Your company computer DO'S and DON'TS

VUSI TAFU

Systems Librarian

Have you ever found yourself in one of the following scenarios?

- You are eating lunch at your desk and checking your Web e-mail account. A friend forwards a YouTube video that is hilarious yet full of swear words. You forward it to an office buddy who you know will also love it.
- You have a disagreement with your manager and let off steam by posting some particularly nasty comments about his management style on your blog.
- You are on a business trip and lose a memory stick that has confidential company documents on it. You were supposed to encrypt this information, but have not gotten around to it yet.

While these scenarios sound relatively innocuous, any one of them could actually get you a dressing-down from your boss, a formal reprimand or worse, fired.

With e-mail, the Internet and mobile electronics that are so ubiquitous, it is easy to forget what you should and should not do at the office or with company electronics. To keep yourself out of hot water, you have to know what your company's electronic communications policy is and stick to it.

It is smart to play it safe. Employees have no reasonable expectation of privacy in the workplace, so companies are within their legal rights to monitor e-mail, blogs, social networks and even text messages sent over your company-provided cell phone to check up on what you do and say. You have to know it's a place of business, not home.

Someone is watching

According to legal and security sources, companies are not spying on employees to catch slackers or people sending too many personal e-mails. In most cases, it is to prevent leaks of confidential information that could result in regulatory fines, lost business or bad press.

So what should you do? Here are some do's and don'ts for using the company computer and protecting yourself and your company.

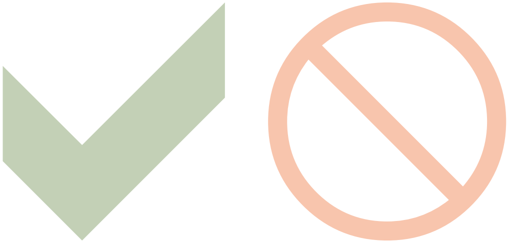
Basic rules

Think before you type

Unlike hallway conversations or phone calls, what is said in an e-mail can last forever, and chances are that more than just the intended recipient will see it. Plus, employers view e-mail communications differently. You could get fired for telling a joke to a fellow employee over the Net that you thought was funny and your boss heard in the cafeteria.

Know your company's e-mail and Internet usage policies

Many companies' rules for using e-mail and the Internet are part of the handbook for employees. Some offer workshops on electronic communications policies. If you are unsure about any aspect, be sure to ask. It is important for companies to inform staff about its policies. Many a time a case is dismissed during a disciplinary hearing as staff will claim that they did not know of the correct procedures. Management should not assume that staff are aware of company policy.



Protect your gear

People lose things all the time. According to a November 2007 survey undertaken by the Ponemon Institute, slightly more than half of 893 people surveyed said they had lost or misplaced a cell phone, laptop, memory stick or other device containing sensitive company information in the recent past. With such a high risk factor, it is imperative to take steps to make sure work data is protected. Use passwords or encryption, so data on lost or stolen devices cannot be read. Keeping your laptop, phone and company files organised in one place, such as a wheeled briefcase, is a good way to prevent things from getting lost in the first place. Using the company computer wisely can save you a lot of headaches - and it might even save you your job.

Whether you work for a small business or a major corporation, you probably access most of your data via a computer network. As a result you should be concerned about network security. Security violations cost organisations billions in lost information, data recovery, and system clean-ups. Therefore, as a user, you must always be aware of the do's and don'ts when working in a networking environment.

Do's

- ✓ Choose your passwords carefully. Make sure they are unique and include both letters and numbers. Never pick obvious ones such as 'password' or 'computer'. And avoid using names of family members and pets. Also, passwords should be changed periodically.
- ✓ Avoid saving company data to floppy disks, memory sticks, et cetera, which can easily be stolen.
- ✓ Utilise network virus protection software. Viruses are programs whose sole purpose is to cause chaos in computer networks. Always perform a virus scan on information you receive on a floppy disk.
- ✓ Report any unauthorised use of your computer. Administrators can review security logs and track all activity performed through your PC within a given time period. They can determine which files were accessed, and what changes were made to your network account. This is called auditing.
- ✓ Lock your workstation when you step away from your computer. Otherwise, anyone who passes by your unattended PC can access your files.
- ✓ Inform administrators of employee departures. Vacant computers often have active user accounts that must be disabled.

Don'ts

- ⊘ Don't reveal your password to anyone. Some people give their network account information to managers, co-workers, or even friends. Passwords are private and should be shared with no one. If you go on leave, have administrators grant access of your files to an appropriate user. Then, after your return, have that access promptly revoked, and change your password immediately.
- ⊘ Don't leave passwords around your workplace. Some people tape passwords to desks or place them under keyboards. This is a definite no-no. Always take the time to memorise your security access information.
- ⊘ Don't save personal or sensitive information on shared network resources. For example, employees' salaries shouldn't be in a folder that can be accessed by the whole organisation.
- ⊘ Don't open suspect e-mails. E-mails often contain viruses that can quickly spread through a large portion of computers in a network. If you think an e-mail might be dangerous, delete it immediately.
- ⊘ If you receive a pornographic e-mail, it is not a crime especially if you opened it unknowing but if you forward it and you get caught you can be fired.
- ⊘ Don't leave sensitive data on your hard drive. Computer hard disks are not usually protected by passwords and can be accessed by anyone. In addition, hard drive information is not subject to the routine backups performed by administrators.
- ⊘ Don't use automatic login features. These will enable anyone to use your account to gain access to the network.

