Data Security Basics for Researchers

Identify Your Data

Determine appropriate level of Confidentiality, Integrity and/or Availability

Determine any threats to or vulnerabilities of your data

- For instance, is your data easy to re-create or difficult? Does it include infectious disease or human subjects' information? Does it use propriety software, difficult to access supplies or specialized equipment?

Be especially aware if someone you don't know asks detailed questions about your data, including by email or at a conference or convention. Collaboration may be legitimate, but it may also be nefarious – verify the identities of the people you collaborate with and be aware of how much data you share with whom.

Consider your data as you go through the best practices and decide which are important and relevant

Safeguarding Best Practices

Backup and Archive

Practice the 3-2-1 Rule

- 3 copies of any important files
- 2 different media types (laptop computer, CSU OneDrive, external hard drive, etc.)
- 1 copy offsite

Passwords and Multifactor Authentication

A strong password is:

- Long – 10 or more characters with mix of capital and lower-case letters and numbers
- Meaningful to you and a phrase, sentence or several unrelated words strung together

A strong password is NOT:

- Your birthday, wedding date, local sports team, or profession-specific term
- A single word found in the dictionary or a phrase or sentence from a book (especially one that can be found electronically)

Implement MFA wherever you can

- MFA can help prevent 99.9% of account compromises
- This can be an SMS (text) message, push notification, phone call or email with a one-time passcode used along with your username and password
- At CSU we use DUO

Physical Security

Lock devices in drawers, cabinets, and offices when not in use

Keep computer and device screens locked when not in use

Be aware of unfamiliar people in your workplace and talk to them if appropriate

Updates and Patches

Keep software and firmware up to date – set to automatically install if possible

This includes computer operating systems, smart phones, smart thermostats, home routers – ask if you do not know how, every device is a little different

CSU-issued devices are likely managed by your department IT, personal devices are up to YOU

If you have specialized equipment that cannot be updated, reach out to your IT department or the Division of IT, there are additional measures that can be put in place

Antivirus and Antimalware

One of your best defenses against malicious code

CSU-issued devices are likely managed by your IT department, personal devices are up to you!

Sanitize before Disposal

Electronics can often hold data in memory even if it appears "deleted"

Especially for regulated data it is vital to sanitize devices before disposal

Depending on the device, the process can vary – reach out for assistance if needed

CSU Surplus in the Department of Central Receiving can assist with this

Phishing

Phishing is when a scammer uses email to deceive you into disclosing personal information

Can be generic, with many spelling errors, or highly sophisticated and appear to come from a trusted source like an authority, a bank or prestigious journal or professional organization

Often include file attachments or website links – be aware of what kind of file (if it's a pdf and ends in .exe, it's probably not legitimate); hover over links in email to see the URL being linked to

Malicious Code

Can create a backdoor on your computer for someone to access, a keylogger which records every keystroke or mouse movement, and/or can corrupt files

Can result from a phishing attack, a malicious actor accessing your computer from an unlocked office or screen, or removable media

Removable Media

External hard drives, USB drives, CDs

Can be very useful! Or can result in lost data or malicious code

Make sure they are encrypted if needed and you are always in control of them

May be restrictions on their use especially if using regulated data

When in doubt, Ask! You don't need to be an IT security expert, but what you do MATTERS.

Reach out to your department IT, the Division of IT, or Kelly Poto (kelly.poto@colostate.edu) or Sarah Robinson with the Cybersecurity Services Team (sarah.robinson@colostate.edu) if you have any questions or concerns.

COLORADO STATE UNIVERSITY