Cybersafety@home

Working safely from home during COVID-19
The effect of COVID-19 on cybersafety and remote working

COVID-19 has forced most of us to work away from campus. This means our home internet, personal IT equipment and perhaps even the family dining table have been co-opted to support our work lives. Few of us are set up to work from home for sustained periods. And some do not have the means to work remotely at all. This is made more difficult because of the inherent uncertainty generated by COVID-19 itself, and the toll it is taking on our households and community.

This unprecedented mix of technical and psychological challenges has made our working lives more complicated, and more vulnerable to cybersecurity threats. Threat actors use circumstances like COVID-19 to seek and exploit vulnerabilities in people and our systems. So unfortunately, the steep rise in remote working has been equally matched with a rise in cybercrime targeting us in our homes.

You won’t be able to call the ANU service desk with matters affecting your home network. So, each of us is now in effect the Chief Information Security Officer for our homes. It is not an easy job to do on top of other personal and work challenges. For many of us it may be the first time we might be thinking about cybersafety at home.

As remote workers we no longer have the inherent protection of the ANU campus network, however there a range of practical things we can do to reduce the potential for cyber-attacks against our home networks and IT equipment. This guide is designed to give you advice on how to think about security and practical steps on how you can work safely from home.

Congratulations! You are now the Chief Information Security Officer for your home network and remote workplace.
Thinking about cybersafety@home

Many of the cyber threats we face on campus are equally applicable in our homes. It is just that we often do not associate being a target with our home internet use – it is not an easy thing to think about. With the lines between home and work now blurred, it is useful to take stock of the things which make us targets for cybercrime.

Why are we targets in our own homes? For most of us, our home network security will not be as robust as our usual work environments. We usually use consumer grade technology with varying degrees of manufacturer support. Threat actors know this all too well. Also, we are now communicating potentially sensitive information from home that we would not usually do. Again threat actors know this.

So, your role at the ANU, your access to information, stresses from COVID-19, potential vulnerabilities in your home IT infrastructure and the prevailing threat environment add up to more ways and reasons to target you for cyberattacks.

To help you think about the cybersafety, while working from home, here is a list of potential threats you are most likely to face in your new (hopefully temporary) workplace:

- **Theft of credentials and passwords.** Credential theft is still the number one goal for threat actors.

- **Phishing.** Using malicious attachments and links in seemingly legitimate emails remains one of the most common methods of compromising your IT. Unsurprisingly COVID-19 themed phishing emails are increasingly common.

- **Exploitation of software vulnerability.** Threat actors exploit weaknesses (known as vulnerabilities) in the operating systems, hardware firmware and applications to gain access to your IT, online services or data.

- **Accidental data disclosure.** Unfortunately, each of us, as users, are a type of threat too. We are busy, worried, trying to balance work and life inside the confines of our homes. So we will make mistakes particularly as we juggle between cloud services, work and personal online services or sharing platforms.

- **Social engineering.** Threat actors don’t just hack systems, they hack people. Scammers use voice calls, emails, social media and websites (to name a few) to try trick you into revealing sensitive or personal information, credentials or to try and make you do something you would normally do like a money transfer or buying iTunes cards.

- **Theft or loss of equipment.** With social isolation, you are unlikely to take your laptop out of the house or be out of your home for an extended period. It is a slim probability but one worth keeping in mind.
As with any form of risk management, it is important to assess to what degree each of the above is applicable to you; and the potential harm to your IT infrastructure, your home users and your work at ANU. Consider what mitigations you may already have in place and use this guide to introduce new ones. The analogy would be the systematic assessment you might do for your home physical security before leaving your home for a vacation, e.g. checking locks, arming your alarm, telling the neighbours.

In thinking about these technical safeguards, it is useful to think of them as layers. Imagine an onion with your most valuable digital or IT assets at the centre. Each layer of protection you add builds on the other layers; providing what is known as defence-in-depth. The more depth you have, the more secure your home network will be. And you don’t need to do it all at once, some layers will be more important to you than others depending on your specific situation. All this needs to be weighed up against usability.

Some of us will be using an ANU issued device. In this situation, some of the mitigations needed to protect you from the above threats are already in place for your issued device. However, even with an ANU issued device it is also important to consider the safety of other users in your home and the other devices connected to your home network.