Network security

Network security should always be taken seriously. Frequent attacks on a network can result in a loss of data, revenue, and ultimately, jobs. Therefore, users have a responsibility to themselves, and to their fellow employees, to protect the information within their organisation, and implement appropriate security measures.

Computers can be our best friends - or our worst enemies. Treat your computer right, and it will give you years of enjoyment and productivity. Treat it wrong, and you will pay in hours lost to troubleshooting and frustration.

Treating your PC right means knowing some basic operational rules and guidelines. Amazingly, most of us acquire a computer and begin using it without ever being told what to do - or what not to do. Here are some guidelines that will get you started.

General guidelines

Hands off that on/off switch

First, do not make a habit of turning off your computer using the on/off switch. The latest Windows operating systems have a *Shutdown* command for a reason: Shutting down your PC through the operating system allows it to close all open applications and files and keeps disk fragmentation in check. Also, using the *Shutdown* command is important to ensure that any unsaved data is written to disk rather than being lost or scrambled the next time you turn on your computer.

Look at the hard drive of anyone who shuts down the computer by using the on/off switch, and you'll see hundreds or thousands of 'tmp' - short for 'temporary' - files clogging up the system. Those files would have been deleted if the operating system had been shut down properly. They cause no harm but they do take up space.

So, what should you do when your operating system freezes and you cannot shut the computer down the normal way? First, try pressing and holding down the Ctrl-Alt-Del keys simultaneously. Doing so should bring up a dialog box that contains a *Shutdown* button. Use that.

If Ctrl-Alt-Del still does not work, you may be left with no option but to use the on/off button. Don't worry. Serious damage is unlikely to result if you resort to this method once in a while. Just be sure to save your work often, since you will lose any changes you have made to a file since the last save if you're forced to use an emergency shutdown.

Pause after shutdown

If you turn your computer off, wait at least a minute before turning it back on. The pause allows your computer's memory to discharge fully. It also permits disk drives and fans to come to a standstill instead of being abruptly jolted back into action.

Turn your PC off before connecting

Be sure to turn your computer off before connecting new hardware that is not designed to be 'plug-and-play'. Any device that connects to the older parallel, serial, or PS/2 connections on your PC will typically not be plug-and-play. Plugging in a PS/2 mouse while your computer is running, for instance, would not necessarily cause your computer to freeze or result in damage, but the device usually would not work until you restart your computer.

USB and FireWire devices, on the other hand, are often designed to be plugged in while the computer is running. As long as you have first installed any device drivers supplied with your USB device, you should have no problems.

Drive safely

Any removable drive in your PC - such as a CD-ROM, DVD, compact flash reader, or floppy disk - will include a light on the front panel. That light lets you know when data is being written to or read from the media inside.

While the light is on, never forcefully remove the media. If you do, it is likely that the data that was being written to or read from the media will not be usable. In a worst case scenario, the rest of the data that's on the media could become corrupt or the media could be unusable.

Many CD or DVD drives have a button that you press in order to eject the media. The button is in part a safety feature; if you press it while data is being written to a disk, the operation will finish before you get the disk. But other types of drives allow manual ejection. Be especially careful with these.

Never use force

Nothing that you insert into your PC - whether it's a disk or a cable - should require unusual force to get it in place. USB, FireWire, PS/2, and all other cables are designed to be inserted into their respective sockets in a particular orientation. Take the time to learn how cables, cards and disks are inserted properly, and what it feels like when they are.

If you attempt to insert a USB or other cable upside-down, you'll meet resistance. Don't ignore it. PS/2 cables - often used for keyboards and mice - are particularly tricky to insert properly. Look at the pins-in end of the PS/2 cord, and make sure that they are aligned properly with the PS/2 port.

Lose the food

Make a habit of eating and drinking around your computer, and sooner or later you will have a mishap. Keyboards do not like crumbs, and they absolutely hate liquid. In fact, any liquid spilled into a keyboard will usually result in the death of the board itself, as an electrical short will result.

No magnets

Never use any magnets around your computer. Most towers have metal sides on them that look like a great place to hang notes on with magnets. This is a terrible idea. Even though most new hard drives can be immune to the effects of the magnet, it is still a magnetic storage medium. One day I went to fetch a CPU of a friend from Gugulethu, put it in the back seat of my car, and took it to my place to fix it. Whilst driving I switched on my powerful sound system, with a very powerful amp and subwoofer. I got home, wanted to work on that PC, and surprise, surprise: the computer could not detect the hard drive. I was so frustrated: what did I do wrong? It was after I consulted my buddies that I realised that the magnet in my subwoofer and amp had destroyed the hard drive, so I ended up having to buy my friend another hard drive, so learn from me: be careful.

Delete old files and programs

Delete old files and programs that you no longer need. This will be more appreciated after you run a defragmentation of your hard drive. Most hard drives these days are large enough that they can hold many programs and files without putting a dent into the hard drive storage capacity of your computer. These files and programs are regularly fragmented through use and become spread out over any available space on your hard drive.

Antivirus scans

Scan CDs with an antivirus scan before installing anything from the CD. Viruses can piggyback on a program or file. Your friend may think he is sharing something cool with you but you may be sharing more than you want.

References

http://www.hawaiinewsnow.com/Global/story.asp?S=10557752
http://www.thegeekweekly.com/feature/company_computer_dos_donts/index.htm
http://www.essortment.com/hobbies/networksecurity_sdeg.htm
http://www.monstersandcritics.com/tech/features/article_1184397.php/Dos_and_donts_How_to_treat_your_PC_right
http://www.pcapprentice.com/dosanddonts.html