UNIVERSITY OF CAMBRIDGE

MRC | Cognition and Brain Sciences Unit

Introduction to Computing at the CBU Overview

Jeff Berry

MRC Cognition and Brain Sciences Unit, Computing group

v. 2024

Computing Resources

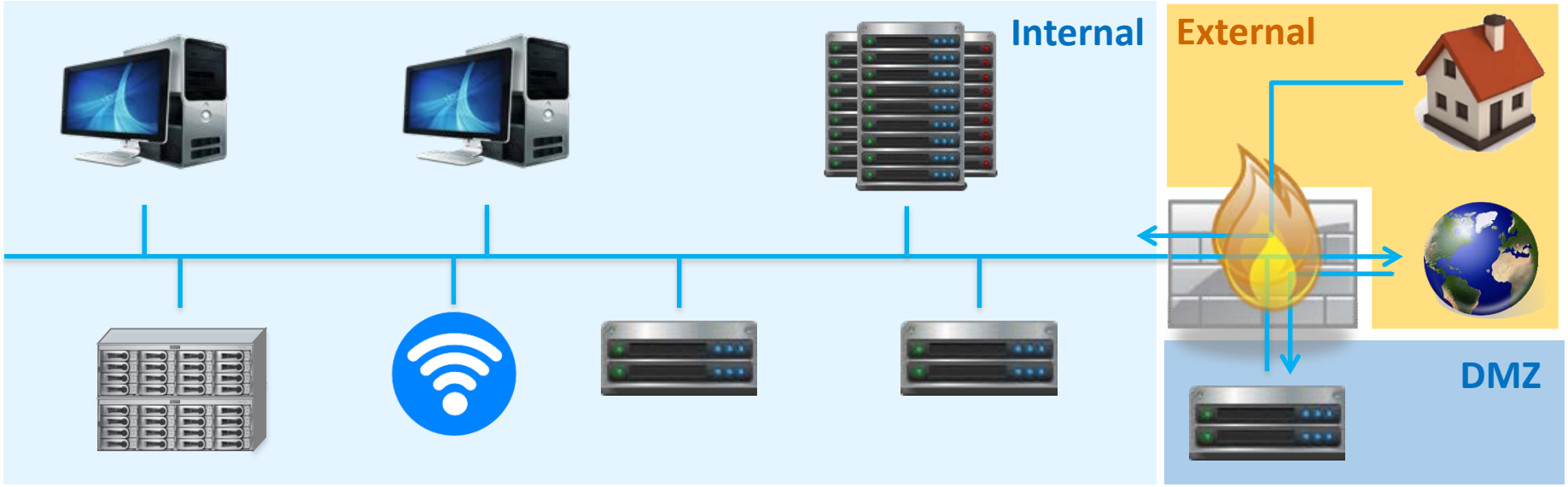
http://intranet.mrc-cbu.cam.ac.uk/home/introduction-to-computing-services/

Desktops, loan laptops

Testing and stimulus delivery machines

High Performance Compute Cluster

Remote access



Network data storage

- Home space
- shared group space
- imaging data storage

WiFi

Email

Microsoft Exchange

Internal services

- software portal
- online room and resource booking
- intranet
- secure data area
- remote desktop servers

Web services

- Unit and lab web sites
- FTP
- SSH
- online experiments
- cloud storage
- webmail
- containerized applications

Network Storage
Home Space

Home space:

- /home/<userid> on Linux (e.g. /home/xy01)
- U: on Windows (by default)
- Personal to you, by default not accessible to anybody else
- Snapshot backups – hourly / nightly / weekly
- Intended to store scripts, figures, documents etc – things that can't be recreated programmatically.
- Limited space – not intended for large amounts of data
- Used by Linux to store application settings, preferences, etc
- 50 GB quota

Network Storage
Shared Spaces

Shared research group areas:

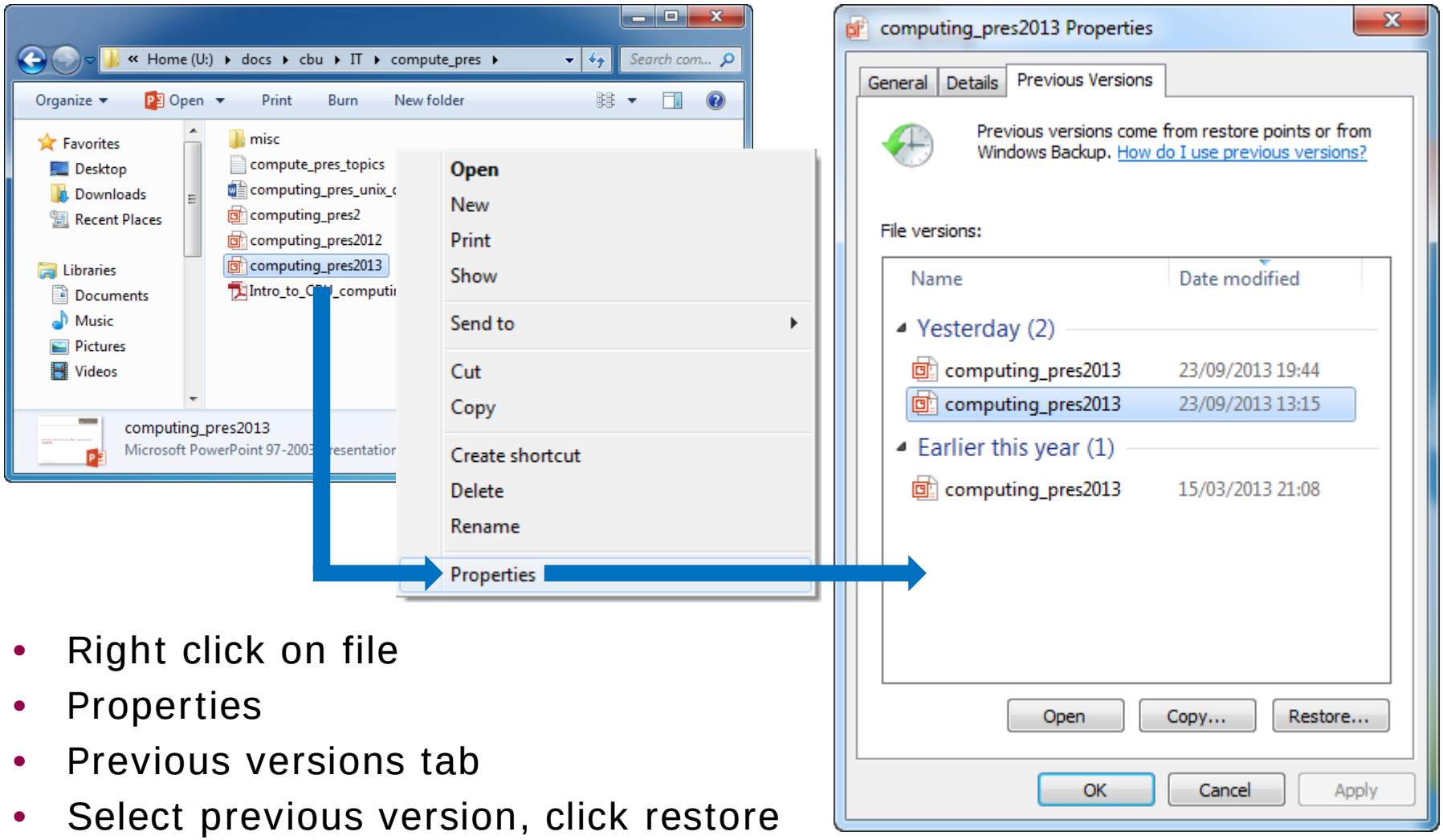
- Created to allow members of specific labs / research groups to share data
- Access limited to members of the relevant research group

Imaging spaces:

- Large storage spaces typically used for imaging data and processing
- Organized by group or project, with limited access
- Individuals can have directories/folders in the shared group area
- Usually accessible from Windows and Linux, but primarily Linux oriented

