Research Data Management Top Tip: How to keep your data safe

Isaac Pratt, PhD
Research Data Management Specialist
pratti@mcmaster.ca
Research data management (RDM) services

We provide RDM services for all researchers on campus - including graduate students.

We can help you with any questions about:

- Data storage & backup
- Data security
- Data organization and documentation
- Data publishing, sharing, archival, and preservation

Check out our online resources: library.mcmaster.ca/services/rdm

Email us at rdm@mcmaster.ca or book an appointment with me.
Your data is vulnerable!

- There are 2 major risks that you need to mitigate to keep your data safe:
  1. Hardware failure or loss
     - Theft or loss of devices, accidental damage or destruction
  2. Malicious attacks
     - Computer viruses, malware, ransomware
How to meet the risks:

1. Hardware failure or loss

Make sure you have more than one copy of your data. Follow a data backup strategy like the 3-2-1 rule:

3

Copies of your data on **different platforms/devices**

2

Copies are on-hand

• a **production** copy (this is the data you are working on)
  • a **backup** copy

1

Copy is in another location (“off-site”), with a **trusted** service provider
How to meet the risks:
1. Hardware failure or loss

If you’re looking for a good place to store your research data, consider using our interactive Research Data Storage Finder webtool, where you can get recommendations customized to your situation.

u.mcmaster.ca/storagefinder

Or check out my recorded webinar on data storage:
https://scds.github.io/intro-rdm/storage.html
How to meet the risks:

2. Malicious attacks

• Enable **Multi-Factor Authentication (MFA)** wherever you can

  • MFA is when you need more than one code or ‘Factor’ to login - typically 2 factors: password and a security code sent to your phone number or generated by a linked authenticator app

  • MFA can be enabled for your McMaster Microsoft account here [https://office365.mcmaster.ca/mfa/](https://office365.mcmaster.ca/mfa/)
How to meet the risks:
2. Malicious attacks

• Follow good password practices everywhere:
  • Choose a new **unique** password for each important website/service
  • Make a **strong** password by combining a series of numbers, letters, and symbols
    • The longer the better
    • Try to combine them into something memorable – like L1br@ryt1pS
  • If you’re forgetful, consider using a password manager
  • **Never** share your password with anyone or send it in an email
  • Use a strong password on your computer **and** phone
Join us at our next webinar for more:
Set yourself up for research success:
Manage your data like a pro, and get your own ORCiD profile

September 23rd 11 am
October 7th 1 pm
October 21st 3 pm
Go to libcal.mcmaster.ca to register