Computer Security Basics

Acknowledge a Higher Power, and that you're not It.

a. Many people use their computers day-to-day as admin, as if they're the Higher Power: often, XP computers were sold with only one account (admin), and with no password! In 2001 that wasn't so bad, but today almost every PC is connected to the Internet. So to minimize malware damage, you need a "standard user" account for your day-to-day use.
b. Use a password on it that's easy for you to remember, but hard for others to guess. Examples: "WdutSR,f,fa!1" is the first letters of "Way down upon the Swanee River, far, far away!" +1.
c. Never use your nickname, birthdate, your spouse's or child's name, "123456" or "password". "Social engineering" is a scheme of finding out basic info about you to access your accounts. Is "IgftUoCi1967." from "I graduated from the University of Colorado in 1967." a bad idea? If you're religious, would "John3:16" or "Psalm23:1" be good passwords? Why or why not?
d. Don't use the same password for other places on the Internet – what if someone guesses it?

You need a "password vault"! Go to www.LastPass.com and set up your account NOW!

a. LastPass works online: it's especially helpful for people who don't have their own computer.
b. Enter your name, email account and a master password to set up your LastPass account. Again, use a new password that's easy for you to remember, but hard for others to guess.
c. Never use your email password as the master password for your password vault. Why?
d. First, store your email account website address, your User-ID and password in LastPass.
e. Next, store your admin and standard user(s) User-IDs and passwords in LastPass.
f. For each new website, enter its address, your User-ID and let LastPass create a password: this will be a virtually unbreakable password, a string of scrambled letters and numbers.
g. Now open LastPass each time you start to go online and let LastPass open all your websites! LastPass can also store secure notes, and fill out web forms automatically.

Now you need a secure place where you can keep your other personal information.

a. Why? Your personal information is your identity – it is you. Guard it from identity theft!
b. To keep your files secure on a PC or flash drive, download **Safe House Explorer**. The free version gives you 4Gb of encrypted storage space that can securely store probably all of your personal information: text files, spreadsheets, photos, maybe even some music.
c. To sync these PC files with a flash or network drive, use the **FreeFileSync** program – keep a backup of your personal files in your possession! Your information is your identity: it is you.
d. Why bother with offsite backups, if you're already syncing with a flash or network drive? What about loss, theft, fire, flood, tornado... when your local backups are gone. (And by the way, most people simply won't backup their files locally because it's a bother and takes time.)
e. For offsite backups, **Google Drive** and **SkyDrive** let you edit your files online and sync with other devices. Other services to store and share your data online are **DropBox** or **Box.com**.
f. Also, consider **JottaCloud** - it gives you 5Gb of free, encrypted automatic backups that you can share and sync with other devices, and you get up to 100Gb free if you recommend your friends.

Install Internet security, and protect against "Zero-Day" and "Drive-By" attacks.

a. I recommend Microsoft's high-rated, free security package, **Microsoft Security Essentials**, which will protect your computer from email and website viruses, trojans and other malware. It downloads daily virus definitions, and scans your PC while you work or play. But what if a brand new virus or trojan hits your PC the day before MSE adds it to its virus definitions?
b. To protect against "Zero-Day" and "Drive-By" attacks, you need something that watches for dangerous activity on websites: use **AVG Link Scanner** to guard against reputable but infected websites, and also evil sites hiding behind those "tinyurl.com" links often used on Twitter, etc., because hackers can hide malware websites behind these shortened URLs.