An NSAC Best Practice

National Society of
Accountants for Cooperatives

136 South Keowee Street
Dayton, Ohio 45402
(937) 222-6707
info@nsacoop.org l www.nsacoop.org

Safe Computing

Contributing Author:
Bill Erlenbush: NSAC Director of Education

December, 2015

NSAC
National Society of
Accountants for Cooperatives

Best Practices: Safe Computing

In today's world, computers are constantly under siege from hackers wanting to steal data or just create havoc for your operations. Here are a few Best Practices to protect your computer systems.

1. **Update, Update, UPDATE!**
   Set up your computer for automatic software and operating system updates. A machine with non-current updates is more likely to have software vulnerabilities that can be exploited.

2. **Install protective software.**
   When installed, the software should be set to scan your files and update your virus definitions on a regular basis.

3. **Choose strong passwords.**
   Choose strong passwords with letters, numbers, and special characters to create a mental image or an acronym that is easy for you to remember. Create a different password for each important account, and change passwords regularly. However, do not require password changes so frequently that employees place passwords on sticky notes attached to the monitor or under the keyboard.

4. **Backup, Backup, BACKUP!**
   Backing up your machine regularly can protect you from the unexpected. Keep a few months' worth of backups and make sure the files can be retrieved if needed. Many backup service providers can back your information up automatically to the cloud.

5. **Control access to your machine.**
   Don't leave your computer in an unsecured area, or unattended and logged on, especially in public places. The physical security of your machine is just as important as its technical security.

6. **Use email and the Internet safely.**
   Ignore unsolicited emails, and be wary of attachments, links and forms in emails that come from people you don't know, or which seem "phishy." Avoid untrustworthy (often free) downloads from freeware or shareware sites.

7. **Use secure connections.**
   When connected to the Internet, your data can be vulnerable while in transit. Use remote connectivity and secure file transfer options when off campus.

8. **Protect sensitive data.**
   Reduce the risk of identity theft. Securely remove sensitive data files from your hard drive, which is also recommended when recycling or repurposing your computer. Use the encryption tools built into your operating system to protect sensitive files you need to retain.

9. **Use desktop firewalls.**
   Macintosh and Windows computers have basic desktop firewalls as part of their operating systems. When set up properly, these firewalls protect your computer files from being scanned.

10. **Most importantly, stay informed.**
    Stay current with the latest developments for Windows, Macintosh Linux, and Unix systems.

Protecting a computer vs. safe computing behavior

- You can see from the list above that safe computing practices include a combination of how you physically or technically protect your computer by using software and security settings, and the actions you take.
- You need both to really make a difference. If you consistently use strong passwords, but then leave your computer unlocked and unattended in public places, you are still putting your data in jeopardy.
- If you use anti-virus software but aren't careful about replying to or forwarding suspicious looking emails, you still risk spreading a virus.

DISCLAIMER FOR NSAC BEST PRACTICES *The NSAC Best Practices are developed from accounting literature, Internet articles, and from personal experiences and are intended to be instructive and illustrative in nature and should not be considered all inclusive, nor a guarantee. If utilized individual results may vary*.