
MOBILE DEVICE SECURITY

Guide

INTRODUCTION

Over the past few years mobile phones, tablets and laptops have become a norm for staff and researchers to use as the 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 a great convenience and increased productivity, they also carry many security risks.

This document is a supplementary guide to BU's Mobile Device Policy. It is highly recommended to read the policy as well as other related information security policies which are available on the staff intranet website.

The IT Service Desk provides 24/7 hour telephone support. Alternatively, report an incident or send us request through our website.

Topics in this guideline apply to all issued BU mobile devices, and if you have any questions, it is highly recommended you to contact IT Services.

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

VARIOUS WAYS TO CONTACT US

Studland House
12 Christchurch Road
Bournemouth
BH1 3NA
+44 (0) 1202 9 65515
<https://itservices.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 malicious or otherwise suspicious email, please send it as an attachment to:

unwantedmail@bournemouth.ac.uk



Any loss of equipment known to contain data which may fall under the Data Protection Act should be reported to:

<https://itservices.bournemouth.ac.uk>



If you become aware of any breaches to the Data Protection Act or BU policy, please send an email to:

<https://itservices.bournemouth.ac.uk>

TABLE OF CONTENTS

#4

Policies &
regulations

#5

Lock your device

#6

Accessing non-
public
information

#7

Keeping documents
& emails private

#8

Connecting to a
public WiFi

#9

Avoid malicious
links

#10

Wiping a device
when lost, missing
or stolen

#11

Software update

#12

Protecting your
device from attacks
& malicious software

#13

Backup

POLICIES & REGULATIONS

Non-public information such as personally identifiable information, financial and other security-sensitive information should be stored, processed and disclosed in accordance with the Data Protection Act 1998 and BU policies.











Policies, such as Mobile Computing and Data Protection Policy should be considered reading as these policies cover the following topics:

- a) remote environments (e.g. in locations other than the BU premises)
- b) mobile device configuration
- c) mobile device connectivity
- d) portable storage devices
- e) consumer devices and BYOD (Bring-Your-Own-Device)
- f) safety store, process and share PII, financial and other sensitive information.


<https://staffintranet.bournemouth.ac.uk/aboutbu/policiesprocedures/>

Make sure you are aware and know how to access BU policies, which can be accessed on the staff intranet website.

Legal

-  [Anti-Bribery Policy and Procedures](#)
-  [Conflicts of Interest Policy and Procedures](#)
-  [Contract Signing Policy and Procedures](#)
-  [Intellectual Property Policy](#)
-  [Intellectual Property Management Procedures](#)
-  [Patents and Inventions Policy](#)
-  [BUF - Guide to Accessing Information](#)
-  [BU Publication Scheme - Guide to Accessing Information](#)
-  [Data Protection Policy for Staff and BU Representatives](#)
-  [Guidance Note on Disclosure of Student Personal Data to Third Parties](#)
-  [Guidance Note on Sharing Information About External Speakers](#)
-  [Related Companies Policy and Procedures](#)

Information Security

-  [Acceptable Use Policy](#)
-  [Access Management Policy](#)
-  [BU Staff and Authorised Users Policy](#)
-  [Information Security Policy](#)
-  [Mobile Computing Policy](#)
-  [Threat and Vulnerability Management Policy](#)

How to setup a passcode on an iPhone or iPad



"To improve your device's security use a more complex password and then use the fingerprint sensor (where available) to improve usability.

Enrol your fingerprint and/or password on smartphone to protect against unauthorised access as well as encrypting the stored information/files."

- Matt Hall
Assistant Director of IT Services

DEVICE LOCKING

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.

"For Windows and Mac, you should be able to use your normal BU login details (e.g. email and Desktop computer). If not, please contact IT Services."

If your device has BU data on it, you must set a passcode and turn-on the auto-lock feature.

FOR WINDOWS

Your Windows laptop is setup to automatically goes into standby and lock the screen after 15 minutes of inactivity. However, if you require changing the time, please contact IT Services.

