LEADERSHIP IN CYBER SECURITY

CYBER SECURITY: WORKING FROM HOME

By Sorin Toma

September 2021

A Comprehensive Guide to protect Organisations and Staff when Working from Home

INTRODUCTION

Working from home may expose employers and staff to greater Cyber Security risks. This includes making staff vulnerable to identity theft, phishing, malware, ransomware, and other types of attacks. And employers vulnerable to data breaches, privacy breaches, unauthorised access by hackers, as well as other types of threats.

Here is what employers and staff can do to protect themselves and the organisation's assets as well as their staff. Please read through all sections of this checklist as specified below.

SECTION 1. ALL STAFF LAPTOPS WHETHER EMPLOYER PROVIDED OR BYOD[1]

Key actions to be taken by organisations for all staff laptops (same action for employer provided machines and BYOD or personal laptops):

1. Software **updates and patches** can be installed or applied to the Operating System (usually Windows 10 in most cases but also MacOS 10.15 known as MacOS Catalina, Linux, or other) remotely.
2. The **latest versions of all relevant application software** are installed, patched and operational. This is especially for email and office type applications as well as any project management, financial and other applications that staff require daily access to perform duties.
3. **Remote login software** including **VPN** (Virtual Private Network) is installed and operational so that staff can safely connect to any employer infrastructure or cloud applications and systems.
4. **Antivirus** or **End Point Security** or **Internet Security** software such as Norton (from Symantec), TrendMicro, McAfee, TotalAV, Bitdefender, Malwarebytes, Avast, AVG or other are installed fully up-to-date and working properly according to the organisation's Cyber Security policies and procedures.
5. Organisations should **enable MFA (Multifactor Authentication)** for access to key or important systems and/or applications. Meaning a code is sent to a separate device such as a mobile phone. This code than needs to be entered to access work applications.
6. Access to **System Administrator Mode** for staff is restricted and **effective support mechanisms** are in place to assist staff working from home.

If staff have never used their laptops or device remotely or from home, they should ideally take the laptop home and verify or test that all the above are working properly at least a couple of days before they plan to start working from home. It's much easier to come back into the office and have problems resolved than finding out on the first day

[1] Bring Your Own Device (BYOD) or personal laptop.

one works from home, that most applications are not working remotely.

If staff are connecting to employer infrastructure via an employer connection, then it is the employer's responsibility to ensure sufficient **bandwidth** is available to enable staff to operate all applications and systems efficiently. If staff are connecting to an employer's infrastructure via a mobile network (Optus, Telstra, TPG or other) using a wireless modem, via hotspot on their mobile phone (mobile phone network), and/or home wireless network and an NBN connection the following aspects are important:

1. **Availability of bandwidth** – mobile networks including NBN may not be able to cope with the volume of internet traffic if students, people working from home, and general population and business are all using the same local infrastructure. Meaning staff may not be able to connect to work networks and are unable to work.
2. Any **data restrictions or volume limits** staff may have on mobile data volumes (typically 15 – 60Gb of data) and NBN connection data (100Gb) after which connection may be terminated or severely limited (slowed down).
3. Staff check home connection plans data limits to ensure they will not incur **additional fees and charges** associated with greater volume of data downloads.

SECTION 2. ONCE HOME

If staff are connecting to work via home wireless network and NBN connection or any other way not provided or specified by the employer, then staff must understand they are responsible for securing:

1. Desktop machine or laptop if BYOD (see section above),
2. Wireless network and/or the way staff connect to employer work infrastructure or Cloud meaning using appropriate encryption and strong passwords at a minimum.
3. Mobile phone, and
4. Any other devices such as Smart Speakers, cameras, TV, and entertainment systems that are connected to their wireless/Wi-Fi/local network or home network.

Most people have difficulty with home wireless networks. Typically the telecommunications provider sends out someone to install home wireless router and connect it to the NBN modem. They may or may not switch on higher level of security and switch encryption on. But in most cases the default passwords remain in use for both the NBN modem and the wireless router. Not to mention any backdoors the average person will not know about, depending on the type of equipment use. Typical vulnerabilities for home wireless networks and NBN connections include:

1. Default passwords in use, including guest passwords.
   Action: Change default and guest passwords.
2. Higher levels of security and encryption not switched on.