Start by thinking about the ways in which your home network, or the work you do remotely, could be compromised.

Remember as you read this guide, you don’t need to do everything all at once, layers of security can be gradually introduced.
Passwords

There is a simple reason for threat actors going after our passwords: most of us aren’t very good at remembering them. Given the number of passwords we need for work and home, it can mean trying to remember a dozen or more credentials – it can get cumbersome and tends to make us use and reuse simple passwords. Thankfully there are some measures we can put in place to help us secure our passwords.

- **Use a password manager.** We are not talking about post-it notes stuck to you monitor. We are talking about software you can install on your device, a browser plugin or use online, which will generate secure passwords and store them in a secure “vault” either on your computer or in a cloud service. You need only then remember the single password to unlock your vault.

  These products can integrate with your browser and auto-populate the fields on a webpage needed to login – much better than post-it notes. There are free and paid versions of password managers and here is a link to a recent review of some of the major ones: [https://www.digitaltrends.com/computing/best-password-managers/](https://www.digitaltrends.com/computing/best-password-managers/). Some of these options will also have versions for mobile platforms.

  For those staying solely within the Apple ecosystem, there is a built-in credential manager called iCloud Keychain. ANU is incrementally rolling out an enterprise password manager for managed devices, in the interim managed users can use a Chrome plugin-based password manager.

- **Use secure passwords.** Many of us have heard about the need to use secure passwords, but what exactly makes a password secure? A secure password is one which has enough length and/or complexity so that it is not easy to guess or break through password cracking techniques. So, passwords which you might draw from a dictionary of commonly used words like “insecure” are easy to guess using password cracking software. Simple passwords like “password123” are also trivial for threat actors to guess or break.

  - How long should a password be? 14 or more characters is ideal. This need not be random characters; it can be four or five words joined together (called passphrases) like the select words out of favourite songs or just plain random like “dreamfreedomnightfadingflower”. There are many online random word/passphrase generators.

  - What about so-called complexity rules? These are rules which enforce the use of numbers, special symbols and upper and lower case characters. Some websites enforce these rules, but length tends to trump complexity, and these rules are slowly being replaced because they are difficult to remember or use. A good password manager will generate secure passwords for you.

  - How often should we change passwords? Each service you use will determine its own rules for this, but generally, it is 12 months. Barring a security event, ANU will only enforce passwords resets once a year.
- **Use multi-factor authentication where it is offered.** Many sites and services offer multi-factor authentication. This is usually a two-step process using a security token, SMS or dedicated mobile app which will ask you for an additional piece of information. Sometimes this is a biometric validation or a sequence of characters sent to you privately. It makes the chances of threat actors breaking into your account much lower. Wherever it is offered, it is highly recommended you use it. You may also wish to consider adding multi-factor to your home devices. Windows and MacOS have in-built and third-party options. Sensitive accounts at ANU already use multi-factor authentication and will be expanded to other users incrementally.

- **Check to see if your credentials have been compromised.** There is a very high likelihood that at some point, one or more services you have registered with will be compromised and your details stolen. This may mean your username and passwords have been compromised or perhaps even your personal information. So it is highly recommended that you periodically check at websites like [https://haveibeenpwned.com/](https://haveibeenpwned.com/) to see if your credentials have been stolen. Some password managers have a built-in service to check for you. If your credentials have been stolen change your password for that service immediately and any other service where you may have used the same or similar passwords. Again, using a password manager overcomes the reuse of passwords.

- **Don’t share your passwords.** If you have a legitimate need to share a password within your household, consider choosing a password manager which has family account functionality.

Password hygiene is an essential element of the cybersafety for your home network.
Device protection aka “endpoints”

Each device attached to your home network is referred to as an endpoint, i.e. a device at the end of the chain linking back through the internet. So, you may hear that endpoint protection is an essential element for cybersafety – and it is.

Protecting computers on your network is reasonably straightforward. There are security programs called internet security suites, which provide antivirus and other protective measures for your device, which can be installed on each of your devices. Ideally, each computer or mobile device should have some form of security software installed.

If you have a managed ANU device, then this form of protection has already been installed on your machine. But you should also consider protecting the non-ANU computers on your network.

