RISD

it | services

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

# How to Proactively Safeguard Your Windows Computer:

**Backup**

User data can be backed up to an external USB drive using Windows Backup (Windows 7 and above).
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.
A third USB drive is not a bad idea.

**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 -- do not store files on the local hard drive.
Use RISD's internal Shared (S Drive) and MyFiles (U Drive) to copy and safeguard sensitive data that is not part of a web based portal or other private system.
Please consult IT or your department's computer technician for assistance for best practices.

**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**

Always lock your computer when leaving your work area unattended (ctrl+alt+delete). Require a password to unlock your computer.

**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.