Security Overview#

Security is of primary import at multiple levels. All of the below is based on the official University of York IT Services Security policy

Basic PC security#

Centrally managed (supported) machines

These have strong security measures in place including the deployment of anti-virus software (Sophos), a centrally managed firewall and spam filtering (Webroot). Some useful web pages include

Computing Service security overview

Computing Service anti-virus software

Computing Service general information about your IT Account

Webroot® Email Security Service

UoY user login and registration for spam management

Unsupported machines including home computers#

Try and make sure you have the same sort of services available as described for supported machines.

Modern computer systems usually have bundled firewalls. You have to make sure it is active.

If you do not have a preferred anti-virus software Sophos can be downloaded under agreement for use on your home PC download Sophos

Other measures#

- Change passwords regularly (an account we have with the University of Essex forces change every six months)
- Use strong passwords
- Never write down a password and leave it where it can be see by others
- Lock your computer (press control - alt - delete keys) when you leave it unattended.
- Make sure your PC operating system and software is regularly patched.
- Install malware protection software and run it regularly.
- Consider using script blocking software such as the mozilla-based browsers extension NoScript.
- External media (i.e. portable drives and disks including those in portable computers) that are also used outside the University firewall can be a major threat to security. Infections picked up outside can be moved into the University?s protective environment. It thus makes sense to scan such media coming into the University environment. This should happen automatically if your anti-virus software is set up correctly

Data loss (see below for ADS data holdings)#

Recovery can only happen if data is backed up. Various options exist for ensuring backup

- On supported machines multiple snapshots (hourly, nightly and weekly) are taken of your M: (also known as H: drive). Clearly this is the securest place in terms of backup to keep important data/documents but space is limited
- ADS (and IA) staff have access to a shared backup drive which can be mapped to their supported PCs. This drive is backed-up nightly by IT Services.

ADS Systems Security#

Passwords#

- Password for all ADS systems are stored encrypted, in a centrally managed Password Manager.
- Unique passwords are created for every website, service and system
- Passwords are updated regularly via the Password Manager
- Passwords are shared to individual members of staff, relevant to their needs and working practices.

Systems Access#

- Users have different levels of permission