ANU used to provide a home licence for staff, but the vendor has replaced this program with their free version. Many vendors offer free and commercial software that you should strongly consider for your home computers and mobile devices. Here is a link https://www.av-test.org/en/ which provides extensive comparisons and regular testing for most commercial and free offerings. From this page choose the platform you are interested in from the “Tests for home users” section.

It is recommended choosing one that is easy to manage, not too heavy on system resources and has a high detection rate for viruses and malware. Once installed, ensure the software is configured to do regular scans of each of your devices.

Computers and mobile devices are not the only things that might be attached to your network. Smart TVs, speakers, home automation, smart hubs, alarms, medical equipment and personal devices like fans and heaters are just some examples. We often refer to these devices as IoT – the internet of things. For such devices, you will need to consult with the manufacturer’s guidance on how to secure them.

Look for a reputable internet security product for your computers and mobile devices.
Encrypting your data

Encryption for data stored on physical media or online is an effective safeguard against data theft, particularly if you are at risk of having your device lost or stolen. Major operating systems have some form of built-in disk encryption. Windows has Bit Locker, MacOS has File Vault and many flavours of Linux use dm-crypt. There are also a range of 3rd party providers (free and commercial) that you may wish to consider. In addition to your devices, you also consider encrypting external drives if you intend to store sensitive data on them.

Another consideration is the encryption of your data that being communicated over the internet. ANU has made available our enterprise VPN client, called Global Protect, for use on your personal devices. This can be downloaded from staff-access.anu.edu and replaces the AnyConnect VPN client you may have used before. Global Protect has already been installed on all ANU managed devices. Global Protect only encrypts traffic between your device and ANU and passes through our University firewall – gaining all the security benefits of our firewall. The Global Protect VPN needs to be running in order to access secure resources like your share drivers. Should you require any assistance in mapping share drives or using Global Protect please contact the ANU IT Help Desk.

Should you not have Global Protect installed on your managed device or you still have CISCO AnyConnect then contact the ANU IT Help Desk for guidance.

All other (personal) traffic uses the normal unencrypted pathway between your device and the internet. For privacy reasons personal traffic does not go through ANU firewall nor gains any additional protection even if Global Protect is running in the background.

You may consider purchasing a separate VPN service for general (non-ANU) internet traffic. These services are subscription-based (but often have free trials) and require you to install software on your machine. Using a third-party VPN solution will mask your IP address which reduces the likelihood of your home internet traffic being subject to unauthorised monitoring. Many VPN users use these services for anonymity and privacy as well as security.

Consider using a VPN for general (non-ANU) internet usage and encrypting your devices.

Always use the ANU Global Protect VPN when accessing ANU resources like share drives.
Storing and backing up data

We have all faced losing data at some point - it happens a lot. It may be due to threat actors installing ransomware on your device or due to device failure, theft or destruction. Devices can be replaced, but it is much harder to restore data that has not been backed up. So, it is highly recommended that any important or sensitive data be backed up regularly to some external medium, e.g. a USB drive or a reputable online service – ideally to several different locations.

There are many commercial and free back up services that you can search for. Some security suites include such services as part of their subscription. Additionally, Office365 subscriptions, including the ANU version, (https://services.anu.edu.au/information-technology/email and then select Office 365 login) come with OneDrive and Apple users can access iCloud.

Where possible do not store ANU data on your personal devices. When using your personal device for work use the ANU share drives, which can be accessed via VPN, or use your ANU OneDrive account - the ANU IT Help Desk can provide assistance on both these capabilities. Data which is stored on ANU share drives and ANU OneDrive will automatically be backed up.

Depending on how your ANU managed device has been configured, files stored in locations like your desktop may not be automatically backed up. To ensure that important files are backed up save your files to either your ANU home drive or a shared drive. These locations will be routinely backed up by ITS. Should you require assistance in setting up your managed device or guidance on how your specific machine has been configured please contact the ANU IT Help Desk.

Ensure all sensitive and important data is backed up.

Store ANU data on ANU share drives or your ANU OneDrive account.