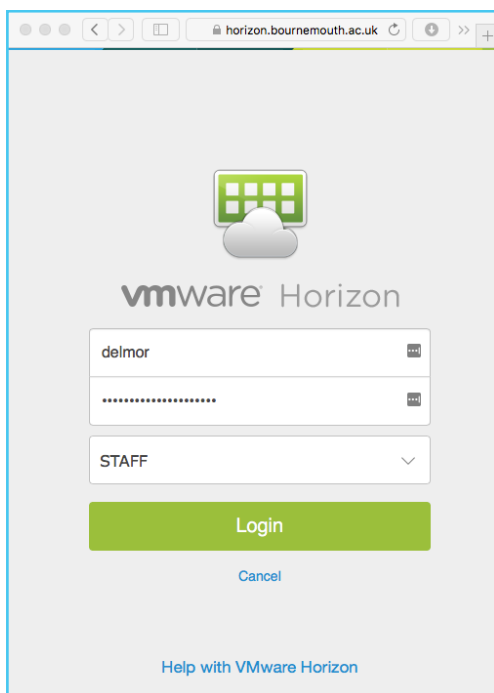
FOR MAC

(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.

FOR IPHONE/IPAD

(1) Tap the **Settings** from the Home screen(2) Tap on **Display & Brightness**. (3) Tap on the **Auto-Lock** to set the waiting time.



ACCESSING NON-PUBLIC INFORMATION



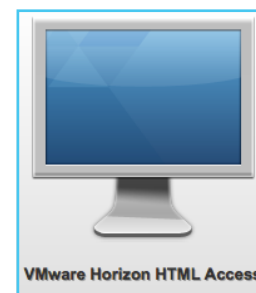
USING CLIENT APPLICATION

- (1) Open an Internet browser and browse to **horizon.bournemouth.ac.uk** and
- (2) click on the **Install VMware Horizon Client** link. (3) Accept all of the default settings. If you

are prompted to add a (Connection) Server, please type **horizon.bournemouth.ac.uk**

USING AN INTERNET BROWSER

- (1) Open an Internet browser and browse to **horizon.bournemouth.ac.uk** and (2) click on the **VMware Horizon HTML Access** link.
- (3) Accept the terms and conditions by clicking the **Accept** button. Now,



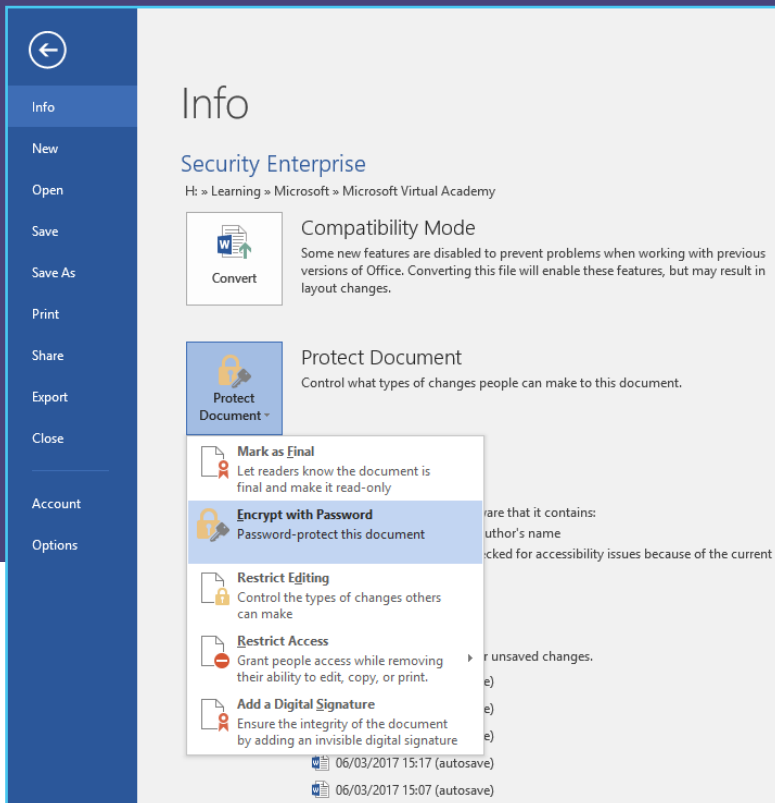
- (4) enter your login details and (5) select **STAFF** from the domain list. Finally, (6) select the **Staff Standard Desktop** to load your virtual desktop.

"Not all browsers support the Web Client feature. Therefore it is important to update your Internet browser to its latest version or try to download a different browser. For additional assistance, contact IT Services."