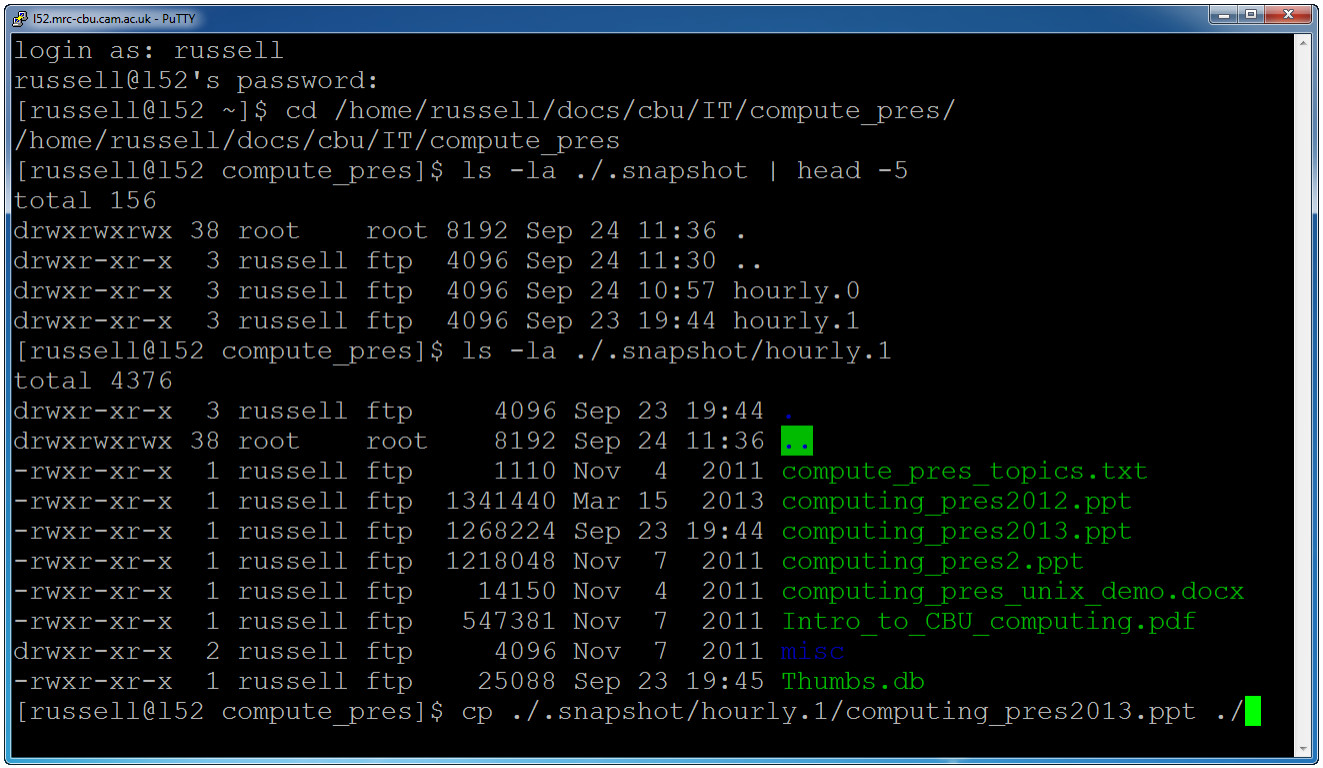
NB: On Linux, group areas/imaging spaces are ‘automounted’ – they must be explicitly referenced the first time they are accessed, simply ‘looking for them’ will not work

Restoring from a snapshot - Windows



- Right click on file
- Properties
- Previous versions tab
- Select previous version, click restore

Restoring from a snapshot - Linux

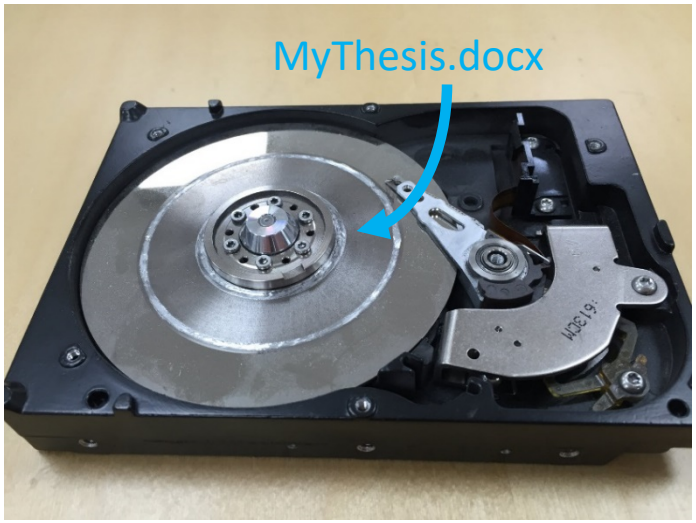


- Every home directory contains a (hidden) .snapshot sub-directory
- Cd into the directory containing the file you want to restore
- Choose which snapshot you want to restore
- Copy ./.snapshot/<*snapshot name*>/<*filename*> to current directory

Network storage - Best Practice

Home space:

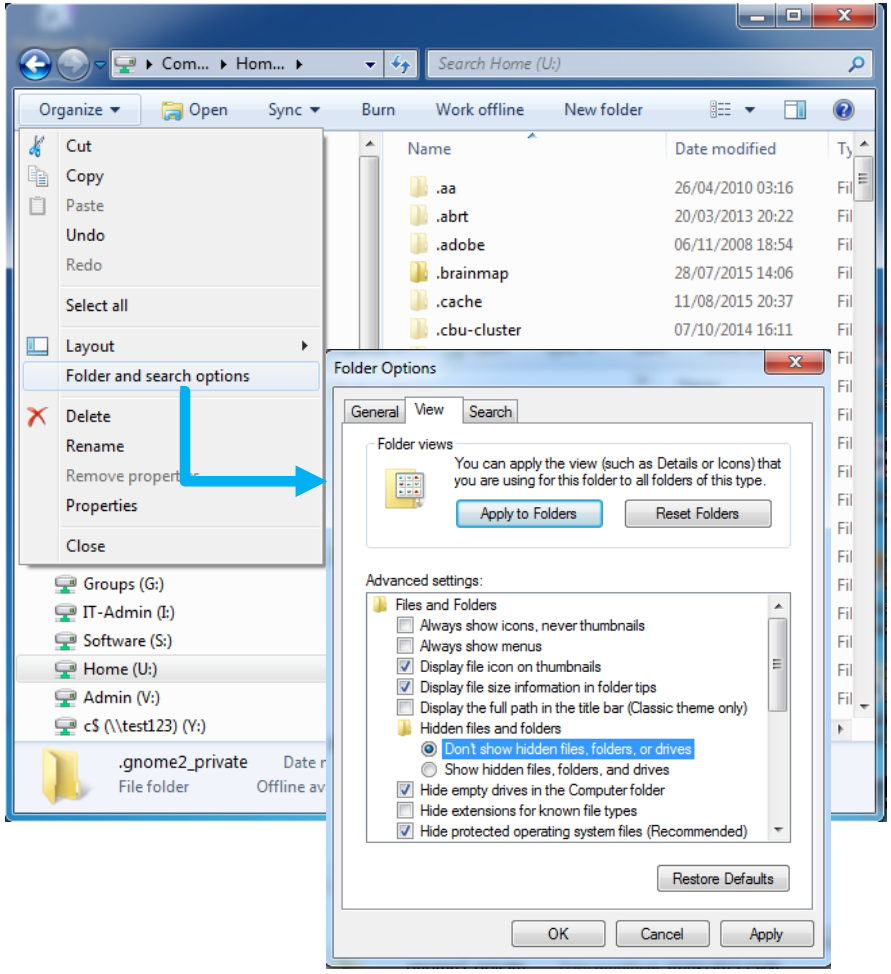
- Try to get into the habit of storing documents in your home space.
  - Home space is backed up – desktop hard drives aren't.
  - You can access your home space from almost every machine – you don't have to create multiple copies of data, or move data around on removable media



- Use your home space to store anything you can't easily recreate (documents, figures, scripts). Don't use it for imaging data – space is limited!

- Data is replicated off-site – in the worst case scenario, analyses could be re-created from raw data and code stored in your home space

Network Storage - Best Practice



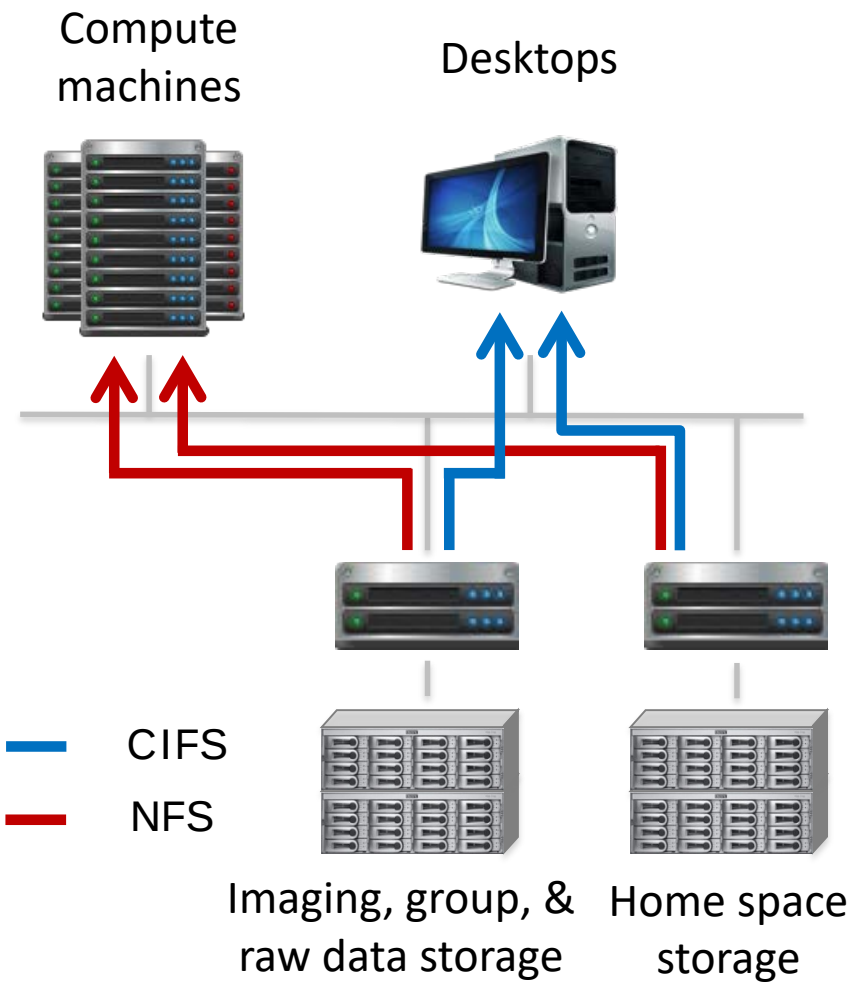
- When you browse your home space in Windows, you may see a lot of files whose names start with a “.”
- These are used by Linux for storing system settings, preferences, etc – don’t be tempted to “tidy” or move them!
- Instead, mark anything you don’t want to see as hidden
  - right click, properties, check “hidden”
- Configure windows explorer not to show hidden files
  - click the “Organise” menu in windows explorer, select “Folder and search options”, click the “View” tab, select “Don’t show hidden files, folders, or drives”)

