RISD

it | services

Service Desk
servicedesk@risd.edu (401) 454-6106
Hours: 8:00AM - 5:00PM (Mon - Fri)

How to Proactively Safeguard Your Apple Mac Computer:

Password security

Create a secure password policy. Too many users insist on no password, easy passwords, or use hints that specify the password, or too many clues about the password.

Data security / encryption

If your computer contains highly sensitive data, such as -- but not limited to -- medical records, social security numbers, student grades, student applications, etc -- then enable Filevault.

> Please consult IT or your department's computer technician for assistance -- prior to enabling Filevault or any other hard drive encryption.

Mac OS X's Filevault is basic 128 bit encryption of the entire startup drive, which also enables password protected booting and prevents booting from external drives, and booting into single-user mode and target disk mode.
For even further protection for sensitive data, consider encrypted disk images with 256 bit AES encryption. Mounting of these disk images can be automated as a login item.

Backup

User data can be easily done via Time Machine to an inexpensive external USB drive. This drive should not be stored in the same location as the computer.
Use RISD's internal Shared (S Drive) and MyFiles (U Drive) to copy and safeguard all personally created docs.
Alternatively -- a cloud based or server based location can be used.
Third to a second USB drive is not a bad idea also.

Location

Find My Mac should be enabled by default. Use Lock and Wipe using iCloud on macs that have been stolen.

Malware / Viruses

Anti-virus software should be installed on all RISD owned computers. However the best malware detection is located between the ears. Antivirus can create a false sense of security for users. Users should always think twice before entering their username and password on any web page. They should ask themselves, is this a legitimate webpage? look at the URL, did I request or navigate to this page? Is this a malicious / phishing pop-up? etc.
Browsers and plugins should be kept up to date.

Configuration

Enable the firewall, automatic OS updates and require password when screen is locked, screensaver is active or computer is sleeping. Disable automatic login. Allow only installation of Apps from the App Store or identified developers.

Identification

Login window image should display a message stating the computer is property of RISD, and Public Safety should be contacted 24/7 if found. Re-introduce a hard to remove label identifying the computer and with the same message about ownership.

Physical security

Computers in locations with inadequate security (no card access, no CCTV, no alarm, too many entry points, etc.) or other high risk targets should be secured using security cables and other locking devices.