Whenever possible you should refrain from accessing non-public information off campus. The security of the Internet outside BU premises is not guaranteed to be safe and may be prone to eavesdropping - whether someone is looking over your shoulder while you are accessing a sensitive file in a public place or intercepting your Internet connection whilst working at home using your personal computer.

To mitigate the above issue, BU provides a virtual desktop environment that allows access to your applications and documents remotely. The system does not protect us from someone who is looking over our shoulder or recording our online activity using a video camera as examples, but it certainly reduces the risk of disclosing sensitive information to people who may attempt to tap into the BU network.

Windows, Macs and Linux computers can access BU virtual desktops. There are two ways to access BU virtual Desktops, using a client software or an Internet browser.



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

ENCRIPTING WORD FILES

To encrypt a Word document:

(1) Navigate through **File > Info > Protect Document**, then, (2) Add a password on the **Password** field. (3) Keep a record of your passwords in a password manager such as **KeePass** and do not send the password protected documents together with the passwords. For example, try to share the location of the encrypted file via email and call the receipt to tell the password.

KEEPING DOCUMENTS & EMAILS PRIVATE

Sending information in an email attachment is quick and easy to do but you need to be aware that there is a risk that someone could intercept your information if you choose this method. The risk is not only present via interception, as emails can also be accidentally/intentionally send to the wrong recipient. This can be particularly important if the data you are sending contains personal, sensitive or financial information.

In order to minimise the risk we would recommend you encrypt your information before emailing it. Encryption uses a software tool to scramble and lock information into meaningless data for all except the people who have the key to unlock and descramble the information.

Some applications have built-in functionality, which offers protection. Meaning you can encrypt and password 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.

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

- James Stevens
Chief Data Governance Officer

PUBLIC WIFI CONNECTION

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



Do not connect to unsecured WiFi. Public places such as parks, airport terminals, buses and cafés, do offer free Internet access but are often targeted by criminals. Hackers can scan your Internet traffic by allowing you to connect to infected unsecured WiFi.



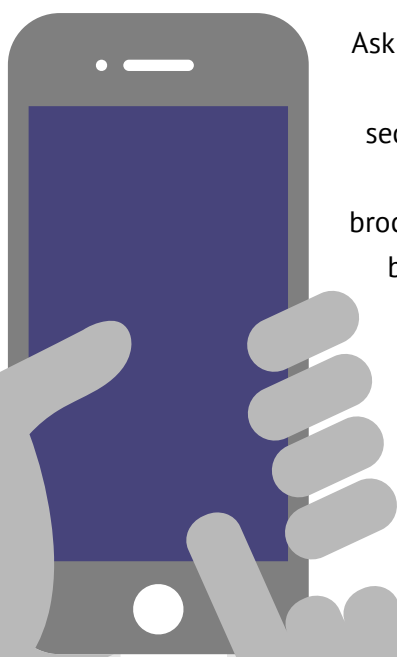
Never leave your laptop/mobile phone unlocked or unattended as criminals can transfer a virus to your device in seconds to record your future digital activities.



Ask the cafe staff or airport personnel on how to safely connect to their secured WiFi, as the password that is floating around (e.g. written on brochures, card or bulletin board) may belong to a rogue WiFi connection.



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



MALICIOUS WEBLINK

Whether a URL or weblink was sent via email, text message or social media post, make sure to double check if the link is genuinely what is said in the text.

Your password is due to expire in 8 days. Please consider changing it before this time.

You can change your password as follows:

www.bournemouth.ac.uk.fakewebsite.com

On Campus:

