Bournemouth University

IT Services

MOBILE DEVICE SECURITY

Guide for Students

Version 3.0

"Information security is everyone's responsibility."

INTRODUCTION

Over the past few years' mobile phones, tablets and laptops have become a norm for students and researchers to use as an alternative to desktop computers, as these devices can transmit and store data, as well as connect to the internet with ease. While these technologies offer us great convenience and increased productivity, they also carry many security risks.

The IT Service Desk provides 24-hour telephone support.
Alternatively, report an incident or send us a request through our website.

The topics in this guide may not apply to all mobile devices, and therefore it is highly recommended you contact IT Services for advice and support.

Information security threats may also change over time, and we advise you to get the latest copy of this document from IT Services or the staff intranet.

VARIOUS WAYS TO CONTACT US

Studland House
12 Christchurch Road
Bournemouth, BH1 3NA
+44 (0) 1202 965515 or freephone (UK only) 0808 196 2332
https://itservices.bournemouth.ac.uk/
servicedesk4@bournemouth.ac.uk

IT Services

Our mission is to deliver service excellence by providing timely, quality, customer focused and professional IT support at every customer contact.

If you do receive a phishing email on your BU email account or your personal email, then mark it spam or junk.
If unsure, ring the IT Service Desk.

Any loss of BU equipment known to contain data which may fall under the Data Protection Act should be reported to the IT Service Desk.

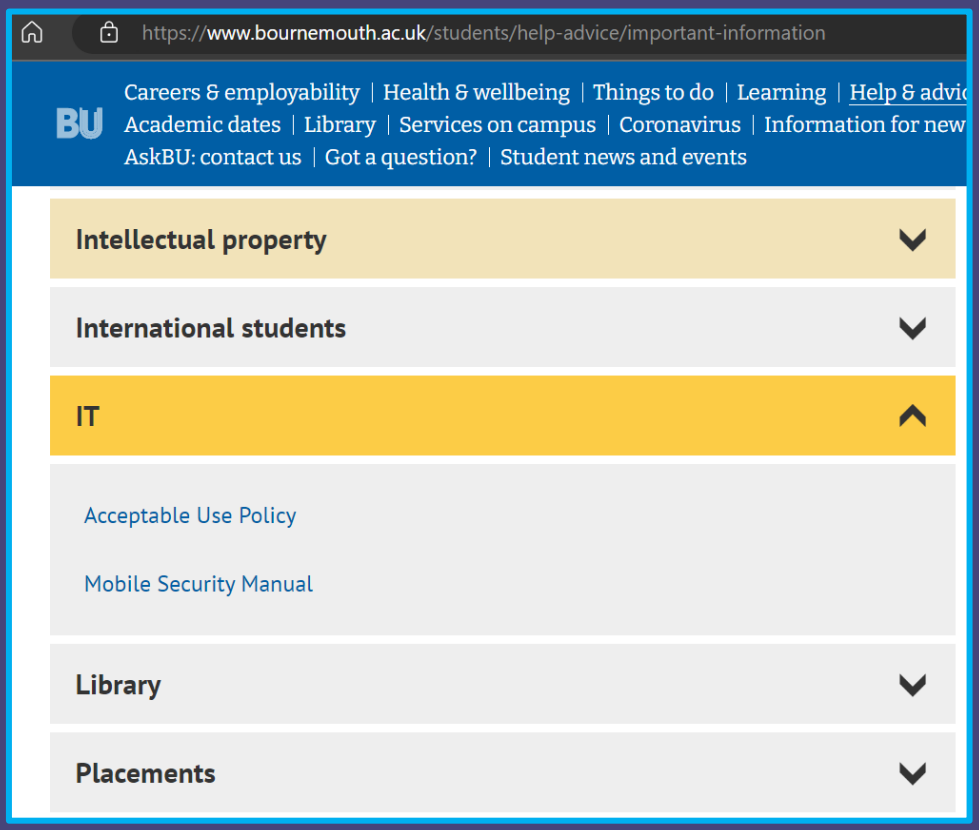
If you become aware of any BU data breaches related to the BU Data Protection Policy, please send an email to dpo@bournemouth.ac.uk

Table of contents

Policies & regulations

If you're handling private information, like someone's personal details or financial data, you must follow the rules set out in the Data Protection Act 2018 and Bournemouth University's policies. IT Services can help you understand and follow the rules.

