Information Booklet

COVID-19: Using Your WSU or Personal Computer to Work From Home (Windows)

ITDS
March 2020

Contents

Background

This document provides information about how you may be able to use your WSU or personal laptop/desktop to work at home throughout the COVID-19 pandemic.

Further information about COVID-19 IT related programs and services can be found at:

https://www.westernsydney.edu.au/covid-itds

This document expands on COVID-19 principles outlined in protocols available from:

Information Technology and Digital Services Protocols During the COVID-19 Pandemic

This document is specifically intended for those who wish to use their:

- WSU issued laptop (Windows)
- Personal laptop (Windows)
- Personal desktop (Windows)
- Any other laptop/desktop that is not a WSU Standard Operating Environment (Windows)

Any of these computers will be referred to as 'your device' throughout this document.

This document is not exhaustive and may rely on other sources information. This approach ensures that information can be kept current in its home location and in turn, provide more accurate information to you.

Need Additional Help?

If you need help, you can always call the IT Service Desk or search our online resources at:

https://www.westernsydney.edu.au/information_technology_services/its/servicedesk

Getting Internet Access

For many uses of your device from home, you will require access to the internet. To do this, you can either connect to the internet through:

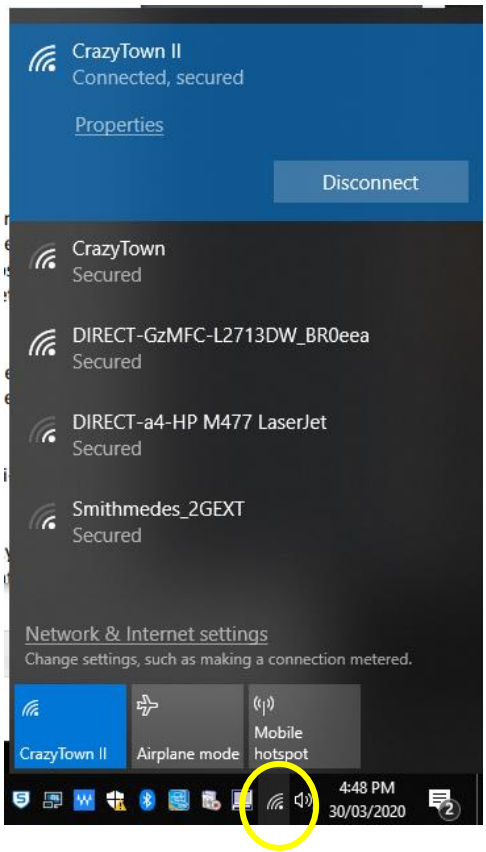
- Your home wi-fi network
- Your mobile phone

Connecting to your home wi-fi network

The most reliable and the fastest method of connecting to the internet from home will be to connect to your pre-existing wi-fi network (if you have one).

To connect to your home wi-fi network you will need to know the "Access Key" (sometimes called the password) used for your wi-fi network.

1. From the Windows Desktop, click the icon for internet access  in the bottom right of the taskbar. You will see a list of the available wi-fi networks (see image below).



PLEASE NOTE: that the wi-fi networks you see at home will be different to the ones shown in the pic above

2. Select your home wi-fi network, and enter the access password. If you enter the password correctly, this should connect you to the internet through your home wi-fi network.

Connect to your mobile phone 'hotspot'

If you do not have a home wi-fi network you may be able to use your mobile phone. This is called 'tethering' as your device is tethered to your mobile.

When using this method, you need to be aware that you will be consuming your data-allowance provided by your mobile phone provider. If you exceed your data-allowance, you may incur charges from your mobile phone provider. These charges are not covered by the University.

Please refer to your phone provider for any concessions available during the pandemic.

There are many mobile phone devices. To find instructions on tethering to your particular phone, you should consult the manufacturers guides or use a search engine to determine the steps.

Access to software

Many WSU staff require only a standard suite of software to undertake their duties. This makes it easier to work from home.

