Families First Therapy
Electronic Security and Safety Tips

Because of increasing concerns with data security, Families First Therapy recommends the following to protect you and your family's information:

- Install antivirus software and keep it up to date regularly. Sophos is a free antivirus software that is highly recommended by security experts in the field.
- Set up your antivirus software to automatically scan for viruses and maleware.
- Set up your computer, cell phone, tablet, etc to automatically install patches to the operating system (typically Apple OS or Windows). An unpatched machine is more likely to have software vulnerabilities that can be exploited.
- Be careful who you loan your devices to, even for only a moment. A toddler playing games on a cell phone has led to data breaches in the past.
- Choose strong passwords with letters, numbers, special characters. Create a mental image or an acronym that is easy for you to remember. Create a different password for each important account, and change passwords regularly.
- Backing up your devices regularly can protect you from the unexpected. Keep a few months' worth of backups and make sure the files can be retrieved if needed. Many android, windows, apple, and other services have automatic options to make this easier.
- Don't leave your devices in an unsecured area, or unattended and logged on, especially in public places - including Athena clusters and Quickstations. The physical security of your machine is just as important as its technical security.
- Ignore unsolicited emails, and be wary of attachments, links and forms in emails that come from people you don't know, or which seem "phishy." Avoid untrustworthy (often free) downloads from freeware or shareware sites. Learn more about spam filtering.
- Never open an attachment from an email address you don't recognize.
- When connected to the Internet, your data can be vulnerable while in transit. Use remote connectivity and secure file transfer options when at remote sites. Accessing your bank account at unsecured internet sites can make your information vulnerable.
- Reduce the risk of identity theft. Securely remove sensitive data files from your hard drive, which is also recommended when recycling or repurposing your computer. Use the encryption tools built into your operating system to protect sensitive files you need to retain.
- Macintosh and Windows computers have basic desktop firewalls as part of their operating systems. When set up properly, these firewalls protect your computer files from being scanned.
- Stay current with the latest developments for Windows, Macintosh Linux, and Unix systems. IS&T provides a news page and we recommend that those interested subscribe to the IS&T Security-FYI electronic newsletter.

You can see from the list above that safe computing practices include a combination of how you physically or technically protect your computer by using software and security settings, and the actions you take. You need both to really make a difference. If you consistently use strong passwords, but then leave your computer unlocked and unattended in public places, you are still putting your data in jeopardy. If you use anti-virus software but aren't careful about replying to or forwarding suspicious looking emails, you still risk spreading a virus.

Source: https://ist.mit.edu/security/tips