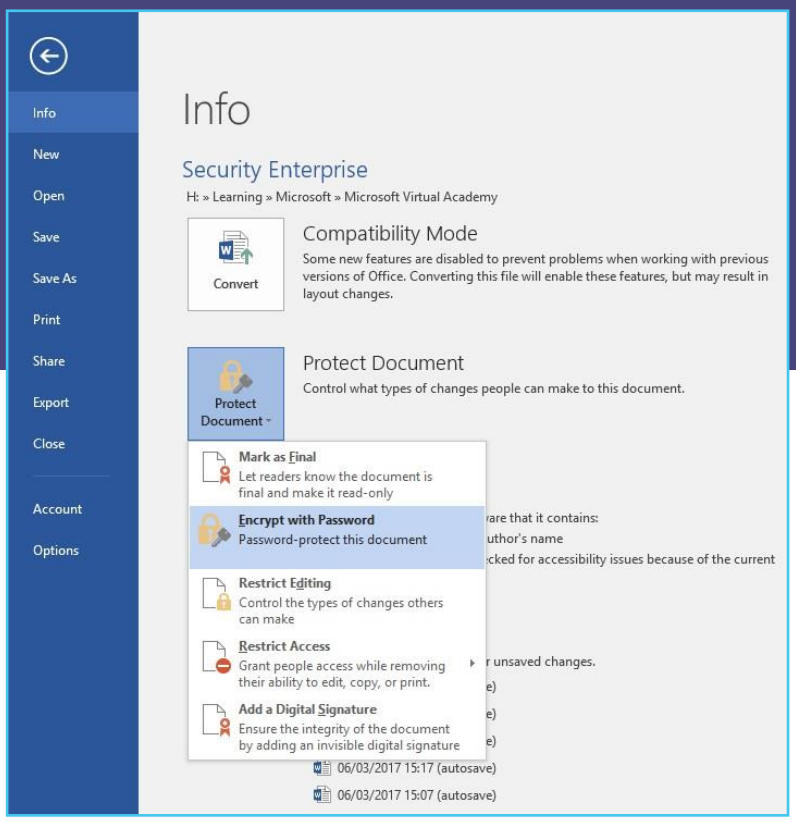
Make sure you are aware of and know how to access BU policies. These can be accessed on the **BU website,** via **students>help-advice>important- information**.



https://www.bournemouth.ac.uk/students/help-advice/important-information

"By default, BU Windows and Mac laptops are encrypted with BitLocker and FileVault. However, for iPhone and iOS devices, you need to add a screen passcode and/or your fingerprint to encrypt the whole device."

InfoSec Team



File encryption

Sending files by email is quick, but it's not always safe, especially if the file contains personal, sensitive, or financial information. Someone could intercept it. **To protect your data, it's best to encrypt the file before sending**. Encryption scrambles the information so only people with the right password or key can read it.

Some applications have built-in protection which means you can encrypt, and password/passphrase protect your document with some simple steps. Steps are normally available within the help feature of an application such as Microsoft Office and Adobe Acrobat.

Encrypting Word files

To encrypt a Word document:

1. Navigate through **File > Info > Protect Document**, then,
2. Add a password/passphrase on the **Password** field.
3. Keep a list of passwords/passphrases in a password manager such as KeePass or LastPass, and do not send the password protected documents together with the passwords/passphrase. For example, try to share the location of the encrypted file via email and call the recipient to tell them the password/passphrase. For quick reference on some of the more common applications you can refer to the following links:

- Microsoft Office: **https://goo.gl/6wjuJt**
- Adobe Acrobat: **https://goo.gl/MqEicS**

BUTransfer: can be used for sending encrypted data (large files up to 50GB) to internal and external users as an alternative to email: **https://butransfer.bournemouth.ac.uk/**

Compression tools: Another approach is to use a compression tool, such as 7-Zip, WinZip or WinRAR to easily encrypt multiple files.

Public WiFi connection

THINGS TO CONSIDER BEFORE CONNECTING TO A PUBLIC WIFI AND ACCESSING SENSITIVE INFORMATION

Do not connect to unsecured Wi-Fi. Public places such as parks, airport terminals, buses and cafés, may offer **free internet access,** but these are **often targeted by criminals**. Hackers set up their own infected unsecured Wi-Fi, often disguised as a common name like 'Café Wi-Fi', or 'Terminal 1 Free' to trick you into joining their network. Once joined, they can monitor all your internet activities, placing your data at risk.

- Never leave your laptop/mobile phone unlocked or unattended as criminals can transfer a virus to your device in seconds to record your future digital activities.

- To stay safe, **ask the cafe staff or airport personnel how to safely connect to their secured Wi-Fi,** as the password that is floating around (e.g. written on brochures, card or a bulletin board) may belong to a rogue Wi-Fi network.

- Do not access non-public information as other people can record your activity from a distance using a camera.

- If you do use public Wi-Fi, this should be secured using a VPN (Virtual Private Network).

How to setup a passcode or password /passphrase on your devices

Device locking

Consider enabling the auto-locking feature.