There instructions below about commonly used products to help you:

- install the Microsoft Office suite of products
- find information about installing/using Citrix

Microsoft Office (Word, PowerPoint, Outlook, etc)

Using Microsoft Office suite of software (e.g. Microsoft Word, Excel, PowerPoint, OneNote etc.), has never been so easy. You have two choices:

- You can use the online version (browser based); or
- You can install the software onto your device.

Installing on your device

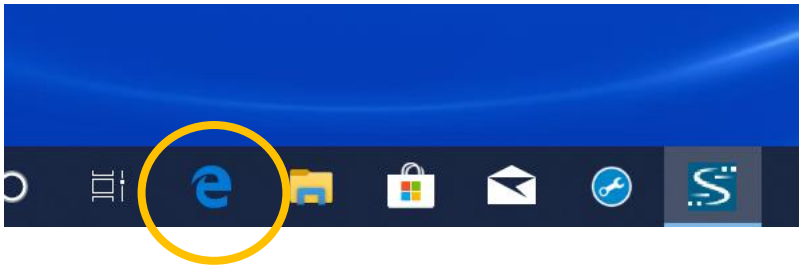
Installing office on your own device will give you greater functionality and the performance will be more reliable.

PLEASE NOTE: It is recommended that you install Microsoft Office using your home wi-fi internet access. Whilst possible, it is not recommended that you install Microsoft Office if accessing the internet through your mobile phone. The installation will consume a significant

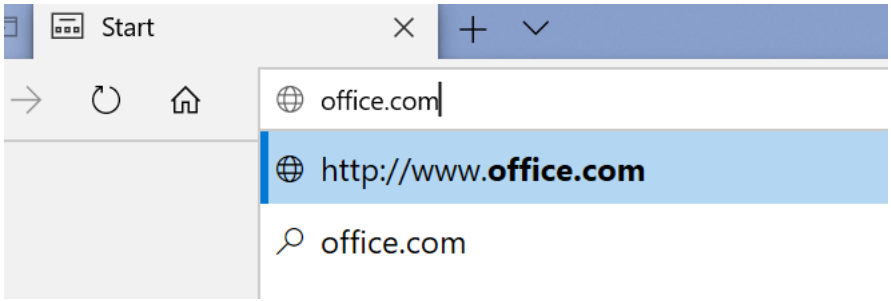
quantity of your data allowance and will be slow. If you don't have a home wi-fi internet access, you could use Microsoft Office online. Just visit www.office.com and 'sign in'.

Once connected to your home wi-fi internet connection, to install and use Microsoft Office on your device follow these steps:

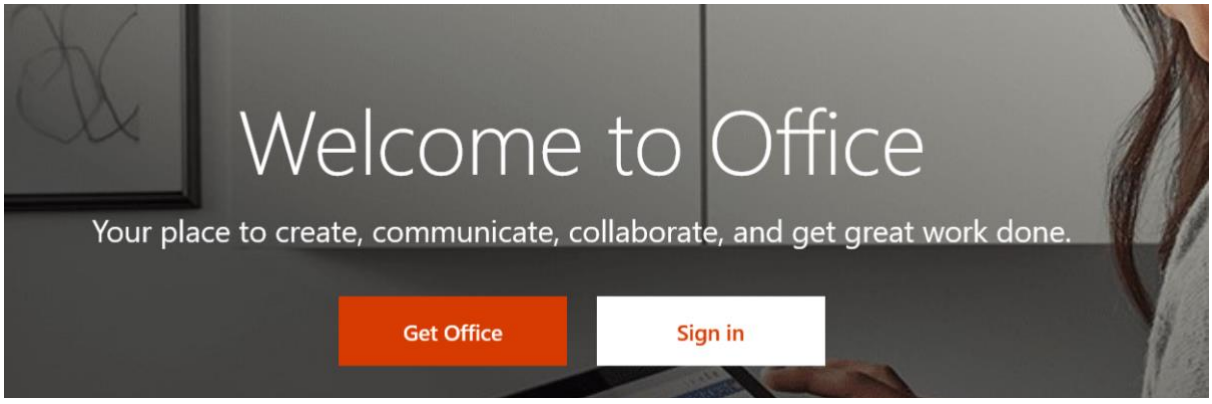
1. Open an internet browser (Microsoft Edge is pre-installed on the laptop).