Network Storage - Best Practice

Imaging / group storage:

- Unquota'd doesn't mean infinite…
- Clean up after your analyses – e.g. delete intermediate pre-processing images once you've finished with them
  - Let's repeat that – clean up intermediate data!
- If you are using AA version 4, make sure garbage collection is turned on
- Don't copy raw data from /mridata or /megata into your /imaging directory
- Don't create multiple copies of the same files
- You can read data from your group's or project's imaging space – you don't need to copy data from one directory/folder to another

Network storage - Accessing Resources

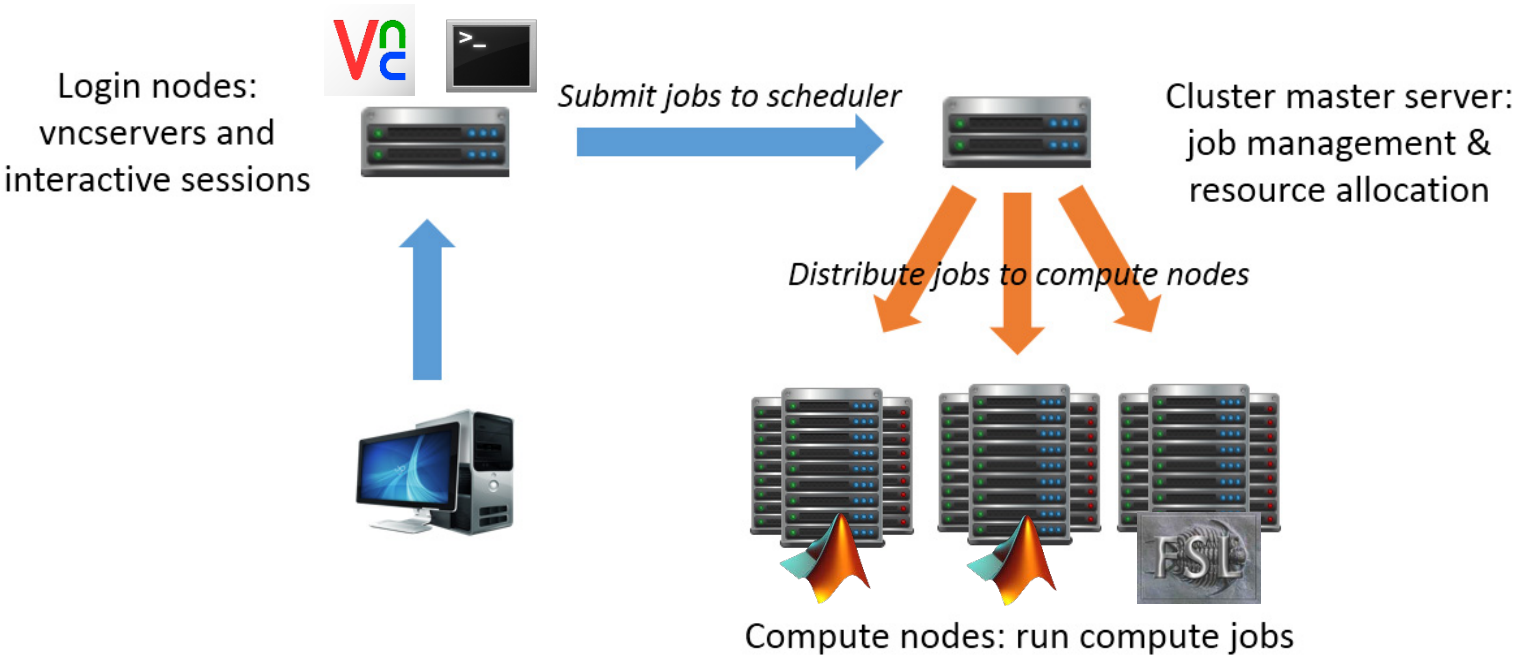


- Network storage is accessible from multiple locations (desktop PCs, compute machines, testing machines, etc)

To Access	From: Windows	From: Linux
Home Space	\\home*username* (usually U:\)	/home/*username*
Group share	\\cbsu\data\group*groupname*	/groups/*groupname*
Raw Data	\\cbsu\data\scandata\mri*project*	/mridata/*project*

High Performance Computing Cluster

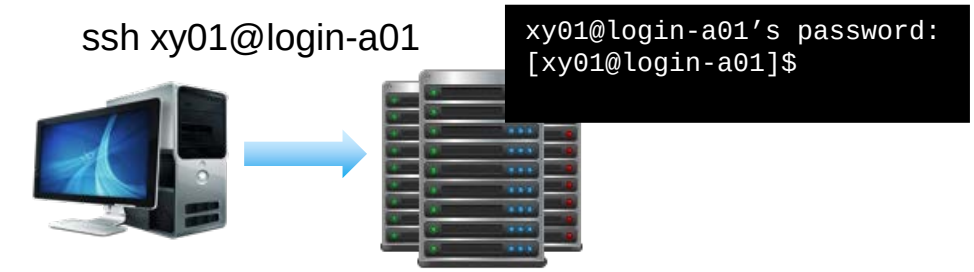
http://intranet.mrc-cbu.cam.ac.uk/intranet_category/compute-cluster-2019/

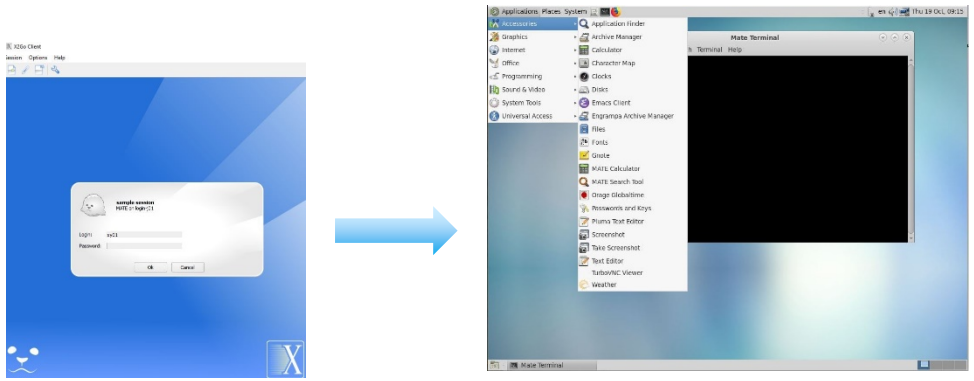


- Shared compute resource for intensive data analysis
- many powerful machines, with many cores, and a lot of RAM
- Login and run interactive sessions on a login node
- Run large compute jobs on compute nodes
- Submit compute jobs to a scheduling system (SLURM) that manages allocation of compute resources

Accessing compute machines

http://intranet.mrc-cbu.cam.ac.uk/intranet_category/compute-cluster-2019/





Pick a login node

A snapshot of machines is available at http://master02.mrc-cbu.cam.ac.uk/

Then

Log in using ssh (=Secure SHell)

- Windows
  - PuTTY
  - ssh from console in Win11
- Linux – terminal ssh command
- Mac – terminal ssh command

This provides a text only terminal

(Compute nodes are only accessible via ssh when you have a job running on them)

OR

Log in using x2go for a graphical session

- x2go is available on the software portal for unit machines.

Software

- Desktop machines come with Office, Endnote, SPSS, Matlab, Adobe Photoshop/Illustrator/Acrobat