*"Having a password or other protection on a mobile device is the **first line of defense** against cyber threats, helping to block unauthorised access and safeguard personal, academic, and sensitive data from being misused."*

InfoSec Team

For iPhone/iPad

1. Go to **Settings** > **Touch ID & Passcode**.
2. Tap **Turn Passcode On.**
3. Enter a six-digit passcode. Or tap **Passcode Options** to switch to a four-digit numeric code, a custom numeric code, or a custom alphanumeric code.
4. Enter your passcode again to confirm. More details on the Apple website: **https://goo.gl/hsaHkX**

For Mac

1. Choose System Preferences from the Apple menu, then click Security & Privacy.
2. Click the General tab.
3. Select the option to require a password after sleep or screen saver begins.

Apple provides some detailed instructions related to securing your device.

- macOS: how to change the login password **https://goo.gl/nKkY2K**
- macOS: Tips for using touch ID **https://goo.gl/QKUXBd**

For Windows

1. Right-click on your desktop and click **Personalise** to open the personalisation settings dialog.
2. Click **Screen Saver** under the themes to change your screen saver settings.
3. Select the screen saver you want, then check the box to display the login screen when you exit the screen saver. Enter the number of minutes you want to wait before your screensaver starts, then click **Ok** to save your settings. Microsoft Windows official instruction page can be found here: **https://goo.gl/zJ66NT**

For Android

On Android devices the menu may vary according to the Android version and the mobile manufacturer but the steps in general are described on the Android webpage **https://goo.gl/1qJq4A**

Malicious web link

Whether a URL or weblink has been sent via email, text message or social media check the link is genuine.

- If you are unsure about the safety of the weblink, try to hover your mouse cursor over the URL to reveal the true web address. Otherwise, do not click the weblink and seek assistance from the IT Service Desk.

- Be aware of phishing and scams. These kinds of emails usually contain malicious links like those mentioned above.

- You must also be aware that apart from emails or text messages, fraudsters are using other methods of deception like telephone calls.

Your password is due to expire. Please consider changing it before this time.
You can change your password as follows:
On campus:
Ctrl+Alt+Delete - Logged on to a BU networked PC, press the 'Ctrl+Alt+Delete' keys and select 'Change a Password.'

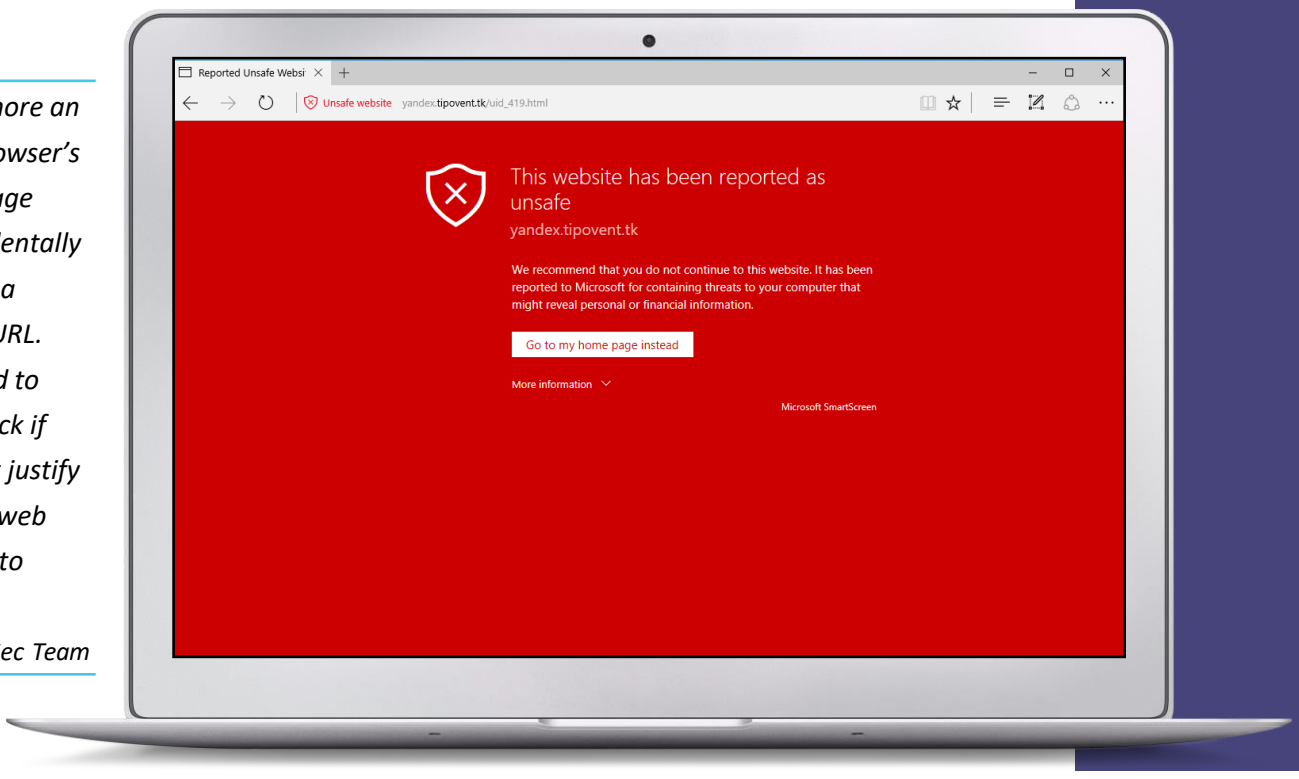
Password Reset Tool - If you have completed your **registration details**, you can request a password reset by using this link: https://password.bournemouth.ac.uk/

Off campus:
Outlook Web Access - Logged on to Outlook Web Access, select the settings icon (cog symbol  , top right next to the ? symbol) and then 'Change Password'.

