Cyber Audit TEAM

WORKING SECURELY WHEN WORKING REMOTELY

CYBER AUDIT TEAM

Working Securely When Working Remotely

After facing a devastating bushfire season, extreme storms, and currently the COVID-19 global pandemic, social distancing has added another driver.

Remote working might provide companies with flexibility, whilst also enabling business continuity, it presents considerable risk that some businesses may not have considered.

Threat actors (cybercriminals) use sophisticated software to actively target a company's weak infrastructure, and they are highly successful in compromising those companies who enable their workforce to work remotely, yet haven't mitigated some of the simplest risks.

Your company might be in this very situation right now and wondering, *"What are the risks of working from home or another remote location?", "What kind of security or privacy issues could this introduce for our company?"* and, *"How do we mitigate these risks?".*

When an organisation and its team are on the same page, with the right mindset, a little bit of know-how goes a long way. As part of our commitment towards protecting our clients' businesses and their staff, we have compiled this simple guide to educate and assist by highlighting leading practices for remote working.

Whilst the following list is not exhaustive. It will provide your business with a practical starting point.

01. Employ a recognised **Password Manager** (or at the very least, enforce the use of strong **passphrases**)

02. Enforce **Multi-Factor Authentication** (MFA) on key platforms (i.e., CRM, finance systems, corporate social media and marketing systems, etc.)

03. Employ a corporate **Virtual Private Network** (VPN), **Remote Desktop** (RDP) or other Virtual Desktop solutions if connecting remotely to on-premise / hosted company systems (Cloud-based platforms are generally secured via **HTTPS**)

04. Ensure effective **Antivirus software** is installed and updated on all computers. BYOD or non-company owned devices should, at a minimum, have **Windows Defender** or comparable antivirus software installed and updated

05. Secure staff home **Wi-Fi** (Router and Modem if appropriate)

06. Enforce regular and automated Windows, Mac, iOS and Android **updates**

07. Check that data backup, file storage / sharing policies and solutions are in place to safeguard company information

08. Be alert for **phishing** emails and '**spoofed**' sites

09. Ensure appropriate device security (i.e. Touch ID, Face ID or other **biometric** / complex passcodes)

10. Enforce **mobile device policy** and controls to protect corporate data

01.

Employ a Recognised Password Manager

Unfortunately, two-thirds (67%) of people (according to a **Google / Harris Poll**) still admit to using the same or a variation of the same password across multiple accounts. This means that all it takes is one compromised password for a threat actor to breach all of your accounts. Threat actors use sophisticated software that then takes your leaked usernames and passwords and attempts to login to other online accounts you may be associated with (banking, Office 365, social media, etc.), a tactic called 'credential stuffing' (more on **Credential Stuffing**).

It is imperative that passwords are unique and complex for every account. Clearly, no individual can be expected to remember multiple complex passwords; that's why good practice is to use a recognised **password manager** to generate unique, complex passwords and store them in an encrypted database.

A password manager should be essential and enforced company-wide. It is important that your internal or external IT team/manager/provider sets this up and manages this system, including creating computer-generated long, complex master passwords. The main reason for this is that if we leave it to the staff; they will inherently reuse passwords, or use ones that do not meet today's recommended guidelines (more info **here**).

02. Enforce Multi-Factor Authentication (MFA)

When computer pioneer Fernando Corbato invented a way to use passwords to protect user accounts back in the 50s, he could not have envisioned that today the average business user has to keep track of 191 **passwords**, with unique passwords being required for each account.

In today's interconnected world and rapidly evolving threat landscape, strong passwords alone are no longer considered sufficient on their own.

Additional layers of security, such as Multi-Factor Authentication (**MFA**), are now mandated by most companies and organisations as an additional layer of security.

Additional steps should utilise authenticator apps, which send One-Time Password (OTP), or a phone itself can receive push notifications and act as an authenticator device.

Authentication factors can also be biometrics (facial recognition or a fingerprint scan), and for those staff members with access to highly sensitive information or privileged access, then a physical token is recommended, such as a **YubiKey**.

03.