Action: Turn on WPA2[2] encryption. This is more secure then WPA or WEP (Wired Equivalent Privacy) because it uses a stronger AES encryption algorithm (Advanced Encryption Standard).

Action: Disable WPS (Wi-Fi Protected Setup) – this is an insecure feature that makes your wireless network more vulnerable to attack.

3. Wireless network visible to any passers-by.

   Action: Switch off broadcasting of network SSID (Service Set Identifier). You should also change your SSID – do not continue to use the default vendor name for your wireless network.

4. Make sure the wireless network is safe – has not been accessed by any neighbours, passers-by or any other third party.

   Action: Enable router logs and check them on a regular basis.

5. Children accessing home wireless network using school laptops most of which are infected from school, other friends' wireless networks, and/or directly from the internet.

   Action: All machines connecting to your home wireless network must have an up-to-date **Antivirus** or **Internet Security** software installed and operational (signatures up-to-date) monitoring connection in real-time.

Network security is a highly specialised area and requires engineering qualifications and understanding beyond the scope of this checklist. However, if possible, staff should make sure **wireless router** comes with a **specialised built-in firewall** that adds an extra layer of protection. Moreover, **switch off the wireless network** if not using it for extended periods of time or if you are away from home. If employer has not provided staff with a VPN connection, then staff can purchase a **VPN** as a service from Symantec (as part of the Norton Antivirus / Internet Security suite as an optional extra). There are many other VPN providers. In fact NordVPN advertises on TV quite extensively. Some like VPN Unlimited are even free.

SECTION 3. BASIC GUIDELINES – KEY SAFETY ASPECTS

The following guideline should keep staff reasonably safe whilst working from home – remembering that nowadays the line between home and work has become unclear meaning that what staff do in their personal life may impact their work when working from home:

1. Although we have made some progress towards a paperless world sometimes it is still necessary to print. Therefore staff should make sure laptop is setup to print to home printers. Otherwise you may find your printed document going to your default work printer (whilst you are at home) potentially creating a risk if personal confidential information is involved.
2. Staff should destroy or shred all paper documents containing any sensitive personal, work, or financial information – do not just discard in the bin.
3. Keep any work and personal documents that contain sensitive or confidential information in a safe place and have a lockable secure mailbox at home.
4. Do not post personal, private, and confidential information online including details that may seem harmless but could be used to guess passwords – for example date of birth, favourite movie or favourite author are key details that can either be used to request a new password or lead directly to your password being cracked.
5. Use strong passwords for everything meaning a short phrase that contains alphanumeric characters like %, $, #, @, + (among others) and capital letters based on a theme known only to you such as "Obscure Historical Figures" example <AristAchus#of#sAmos> or "Asian Rivers" example

[2] Wi-Fi Protected Access 2 (WPA2).

<GanGes@India>. Do not use your middle name, your date of birth or another sibling's nickname – or anything that is obvious and can be gleaned from your Facebook page. Passwords should be 12 or preferably 15 characters long to make them as strong as possible.

6. Store passwords securely – if it's on a mobile device or in the cloud – they are hackable. Change passwords regularly (every 3 – 6 months) according to the Theme to make it easier to remember. It's possible to create an infinite number of Themes based on "food you like", "combinations of plants and herbs", "obscure cities or suburbs", almost anything you wish.
7. Limit the use of USB's – almost certainly never use any USB that is not scanned or unknown.
8. For all home devices (laptops, tablets, mobile phones, and computers) connected to the wireless network especially children's school laptops:

a. Make sure all the operating system software is up-to-date (all latest patches). Check the operating system and disable any file-sharing or any other remote access (depends on the type of operating system - check manufacturer specifications and technical magazines).

b. Use an Internet Security Protection Software Suite such as Norton from Symantec (there are many others) including a firewall, anti-virus, anti-spyware and anti-phishing tools to protect you from direct and indirect attacks.

c. Beware that if you kids are running YouTube or playing movies from the internet, this will slow down your connection preventing you from either accessing work facilities or making you less productive due to a slow connection.