"Be cautious when answering phone calls and don't reply back or reveal personal information when you are unsure of the authenticity of the phone call".

"Do not ignore an internet browser's warning page when accidentally clicking on a malicious URL. Ask a friend to double check if you cannot justify whether a web link is safe to click".

InfoSec Team



Remote wipe application

"It is important to have a remote wipe application configured on your mobile device so access to sensitive information can be prevented if the device is lost, stolen or goes missing."

InfoSec Team

Apple remote wipe

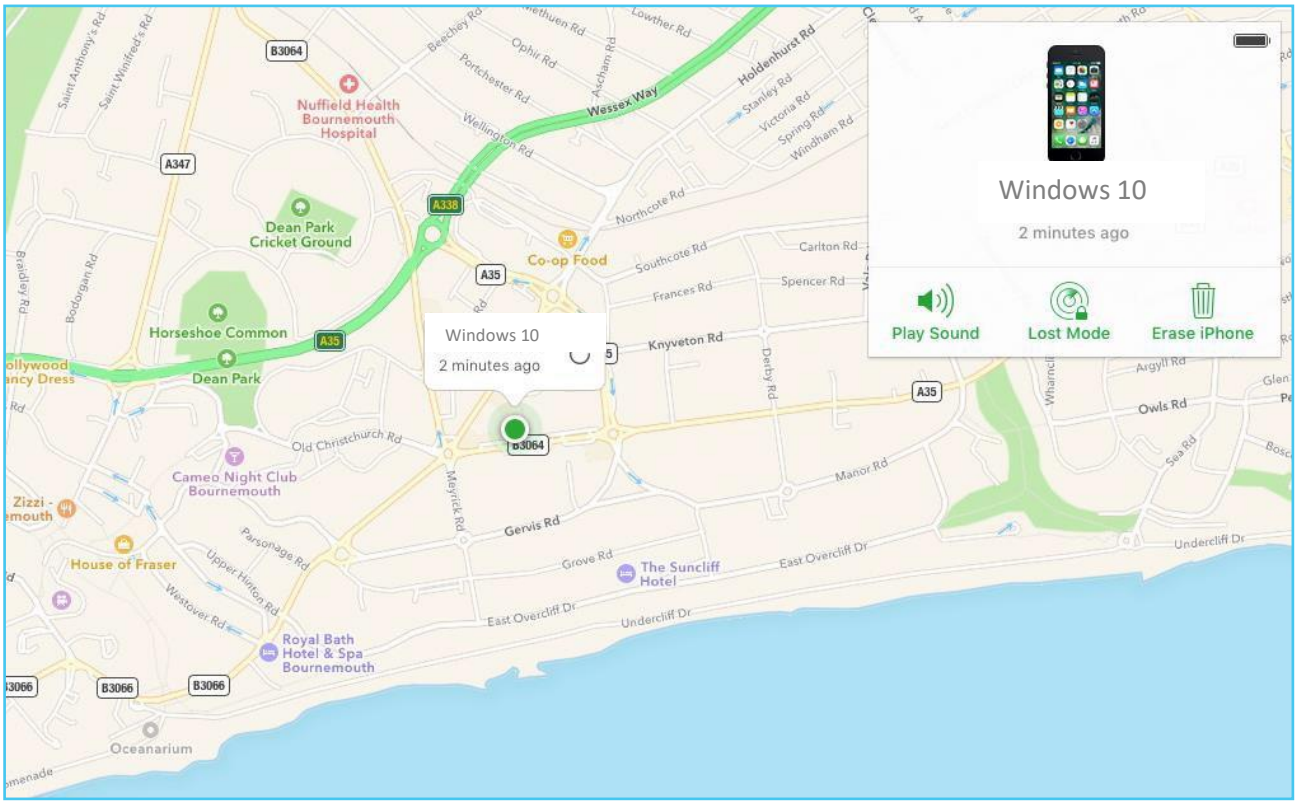
Before using your Apple devices, such as Macs, iPads and iPhones, it is important to familiarise yourself with how to use Apple's remote wipe service.

Apple remote wipe to erase your iPhone, iPad or MacBook using iCloud:

1. Go to **Find My iPhone** on iCloud.com.
2. Click **All Devices**, then select the device you want to erase.
3. In the device's Info window, click **Erase**.

