**Makerere University**

# GOOD ICT SECURITY HABITS

There are some simple habits you can adopt that, if performed consistently, may dramatically reduce the chances that the information on your computer will be lost or corrupted.

**How can you minimize the access other people have to your information?**

You may be able to easily identify people who could, legitimately or not, gain *physical* access to your computer—family members, roommates, co-workers and maybe others. Identifying the people who could gain *remote* access to your computer becomes much more difficult. As long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing or corrupting your information; however, you can develop habits that make it more difficult.

- **Lock your computer when you are away from it.** Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.

- **Disconnect your computer from the Internet when you aren't using it.** The internet has made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled and a genuine security solution/anti-virus installed.

- **Evaluate your security settings.** Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, re-evaluate your settings to make sure they are still appropriate.

### What other steps can you take?

Sometimes the threats to your information aren't from other people but from natural or technological causes. Although there is no way to control or prevent these problems, you can prepare for them and try to minimize the damage.

- **Protect your computer against power surges and brief outages.** Use an uninterruptible power supply (UPS) whenever possible to avoid computer damage and/or data loss due to power surges and/or abrupt outages. During a lightning storm or construction work that increases the odds of power surges, consider shutting your computer down and unplugging it from all power sources.
- **Back up all of your data.** Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. You have probably already experienced this at least once— losing one or more files due to an accident, a virus or worm, a natural event, or a problem with your equipment. Regularly backing up your data on a CD, external drive or the cloud reduces the stress and other negative consequences that result from losing important information. Determining how often to back up your data is a personal decision. If you are constantly adding or changing data, you may find weekly backups to be the best alternative; if your content rarely changes, you may decide that your backups do not need to be as frequent.