9. The Professionals and the paranoid – use encryption. But before encrypting your laptop keep all your data backed-up on an external Hard Disk Drive in a secure location to avoid the pain of losing it.
10. Whenever using a browser for transactions only use the HTTPS secure protocol. Check browser facilities and disable specific features such as plugins and remote access. Also use browser add-ons Disconnect and uBlock Origin which are available for all major browsers. uBlock Origin is an ad blocker (also blocks dangerous domains usually known for malware and identity theft. Disconnect strips out tracking objects from web pages you visit such as tracking cookies, social media widgets and other online tracking techniques.
11. Don't forget to enable browser extensions from your Internet Security Suite. You can disable your browsing history being stored. You can also use the In-Private/Incognito mode for all browsers to protect your privacy.
12. Be smart when travelling in public Wi-Fi zones. It is amazingly easy to set-up a rogue Wi-Fi hot spot to steal all your credentials. Incredibly people log-on to unprotected Wi-Fi networks in cafes, shopping centres, airport and hotel lounges from unprotected devices. Within minutes a reasonably skilled hacker will obtain many passwords in a busy facility.
13. Never login to work or financial accounts using public wi-fi. If you have a mobile create a password protected hotspot, link your laptop to your mobile, and login via your own mobile phone network – much more secure.
14. Do not click on any links in emails that are suspicious – for example why would your local bank send you an email from Turkey or Ghana? They don't. Also, never click on any website links in emails or mobile phone text messages. Go to the verified bank website direct using your browser.
15. Beware of phishing emails. Even emails forwarded by a trusted colleague may be a phishing email. Never click on any attachments in suspicious and unverified emails.
16. Setup your privacy settings for Social Media to ensure only close friends have access to your page and limit access to any

personal information. Better still to limit or not to put any personal information on Social Media.

17. Never respond to any unsolicited emails or click on any links in such emails.
18. On your mobile only install apps from the official vendor app-store (Apple, Google, etc…) and from work, and most importantly always check online first to make sure the app is safe.
19. Any files, documents and/or software downloaded or installed from the internet should be done only if it comes from verified reputable sources or providers, should be scanned by the Internet Security Suite, and verified as safe before installation and/or use. Your browser may also scan downloads however it is best to set your Internet Security Suite to scan downloads.

20. If you have to use the cloud, remember most cloud providers provide additional security features for an additional cost. The likelihood is that if it's in the cloud it can be hacked, not always because of cloud providers, it's how you connect to the cloud that creates a vulnerability.
21. Never post photos of yourself having a holiday in Bali on Facebook thus telling the entire world you are not home (I guess nowadays in middle of pandemic we can't go to Bali).

From a personal perspective (remembering this may indirectly impact your work) especially if you have procurement or purchasing responsibility, make payments on behalf of your employer, have a work provided credit card, and/or access sensitive financial information (your employer's or yours):

1. Don't let your credit card out of your sight – example vendors may take the credit card away and can swipe it through the machine away from the counter and you.
2. Check your bank and credit accounts regularly / weekly looking for suspicious or unusual transactions with vendors or organisations you've never heard of before – this is to protect you against identity theft. Once your credentials are stolen, they may be used to access your employer's systems and applications.
3. Put alerts on your accounts (if facility offered by your bank) where you get text messages or emails in case of major transactions going through your account, any password changes, or any other changes such as address, email address and mobile phone number changes.
4. Prepare a list of all key financial institutions you are a customer of – including phone numbers, web addresses and other contact details.
5. Monitor your credit record and credit score with Veda/Equifax in Australia.
6. For all the latest gadgets and payment methods via mobile devices, it's highly recommended that consumers wait at least 6 – 12 months before using. Let others iron-out the initial issues and problems usually experienced by new immature products.
7. For all banking access enable multi-factor authentication where your bank sends you a one-time use code via text message or

even better via their own secure PIN protected application to enable a transaction.

8. For mobile phones – protect your access with your service provider using a PIN and/or a telephone password.

SECTION 4. ADDITIONAL DEVICES AT HOME

Other Components to make safe include (especially if BYOD laptop):

Windows 10

1. Depending on your company's policies or whether it's a BYOD Laptop.

Action: Rename the Local Administrator account. Harder for the bad guys to hack you if they don't know this.