The Apple's Find My iPhone is an example on how to remote wipe an iPhone device, but similar instructions can be found on the internet for Microsoft, Android and other Apple devices:

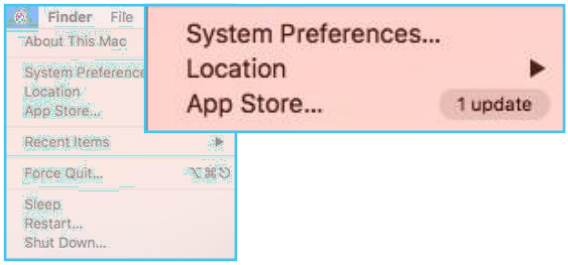
- **Microsoft**: find and lock your lost Windows device **https://goo.gl/VhRbo7** . Wipe all your data remotely from a Windows 10 laptop **https://goo.gl/8ohYGQ**
- **Android**: Detailed guide on how to find, lock and erase your Android device: **https://goo.gl/zdMr91**
- **Mac** and **iOS**: Locate your missing device with the iCloud find my iPhone feature **https://goo.gl/5GF2HN** . How to find and protect your information if your iPhone, iPad or iPod is lost or stolen **https://goo.gl/a2qkNJ**



Software updates

Software vulnerability

There is no 'bug-free' software. A bug is a weakness in the software that can disrupt the normal operation of the software. The software becomes vulnerable if the bug can be exploited by hackers and thus requires you to install any updates when they become available.



Operating system updates

There are several ways to access update settings for **Mac OS X**, and the easiest way is to

1. Click on the **Apple Menu** and
2. Select the **App Store**.
3. When the App Store opens, click on individual update button or press the **UPDATE ALL** button to download all updates.

For **Windows 7, 8, 10 and 11**

1. Open the **Start Menu** and
2. Type **Windows Update** in the search field.
3. Click the suggested link for **Windows Update** and click the **Check for updates**.

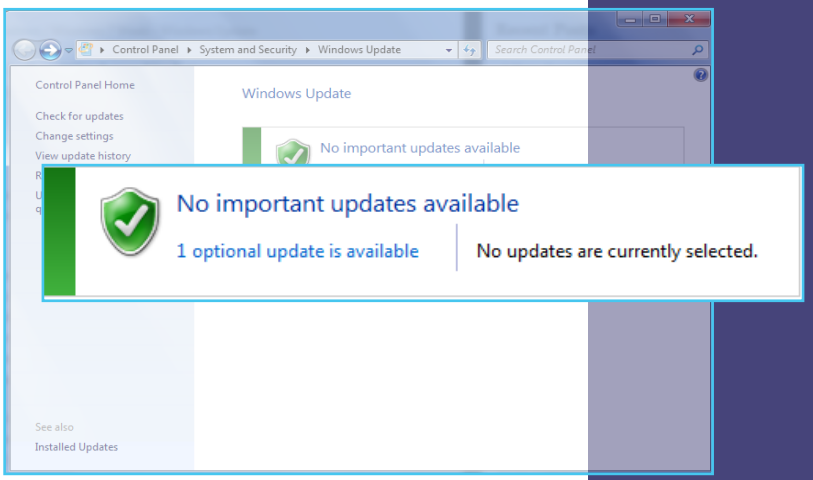
To update **iOS** devices such as iPhone and iPad:

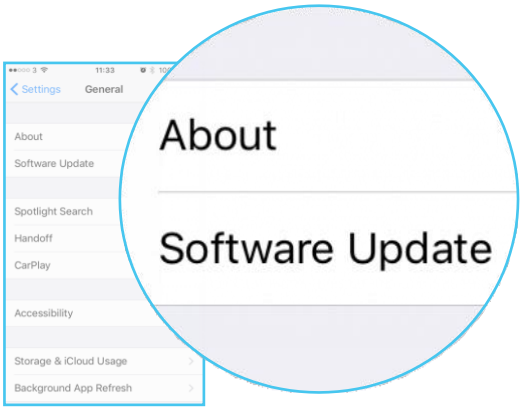
1. Locate and open the Settings app and
2. Navigate through **General > Software Update**.

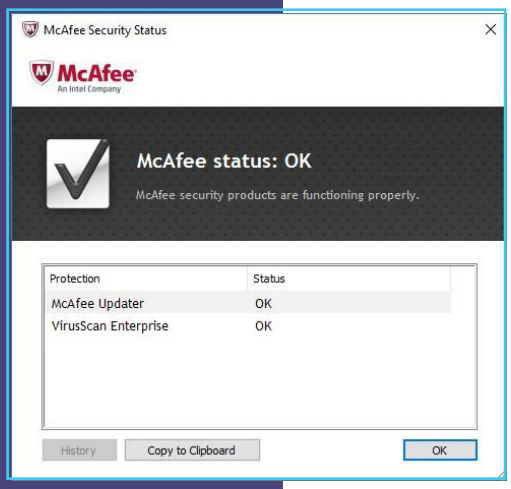
Application updates

It is important to regularly update not only the operating system but also all individual applications. Many applications provide helpful information within the app on how to update their software.