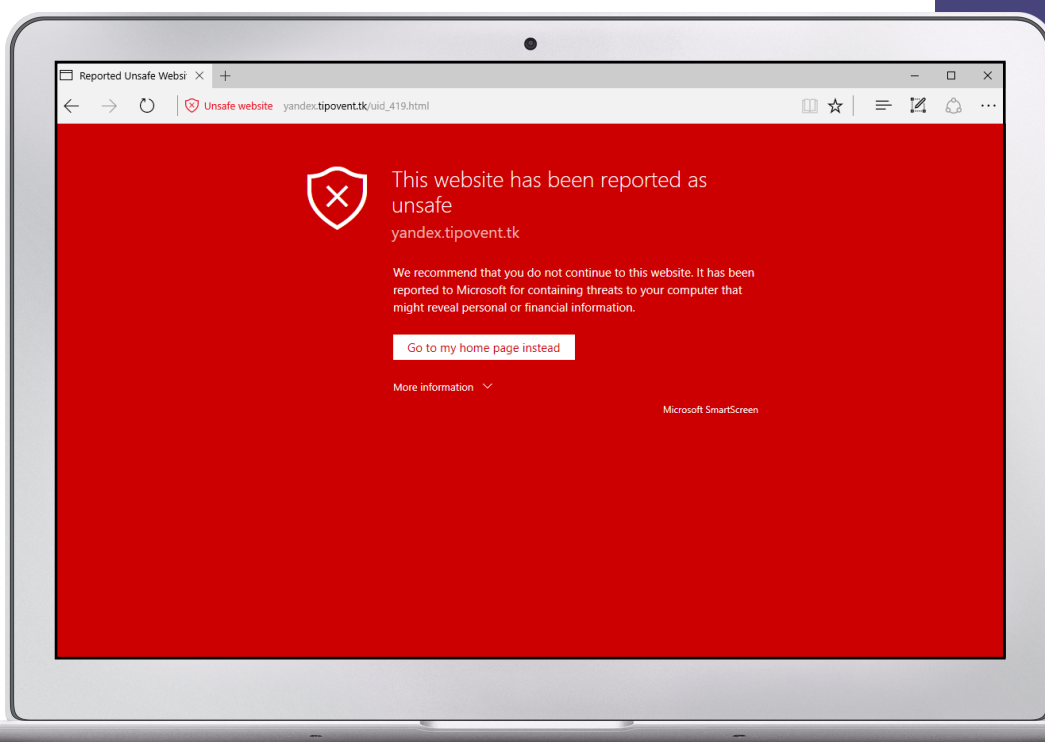
Ctrl+Alt+Delete - Logged on to a BU networked PC, press the 'Ctrl+Alt+Delete'

"Do not ignore an Internet browser's warning page when accidentally clicking on a malicious URL. Contact IT Services if you cannot justify whether a weblink is safe to click."

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. www.bournemouth.ac.uk

If unsure about the safety of the weblink, try to hover your mouse cursor on the URL to reveal the true web address. Otherwise, do not click the weblink and seek assistance from a colleague or IT.



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

WIPING A DEVICE WHEN LOST, MISSING OR STOLEN

Before using your Apple devices, such as Macs, iPads and iPhones, it is important to familiarise yourself on how to use Apple's remote wipe service. If you are not familiar with this service and need help, please do not hesitate to contact IT Services.

