Top Ten Security Tips

Below is a quick list of security reminders that should be followed to keep SMCS computers and networks safe and secure. For complete guidelines on computer use please review the Workstation Use Policy and Procedures.

1. Don't be tricked into giving away confidential information.

- Don't respond to emails or phone calls requesting confidential company information. Always keep in mind that bad guys are successful because they are convincing.
- Recent news stories out of Canada reported scammers were tricking people into giving away information with fake tech support calls claiming to help.

2. Use the computer and internet for business purposes only.

- The internet is the primary source of viruses and malware. One infected computer can impact all computers.
- Do not save personal files like music or picture to your computer. Computer problems occur less often if they are used for business use only.

3. Prevent patients and visitors from viewing your computer.

- Use a privacy screen on monitors in public areas or on monitors viewable by other employees.
- Use a password protected screen saver.

4. Lock your computer when not in use.

- Always lock your computer. You work on important things, and we want to make sure the information stays safe and secure.
- Locking these devices keeps the organization's data safe from prying eyes.

5. Stay alert and report suspicious activity.

- Do not allow unauthorized use of computers. If you see a visitor or an employee that should not be accessing a computer ask them to stop.
- Report virus and malware warnings to the Help Desk ext.7635.

6. Do not save sensitive information to your computer.

- Always save important and or sensitive files to network files servers.
- Do not save sensitive information on your computer or to removable media such as DVD's and thumb drives.
- Do not use the email system to communicate sensitive information unless you know it is properly encrypted.

7. Use hard-to-guess passwords.

- Don't use obvious passwords like “password,” “cat,” or obvious character sequences.
- Create complex passwords by including different letter cases, numbers, and punctuation.
- Never share your passwords and never allow anyone use your login credentials to access a system.
- Never keep written passwords near your computer.

8. Be cautious of suspicious emails and links.

- Hackers try to steal email lists from companies, which happened recently to Toshiba. SMCS email addresses are valuable to attackers, allowing them to create fake emails from "real people. “
- Always delete suspicious emails from people you don't know. And never click on the links. Opening these emails or clicking on links in them can compromise your computer without you ever knowing it.

9. Don’t plug in personal devices without the OK from Technology Management Services.

- Don’t plug in personal devices such as USB memory sticks, MP3 players and smart phones without permission from Technology Management Services. Even a brand new iPod or USB flash drive could be infected with a virus or malware.
- These devices can be compromised with code waiting to launch as soon as you plug them into a computer.
- Talk to Technology Management Services about your devices and let them make the call.

10. Don’t install unauthorized programs on your computer.

- Malicious applications often pose as legitimate programs like games, tools or even antivirus software. They aim to fool you into infecting your computer or network.
- If you need an application and think it will be useful, contact Technology Management Services and we’ll look into it for you.