2. **Action**: Disable Guest account.
3. **Action**: Maintain your privacy – switch off Microsoft's prying in "Settings > Privacy" then click on General Tab and switch everything off except SmartScreen Filter.
4. **Action**: Disable older authentication protocols such as LM (LAN Manager) and NTLM v1 (New Technology LAN Manager).
5. **Action**: Disable LM hash storage – LM password hashes are easily convertible to their plaintext password equivalents. Don't allow Windows to store them on disk, where a hacker hash dump tool would find them. This should be disabled by default, but you need to check.
6. **Action**: Set minimum password length to at least 12 characters. 15 characters is even better because it closes all sorts of backdoors.
7. **Action**: Set maximum password age to 90 days. If 15 characters, it may be ok to have this at 1 year.
8. **Action**: Enable Event Logs (and check them on a regular basis). The vast majority of attack victims would have detected the breach sooner if their event logs had been turned on and they made a habit of checking them. Make sure you're using the settings recommended in the **Microsoft Security Compliance Manager** tool and use the audit subcategories instead of the legacy category settings.
9. **Action**: Disable anonymous SID enumeration. Should be disabled by default but check because this could be a significant vulnerability.
10. **Action**: Enable User Account Control even if you are the only user of your machine.
11. **Action**: Scan your machine regularly using your Antivirus Internet Security Suite. A slow machine may be an indication that your machine has been infected.
12. **Action**: Don't forget to back-up your laptop on a regular basis meaning weekly at least.

Smart Devices or **Smart Speaker** from Amazon, Google, Apple or any other provider

These devices may be permanently listening in your home giving their manufacturer immense power and advantage commercially (e.g. recommending products and services, searching for restaurants, booking holidays, downloading entertainment, and so on) and also providing hackers with yet another target. It is important to understand:

- Smart Devices may be listening all the time 24 hours a day if it's not muted or turned off for its keywords. This is a major privacy issue. When you buy a Smart Device, you automatically give your consent to be profiled but any visitors to your home may inadvertently be included in your profile without consent. This may have significant implications if you are working from home and having sensitive conversations that include confidential, private, or privileged information.
- If hackers obtain access to to your Smart Device, they may be able to view an owner's cloud credentials and authentication tokens, and steal sensitive information.
- If a home security camera is linked to a Smart Device – the hackers will most likely be able to see as well. Whether you are home or not … Careful where you put that camera! May be wise to tape all cameras in your home, especially if working from home.
- It can result in Wi-Fi congestion especially if multiple heavy use devices connected. This will impact your productivity if working from home and could result in weaker security if you switch off security features on your networks to squeeze more bandwidth.
- The greatest risk is access to your voice print which can be a way of authenticating you. Your voice print is now recorded and stored on Amazon cloud.
- A physical attack may get hackers access to the underlying Linux operating system shell allowing them to install malware and you the user may be none the wiser.

This is what you can do to secure Smart Devices:

1. Change “wake” words – customise Alexa so that it can only be operated by you.
2. Enable a PIN on any purchases or financial transactions.
3. Don't connect Alexa to any other critical systems, devices or appliances that provide access to sensitive personal information such as a video camera.
4. If you are in doubt e.g. having an important conversation with your spouse or kids, taking business calls – working from home, or simply relaxing then please turn it off or mute it.
5. Manage your device's history - go online and delete it (still to see whether this is yet possible - but it is possible for older Amazon devices like Echo).

Mobile Phone (especially if used to access mobile work apps)

You probably do not realise how much your smart phone knows about you. You may even use it to make payments. Your bank and/or your work may be using authentication on your mobile phone to enable transactions. It knows your location. Google tracks everywhere you go. Your contacts and emails are in your mobile phone. You may even connect to your car via Bluetooth and other devices to play music and download videos.

Final point – you probably don’t realise how easy it is for hackers to port your mobile phone to another provider and steal your identity, your data (your employer’s data if working from home), and your money.

To secure your mobile phone (generic guideline regardless of whether iPhone or Android phone):

1. Don’t lose it. Don’t misplace it. Beware of your mobile being stolen. Treat it the same way you would money or a credit card.
2. Apply updates and patches from manufacturer immediately – as soon as available.
3. Don’t install any third party apps except from the official stores and only where you know or have checked that software provider is legitimate and safe (avoid mobile malware/ransomware).
4. Beware of phishing, social engineering, and other such scams. No – the Tax office doesn’t provide refunds, nor will they arrest

you if you don't pay them with Apple iTunes money cards. And your bank will not get you to login to change your PIN by sending you a link. In fact don't click on any links unless you personally know the sender.