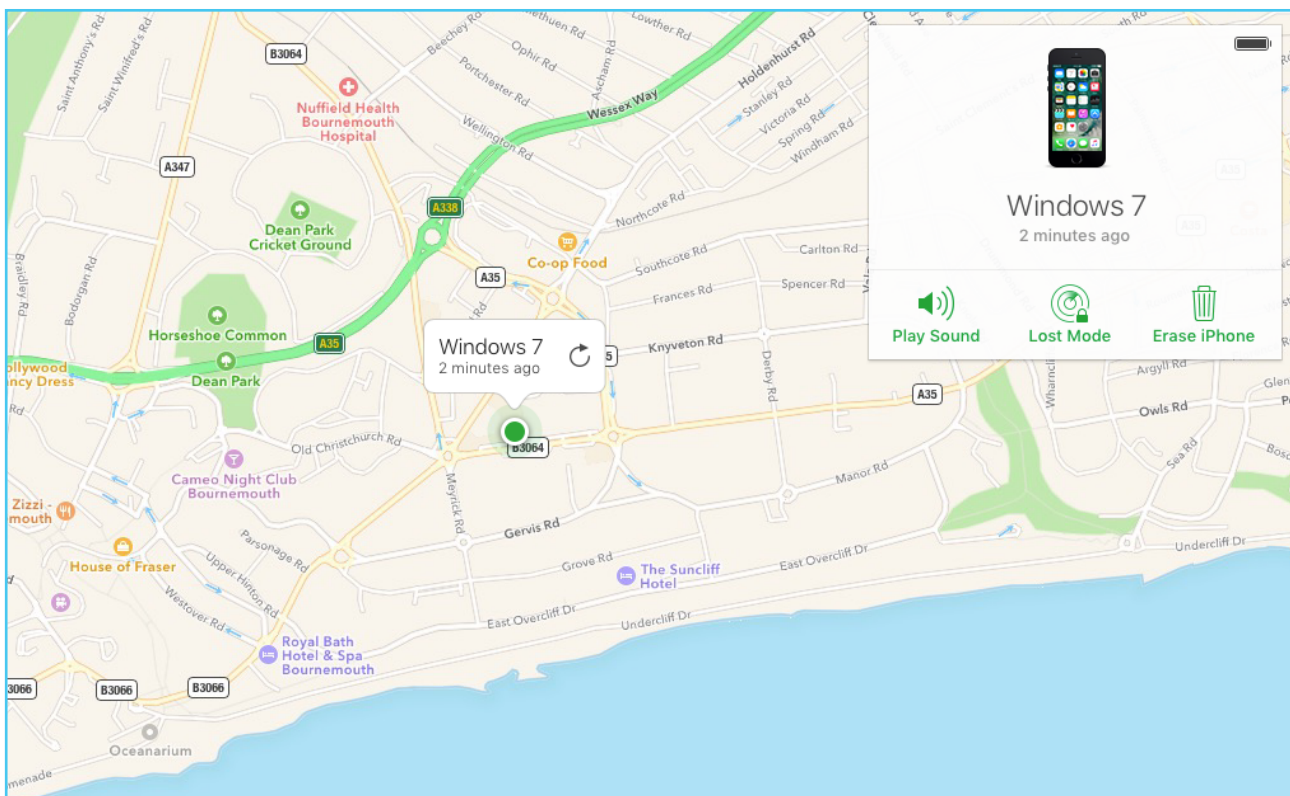
APPLE REMOTE WIPE

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**.

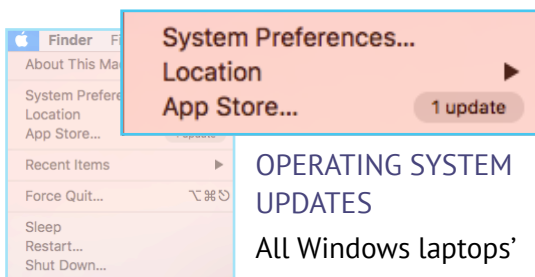
Note: At the time of writing this document, BU Windows and Linux laptops are not configured for remote wipe system so check with IT Services if the remote wipe feature is now available.



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 us to install any updates when it becomes available.



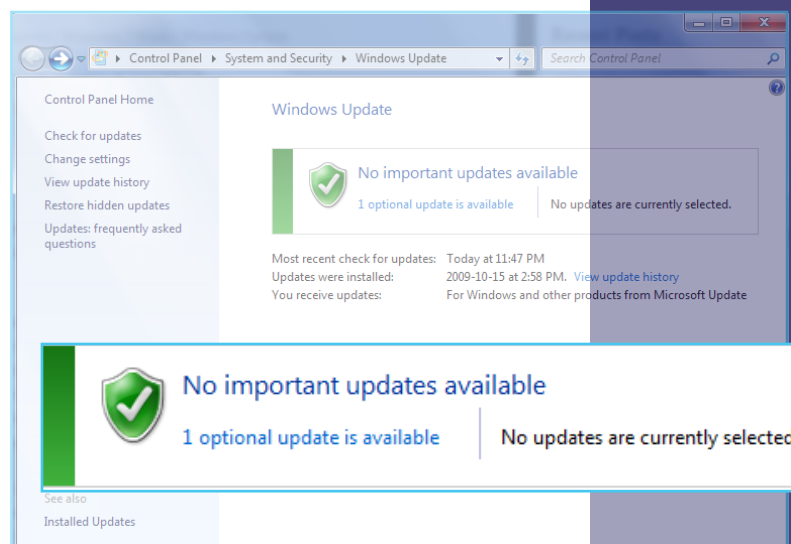
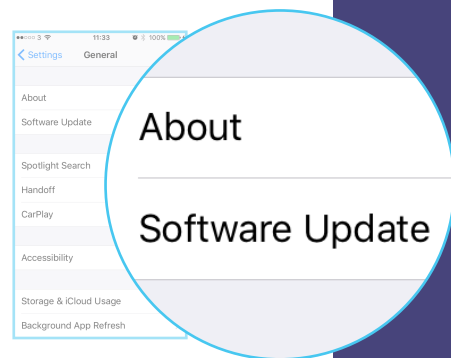
OPERATING SYSTEM UPDATES