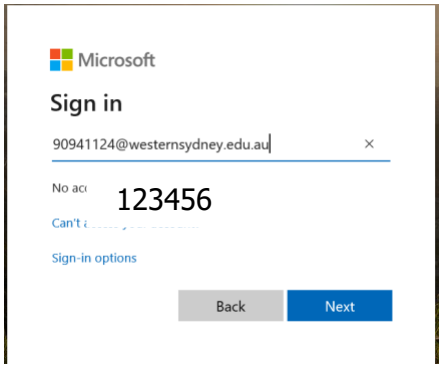
1. Navigate to www.office.com



2. Click "Sign In"

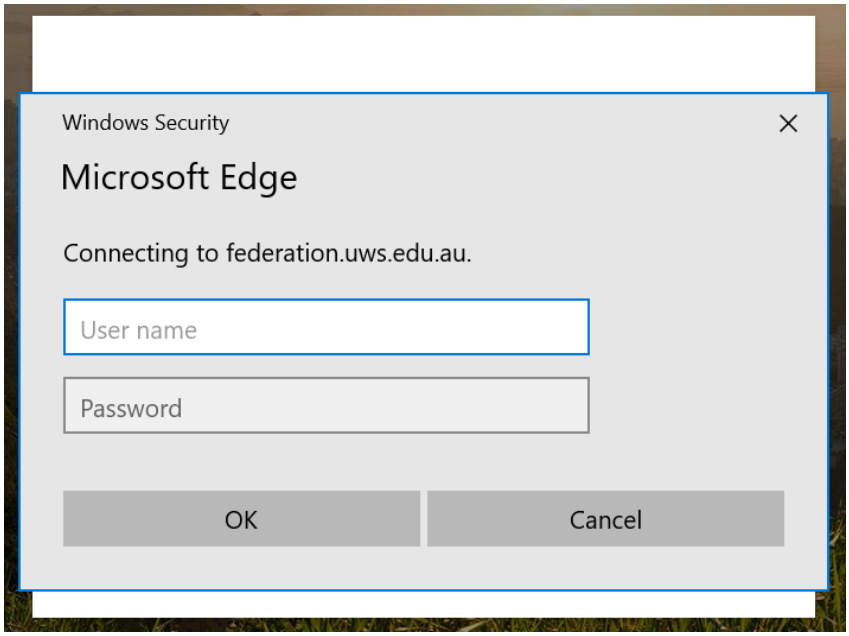


4. You Microsoft Login is your staff ID Number, followed by "@westersydney.edu.au"

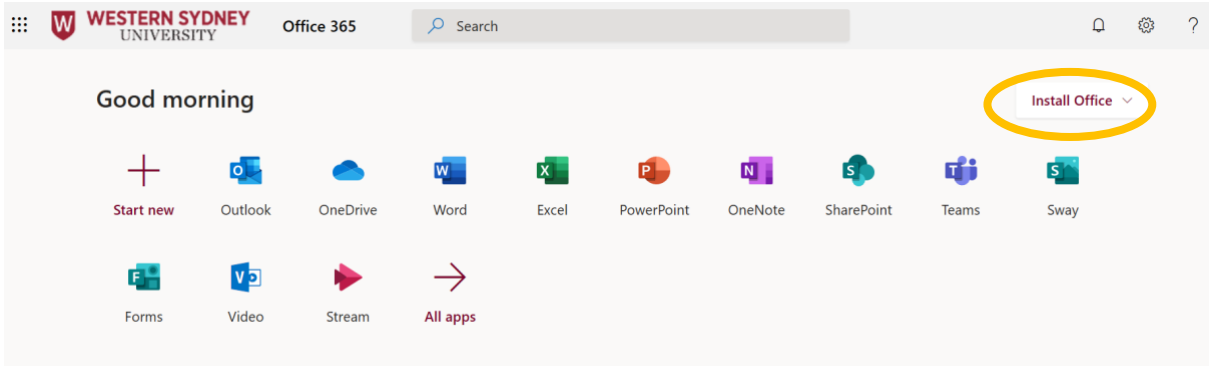


5. You may be asked to authenticate and enter your username again. This time the details are:

