Standard Recommendations

Industry Best Practices For A Secure Computer

This is not an all inclusive list, but it is a good place to start if you want to have a better, more secure computing experience. Following this set of recommendations will help to eliminate many of the headaches that effect most computer users.

General

1. Use a router based firewall to protect your network.
2. Use a good reputable full featured Anti-Virus/Malware program on all of your computers.
3. Password protect the Anti-virus software.
4. Have a proven & tested data Backup & Recovery plan.
5. Routinely clean your computer and remove any unnecessary programs.
6. Train your employees so they are aware of security threats & proper computer use.
7. Keep updates current for Windows, programs and security.
8. Don't install any software unless you are 100% sure you need it.
9. Use Business email accounts, not personal or freebie accounts.
10. When traveling do not use public or open unsecured wifi connections.

User

1. Users operate under a "limited" account instead of "administrator" account.
2. Users don't install new programs and/or updates.
3. All computer user accounts have a good password.
4. File sharing is limited to a single shared folder on 1 computer and does not use the built in "Everyone" group.
5. Local documents are stored in the user's My Documents folder.
6. All shared documents are located on a shared drive with appropriate permissions for viewing and changing based on the User.
7. Do not use USB sticks for sharing files.
8. Don't install any software unless you are 100% sure you need it.
9. Don't let other people use your computer.
10. Don't open suspicious emails.
11. Don't share your private information.
.

Mobile

1. Physical Protection – Case & Screen Protector
2. Correct Charger
3. Screen Lock Code
4. Security App
5. Mobile Device Management App
6. Don't use Public "Open" wifi, such as at hotels & conference centers.

We are The Technology Service Provider for Housing Authorities!
Let Us Start Helping You!