All Windows laptops' updates are managed by

IT Services, but it is important to regularly connect your laptop to the BU network to receive the latest updates. For Apple devices such as MacBooks, iPads and iPhones, managing of updates requires your attention. However, IT Services is in the initial phase of developing a new system that will manage Apple devices' updates. We are running a scheme for early adopters, and if you are interested in becoming part of this scheme, then please contact IT Service Desk.

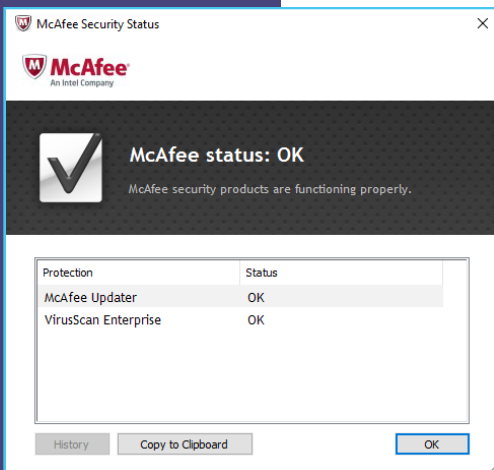
There are a number of ways to access update settings for **Mac OS X**, and the easiest way is to (1) click on the **Apple Menu** and (2) select the **App Store**. (3) When the App Store opens, click on individual update button or press the **UPDATE ALL** button to download all updates.

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 systems (e.g. Windows) but also all individual applications (e.g. MS Word). As for Windows laptops, IT Services is managing your application software updates but for Apple devices users have to update the applications manually. Many applications provide a helpful menu to guide their user on how to update their software, but if you need any help contact IT Services.

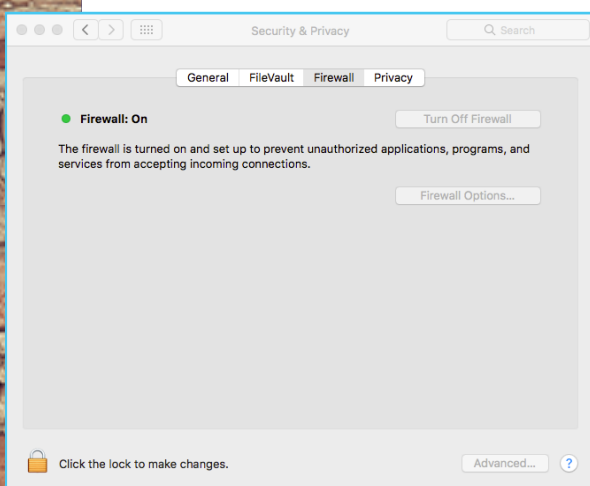


PROTECTING YOUR DEVICE FROM ATTACKS AND MALICIOUS SOFTWARE

Make a habit of scanning files that were last modified by someone before opening them. We use McAfee as one of our primary malware protection systems. If no anti-malware software installed on your

device or you notice the anti-virus software is not working properly, please contact IT Services.

"Do not rely on anti-malware and 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 of your mobile devices, contact IT Services and do not tackle malicious software by yourself."



Enable the firewall on Mac OSX

protection against this attack is the use of a firewall system, and fortunately, Windows and Macs(OS X) have built-in firewall system.

ACCESS THE FIREWALL

The firewall on your device should be on when IT Services handover the device to you; otherwise, please contact us for assistance. To enable your firewall on your Mac, navigate thru **System Preferences > Security & Privacy > Firewall**. For Windows, IT Services manage the firewall settings so please contact us if you notice the firewall has been disabled.