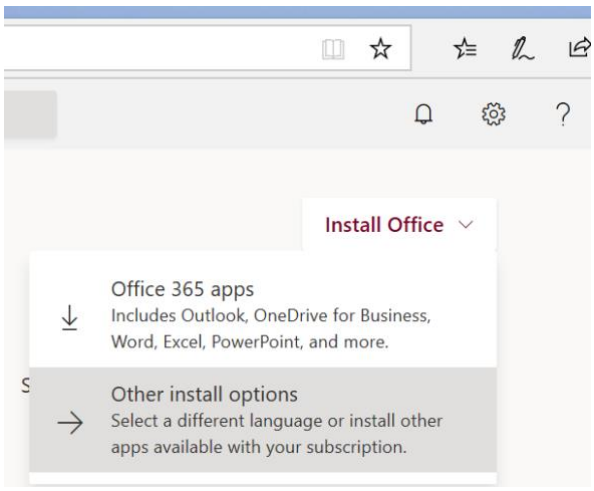
Login Details:
Username: Your staff number (nothing more)
Password: usual WSU Staff Number



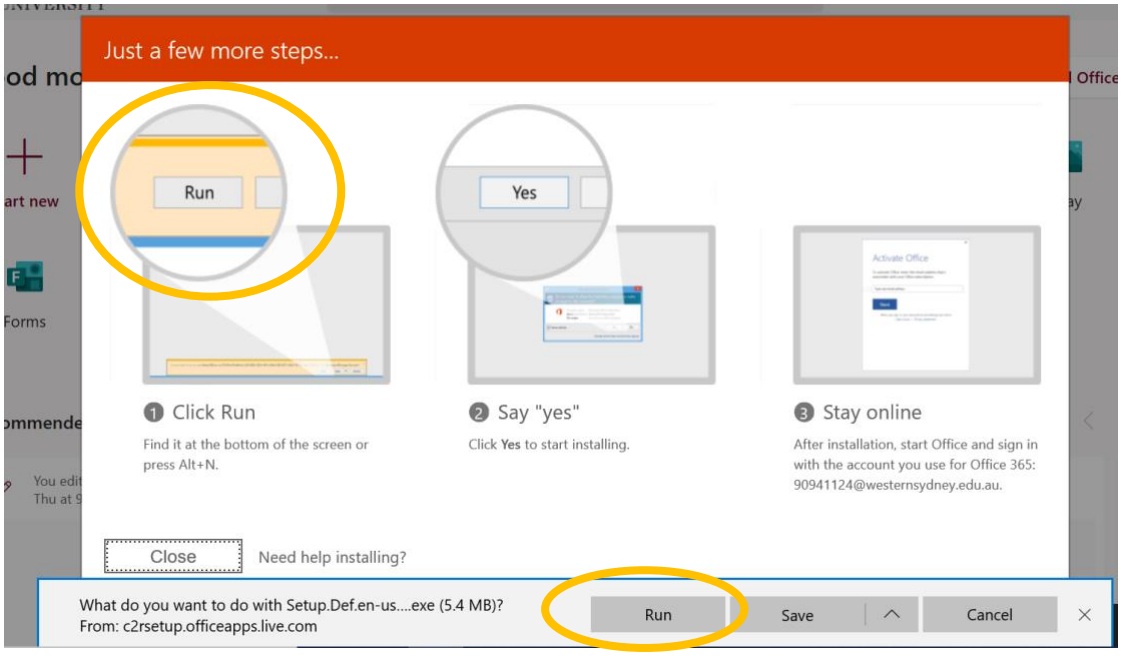
6. With the correct username and password, you will be taken into Office Online. Select "Install Office" in the top right of the window.