Patching your devices and software

Almost all software and hardware, at some point in their lifecycle, has had vulnerabilities. These are unintentional weaknesses in coding or construction of a device or software which if exploited, will allow a threat actor to gain unauthorised access to devices and data. To counter the risks which arise from this type of threat you should:

- **Ensure your devices are using the most up to date version of the operating system and applications.** The hardware on your devices also has built-in software called firmware as well as specialised software called drivers to make them work. You should also update your device firmware and driver software by going to the device manufacturers website and following the instructions for your specific device. Operating systems like Windows, MacOS and Linux also have built-in update mechanisms for the operating system and drivers, as well as some applications, but usually not firmware.
- **Ensure devices, applications and operating systems are supported by the developer or manufacturer.** In addition to installing updates, you should (unless it can not be avoided) only use currently supported products. Older, unsupported, products often have many unpatched vulnerabilities as the manufacturer may no longer be releasing updates.

- **Ensure your non-computer devices are also patched and supported.** TVs, network-connected hubs, home automation, alarm systems and internet modem/routers all follow the same rules as normal computers. Anything that has a network connection is worthy of closer inspection. For routers and modems, you may need to contact your internet provider if you have purchased the equipment from them.

Here is a great online guide for patching your operating system, it also includes some suggestions for third party software that can help keep your device up to date: [https://www.av-test.org/en/news/software-system-updates-for-more-security](https://www.av-test.org/en/news/software-system-updates-for-more-security). iOS and Android devices have built-in notifications for system updates and use their respective app stores for application updates. The same patching rules apply to these devices.

If you are using a managed device updates are generally pushed out monthly and your machine will automatically update, provided you are connected to the internet. Should you notice that software on your managed device is out of date or vulnerable please contact the ANU IT Help Desk as soon as possible – in some cases ITS will need to remotely administer your managed device to update software.

Ensure all your devices are supported and fully patched.
Email protection and phishing

Email scams and phishing are the most common method of compromise. We all use email, and we don’t always pay attention to every email we receive, particularly when we are busy or under stress. Threat actors know this and exploit it every day.

The best possible defence is our own awareness and vigilance. Pay attention to the emails you receive, if it doesn’t seem right, it probably isn’t. Validate unusual requests from emails purporting to come from supervisors or co-workers. A simple scam technique is to send a fake email from an address which looks, superficially to be genuine. For example some mail clients may display the email Vice-Chancellor@hackermail.com as simply Vice-Chancellor – which is also how it would display the legitimate address of vc@anu.edu.au. To avoid this, expand all email addresses to validate the sender – particularly on mobile mail clients. If you are busy file or junk the email to be read later when you have more time and can validate the sender and content.

There are, of course, also technical safeguards. Your ANU email already has quite a range of security measures activated already to guard against phishing and scam emails. We have filters designed to cut out spam and systems which catch malicious content. This is in place irrespective of which mail client you use or even if you use webmail. If you are using the same device to access your personal email and your ANU mail, it is possible to cross-contaminate malicious attachments and emails.

For the safety of your home network and users, we highly recommend that you invest in a security product which includes email protection. Most of the major ones do, and there are also dedicated mail security products for users with more sophisticated setups. Again there are some suggestions you can find in the Home users section at https://www.av-test.org/en/.

Expand out the email address of the sender, particularly on mobile devices, to validate addresses of suspicious emails.

Be vigilant about the emails you receive, trust your instincts if an email looks suspicious and strongly consider email protection.
Firewalls

The ANU network has a device at its perimeter called a firewall which is designed to control access to our network and block malicious content. Your home network may or may not have a similar setup. You may have a modem router provided by your internet service provider. Many of these devices have built-in firewalls and if configured correctly, will help protect your whole network. So, it is worth talking to your internet provider about your equipment, and they may have advice on how best to secure your modem router. If your router setup does not have a firewall, consider replacing it with one that does.

Also available are software-based firewalls which can be installed as part of a security suite. It should be noted that these will only protect the devices on which they are installed and usually will not cover non-computer type devices. Windows, MacOS and most Linux distributions also have built-in firewalls but may require some configuration.

Wi-Fi protection

Most of us use Wi-Fi at home, and like any other part of your home network, it requires some configuration to protect it from misuse. Almost all Wi-Fi access points or wireless routers will allow you to choose what is known as the security protocol. The correct one to choose for most situations is called WPA2 with AES encryption. Do not use WPA or WEP as these are known to be vulnerable and may not even appear as an option. More sophisticated setups, e.g. a RADIUS server, are beyond the scope of this guide.

