Computer Security Best Practices

Salisbury Bank works to protect our customer and financial data and would like to share some of the best practices we have learned to help your business and your employees avoid becoming victims of a computer security breach.

While some specific examples in the document focus on PCs, Mac owners will also benefit from most of the concepts and suggestions provided.

Computers are most often infected with viruses and other malware when users:

- ❏ Browse to and/or click on links to malware infected sites.
- ❏ Open spam or phishing emails and click on links.

You can find definitions for malware, spam, and phishing at the end of this document.

Personal behaviors you can control to prevent infections:

- ❏ Be careful when browsing the Internet; be aware of questionable links or pop-up windows.
- ❏ If you frequently see pop-up windows and they do not seem to be linked to a particular website, you may have an infection already, and will need to scan your computer.
- ❏ Be careful of spam or phishing emails and any links that may be in them, or any requests for personal information even if it seems to be from a trusted source. Even if you are emailing a known trusted source, email, is not a secure way to transmit data and can be intercepted.
- ❏ Social networking sites can be portals for hackers to infect your computer. When browsing these sites, your computer can be infected if you click on a malicious message.
- ❏ Computers used for business purposes should not be used for personal matters, even when employees are on breaks, as it may put the computer at significant risk. Any sensitive data that is held on the computer or is keyed into the computer is vulnerable to possible security risks picked up from personal browsing and email access.
- ❏ Do not allow web browsers such as Internet Explorer or Firefox to save your passwords. The password file can be compromised and used by a hacker.

Computer security features you can utilize to prevent hackers from infecting your system:

- ❏ If you are using a computer with a Microsoft operating system, make sure that your computer is set-up to receive Windows automatic updates (Windows 7, XP, Vista, etc.).
- ❏ Don't believe the hype. If you own a Macintosh (Apple) computer you can get viruses too. Macintosh systems are also vulnerable to phishing emails and malware attacks from web browsing. Macintosh systems are less frequently attacked because they are not mainstream business computers, however they are still vulnerable.
- ❏ Make sure you have a security software suite installed on your computer that includes protection against spam, malware, spyware, and viruses.
- ❏ Update your security suite at least daily, and schedule it to scan the entire computer with no exclusions at least weekly.
- ❏ Be knowledgeable about free security services that may be available from your Internet Service Provider such as spam filters.
- ❏ Know your computer's history of infections. Just because an infection was cleaned out six months ago doesn't mean information gathered from that infection cannot still cause harm to you or your business. If your computer has had a history of infections, even if it appears clean now, you should perform the steps outlined in the section labeled "If an infection is found on your computer."

continued

If an infection is found on your computer

Any infection should be taken seriously. Infections can result in allowing hackers to steal your banking information, credit card information, or even your identity. Hackers can monitor your browsing habits, pose as you on a social networking site, or even log every keystroke you make on the keyboard.

You can look up security issues you find at security vendors' websites to find out about the nature of the infection you have. It is important to use the following rules to mitigate any risk for any infection found.

- ❏ If the infection was successfully removed, deleted, or quarantined, make sure by restarting the computer and rerunning the scan. If the infection is found again, it may need to be removed by a qualified IT professional.
- ❏ If and only if the infection is verified to be removed from your computer, it is imperative to change all online passwords, and if used during the time of infection, all security phrases, or challenge questions. For situations where you can easily change the username, it is recommended to do so in addition to the other items discussed.
- ❏ It may also be a good idea depending on the infection to notify any credit card companies or banks that you do online business with so they can put in place appropriate safeguard procedures to protect any potential breach of information the threat may have caused.

General security guidelines

- ❏ For a password to be considered secure and not easily cracked by a hacker it should be at least 8 characters, if not 10 or more. The password should contain upper case and lower case letters, as well as numbers and symbols whenever possible. The password must not contain consecutive characters, abbreviations, names, or any word in the dictionary. For example DayTona55 is not a secure password.
- ❏ Login information such as User IDs and passwords should be kept in a secure location and should not be written anywhere.
- ❏ Passwords should be changed frequently. Best practices recommend at least every 90 days, more frequently if possible.
- ❏ Passwords should not be shared or emailed, as email is not a secure form of communication without encryption.

Ways to identify when something is wrong with your computer

Whenever something seems suspicious with your computer you should always run a full scan to verify that there are no infections. Scans should be set to run automatically at least weekly. If you do notice any of the following in between scheduled scans, it is recommended to run another scan to be safe.

- ❏ The computer is running much slower than usual.
- ❏ There are a lot of pop-up messages, sometimes even when not surfing the Internet.
- ❏ Web searches return weird, unexpected results, or pop-up additional pages or ads.
- ❏ The first page you see when opening your Internet browser unexpectedly changes from what it used to be.

Definitions *Provided by – www.dictionary.com*

Malware is malicious computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

Spam is a disruptive, especially commercial message posted on a computer network or sent as email.

Phishing is a request for confidential information over the Internet under false pretenses in order to fraudulently obtain credit card numbers, passwords, or other personal data. Most often this is done using company logos, look, and feel in a fake website, or email communication.

Salisbury Bank and Trust Company

5 Bissell Street
Post Office Box 1868

Lakeville, Connecticut
06039-1868

t: 860.435.9801
t: 800.222.9801

www.salisburybank.com