5. Lock your phone. Password, PIN, fingerprint, face recognition, etc…
6. Consider encrypting your data. Doing so is especially useful for protecting sensitive data, whether that's business emails or investing and banking apps.
7. Set up remote wipe. If your phone is lost or stolen, you'll be able to wipe all of its data remotely (and therefore keep it out of the hands of criminals). You can often also use remote wipe to find your phone's location.
8. Back-up your phone regularly (if iPhone synchronise and backup).
9. Don't use public Wi-Fi – not safe for any device.
10. Install Antivirus/Security for mobiles (same as for you laptop) – most Antivirus vendors can protect your mobile phone too.
11. Turn on Multi-Factor authentication using two separate devices not the same one.
12. You can use a VPN with a mobile phone too.
13. Enable Find My Device or Find My iPhone capability.
14. Avoid jailbreaking your mobile - To jailbreak a phone is to modify it so that you have unrestricted access to the entire file system. This access allows for changes that aren't supported by the phone in its default state. Jailbreaking can be thought of as metaphorically breaking the phone out of its jail or prison. When the phone is free from certain bounds set by the manufacturer or wireless carrier, the device owner gains more control over the device and how it performs.
15. Change passwords regularly and abide by password selection guidelines or policies (length, characters, upper case, etc …) both iPhone, AppStore, iCloud and other apps.
16. Revoke permission for apps to use microphone, camera, and/or location services.
17. Turn-off Wi-Fi and Bluetooth if not using them and only connect with safe devices and or networks. If you don't use any particular Apps uninstall them.

SECTION 5. CONCLUSION – BEWARE

CRITICAL TO REMEMBER:

Working from home is not a trivial matter. There can be a significant transfer of liability from employer to staff depending on your facilities and how you connect to your work's applications and systems. Surveys indicate home based staff spend between 10 – 22 percent of their time overcoming technology issues and problems.

Working from home may be liberating and desirable and/or in some cases unavoidable (e.g. given Pandemics such as COVID-19). It also comes with its own challenges and responsibilities.

EMPLOYER'S POLICIES AND PROCEDURES:

Please make sure that you check your employer's policy on "Working from Home" (if there is one – some companies may not yet have such a policy) and you are fully aware of your rights and responsibilities including technical support and other facilities available to you when working from home.

KEY INSIGHT

Even when home your organisation's policies and procedures may still apply. If a major event occurs due to an unsafe home connection your organisation may hold you liable for exposing them to greater risks. Please be aware of all the relevant policies including email, office and mobile device usage policies and make sure you do everything possible to comply.

TRADE-OFFS – IMPROVED SECURITY HAS A COST:

Better security involves **trade-offs**. For example MFA (Multifactor Authentication) significantly reduces the likelihood of unauthorised access by hackers. At the same time if your secondary device (most likely your mobile phone) can't connect to a telecommunications network, then you may be unable to login to work applications and systems thus becoming unproductive. Understand this, plan for it (reset your expectations), and then deal with it.

INFECTION CONTROL:

It is now essential that greater standards of cleanliness or hygiene apply to all computer equipment. www.howstuffworks.com and www.health24.com have found that laptop and computer keyboards, mice, touch screens, headsets, and pens can contain bacteria and germs at levels five times higher than a toilet seat. If your equipment wasn't new (someone else used it before you), if you eat at your workstation or drink coffee whilst working, or if you have pets in your home – then your computer equipment and accessories may contain harmful levels of germs. It is essential that a cleaning kit using a keyboard vacuum or compressed air, and alcohol wipes are used to clean your computer equipment on a regular basis.

TOPICS NOT COVERED:

Social Media is key aspect of many people's lives. Securing Facebook, Instagram, LinkedIn, YouTube, Twitter, Tumblr, and others is a topic in itself. Needless to say whenever you are posting on some of these sites you are broadcasting the fact you may not be at home. Posting any personal information that can be used to "guess" some of your credentials is not smart. Please be careful with all social media activity.

Google, Amazon, eBay, and many **online retail websites** track your activity and store a lot of data in terms of your activity online, your profile, preferences, interests, and personal information. Again user beware.

This checklist only covers Windows 10. Consequently if you are using **MacOS** or a version of **Linux** on your laptop – there are many magazine articles as well as online information on securing these operating systems. As long as the information comes from professional organisations, it will be fine.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Prepared by Sorin Toma at Act2Secure Pty Limited

E: Sorin@Act2Secure.com M: +61 419 631 023

DISCLAIMER:
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~