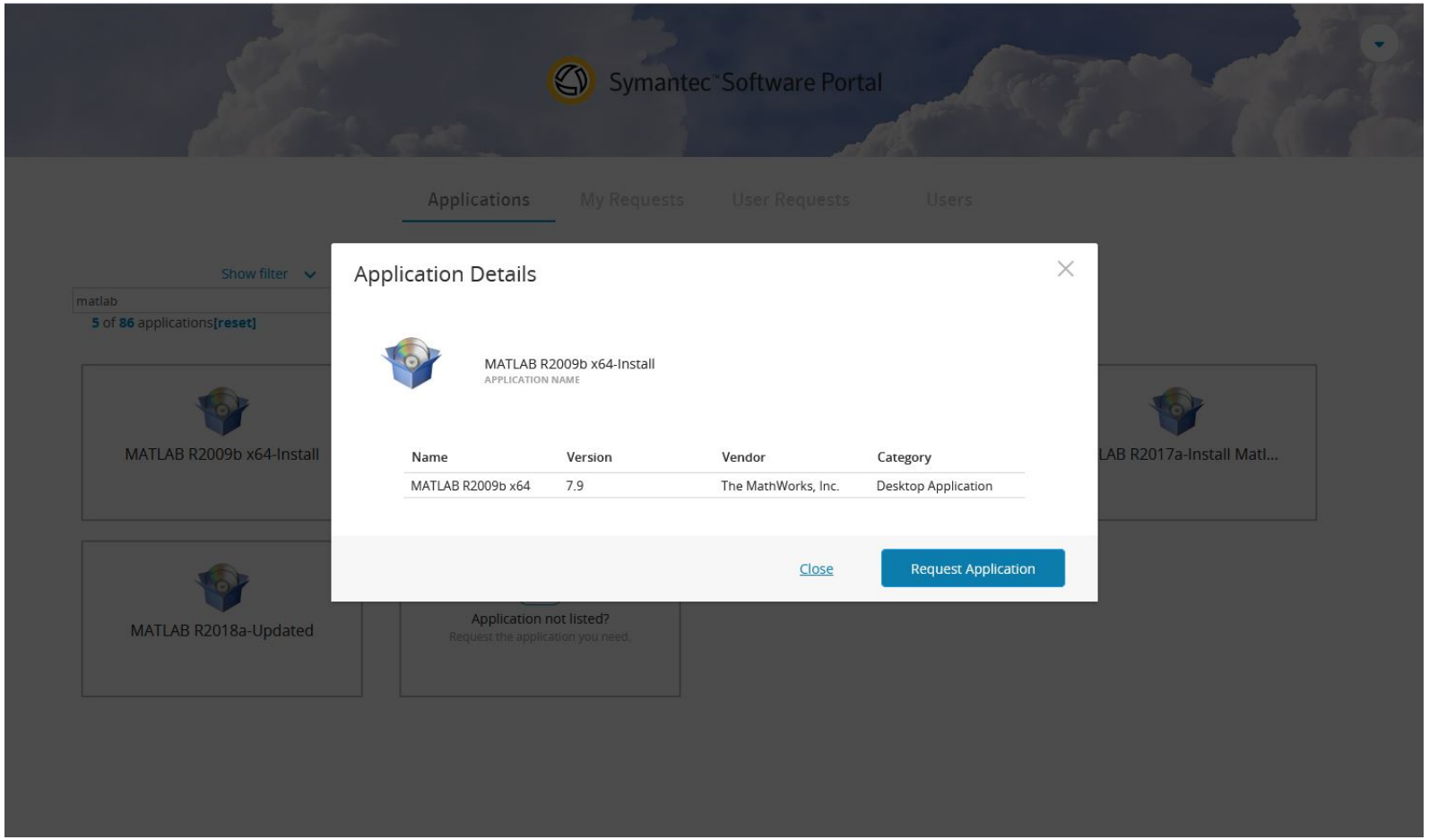
- Stimulus delivery software:
  - Eprime, Presentation, Matlab (Psychtoolbox, Cogent)
  - Write your own

- Other software available on request – email it-help@mrc-cbu.cam.ac.uk, or visit the software portal

- Compute cluster:
  - Matlab, SPM, FSL, Freesurfer, Python (Anaconda, inc Spyder), R/Rstudio
  - /imaging/local/software, or /hpc-software
  - http://imaging.mrc-cbu.cam.ac.uk/imaging/AvailableSoftware

Software Portal

http://wsr-smp-01.mrc-cbsu.local/Altiris/SoftwarePortal/UserPortal/Home.aspx



Wifi networks

intranet.mrc-cbu.cam.ac.uk/computing/wireless/
www.mrc-cbu.cam.ac.uk/wireless-access/eduroam/

cbsuwlan

- Internal CBU wireless network.
- Full access to internal resources
- CBU equipment only

- **Edu**cation **Roam**ing
- Access service developed by an international consortium of research and educational institutions.
- Federated authentication – users of participating institutions can use their credentials to connect to other institutions' wifi networks.
- Accessible by personal / non-CBU equipment
- No access to internal resources

guest

- Guest wireless access for non Unit visitors
- Anyone can join
- No access to internal resources
- Username / password available from reception

University user account

- Also referred to as a Raven account
- 5 or 6 character user name, also referred to as CRSID
- https://help.uis.cam.ac.uk/new-starters/it-for-students/student-it-services/your-crsid

- Used to access resources provided by the University
  - Employee self service portal / CHRIS HR system.
  - Microsoft Teams
  - University HPC services
  - University IT help

Other resources provided by the University

- Log in using University Raven account rather than CBU account
- University Information Services (UIS) overview:
  https://help.uis.cam.ac.uk/service
- UIS helpdesk:
  https://help.uis.cam.ac.uk/
- Microsoft Teams:
  https://universityofcambridgecloud.sharepoint.com/sites/MicrosoftTeamsHub/SitePages/Home.aspx
- UIS software distribution:
  https://software.uis.cam.ac.uk/
- University High Performance Computing service
  https://www.hpc.cam.ac.uk/
- Employee Self Service / CHRIS HR system
  https://chris.cam.ac.uk/hrlive_ess/ess/index.html#/login

Remote working

http://intranet.mrc-cbu.cam.ac.uk/intranet_category/working-from-home-off-site/

- Connect to our network using a VPN (Virtual Private Networking) client:

- Traffic for bound for destinations on the CBU network is encrypted, re-encapsulated and sent over the internet

VPN
(Virtual Private Network)

A VPN is an encrypted channel which allows a remote machine to be placed ‘virtually’ on a different network. The unit VPN allows remote machines to function as if they were behind the firewall and access unit resources.

- unit machines have a built-in VPN client
- Windows 10/11 machines can use Capsule VPN
- other machines can use the vpn portal site
- connections to the VPN use the usual unit credentials

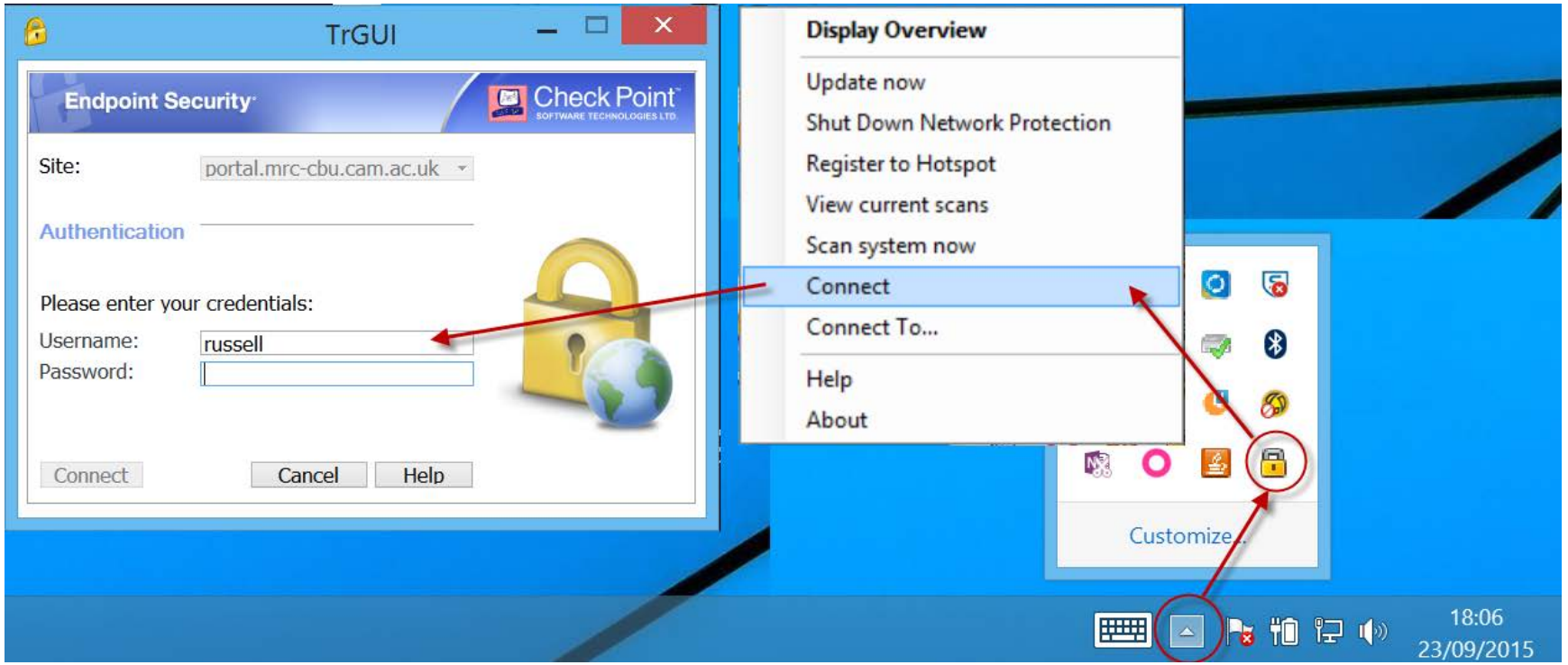
More information at:

http://intranet.mrc-cbu.cam.ac.uk/home/01-working-from-home-off-site/

Remote access

http://intranet.mrc-cbu.cam.ac.uk/intranet_category/working-from-home-off-site/

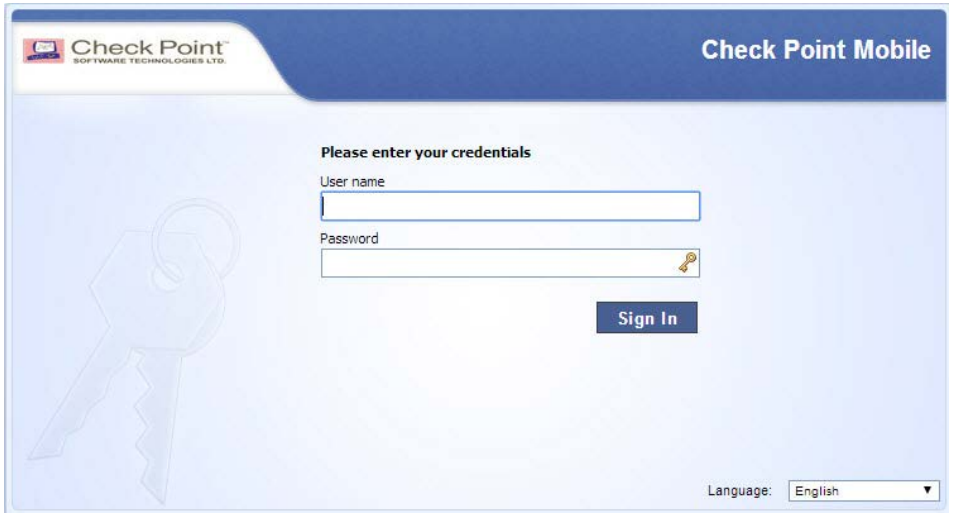
- From a CBU owned machine:

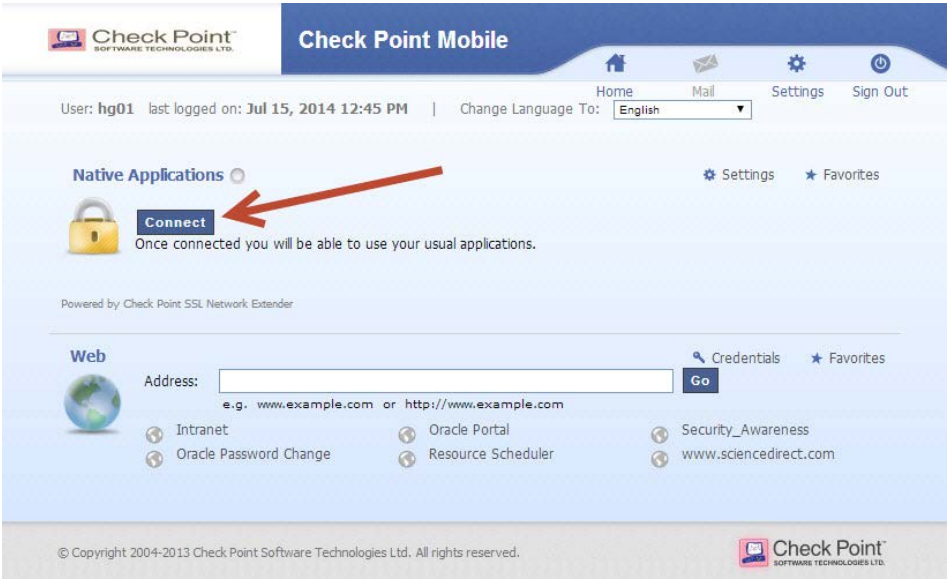


Remote access

http://intranet.mrc-cbu.cam.ac.uk/intranet_category/working-from-home-off-site/

- From a non-CBU machine:
  - browse to portal.mrc-cbu.cam.ac.uk
  - Sign in using your CBU credentials
  - Click “Connect”





Remote access

http://intranet.mrc-cbu.cam.ac.uk/intranet_category/working-from-home-off-site/

- Once you are connected and have an IP address on our network, you can access internal resources as if you were at the unit, including:
  - Compute cluster (ssh, x2go,vnc)
    - *http://intranet.mrc-cbu.cam.ac.uk/home/accessing-the-cbu-cluster-2019/*
  - Windows desktops
    - including your own PC, or the remote desktop servers
    - *http://intranet.mrc-cbu.cam.ac.uk/home/remote-desktop-services/*
  - Network storage
  - Resource scheduler and intranet
  - Journal articles
- No need to transfer data on removable media / cloud storage – just connect remotely to your CBU PC or the remote desktop servers

Your responsibilities

- Data Protection
- Security and usage policy

- Full policies are included in the induction pack.
- By signing the user form, you are agreeing to abide by those policies
- Mandatory induction and security awareness training:
  - https://learning.mrc-cbu.cam.ac.uk/login

Your responsibilities

- **General principles:**
  - Protect other peoples' personal data
  - Protect our machines, data and users
  - Protect the integrity and reputation of the MRC and UoC
  - Preventing illegal or inappropriate activities

Data Protection - Protecting other peoples' data

- We have a **legal** obligation to protect the rights and privacy of staff, participants and members of the public
- There are serious consequences for non-compliance

- Data Protection Act (DPA; 2018) based on the EU General Data Protection Regulations (GDPR)
- Defines how this personal data can be used
- Attempts to balance legitimate needs to use personal data with the rights of individuals to privacy.

- Participant data, but also data from other members of the public – e.g. workshop attendees

Data protection

Personal data shall be:

1. Processed fairly, lawfully, and in a transparent manner
2. Processed only for specified, legitimate purposes and not processed further
3. Adequate, relevant and limited to what is necessary
4. Kept in a form that permits identification for no longer than necessary
5. Processed in a manner that ensures appropriate security of the personal data.

Data protection

Some guidelines:

- Get explicit consent to store and process participants' data.
- Explain what information you'll collect, what you'll use it for, and who will be able to access it
- Only use data for purposes to which participants have consented.
- Never share participants' personal information with anyone unless you have explicit authorisation to do so.

Data protection

At the core of the Data Protection Act are 6 data protection principles.

Personal data shall be:

1. Processed fairly, lawfully, and in a transparent manner
2. Processed only for specified, legitimate purposes and not processed further
3. Adequate, relevant and limited to what is necessary
4. Accurate and up to date
5. Kept in a form that permits identification for no longer than necessary
6. Processed in a manner that ensures appropriate security of the personal data

- GDPR prohibits transfer of personal data outside the EU unless the destination country has implemented comparable levels of data protection, or unless data subjects have had the risks explained and then given explicit consent
- Organisations that process personal data are obliged to demonstrate compliance with the data protection principles

Data Protection – What is personal data?

- What counts as personal data?
  - "**Any** information relating to an individual person who can be identified directly or indirectly by reference to an identifier"
  - Data that is about or clearly relates to an **identifiable**, **living individual**
  - Data that could be used to learn something about an individual or compromise their privacy
  - Context is important – can an individual be identified by taking into account other data held by the same data controller, or other publically available information? A list of names might not on their own constitute PID, but a list of names titled "Depression Patients" would.
  - Anonymised or aggregated data is not covered by the Data Protection Act
- Special category personal data – may cause distress or discrimination if released:
  - Medical information, information about political views, ethnicity, sexual orientation.

Data Protection – What is personal data?

Types of identifier (not exhaustive):

- Name
- Address
- Email address
- Telephone number
- Official ID numbers (e.g. national insurance number, NHS number, passport number, driving license number, etc)
- Date of birth
- Birthplace
- Genomic information
- Face, fingerprints, or handwriting
- Credit card numbers
- IP address
- Digital identity
- Login name, screen name, nickname, or handle

Data Protection – What is personal data?

- Context is important – how could the privacy of a living individual be compromised?

Filename = /home/Depression_study/IQ_and_depression_scores.xls

ID	DoB	IQ	Depression
001	19/04/1982	93	28

Yes

Filename = /home/Study1/scores.xls

ID	DoB	Score1	Score2
001	19/04/1982	93	28

Possibly

Filename = /home/Depression_study/IQ_and_depression_scores.xls

ID	Age (months)	IQ	Depression
001	419	93	28

No

Data Protection - Protect yourself

- You must have a lawful basis for processing personal data
  - Research in the public interest, consent

- You must abide by the data protection principles
  - Processed lawfully and fairly, collected for specific purpose and not processed further, processed in a manner that ensures security

- You must respect data subject rights
  - Right to be informed, right of access, right to erasure, right to rectification

Data Protection - Protect yourself

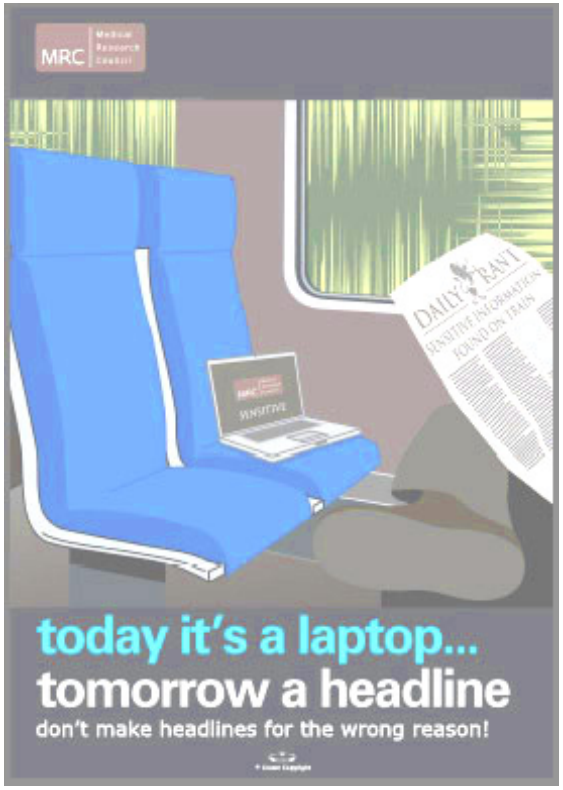
- In practice:
  - Explain what information you'll collect, what you'll use it for, and who will be able to access it (information sheet, privacy statement)
  - Only use data for purposes to which participants have consented.
  - Never share participants' personal information with anyone unless you have explicit authorisation to do so.
  - Separate research and personal data.
  - Where possible, **anonymise your research data**
  - Alternatively pseudonymise data by replacing personal identifiers with id numbers
  - **Store electronic personal data** (and keys linking ID numbers to personal data) **in our secure data area**
  - Store paper data in a locked drawer or filing cabinet

Data Protection - Protect yourself

- Don’t transfer personal data using laptops, removable media, email or cloud storage.
- If you must transfer data this way, the data **must** be encrypted.
- Don’t upload PID to cloud storage – this risks breaking the law.
- Don’t transfer PID to third party data processors without checking first.