To update **Android** devices:
https://goo.gl/CDmTwp







Security software

Security software such as antivirus (AV) and firewall are critical parts of your device's protection. There are many paid or free versions of such software. It is recommended that a paid one is installed as they provide better overall performance and support.

In the following links there are instructions on basic principles related to antivirus software for Microsoft, Apple, Ubuntu and mobile devices with iOS and Android operating systems.

Microsoft

Protect yourself with the embedded windows antivirus software, Windows Defender **https://goo.gl/X6T3do**

Mac

Apple's Gatekeeper is the default Apple antivirus software **https://goo.gl/jHBXGm**

Ubuntu

Antivirus software solutions are essential also for Ubuntu. There is the perception that Linux based systems are safe, however, this has been proven to be inaccurate. Cyber criminals have targeted Linux based systems many times with success and there are regular discoveries of exploits within these systems including Ubuntu. Information on how to install antivirus software on an Ubuntu machine can be found here: **https://goo.gl/fYqGXW**

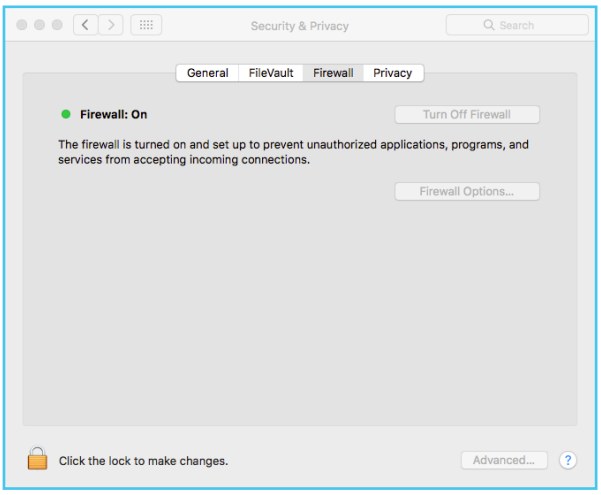
Android and iOS

Mobile devices are also a common target for hackers.

1. Mobile devices like smartphones and tablets are tempting for cyber criminals.
2. Exploits and new methods of attack, developed to specifically target Android and IOS systems, are being revealed by security experts every day.
3. Smartphones are a tempting target for hackers as we store a lot of personal information on them such as photos, social media accounts and details of our credit card numbers etc. As a result, we must safeguard the information we store on our personal devices such as smartphones.
4. By installing an antivirus application on our mobile we enhance the security of the device. There are some free and paid versions of AV applications for both Android and IOS. It is better to have one installed on our devices rather than having nothing and being unprotected.

Free AV for **Android**: **https://goo.gl/3rJfPY**
Free AV for **iOS**: **https://goo.gl/GQQG8p**

Security software



Enable the firewall on Windows and Mac

A firewall is a security system to protect your device from untrusted incoming/outgoing network traffic. Cybercriminals do not need to physically access your device; instead, they use the network you are connected to, such as the internet, and can launch an attack from a remote location. One identified protection against this attack is the use of a firewall system. Fortunately, Windows and Mac (OS X) have built-in firewall systems.

Access the firewall Mac:
To enable your firewall on your Mac, navigate through **System Preferences > Security & Privacy > Firewall**.

Windows:
The setting is available by going to **Start Menu > Settings > Network & Internet > Windows Firewall**.

"Do not rely on anti-malware and the firewall to protect you from attack and malicious software. Security software is only good if the threat is identified and a known mitigation is available. New and latest threats may not be detected immediately by any anti-virus software; therefore, malicious software (e.g. virus) can potentially compromise your computer without being noticed. If you see abnormal behaviour on your mobile device, contact IT Services and do not tackle malicious software by yourself."

InfoSec Team

Backup practice

Our data is important. It takes a lot of time to collect but can be lost in seconds. A potential hard disk failure or an accidental deletion are some of the scenarios we should always take into consideration. To avoid losing your documents like your assignment, your holiday photos, music etc. you should get into the habit of routinely backing up your data daily.

How to back up your data

1. Find an appropriate storage device: This device could be anything from an SD card to an external hard drive or cloud storage. The important thing is that this device should be capable of storing all your data.
2. You can back up your files manually or by using special backup software that automates the backup process.
3. You can backup data to your BU OneDrive account. You can access your OneDrive when using other devices (such as Library machines).

