□ Do not use the "Remember Password" feature of applications.

□ Do not use the same password to access multiple systems.

Software Security Patches

Hackers like to find and exploit bugs in operating systems and software products such as Internet browsers and email programs. To protect your business, download and install software patches and updates as soon as they become available.

□ Update your operating systems with appropriate security patches.

□ Update other software programs with appropriate security patches.

continued

In addition to the checklist above, it is also a good idea to be aware of and check for the following:

Remote Connections

The ability to connect remotely to your office computer via the Internet can be a major advantage for business efficiency. The downside is that if you can tap in, others can too. That's why security, including encryption and authentication, has to be a priority.

❑ Use a virtual private network (VPN) to set up remote connections and hire a security or IT consultant to properly configure the VPN.

Confidentiality of Private and Sensitive Data

The need for ensuring the privacy of your business's data has never been greater as Internet usage increases and compliance and security requirements become more demanding.

❑ Restrict access to private and sensitive data to only those employees who need to know.

❑ Institute a "clear desk" policy to ensure your staff secures sensitive and confidential files when they are not working on them.

❑ Monitor the work of temporary employees or student employees closely.

❑ Encrypt the electronic transmission of sensitive data.

Data Backup

Backing up critical data regularly is like an insurance policy. It allows your business to get up and running quickly after a data loss.

❑ Perform regular backups (ie: daily, weekly) of all data files.

❑ Periodically test restoration of data files to ensure the backup files work.

❑ Store at least one copy of the backup data in a secure, off-site location.

❑ Periodically review your backup requirements.

Disaster Recovery

If a fire destroyed your office, what would you do? Having a disaster recovery plan can help minimize the impact on your clients and get your business up and running again.

❑ Create a written continuity plan in the case of a major disaster such as a fire.

❑ Store at least one copy of your data and application software in a secure, off-site location.

❑ Maintain a current inventory of your computer, software and critical files.

Physical Security

Ensuring the physical security of your computers is a key step in securing the information stored on them.

❑ Place computers and workstations in areas that are not easily accessible to outsiders.

❑ Be sure to lock doors and windows each day.

❑ Equip desktop and laptop computers with anti-theft devices.

❑ Secure network servers in a separate area.

Reference: www.advisortek.com

This document is designed to provide informative material and is distributed with the understanding that it does not constitute legal or other professional advice. We suggest that you consult with your systems administrator, IT consultant, technical advisor or attorney with regard to your business' particular situation. Opinions expressed herein are subject to change without notice. Information has been obtained from sources believed to be reliable, but its accuracy and interpretation are not guaranteed.

Salisbury Bank and Trust Company (the Bank) has provided the websites listed in this newsletter solely for your convenience, but we are not responsible for the content, links, privacy policies or security policies of these websites and do not imply any endorsement of or responsibility for the opinions, ideas, products, information or services offered at such sites or any representation regarding the content at such sites. The Bank makes no warranties, either expressed or implied, concerning the content of such sites, including the accuracy, completeness, reliability or suitability thereof for any particular purpose, nor does the Bank warrant that such site or content is free from any claims of copyright, trademark or other infringement of the rights of third parties or that such site or content is devoid of viruses or other contamination.

© Salisbury Bank and Trust Company Member FDIC