Firewall is a security system to protect your device from untrusted incoming and outgoing network traffic. Cybercriminals do not need to physically access your device; instead, they use the network your devices are connected with such as the Internet and launch an attack from a remote location. One identified

HABITUALLY SAVE BU FILES ON I:\ OR H:\ DRIVE

Backup all BU important documents, especially the ones that are hard and time-consuming to re-create. It is important to know that you should not be storing your documents locally on your device as it is not backed up and you could lose all your data. In addition, make sure not to back up BU documents on external hard drives (e.g. USB sticks), Cloud storages (e.g. Dropbox) and email as these are not

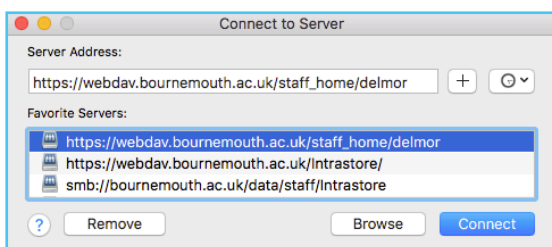
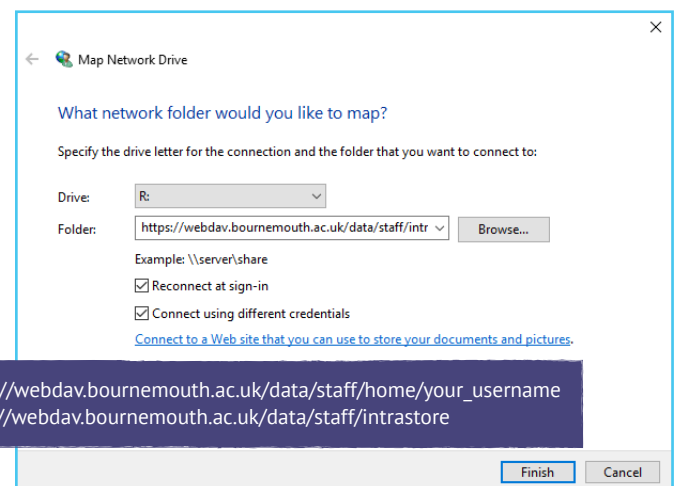
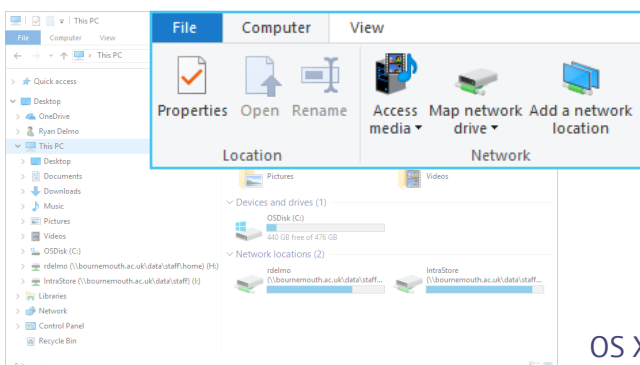
standard practice for BU to store BU information. Instead, use our network storage such as H or I drive as we regularly back them up just in case your files get corrupted, accidentally deleted or even if you want to go back to a previous version.

If you have an issue connecting to H or I drive, follow the instructions below or contact our IT Service Desk for more help.

WINDOWS DRIVE MAPPING

On Windows, both the **H** and **I** drives are pre-configured once you logon using your BU account. If for some reason you cannot access the networked drives, then, reconnect them again by (1) accessing the **Map network drive** in **Windows Explorer**. (2) Type in the web address

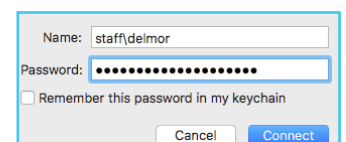
for H or I drive in the **Folder** field and tick the box for **Connect using different credentials**. (3) Click **Finish** and enter your IT account (e.g. staff\username).



OS X DRIVE MAPPING

To map either **I** or **H** drive on Mac(OSX) devices: (1) Open the **Finder**, and on the menu bar select **Go > Connect to Server** (2) In the **Server Address** field

enter the WebDav address for H or I drive and click **Connect**. (3) A pop-up window will appear, then type-in your BU username (e.g. staff\username) and password, and click **Connect**.



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** or raise a request/report a problem at **snow.bournemouth.com**

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.

www.bournemouth.ac.uk/knowledge-base

You can also chat us via **snow.bournemouth.com** to ask us questions or queries between 8:30am and 4:45pm Monday to Friday.