For Mac

Apple computers use special built-in software for backups called Time Machine:
https://goo.gl/XauyJv

For Android

Instructions on how to backup an **Android** phone can be found on the official **Android** website:
https://goo.gl/hSTEtR

For iOS

Apple gives its users two options to back up their device data. These two options are the iCloud and the iTunes: **https://goo.gl/bosF25**

For Windows

More information about how to backup **Windows** computers can be found in the following link:
https://goo.gl/D9NvYP

HABITUALLY TRY TO SAVE YOUR FILES DAILY ON A SECONDARY STORAGE SYSTEM

Backup all important documents, especially those that are difficult and time consuming to recreate.

It is important to know that external hard drives and cloud storage (e.g. OneDrive and Dropbox) are suitable locations you can use to backup coursework, assignments and project documents, in case your files become corrupted, accidentally deleted or if your device fails.

"Get into the habit of backing up your work at least once a day".

InfoSec Team

Passwords and passphrases

"Using a strong password or passphrase, supported by Multi-Factor authentication (MFA), is the first line of defense in protecting your online accounts and personal information from unauthorised access".

InfoSec Team

Everyone uses passwords or passphrases daily, whether it's on a website, accessing an email account or logging onto your computer. The use of a strong password or passphrase is therefore essential to protect your security and identity. Even if you use a state-of-the-art security system, this will be deemed useless if your passwords are weak.

Passwords and passphrases are cracked in the following ways:

Brute force: is the process of automated or manual guessing of a user's password or passphrase.

Interception: Passwords and passphrases can be intercepted as they are transmitted over the network - this method is also known as Man-In-The-Middle attacks.

Social engineering: use of social engineering techniques like phishing emails or websites.

Malware: There is malicious software available that allows the hackers to view exactly what the user is typing, as they are typing it.

Shoulder surfing: observing someone typing their password or passphrase.

There are three basic guidelines in creating a strong password or passphrase

1. Use a **passphrase** which includes **a combination of three unrelated, but easy-to-remember words plus numbers and special characters** to meet the BU password requirements. For example, "ParisLego3Gold£" and "FriendDog7House%". Passphrases rely upon the length for their security strength which is a common (and recommended) requirement for passwords. Passphrases are both easier for us to remember, and harder for hackers to crack.

2. Avoid using a single dictionary word, or recognisable patterns of letters and numbers such as 'Password123' or using commonly combined words such as manchesterunitedfootball. **Don't include personal information such as your name, initials, and date of birth** in your passwords. For example, if your name is James, the password '**James2002**' would be a poor password choice as it is a combination of your name and year of birth. This information could be easily available to a hacker via your social media presence, who may be able to guess the password in minutes.

3. **Don't reuse passwords or passphrases**: Reusing passwords or using the same password for multiple accounts is bad practice. If someone figures out your password for one account, that person could sign in to your other accounts.

Passwords and passphrases

"Keep your BU account safe and never share your password/passphrase, username or access with others. Don't use your BU email address to register for non-BU-affiliated websites such as retail sites".

InfoSec Team

Hackers are interested in passwords/passphrases and authentication credentials, as they provide a means for accessing information without triggering alarms generated by the identification of vulnerabilities, malware or other methods of compromise.

This allows them to impersonate the victim and log into their victim's accounts to attack colleagues, relatives and friends. By doing this they are literally invisible, and they can slip under the radar of every security mechanism. Choosing a strong password that's unique to each account is mandatory and it is a common way to protect your digital identity from being stolen.

BU password/passphrase requirements

Having a strong password/passphrase is an essential starting point in protecting personal and sensitive data from cyber-attacks. The BU password requirements are in place to help support and achieve this goal.

For security reasons your BU password/passphrase needs to:

- Be a minimum of 12 characters long (with no spaces)
- Be different to your last 12 passwords/passphrases
- Not be made up of all numeric or alpha characters
- Include a combination of at least 3 of the 4-character types below with no spaces:
- Lower case letter
- Upper case letter
- A single-digit number (0-9)
- A special character (e.g. ! @ # $ % ^ & * () = - {} [] " ; ? , /)

Password/passphrase best practices

Do:

- change passwords/passphrases regularly
- store safely

Don't:

- reuse passwords or passphrases
- share your passwords or passphrases
- send it in an email
- write it on a post-it note
- store on unprotected storage
- enter on an unsecured website
- embed it within source code or scripts
- use the same password/passphrase across multiple login accounts
- disclose it to the IT Service Desk or any other support channel. A reputable company will never ask for your password or passphrase.

Portable storage

"Portable storage devices are the most common way of transferring data between different devices. USB sticks, CDs, DVDs, external hard drives and SD memory cards are some of the most popular external storage devices. However, portability and convenience may cause different threats to your information."