- More information:
  - CBU Data Protection Policy (CBU_IT_002, in your induction pack)
  - http://intranet.mrc-cbu.cam.ac.uk/home/data-protection/

- If in doubt, ask!



Data Protection - Protect yourself

- Additional practical steps:
  - Think carefully about whether your data could identify an individual person – e.g. rare medical conditions, facial information in structural MRI.
  - Minimise data (e.g. replace DoB with age in months, recode descriptive data, obscure variable names)
  - Protect personal data with appropriate file system permissions,
  - Destroy participant contact details when you have finished with them
  - Don’t share participant contact details with anyone, even other members of the unit
  - Be careful of dicom data – dicom headers can contain personally identifiable data such as name or date of birth
  - CBU dicom data does not contain name, and date of birth is obscured

Data Protection – Secure Data Area

http://intranet.mrc-cbu.cam.ac.uk/home/secure-data-area/

- The Secure Data Area (SDA) is designed for secure storage of personally identifiable and sensitive data.
- Provides an enhanced level of protection by controlling access to this data, and controlling what can be done with the data (e.g. printing, emailing, copying data out)
- It consists of a number of Windows servers running Microsoft Remote Desktop Services (the “session hosts”) and a set of network file shares where sensitive data can be stored (the “secure shares”).
- You can access the SDA either by launching a remote desktop session on one of the session hosts, or by launching a remote application.
- Remote desktop sessions on the SDA hosts work in exactly the same way as a remote desktop session on any other PC (e.g. your CBU desktop PC, which you may be used to accessing remotely).
- Once you have logged in, you will have access to a full Windows desktop on one of the session hosts and be able to interact with it as you would a local PC.

Data protection

Other issues relating to data management:

- Intellectual property
  - Any data you collect, as well as any IP you develop (software, tests, imaging sequences, etc) belongs to the MRC and shouldn't be shared without explicit permission.
  - Collaboration and data sharing agreements.
  - Be careful of cloud storage / social media T&C's – you could be giving away (y)our IP!

- Sensitivity
  - Internal policy documents
  - Politically sensitive or emotive data – e.g. data from animal studies

Security – Protect our machines, data and users

- Common security threats:
  - Phishing
    - Attempts to obtain sensitive information or gain access to your computer by deception
    - Commonly via email, but also by phone, face to face, or via accidentally mistyped URLS (www.microsfot.com)
    - Can be quite subtle and highly targeted (“Spear Phishing”)
  - Malware
    - Malicious software that may try to encrypt or delete data, harvest sensitive data (passwords), use a compromised machine as part of a “botnet”, allow unauthorised access to a machine or network.
  - Password attacks and compromised accounts

Security - Phishing

- Attempts to obtain sensitive information by deception – passwords, usernames, financial details, sensitive institutional information
- Email is the most common route, but not the only one. Phishing can also occur via the phone or face to face.
- Generic attempts may be relatively easy to spot – play on common hopes and fears (you've won a prize, your machine is infected, your account has expired, etc)
- "Spear phishing" can be highly targeted and very subtle. Can use information about you from other sources to give the impression of credibility.
    - Admin staff targeted with fake invoices at the end of the financial year
- Attacks can involve multiple stages – gathering seemingly innocuous information from some people, then using that to make a more credible sounding approach to others.
- Phishing attempts may spoof the email "From" field making it appear to come from a trusted source

Security – Phishing and malicious email

- Phishing attempts may be combined with attempts to install malicious software (malware)
- Common tactics include:
  - Asking you to open an email attachment
  - Asking you to click on a link in an email
  - Asking you to input details on website
  - Asking you to download and install software
    - Phone calls from “Microsoft technical support” asking people to visit a web site and install “support software”

Security – Malware

- Email a very common route for dissemination of malicious code, but it is by no means the only one:
  - Infected files (transferred by removable media, downloaded from the internet, etc)
  - Code embedded in documents (e.g. macros in MS Office applications)
  - Self propagating (worms)
  - Software downloaded from the internet (including from apparently legitimate sites)
  - Software with a dual or hidden purpose (trojans)
  - Bundled with legitimate software (“drive by install”)
  - Sharing pirated software or media
  - Code run by malicious web sites

Security – Malware

- Common aims of malware include:
  - Steal information or track behaviour (passwords, sensitive data, financial information; spyware)
  - Record keystrokes (key logger)
  - Allow unauthorised access to a computer or network
  - Encrypt data and demand money for decryption (ransomware)
  - Bombard you with adverts (adware)
  - Use a compromised machine in a “botnet”
    - For co-ordinated attacks on other machines or web sites (DDOS attack)
    - To process data (e.g as part of a brute force attack, bitcoin mining)

Security – Password attacks

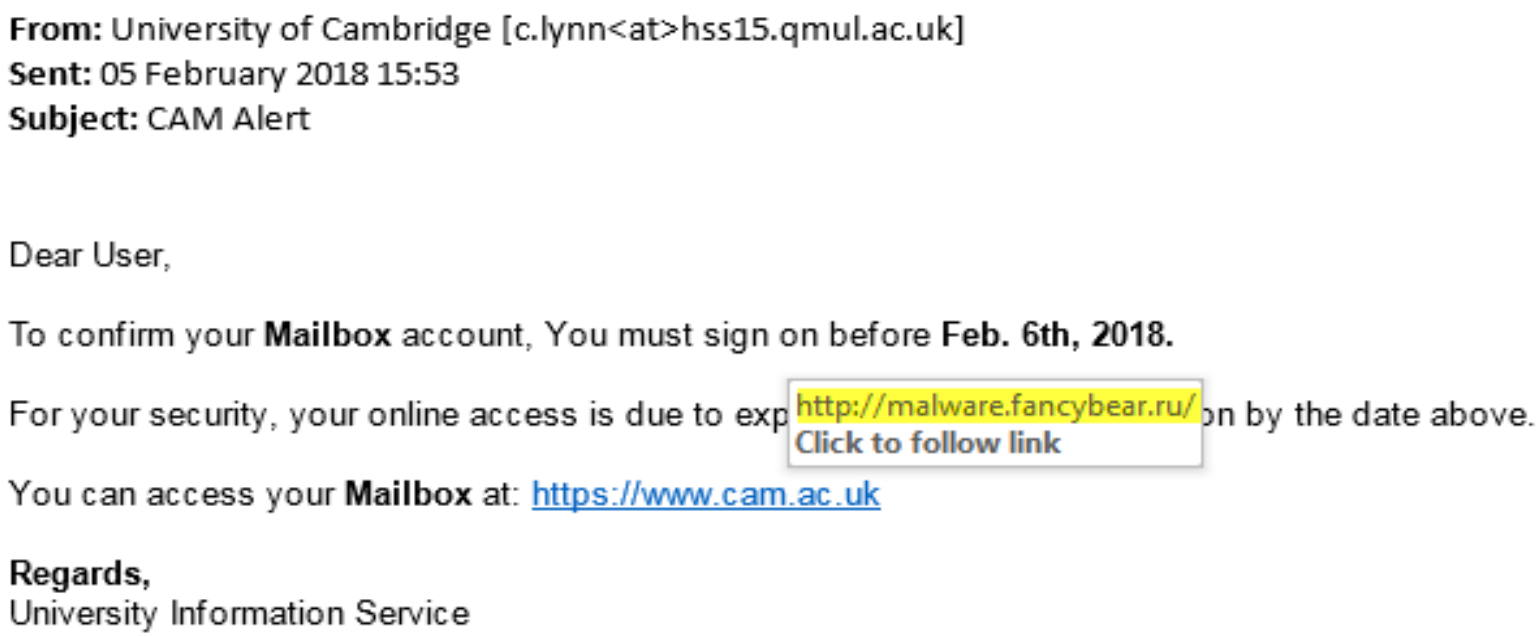
- Attempts to gain unauthorised access to a system and data by compromising user accounts
  - Social engineering or phishing attacks designed to trick you into revealing username, password or other information
  - Social engineering or phishing attacks designed to trick you into entering your credentials in a malicious website
  - Attempts to guess passwords
    - Brute force attack
    - Brute force guided by personal knowledge (family members names, interests, favourites)
    - Dictionary attack
    - Rainbow tables
- Once an attacker has access to a system via a compromised account, they will try to escalate their privilege (e.g. gaining access to root or administrator accounts) until the system is under their control.

Security – Avoiding common threats

- It is surprisingly easy to spoof email to make it look like it came from someone else.
- Treat any unexpected emails with extreme caution, **even if they seem to come from an address you recognise**, particularly if they ask you to
  - Download files
  - Follow a link
  - Open an attachment
  - Enter your details on a web site
  - Provide personal details
- Please be extremely cautious about opening email attachments, particularly attachments that can contain executable code (e.g. MS Office documents).
- Do not allow any embedded code or macros to run, or enable editing mode, unless you are absolutely certain of the document's origins.
- If you are in any doubt at all, don't download any files or open any attachments, and contact it-help for advice

Security – Avoiding common threats

- Hover your mouse over any hyperlinks to see the true target, even if you think the message may be legitimate. If the target is completely unrelated to the text, treat the email with extreme suspicion.
- If you are in any doubt, don't click on the link and contact it-help for advice



Security – Avoiding common threats

- Avoid installing software or running code / containers unless you are **absolutely** sure both the software and the source you are obtaining it from are reputable.
- Be very careful of “drive by installs” – unwanted software bundled with legitimate packages.
- If you are in any doubt, please do not download or install the software - even some supposedly reputable sites will bundle unwanted applications along with the software you have requested
- Be very careful of software that allows remote access to CBU computing systems, e.g. remote support packages like Team Viewer. Only use this software with people you know, and make sure the software is not still running after you have finished.