Employ a Corporate Virtual Private Network (VPN) or Remote Desktop (RDP) Solution

If your IT systems are still on-premises or hosted, you may need to deploy **VPNs** or remote desktop solutions to enable staff to work remotely.

A VPN encrypts all communications, to provide a secure way of transporting private data across public networks (internet). Business-grade VPNs are essential for any company with remote-working or travelling employees accessing corporate or hosted infrastructure.

Remote desktop solutions provide similar remote access for Windows environments but **need to be secured** to avoid common vulnerabilities. For businesses that have adopted cloud services, they are already equipped for flexible working arrangements. There are, however, more and more options available such as Virtual Desktop Infrastructure (**VDI**) or Desktop-as-a-Service (**DaaS**), that make flexible computing even easier to deploy.

04. Deploy Effective Antivirus Software

Your business should be running next-generation **antivirus software** to protect your corporate devices; however, have you checked to ensure that your staff have sufficient security on their personal devices?

It is vital that your business check with any staff that are using their personal laptop, computer or other mobile device that there the device is running commercially acceptable antivirus software.

Many personal devices run 'free' antivirus or Internet security software that is not fit for purpose in relation to protecting corporate information.

Consider purchasing additional antivirus licenses for any staff using personal devices to mitigate the risk to your organisation.

05.

Secure Staff Home Wi-Fi

Do you know if your staff have secured their home network? Have they changed their router password from the default one provided by the provider? Do they have a guest network set up, or do they let friends and extended family sign into their network?

Many people don't understand that their routers might be the most important electronic devices they have in their homes. Routers link most of their other devices together and to the outside world, giving the router a highly privileged position that cybercriminals often look to exploit.

Changing your router default admin password is the first step your staff should take. Here are some other practical 'best practice' steps that staff should take to ensure that their home environment does not expose your business to unnecessary cyber risks.

1. Change the default admin password

Many routers come with default administrator passwords, and attackers constantly try to break into devices using these publicly known credentials. After you connect to the router's management interface for the first time through your browser — the address should be the router's default IP address found on its bottom sticker or found in the set-up guide — make sure the first thing you do is change the password (and remember your password / passphrase hygiene).

2. Choose a strong security protocol

WPA2 (Wi-Fi Protected Access II) and the newer WPA3 should be the options of choice, as the older WPA and WEP versions are susceptible to brute-force attacks. If the router offers the option, create a guest wireless network, also protected with WPA2 or WPA3, and with a strong password. Use this isolated guest network for visitors and friends instead of your main one. These users might not have malicious intentions, but their devices might already be compromised or infected with malware prior to connecting to your network.

3. Secure all smart devices / IoT (Internet of Things)

If you have IoT devices (fridges, CCTV, lights, etc.) connecting to your network, ensure that they connect to your guest network rather than the main one.

Also, make sure you change the IoT device's default password for the same reasons explained above.

4. Keep all device firmware up to date

Ensure that the router's firmware, and any IoT devices, are up to date, and updated regularly so security vulnerabilities can be patched.

Some routers allow checking from the management interface if firmware updates are available, and a few even offer automatic updates. However, sometimes these checks might be broken due to changes made over time to the manufacturer's servers.

It's a good idea to regularly check the vendor’s support website for updates for your device. These updates need to be downloaded manually then flashed through the router’s web-based management interface.

06.

Enforce Regular Updates

Updates to device software and other applications can be a source of annoyance, but they are essential to a company's infrastructure. Without regular updates, threat actors can disrupt a company's operations or steal their data. Updates often include patches for security vulnerabilities that have been uncovered since the last iteration of the software was released.

Patches are systematic updates of software and operating systems. Not all patches are security-related, though, as some are just new feature updates, but through vulnerability management, security vulnerabilities can be actively discovered and categorised.

In many cases, you can set updates to run automatically, often while you're sleeping, so you don't have to worry about downtime (more info **here**).

For a business that allows staff to use BYOD devices running Windows, it is highly recommended to ensure that the device is not running any '**end-of-life**' software, such as Windows 7 or Windows XP. If a device is running an older version of Windows, it is highly recommended that these devices be prohibited from being used, and instead, a corporate device provided. This is primarily due to the severe risk the device might posse due to the older Windows version being highly vulnerable to attack.