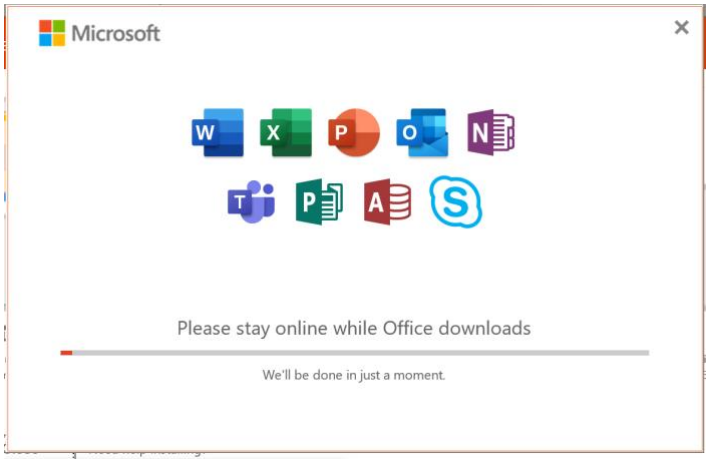
7. Select "Office 365 Apps"



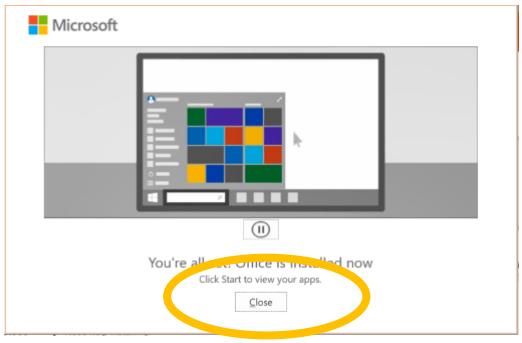
8. Click "Run"



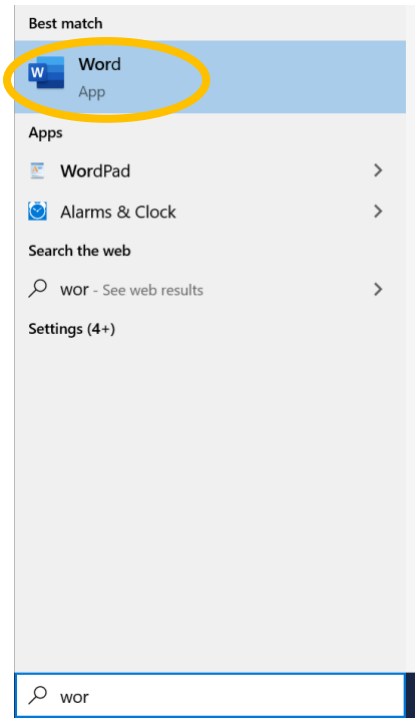
9. The Microsoft Office installer will start. The installation will take some time, depending on the speed of your internet connection. Just leave the installation to run



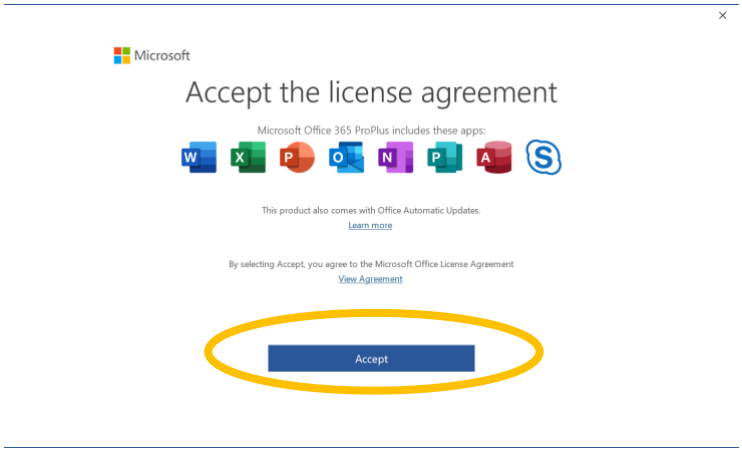
10. Once the installation is complete, you will see a confirmation message. Click "Close"



