

Viruses and trojans

There's always a risk of infecting your PC with viruses, trojans and other malware. Here are some things you can do to minimise this risk.

- Make sure your virus checker is up to date. You should scan your files regularly, especially if you have plugged your mobile device into another computer. Back up your files regularly.
- It's best not to open any files attached to an email from an unknown, suspicious or untrustworthy source.
- If you're not sure about the content of attachments to emails, don't open them – especially if the email has an odd title or poor spelling or grammar.
- Delete chain and junk emails rather than forwarding or replying to any of them.
- Be careful when downloading files from the internet. Ensure that the source is a legitimate and reputable one. It's better if an anti-virus program checks the files on the download site. If in doubt, don't open, download, or execute any files or email attachments.

Encryption

Encryption is the conversion of data into a form that can't be easily accessed by unauthorised people. All confidential, personal and sensitive data should be stored securely, especially on laptops, tablets, USB sticks and phones.

If your assignments and project work have information relating to personal data – for example age or ethnic origin – it's your responsibility to protect that information. Encryption is the best way of doing this.

Search 'encryption' on shuspace to find out more.

Password policy

The password and user name used to access your account are the only two pieces of information required to see your files and emails, so your password should be treated as securely as any other piece of confidential information.

It must be at least 8 characters long and contain at least one each of

- an uppercase character
- a lowercase character
- a number

It shouldn't contain your name or login code, family names, pet names, car details or any other easily identifiable information.

Protect your password at all times.

More information

To find out more go to the 'information and IT' and 'personal information' sections of the academic regulations and student policies web page at students.shu.ac.uk/regulations

Got any questions or concerns about your IT security?

Contact IT Help, part of Information Systems and Technology.

Phone **0114 225 3333**
Email ithelp@shu.ac.uk
or see shuspace.shu.ac.uk/it

A PDF version of this document is available at eisf.shu.ac.uk/itsecstudent.pdf

For free expert advice, visit getsafeonline.org

Did you know?

According to a recent survey, most students have only met half of their Facebook contacts, and consider only 25% or less as close friends. But they still share personal information on their page.

- 73% include their relationship status
- 72% include their date of birth
- 41% share their email address
- 14% display their phone numbers

And men are at higher risk of student finance fraud than women, because they're significantly more likely to make their profile public, accept anyone as a friend, and be less vigilant with their personal details.

IT security

Sharing data in this way can make you exposed and vulnerable. While you're at University, you'll use a wide range of IT systems and services, not all provided by Sheffield Hallam.

We take great efforts to ensure the security of our IT systems. By taking some commonsense steps, you can help keep your personal data and equipment safe.



Safe browsing

- Remember to log off or lock a PC if you leave it, so other people can't use your accounts, printing credit and personal network storage space. Don't share your login details on social media sites, or with other people.
- Are your friends really friends? In Facebook, use the Privacy link to change your settings in order to make your details harder to find.
- 'Shoulder surfing' is another way people can collect information like your passwords and pin numbers. By reading the screen over your shoulder, or watching you type, this information can be used by someone who wants to borrow your identity to construct an accurate profile of you, and then impersonate you to obtain credit cards and bank accounts in your name.
- Always set a password on your own PC and mobile device, and don't tick 'remember my password' or similar options.
- Public Wi-Fi hotspots can be a great help when you're not on campus, but they can be insecure, especially if you're not prompted for any security key.
- Treat sensitive and personal information about your friends and colleagues as you would your own information.

Physical security

Although the University is a relatively safe environment, be careful not to leave your personal IT equipment unattended.

Be wary of people trying to manipulate you into giving them information or belongings, perhaps through impersonation. This is known as social engineering. For example, they may claim to be from IT Help and remove your equipment to fix it elsewhere, or ask for your password.

We will never ask for your password, so don't give it to anyone else.

Identity theft

When banking online, only submit your credit card or bank account details to the website of a well-known and respected organisation. Make sure you've typed in the web address yourself, rather than clicking on a link from an email.

When you log into a financial site, the web address should start with 'https' and there should be a padlock icon in the bottom right corner of the browser.

Cookies are mostly harmless files that websites use to remember you. But they can be used by malicious sites for targeted advertising or for identity theft. Search engines use them with your IP address, which means that your searches are not anonymous. You can set your browser to block or to warn you about cookies using the Security and Privacy options.

Online fraud

From time to time you may receive unsolicited emails carrying branding to make you believe the University or another reputable company requires some personal information from you. It may try to convince you that your computer has a virus, or of problems with your bank account. This is known as phishing.

Never respond to these unsolicited requests for confidential information. The Student Loan Company will never ask for bank details or personal information by email. If in any doubt contact the organisation directly using a trusted means of communication.

Similar fraudulent attempts to get your details may come through texts or phone calls. The latter is known as voice phishing, or vishing.