Security – avoiding malware attacks

- Don’t attempt to disable or circumvent security measures or security software installed on CBU machines or on the CBU network:
  - McAfee Anti-Virus
  - Checkpoint Endpoint protection (full disk encryption, media encryption, local firewall)
  - Perimeter Firewall
  - Spam filtering
- Updates are downloaded automatically, but may require your machine to be rebooted before they are applied.
- Please apply any updates and reboot your machine if you are prompted to do so.
- Security is a collaborative effort requires everyone to be alert to possible threats and act accordingly

Security – Protect (y)our data

- Use network storage rather than local hard drives
- Network storage is protected by snapshots and replication offsite – we can recover it if you are the victim of ransomware.
- Do not transfer MRC data out of our system without the director's explicit permission.
- Avoid transferring data on removable media.
- If using removable media is unavoidable, make sure the media is encrypted.
- Scan removable media for viruses when you plug it into any CBU equipment. We do not enforce virus scanning of removable media, but it is still good practice.
- Don't use any unblocked cloud storage

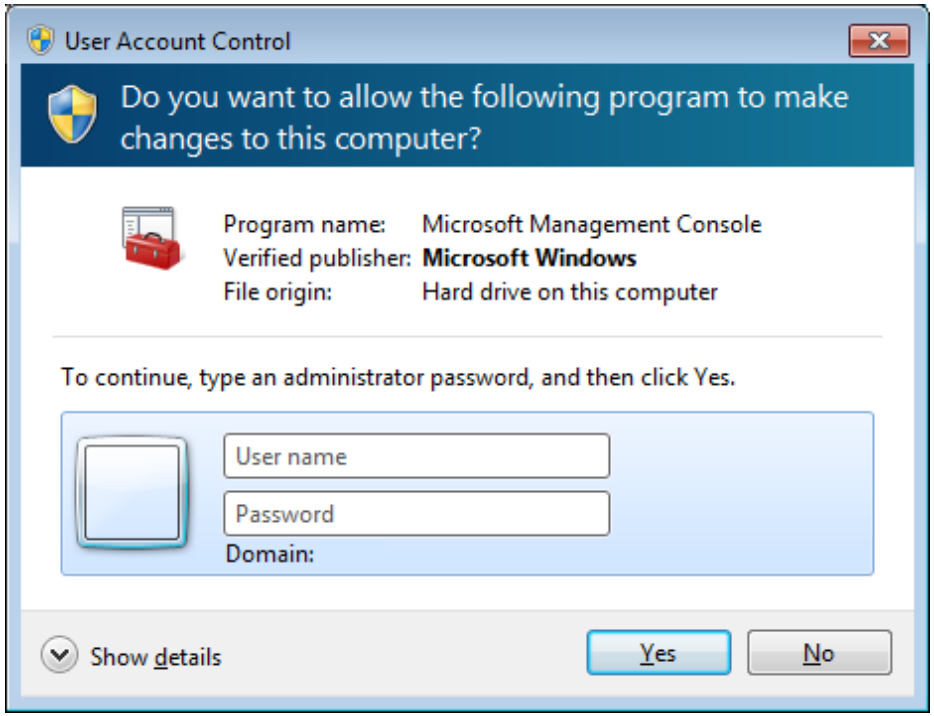
Security – Avoiding common threats

- Lock your screen whenever you leave your desktop PC (windows + L)
- Be careful of people asking for details over the phone, asking you to visit technical support websites.
- Do not allow web sites to run active content (e.g. java, JavaScript) unless you are absolutely certain the site is reputable.
- In all cases, if you are at all in doubt, please send an email to it-help@mrc-cbu.cam.ac.uk and we will try to help.

Protect our machines, data and users

- Contact it-help@mrc-cbu.cam.ac.uk immediately if Sophos Anti-Virus warns you that it has blocked a potentially unwanted application. Please do not allow the application to run.

- If you are prompted to enter your credentials by Windows User Account Control, check which program is asking for permission to run, particularly if the dialog box appears unexpectedly.

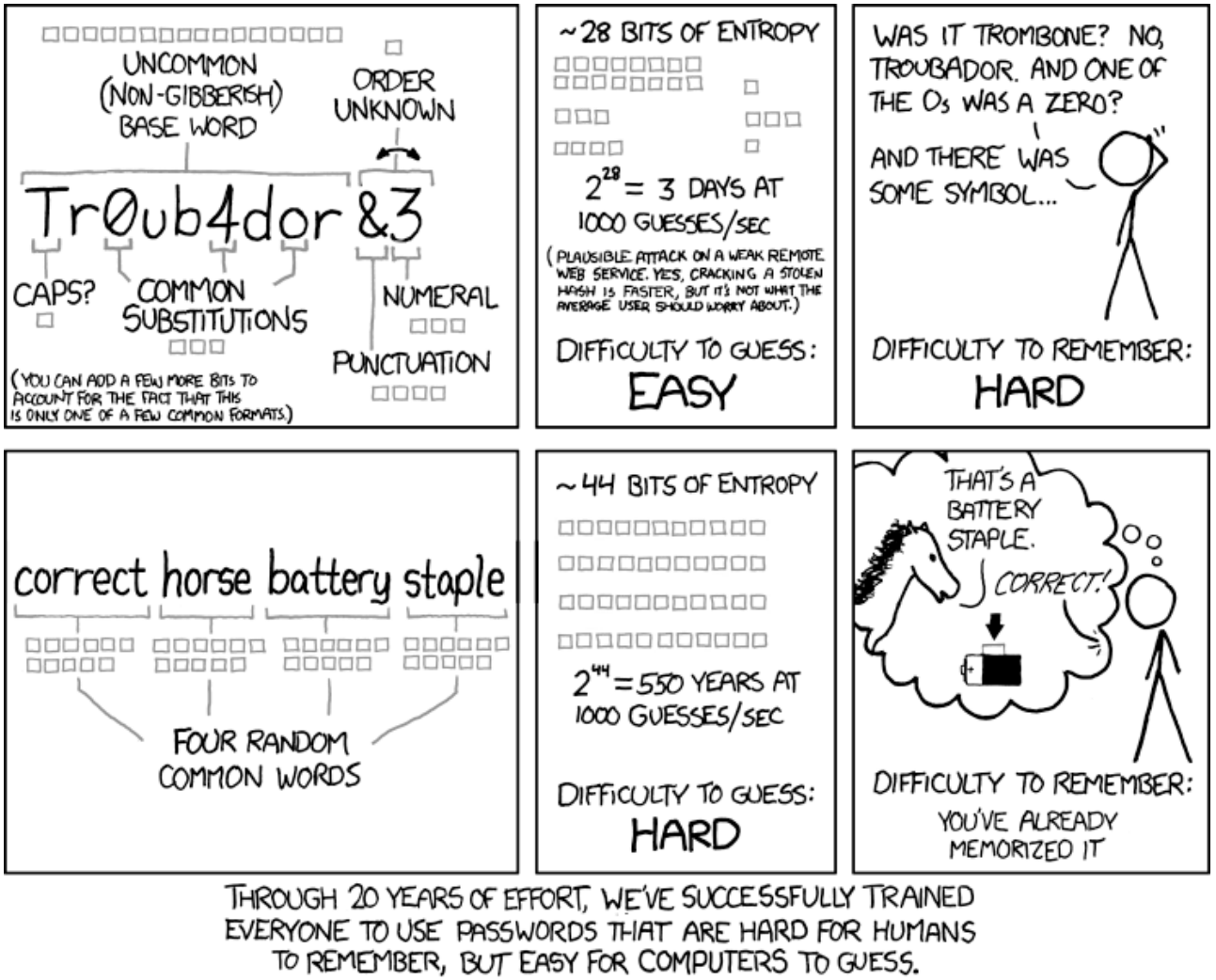


Security – Passwords

- Use a strong password
  - CBU minimum requirements:
    - 10 characters
    - Characters from 3 of the 4 following groups: Numbers, uppercase letters, lowercase letters, non-alphanumeric characters
    - Not based on name or username
- Use a password that is unique to your CBU account
- **Don’t share your password with anyone else**, even other members of the unit
- Don’t use anyone else’s account or allow anyone else to use your account

Security - Passwords

- The xkcd strategy…



https://xkcd.com/936/

Security - Protect the reputation of the CBU

- Use your CBU email account for CBU business, and personal email accounts for personal business.
- Don’t share sensitive information outside the organisation (personal data, institutional policies or procedures, financial information, etc)
- Avoid misrepresenting the CBU through unauthorised or inappropriate publishing / posting, or by presenting personal views as institutional positions.
- Avoid participating in, facilitating or encouraging illegal or inappropriate activities.

Security and Usage Policies

- Examples of forbidden activities (automatic disciplinary action or dismissal):
  - Attempting to gain unauthorised access to computer systems or information
  - Theft of electronic data, including software piracy
  - Identity theft or impersonating someone else
  - Destroying, corrupting or denying access to systems or data
  - Deliberately accessing, storing, or making available inappropriate material, e.g.
    - Pornography
    - Hatred / discrimination
    - Criminal or terrorist
    - Defamatory / libellous
    - Bring the MRC into disrepute
    - Known to be infected with malicious software
    - Infringes privacy or data protection rights
  - Bullying, threatening or harassing other people

Security and Usage Policies

- Specific examples of unacceptable activities:
  - Using MRC resources for personal gain / profit, or allowing others to do so
  - Accessing, storing, or making available material that infringes copyright
  - Creating, storing, or transmitting information that breaches data protection regulations
  - Using unauthorised electronic communication services or cloud services
  - Using unauthorised email accounts for MRC business
  - Sharing username / password
  - Sending sensitive information outside the organisation
  - Disabling or circumventing security measures, or failing to comply with security policy.
  - Misrepresenting the MRC through unauthorised or inappropriate publishing / posting.