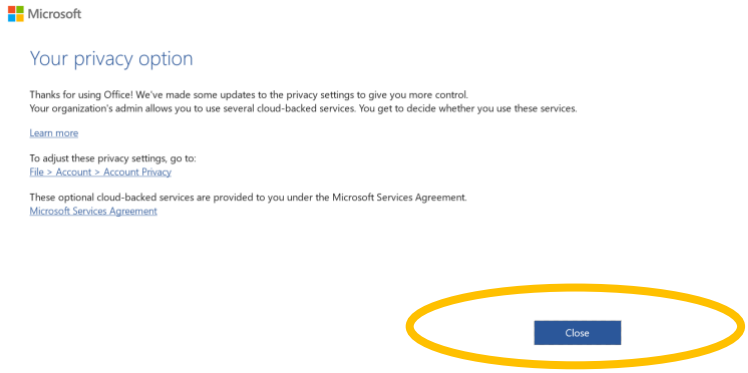
11. You should now be able to run any of the Microsoft applications. Click the windows icon at the bottom left of the screen and type "Word" (or Excel, PowerPoint, etc) and the icon for Microsoft Word should appear.



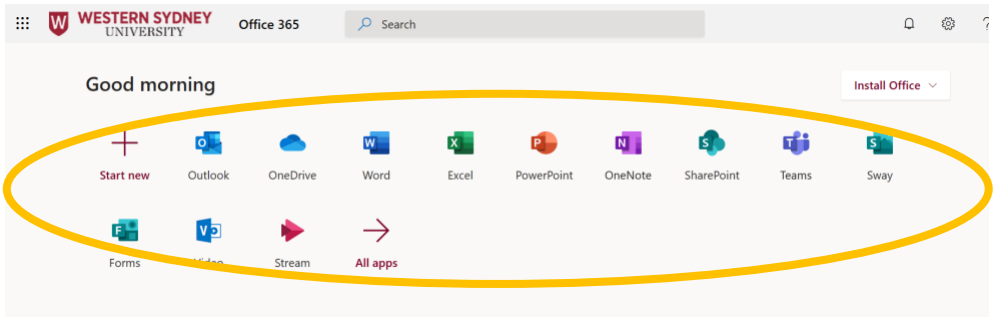
12. Accept the license agreement



13. Acknowledge the Privacy Information, and click "close"



That's it! You should be up and running with the Microsoft suite of products Remember, you can always use Microsoft Office online if you get stuck. Go to www.office.com and sign-in. Click any of the icons to use the online version of that product.



Citrix

Citrix enables you to run University applications without having to install them on your device. To use Citrix all you need is a connection to the Internet. You do not need to connect to the University network using the VPN solution outlined previously.

To access Citrix, simply point your web browser to:

https://access.westernsydney.edu.au/logon/LogonPoint/index.html

Mac & tablet (iPad & Android) users that have compatibility problems accessing network folders, Staff eForms, Basware, Staff Online, MS Office and other applications, can use Citrix for a reliable, supported, and compatible experience.

In-depth instructions about how to use Citrix are contained in the knowledge base article: KB0014262.

Other software & devices

You may need other software to undertake your role. There are many software packages used across Western – too many to list. Should you require additional software (including QMaster or NEC Softphone), the ITDS Service Desk may be able to assist.

In most cases, other software will require that special software be installed to create a "Virtual Private Network" that allows your device to talk directly with the WSU network. Access to other software and the VPN will be arranged on a case by case basis. The ITDS Service Desk can assist.

Please note that the COVID-19 response is extraordinary and as such there may be situations whereby some software simply cannot be installed on, or is incompatible with your device.

University Call Centres & QMaster

The University will continue to operate its call centres on campus as long as it can and in the event of a closure, remotely where possible. The call centres are:

- Contact Service Centre
- Student Central
- Transition Success
- Western Success
- Client Services
- Team Student Experience, Administration and Enquiries
- IT Service Desk
- Human Resources

Staff in these call centres are considered critical forward-facing staff and as such, special technology considerations will apply in terms of laptop distribution, telephony support, etc. Staff in these areas should contact the ITDS Services if they require assistance.

