Viruses, Trojans, Malware and Spyware

Viruses - harmful computer programs that can be transmitted in a number of ways and are designed to spread themselves from one computer to another.

Spyware - can be downloaded onto your computer without your permission, and can track your online movements, steal your passwords and compromise your accounts.

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 you have an up to date virus checker and that you scan and back up your files regularly.
- Don't open any files attached to an email from an unknown, suspicious or untrustworthy source, especially if the email has an odd title or poor spelling or grammar.
- Be careful when downloading files from the internet. Ensure that the source is a legitimate and reputable one.

As Staying Safe Online.org states, 'When in doubt, throw it out'. Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

Spam, Scams and Phishing

From time to time you may receive unsolicited emails carrying branding to make you believe the University or another reputable company requires personal information from you. For example, they may try to convince you that your computer has a virus, or that there is a problem with your bank account. This is known as phishing. Similar fraudulent attempts to get your details may come through texts or phone calls (vishing).

Never respond to unsolicited requests for confidential information. Banks, for example, will never ask for banking details or personal information by email. If in any doubt contact the organisation directly using a trusted means of communication, and make sure you've typed in the web address yourself, rather than clicking on a link from an email.

More Information

Got any questions or concerns about your IT security?
Contact IT Help
Phone: **0114 225 3333**
Email: ithelp@shu.ac.uk

For more information visit the IT Help pages on the staff intranet.

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

For free expert advice visit getsafeonline.org

Sheffield
Hallam
University

Staying safe online

A staff guide to IT security

IT Security

With 2.5 million cyber-crimes in the UK alone last year, cyber security is more important than ever. This means protecting both your hardware and online information to ensure that it is safe from people looking to misuse it.

The following information outlines how you can protect both personal and University data.

Physical Security

Although offices and the University are a relatively safe environment, be careful not to leave portable IT equipment unattended. This is even more important when working away from the University.

Be wary of people trying to manipulate you into giving them information or belongings, perhaps through impersonation. For example, using this kind of 'social engineering', someone may claim to be from IT Help and remove your equipment to fix it elsewhere, or ask for your password.

Remember you are responsible for your account, so log off or lock a PC if you leave it to prevent other people using your credentials. IS&T will never ask for your password, so don't share your login details or passwords with anyone.

Always set a password on your own PC and mobile device(s), and don't tick 'remember my password' or similar options.

Protect IT

Lock it before you leave it.

Safe Browsing

Many people use the Internet on a daily basis without trouble, but seemingly reputable sites may contain spyware/malware, or the sites themselves may be counterfeit (phishing sites) posing as the real thing to lure you into their scams. Certain sites are more prone to be a source of spyware/malware, including adult sites, file sharing sites and Social Networking sites .

Be wary of:

- **unsecured or unknown websites,** especially when making online purchases. Ensure any transactions you make only take place across secure web pages which you can identify from the padlock sign in your browser address bar and where the address says https:\\
- **what links you click on.** Avoid clicking links in an email or on social networks unless you are sure the message is legitimate and safe.
- **people looking over your shoulder** when entering passwords and pin numbers. This is known as 'shoulder surfing' which can be used to steal your identity and to impersonate you to obtain access to University systems using your credentials.
- **using public Wi-Fi hotspots.** They can be a great help when you're not on campus, but they can be insecure, especially if it's an open hotspot and you're not prompted for any security key, or there's a shared security key. It's best not to use public Wi-Fi for anything that is sensitive/personal or requires a password.

Encryption

Encryption exists to protect information from unauthorised access. All confidential, personal and sensitive data should be stored securely, especially on laptops, tablets, USB sticks and phones.

It's your responsibility to protect such information, and encryption is the best way of doing this. To find out more about how to encrypt sensitive data. go to the IT Help pages of the staff intranet.

Passwords

Your password should be treated as securely as any other piece of confidential information. It should be protected at all times and not shared with anyone..

When creating a password make sure it is long and strong. It must be at least 8 characters long and contain at least one of each character from three out of the following four categories:

- Uppercase letters A to Z,
- Lowercase letters a to z,
- Numbers 0 to 9,
- Special Characters !#$%@'()+-?[]^_{}~

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

Mobile Devices

All devices connected to the Internet should be protected. This includes computers, smartphones, tablets and other web-enabled devices, which all need protection from viruses and malware.

Use common sense when you connect. If you're online through an unsecured or unprotected network, be cautious about the sites you visit and the information you release.

Secure your phone using a strong passcode to lock your phone, and if working with personal or sensitive information, then it should also be encrypted.

Think before you app. Review the privacy policy and understand what data (location, access to your social networks etc.) the app can access on your device before you download.

For more information:

http://staysafeonline.org/stay-safe-online/mobile-and-on-the-go/mobile-devices

Remember, what you do online has the potential to have a knock-on effect, do you know who can view your social media profiles? Practice good online habits and review before you post!