

Data Security and Encryption

Scott Summers

UK Data Service

University of Essex

Newcomers

9th January 2018

UK Data Service



Presentation Structure

- What is the UK Data Service?
- Data Security
 - Passwords
 - Encryption
 - Encryption programmes
 - Data Disposal
- Hands on Experience with tools

What is the UK Data Service?

- Funded by the ESRC
- Single point of access to a wide range of secondary social science data
- We provide support and training for data creators with accessing, managing, sharing and using data
- Delivered by staff based at universities across the UK (Essex, Manchester, Leeds, Southampton, Edinburgh & UCL)
- UK Data Archive – manages the UK Data Service and curates the data

UK Data Service



Data security

Protect data from unauthorised:

- Access
- Use
- Change
- Disclosure
- Destruction



Who knows who is watching, listening or attempting to access your data...



UK Data Service



Stuff happens: data theft

- What would happen if your data was stolen?
- Imagine if seven years worth of your Ebola research was stolen – this situation happened to Dr Fitzgerald



- Source:

<https://www.standard.co.uk/news/crime/burglar-stole-laptop-with-seven-years-of-ebola-research-from-doctor-s-house-a3689406.html>

Data security strategy

- Control access to computers:
 - use passwords and lock your machine when away from it
 - run up-to-date anti-virus and firewall protection
 - power surge protection
 - UPS power supplies
 - utilise encryption
 - on all devices: desktops, laptops, memory sticks, mobile devices
 - at all locations: work, home, travel
 - restrict access to sensitive materials e.g. consent forms and patient records
 - personal data need more protection – always keep them separate and secure
- Control physical access to buildings, rooms and filing cabinets
- Properly dispose of data and equipment once your project is finished

Passwords

- Strong passwords are crucial
- Avoid using weak or easy to guess passwords and reusing passwords
- Consider password managers, complex passwords or stringing words together to create stronger passwords
- But, remember that you need to be able to remember the passwords!
- **Why does this matter?**
- No matter how good the encryption is that you use if you use a weak password the encryption will offer little protection

Password Security

HOW SECURE IS MY PASSWORD?



Your password would be cracked
“Password”
INSTANTLY

Why not try **Dashlane** to create and remember stronger passwords? **It's free!**

Password Security

HOW SECURE IS MY PASSWORD?



It would take a computer about

27 UNDECILLION YEARS

to crack your password

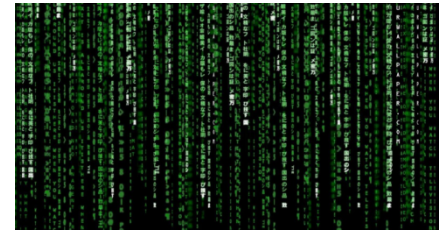
Dashlane can help you remember all of your secure passwords - and **it's free!**

Encryption



- Encryption is the process of encoding digital information in such a way that only authorised parties can view it
- Basic principles
 - Applies an algorithm that makes a file unreadable
 - Needs a 'key' of some kind (passphrase or / and file) to decrypt
- Some types of encryption provide greater protection than others, the type and level of encryption used should correspond to the sensitivity of the data being protected
- As a general rule, more bits equals stronger encryption, therefore, 256-bit encryption is stronger than 128-bit encryption

Encryption



- When using encryption 128-bit encryption should be the minimum level used
- **Always** encrypt personal or sensitive data
 - = anything you would not send on a postcard
 - e.g. moving files, such as interview transcripts
 - e.g. storing files to shared areas or insecure devices
- The UK Data Service recommends Pretty Good Privacy (PGP)
 - More complicated than just a password, but much more secure
 - Involves use of multiple public and private keys

Encryption Software

Encryption software can be easy to use and enables users to:

- encrypt hard drives, partitions, files and folders
- encrypt portable storage devices such as USB flash drives

VeraCrypt



BitLocker



Axcrypt



FileVault2

We will run through demonstrations of all of these later, time permitting!

UK Data Service

VeraCrypt

VeraCrypt

- Derivative of TrueCrypt (now defunct)
- Multi-platform encryption software (Windows, Mac and Linux)
- Full disk and container encryption
- Advanced features
- Free and open source
- Tutorial: <https://www.youtube.com/watch?v=Ogm9QHQpFqU>



BitLocker



BitLocker

- This is standard on selected editions of Windows
- It can encrypt disk volumes and USB devices
- It can also perform 'whole computer' encryption
- If you have Windows installed you can unlock a drive that has been encrypted using BitLocker even if you do not have the programme installed on your computer
- BitLocker is compatible only with Windows OS and is proprietary
- Tutorial: <https://www.youtube.com/watch?v=y4losu-Yfsw>

FileVault2



FileVault2

- This is standard on Apple Macs
- Full disk or drive encryption
- The password can be linked to your iCloud account to unlock the Mac hard drive if you forget your password
- Proprietary
- Uses XTS-AES-128 encryption
- Tutorial: <https://www.youtube.com/watch?v=JIZ9EFMS0ic>

Axcrypt

Axcrypt

- Open source
- File-level encryption
- New version works on Windows and MacOS
- Includes 'digital shredding' ability
- Tutorial: <https://www.youtube.com/watch?v=ACcRInsoYZg>



Data Disposal

- When you delete a file from a hard drive, it is still retrievable (even after emptying the recycle bin)
- Even reformatting a hard drive is **not** sufficient
- Files need to be overwritten multiple times with random data for best chances of removal
- The **only** sure way to ensure data is irretrievable is to physically destroy the drive (using an approved secure destruction facility)

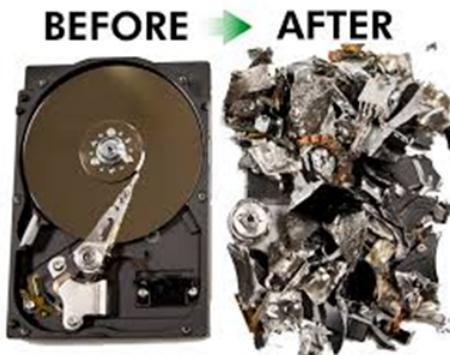
File on hard disk drive



File deleted from disk



File overwritten multiple times on disk



Data Disposal Software



- **BCWipe** - uses 'military-grade procedures to surgically remove all traces of any file'
 - Can be applied to entire disk drives



- **AxCrypt** - free open source file and folder shredding
 - Integrates into Windows well, useful for single files
- Physically destroy portable media, as you would shred paper



Hands on Exercises



Contact

Producer Relations team

UK Data Service

University of Essex

ukdataservice.ac.uk/help/get-in-touch

UK Data Service