Security: Safe & Secure Practices for Working from Home

Along with your health and well-being, it is equally important to ensure that you are individually secure and the University remains free from compromises. It is crucial that we work together during this time to protect our information. Here's some information and resources that ITDS have developed specifically to assist University staff in protecting themselves, their friends and family, and as a result the University at large

As we know, scammers are opportunistic and will use the COVID-19 pandemic to take advantage of staff and students. The simple rules are, make sure you:

- Run virus/malware protection software on any computer you use to do university work (all University-issued devices have this by default);
- Be extra vigilant for email phishing; and
- Report anything suspicious via the IT Service Desk.

Here some more tips from our **ITDS Security Corner** to help you when working from home:

Is your Antivirus Software Up-to-Date?	**Learn More**
University laptops come with antivirus installed, but If you're using a University laptop away from campus for an extended period of time, make sure that the antivirus is up-to-date. This will be the same for personal laptops, particularly as you will be using University systems and applications. It is important that you are protected. There are several trusted vendors such as: Sophos, McAfee, Norton, Bitdefender, Avast, Avira and Kaspersky. Still don't know which software to choose? The University currently uses Sophos for securing out desktops and laptops, and we have an arrangement offered through Sophos to provide the software to University employees for free. Please see the link provided.	Sophos Commercial Home version - (University email required)
Keep your Software up-to-date!	
It is equally important to keep your operating system and applications up-to-date, it will protect you being hacked. Try to make it a priority. By updating your devices, you will ensure that you do not have any vulnerabilities (weaknesses in software) so hackers, malicious programs or viruses will not exploit your computer or devices.	Software Updates | StaySmartOnline

Storing your Devices!	**Learn More:**
Make sure your devices are locked (or otherwise not accessible) when not in use – even if the device is a home computer, you are accessing University systems. Whether working on campus or from home, it is our collective responsibility to ensure personal and sensitive data held by the University isn't breached.	Storing your Devices | StaySmartOnline
Backup your Device Regularly	**Learn More:**
It is best practice is to make backups regularly. For University devices such as laptops, backups happen automatically whenever you're on campus. But, if you're going to be spending some extended time away from Campus, please note that this will not continue to happen. For personal devices, backups should be stored separately to the device itself, so that they can be accessed and used if the device is damaged, lost, or compromised.	World Backup Day Backups | StaySmartOnline
Don't Take the Bait! Phishing Scams	**Learn More:**
Phishing is a scam to try and steal your identity, your money, or both. Don't get hooked! Protect yourself and others: Be smart, be sceptical, be secure. • Avoid clicking on promotional links in emails • If there is general information that can be 'googled' and found, do that instead of clicking on a link from a suspicious sender • Don't click on baits such as an '80% discount on an exclusive cure' or 'treatment for coronavirus' • If unsure about the authenticity of a website, do not proceed with any login procedure	Email Security | Don't Take the Bait How to report Phishing and Spam email to ITDS
Sensitive Information	**Learn More:**
Take extra care to ensure the security of sensitive data when handling it away from campuses. University staff have responsibilities – including legal responsibilities – when it comes to handling data that is proprietary, sensitive, personal, or related to healthcare. If possible, place University data and documents you use for work in University storage (OneDrive, SharePoint, etc) so that you can avoid saving any copies of personal or sensitive data to a personal device. If you're not connected to the internet or this is otherwise	Confidential and Sensitive Information Considerations for Staff Personal Information and Privacy | StaySmartOnline Saving Docs to a SharePoint Portal

impossible, ensure any University data is removed from any personal device(s) used in the interim once you're back on campus. This also applies to any backups made during this time.	Microsoft Office | Saving Documents to OneDrive in Windows 10
WSU Cyber Security Learning Module	**Learn More:**
A Cyber Security overview training module has been procured by ITDS for all University staff. The module is called **'Cyber Security at Western Sydney University (Basics)'** and is accessible to University staff through MyCareerOnline and vUWS. Searching for 'cyber security' in MyCareerOnline will produce the module. Staff without access to MyCareerOnline, can enrol themselves in the vUWS site.	How-to-Access (PDF) Or visit ITDS' Security Corner website.

You can find more resources on the WSU website and WesternNow respectively, such as:

https://www.westernsydney.edu.au/covid-itds

Working Remotely – Help for Staff.