Computing Support

MRC | Cognition and Brain Sciences Unit

- Computing group intranet pages:
  http://intranet.mrc-cbu.cam.ac.uk/intranet_category/computing/
  http://intranet.mrc-cbu.cam.ac.uk/home/introduction-to-computing-services/
- IT helpdesk: it-help@mrc-cbu.cam.ac.uk

- Methods group and software gurus:
  http://imaging.mrc-cbu.cam.ac.uk/imaging/AvailableSoftware

Jeff

Howard

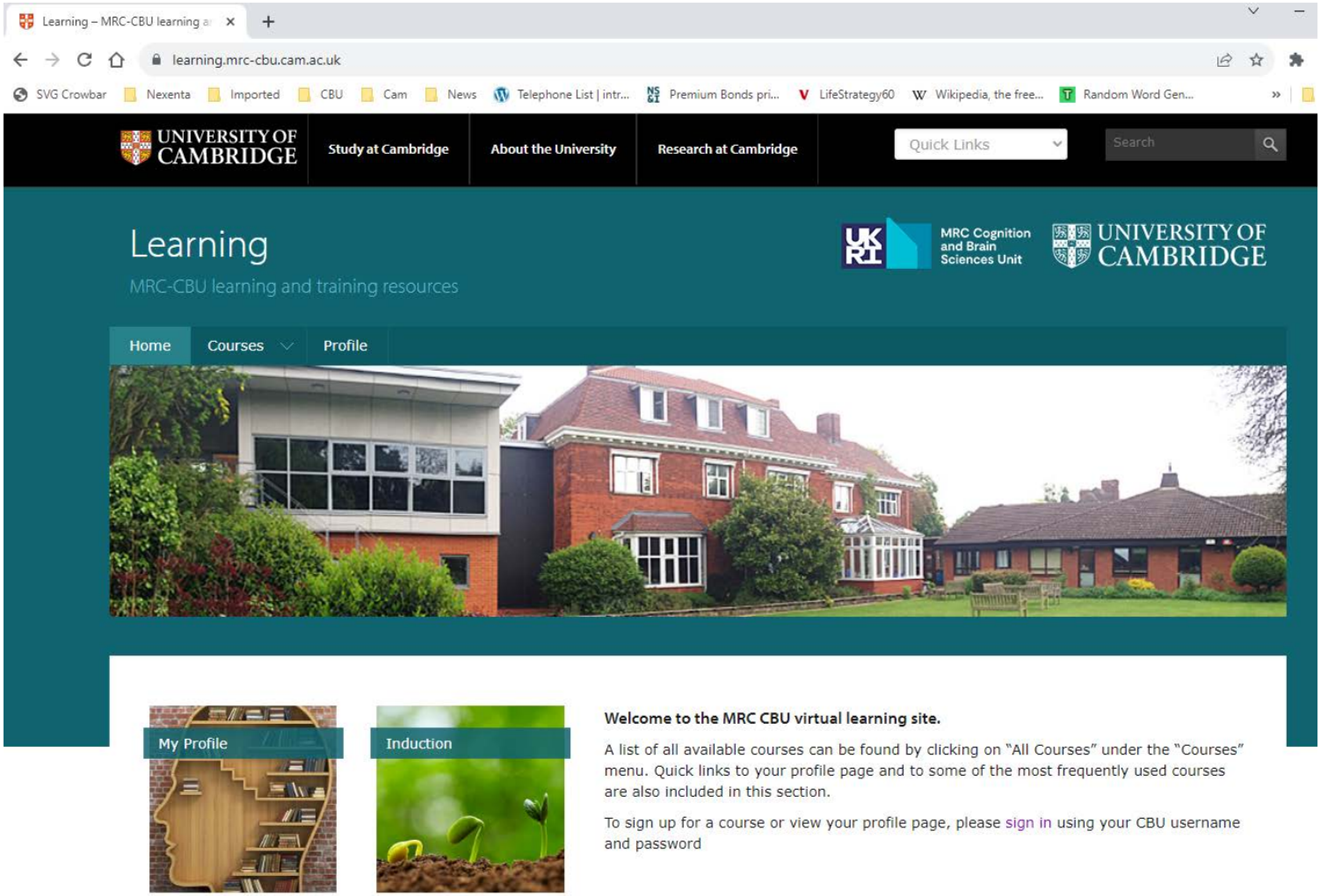
Anthony

Russell

Getting information

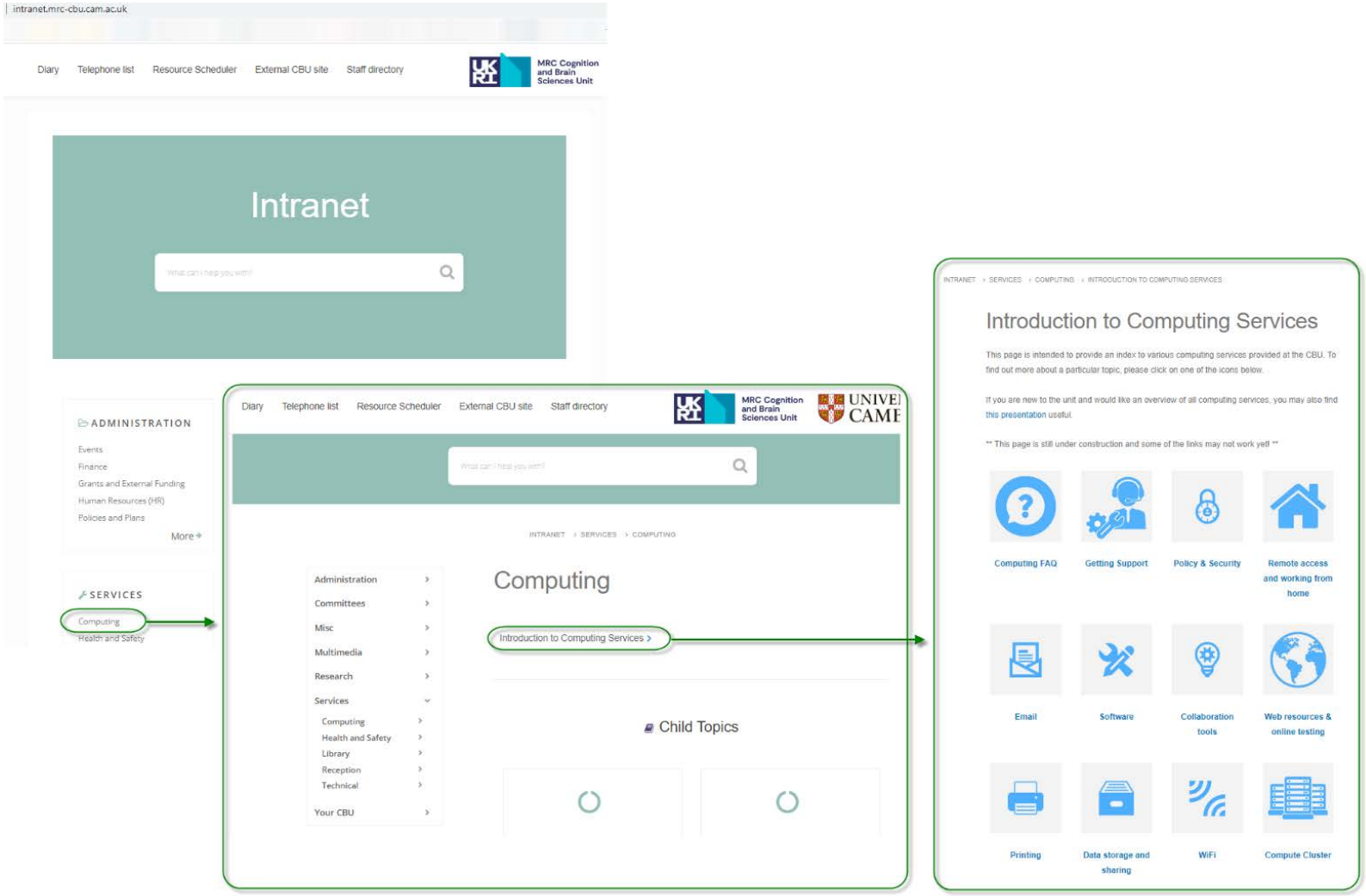
https://learning.mrc-cbu.cam.ac.uk/courses/induction/

MRC | Cognition and Brain Sciences Unit



Getting information

http://intranet.mrc-cbu.cam.ac.uk/home/introduction-to-computing-services/



Web resources

www.mrc-cbu.cam.ac.uk	Main external web site - includes personal page(s) where you can describe your research
intranet.mrc-cbu.cam.ac.uk	Lots of information about resources and policies
imaging.mrc-cbu.cam.ac.uk	Information about imaging / methodological topics
forum.mrc-cbu.cam.ac.uk	Community help forum – ask a question anonymously and get help from members of the unit
resources.mrc-cbsu.local	Resource scheduler, use this to book testing labs, unit vehicles, etc
portal.mrc-cbu.cam.ac.uk	Remote access portal – connect to cbu resources externally
cas.mrc-cbu.cam.ac.uk	Webmail client
ftp.mrc-cbu.cam.ac.uk	FTP server
studies.mrc-cbu.cam.ac.uk	Online experiments