UNIVERSITY OF Southampton

Dos and don'ts. IT security

Technology and information. Brought to you by iSolutions

Information security is the responsibility of us all. Follow the tips in this handbook and you'll be helping to keep yourself, your peers and University information safe.

Information security helps us to do what we do best – teaching and research. It's simple and mostly common sense.

Make sure you let your family and friends know what to do too, so they're safe online.

Don't be tricked into giving away confidential information

Don't respond to emails or phone calls requesting confidential University information – including staff and student details, confidential research data or corporate information.

It's easy for an unauthorised person to call us and pretend to be an employee or a concerned parent.

Stay on guard to avoid falling for this scam and report any suspicious activity through ServiceLine. Protect your personal information just as closely.

Do stay alert and report suspicious activity

Always report any suspicious activity through ServiceLine. Part of our job is to stop cyber-attacks and to make sure our data isn't lost or stolen.

All of our work at the University depends on keeping our information safe. When something goes wrong, the faster we know about it, the faster we can deal with it.

Don't leave confidential info lying around

Don't leave printouts containing confidential information on your desk. Lock them in a drawer or shred them.

Keep your desk tidy and documents locked away. It makes the office look more organised and reduces the risk of information leaks.

Do lock your computer and mobile phone when not in use

Always lock your computer and mobile phone when you're not using them. You work on important things, and we want to make sure that they stay safe and secure.

Locking your phone and computer keeps your data and contacts safe from prying eyes. If you're working in a student public workstation area, always remember to log off before you leave the computer.

If you have a smartphone, you should also make sure you enable Find my iPhone (Apple) or Device Manager (Android) to help you find it or erase it remotely if lost. For other makes of 'phone, please check with your provider

Don't use an unprotected computer

When you access sensitive information from an insecure computer, like a shared machine at home, you put the information you're viewing at risk.

Make sure your computer is running the latest approved security patches, antivirus and firewall software. You should use user mode, not administrator mode, whenever possible to help prevent some malicious software from working.

Do password-protect sensitive files and devices

Always password-protect sensitive files on your computer, USB and smartphones.

Losing items like phones, USB flash drives and laptops can happen to anyone.

Encrypting your devices and protecting them with strong passwords means you make it more difficult for someone to steal your confidential data, whether it's your personal contacts and text messages or your latest research breakthrough.

Don't use obvious passwords

Don't use obvious passwords, like "password", "cat", or obvious character sequences like "asdfg" and "12345". It's best to use the longest password you can remember. Adding complexity with numbers and punctuation also helps to make the password difficult to discover.

You should use different passwords for different websites and services. If one site is hacked, your other accounts won't be compromised.

Don't let curiosity get the best of you

Always delete suspicious emails and links. Even opening or viewing these emails and links can compromise your computer and create unwanted problems for you and others without your knowledge.

If something looks too good to be true, it probably is.

Don't plug in devices without making sure that they are safe

Have you found a USB drive on the floor? Be careful, as it may contain malicious software.

These devices and even the documents stored on them can be compromised with code waiting to launch as soon as you plug them into a computer.

If you're in doubt, speak to ServiceLine for assistance.

Don't install unauthorised programs on your work computer

Malicious applications often pose as legitimate programs, like games, tools or even antivirus software.

This is the main reason of our PCs becoming infected with viruses and other malicious software.

If you need an application for your work, let ServiceLine know and they'll make sure it's safe to use before installing it.

An ongoing effort

Keeping our information secure is an ongoing effort. It's not clear where future threats will come from or what they'll look like. You can be better prepared by using the tips in this guide, and above all using common sense to keep safe when using your computers and phones.

Get IT help

Contact ServiceLine
www.southampton.ac.uk/ithelp | 023 8059 5656

www.southampton.ac.uk/isolutions