InfoSec Team

Types of external storage devices could be the following

- Portable flash memory devices
- Portable external hard drives
- Card readers (SD cards)
- Portable Media Players (MP3 players)
- Digital cameras
- Mobile phones

Dangers of using portable media

- Malware can be easily spread through external storage devices.
- Portable devices are easily stolen. As a result, your information could be exposed to unauthorised people.
- Someone may enable the auto run (autorun.exe) module within the portable media which can be hacked to install multiple types of malicious software such as malware and viruses.

Do's

- Format the USB drives for first time usage.
- Scan the portable media with your antivirus software before using it or opening any files in it.
- Wipe out the drive securely to clear the contents.
- Protect your USB device with a password/ passphrase and encryption if your device supports it.
- Encrypt the files / folders on the device.
- Always protect your stored documents in a portable media device with a strong password or passphrase.
- If you are using these devices in corporate computers read the BU Mobile Computing Policy to ensure you are compliant.

Don'ts

- Do not accept any promotional USB device from unknown sources.
- Never keep sensitive information like username/passwords on a USB disk.
- Never keep sensitive data or personal information without password protection and encryption.
- Don't insert an unknown USB device into a BU system.

Social media

"It's so easy to accidentally share a lot about yourself, or others on social media that can be used by the wrong people. It's important to think before you post and never disclose the personal data of another individual on social media. Once something is published online, it can be easily copied and redistributed before you have the chance to delete it".

InfoSec Team

To help you stay safe when using social media, here are three things we encourage you to do right now:

1. **Remove your birthday, middle names and home address information from any personal bio's**. This information can be used to impersonate you or encourage unwanted attention.
2. Familiarise yourself with how individual social media applications work and **review and update your privacy settings** to control and restrict who can see the information you are sharing online. **Turn off your location tracking settings** on your social media accounts and apps.
3. **Use filters to cover up or blur any personal information in photographs** you share including letters with your address on, bank cards, and your student ID card.

Blur out personal information from photographs

When you graduate

Graduation is an exciting time for us all, and we encourage you to share and relish your achievements.

However, cyber attackers are aware of this time in the academic calendar and will look to social media to gather personally identifiable information to steal your identity.

If you decide to share an image of your certificate or results letter, we recommend you obscure information such as your full name, student ID, and date of birth to protect your data.

As part of the BU rules and regulations, we ask all students to adhere to the Student Disciplinary Procedure which includes social media activity.

Mobile security top tips

QR Codes

QR code scams are on the rise and unfortunately here to stay. These codes can be linked to malicious websites and download spyware on your devices.

Be sure to:

- ☑ Avoid scanning codes without knowledge of their origin.

Email Phishing

Email Phishing is still the most common attack cybercriminals use to deceive people.

Before reacting always remember to check:

- ☑ The subject line
- ☑ To, From, and Reply to lines
- ☑ Time and Date lines
- ☑ Links and attachments
- ☑ Urgency to action

Red flags are everywhere. You just need to know how to spot them. Remember to **stop, look,** and **think** before taking any action!

Social Media

Oversharing on social media has made cybercriminal's attacks more effective since the attacks can be more tailored to potential victims.

Be wary of:

- ☑ Profiles with model-like photos
- ☑ Profiles with few connections
- ☑ Generic profile information
- ☑ Direct messages posing as government officials or copyright violations

Ransomware

Cybercriminals will attach ransomware, a type of malware, to links and attachments found in emails that will lock users out of their own system if clicked on.

Remember:

- ☑ **Don't pay that ransom!** Paying the ransom does not guarantee you will receive your data back.
- ☑ Always double-check any links or attachments found in emails.

I DON'T ...

- leave my device unattended, especially in places where it can be easily stolen.
- save login information on my device.

I DO ...

- use a strong password along with two-factor authentication.
- always use an organization approved Virtual Private Network (VPN) when I am connected to public Wi-Fi.
- stop, look, and think before I take any action.

If your phone displays any of these symptoms, it may be infected:

- The battery does not last.
- You get random pop-ups.
- The performance of the device drops.
- You find apps on your device that you didn't install.

To avoid infection:

- ✓ Only download apps from official app stores.
- ✓ Don't click on suspicious links.
- ✓ Check your apps frequently and delete unused ones.

Click and hold a link to preview where the URL leads. If it doesn't look right, don't follow the link.

Bournemouth University

IT SERVICE DESK

We offer a 24-hour telephone support service which is available to all BU students and staff and operates seven days a week, 365 days a year.

HOW TO CONTACT US

You can call the Service Desk on:
+44 (0) 1202 9 65515
freephone (UK only) 0808 196 2332
or raise a request/report a problem
https://itservices.bournemouth.ac.uk/

Alternatively, you may be able to find what you are looking for in our Knowledge Base. For example, the instruction on how to add BU emails to your smartphone.
https://goo.gl/DF4Pj1

You can also chat with us via **https://itservices.bournemouth.ac.uk/** to ask us questions or queries between 8am and 4:45pm Monday to Friday.

"Information security is everyone's responsibility."

Version 3.0 August 2025