You will need to set a password for your Wi-Fi and the password rules, as per the password section, still apply. You most likely will need to set an administrator password for accessing the administration interface of your wireless router or access point as well as a password for the actual Wi-Fi. And as per the section on patching, the same rules apply to your Wi-Fi access points and routers.

If you are comfortable doing so, you may also wish to change the default IP settings for your Wi-Fi access point or router. Threat actors tend to try default settings as a starting point. And we also encourage you to disable any features which allow remote access to your Wi-Fi access point or router.

Choose WPA2 with AES as the security protocol for Wi-Fi and choose a secure password.
Teleconferencing

By now, most of us are using teleconferencing daily for work and keeping in touch with our friends and family. ANU provides two enterprise supported teleconferencing services: Zoom and Microsoft Teams.

Recently there has been significant press coverage and commentary on the security and privacy posture of Zoom. The ANU Cyber Integration Centre has undertaken a risk assessment of Zoom and our settings. The ANU version of Zoom is hosted on AARNet (the tertiary sector’s internet provider). So encryption is handled by AARNet and recorded data is stored within AARNet’s cloudstor platform. Also, ANU has hardened Zoom privacy and security settings to ensure that our users have the best possible protection. So, it is OK to use Zoom for most scenarios. However, should you need to conduct more confidential discussions then Teams is recommended. ANU will release a guide for Zoom shortly and update advice on its use as new information comes to light.

Teams can be installed through the ANU Office 365 portal. You can login to Office 365 here https://services.anu.edu.au/information-technology/email and navigate to the Office online application (the nine little squares at the top left corner) and select Teams. This will get you to the online version of Teams where will see a link to download the Teams desktop application. For further guidance on using Teams please contact the ANU IT Help Desk.

If you are using the public version of Zoom (or some other teleconferencing app) for personal use, it is recommended that you review the security and privacy settings and policies. As always keep these applications up to date.

Securing your physical work environment

Some of us will be fortunate enough to have a set place to work from home, free from external interruption. However, many of us will need to improvise and work to the realities of our homes. In either case, it is essential to understand what risks exist for private information to be accidentally disclosed. This is particularly important if you are routinely dealing with sensitive information. Be mindful of who else may see the information on your device or be within listening distance of a confidential phone call.

There is no one set of rules to cover this, and it will be up to your discretion and judgement as what you believe the risk to be. In many cases, our households (and therefore workspace) may just be immediate family, but in other share house arrangements it could be quite different.

If you use shared devices, i.e. devices shared with other members of your household, it is highly recommended that you create different accounts on your device, i.e. one for each user and a separate account for your work-related activities. If possible, keep any sensitive or work-related data on an external (preferably encrypted) hard drive or USB key.

Review your physical work from home environment and identify any possible risk of accidental data loss.
Making your household security aware

Most of the technical safeguards in this document are reasonably easy to implement and are designed for general users. That said, by far the most challenging aspect of your home cybersafety program is developing an appropriate mindset.

The best defence you have is to regularly think about the security dimensions of your home network and your online activities. Scams and other attacks can happen on social media platforms. Many of us share data online that can be used to scam us or others. Given the heightened threat environment, consider carefully the information you and your household post online.

An important aspect of making your home cybersafe is to have a conversation with your household about internet safety and the risks you face. Cybersafety is a team sport, and to be effective, all users of your home network need to adhere to the same norms.

That said, it is not easy for any of us to think of ourselves as a target, let alone our homes and family. So, it can be difficult to have this conversation with our households. Your position at ANU makes you a target and because of COVID-19 and the need to work from home, so too is your home network and all the users on it. Threat actors have ramped up their activities at the moment, and this is on top of the general waves of cybercrime which occur every day on the internet, to which we are all subject to.

Where possible this document has tried to use the term safety over security. It is a more approachable construct to frame a conversation about online threats. Most of us understand safety, e.g. cross the road or lab safety. We recognise the inherent risk management that safety entails. Cybersafety is no different, and it need not be a confronting conversation.

Remember you are not alone in your cybersafety journey. ANU will be standing up a moderated online forum so that you can ask our Cyber specialists and the ANU Chief Information Security Officer any cybersafety question and share your own insights.

Be patient and proportionate in how you introduce new cybersafety measures – you don’t need to do it all at once.

Frame the conversation around cybersafety in a way that makes the most sense to your household.