07.

Data Back-Up and File Storage / Sharing

Data can be lost in a number of ways, including human error, physical damage to hardware, theft, or a cyber-attack. Ransomware and other types of malware can wipe entire systems without you having a chance to even spot or stop them.

It's important that staff aren't saving company documents or information to their personal devices, removable/ portable hard drives, or to other unsanctioned cloud storage platforms such as Dropbox, Google Docs, or iCloud, etc.

There should be a single source of truth (SSOT), a common database that is secure. However, what commonly ends up happening in companies is that employees turn to technologies outside the knowledge or control of the IT department. This is called **Shadow IT**, and it is used for sharing files, documents, and collaboration. This can occur using flash drives or using cloud services, as is more common these days. Shadow IT can not only cause data duplication, inconsistency, and increase the likelihood of errors, but it also opens the door for cyberattacks by leaving gaps in the business system.

You must also take into account the potential for any staff members who are leaving or even considering leaving the organisation, downloading sensitive information from your CRM or financial platforms. This could not only be a case of theft, but could also constitute a data breach. Data Loss Prevention (DLP) **policies** and **practices** are key to prevent these issues.

08.

Be Hypervigilant Against Phishing, Vishing, Smishing Attacks and ‘Spoofed’ Websites

Phishing emails, voice solicitation (**Vishing**), and text message scams (**Smishing**) are just some of the tactics, techniques, and procedures (**TTPs**) used by threat actors to elicit information or access to sensitive company information. This information is usually used in future attacks or scams, such as 'spear-phishing' campaigns (targeted phishing attacks), credit card fraud, and account takeover fraud. TTPs have significantly increased in the last few months, due to COVID-19 (more info **here**).

Staff must be educated that over the last few months, thousands of malicious 'spoofed' websites have been created to look like legitimate websites but can download malicious software or request sensitive information from the visitor (more info **here**).

During the Covid-19 pandemic, it is highly likely that staff are going to receive an increase in phishing emails, scam phone calls, or malicious texts disguised as government agencies, health providers, or other trusted agencies similar.

It is therefore vital that they remember the basics and do not click on any links in emails or in text messages, divulge any personal or financial information in person, or on suspicious websites.

Staff should remember to "break the chain", and call them back on a published number, or manually visit that contacting organisation's official website before logging in.

09.

Ensure Appropriate Device Security

If your staff are going to work remotely, whether from home, or at a public space, then device security is paramount.

Whether at home or in public, staff must adhere to cooperate guidelines. For example, when at home, they should ensure that they screen lock their device. When in public, the device should never be left unattended to go to the toilet or to get a coffee. Their mobile phone should also be screen locked, and not left unattended in public.

You may wish to consider additional security for those staff who are working remotely via full-disk encryption tools such as **BitLocker** or **FileVault**.

If you need to physically lock your device, for example, at a library or hospital, **Kensington Lock** is a great option.

10.

Enforce Mobile Device Management

Having a corporate-owned device is a sure shot way to ensure higher security as they can be monitored and meticulously configured to interact only with approved applications and networks. But these days, employees prefer to use their own devices at work, which often lack the tools built into corporate devices such as strong antivirus software, customised firewalls, and automatic online backup tools.

This increases the risk of malware finding its way onto devices and both personal and work-related information being leaked. While BYOD devices do reduce the business' expenses in a way, they can pose a serious risk for the business if ground rules are not set - *"How to ensure that any corporate information is completely safe?", "How to deal with infected or stolen devices?", "Can sensitive data off lost devices be remotely wiped for good?".*

Consider **Mobile Device Management** (MDM) and **Mobile Application Management** (MAM), especially if your business supports a bring your own device (BYOD) policy. Device management solutions help manage and secure mobile devices and applications. These tools can also allow organisations to remotely implement a number of security measures, including data encryption, malware scans, and wiping data on stolen devices.

Additional Information to Consider

Unsecured Wi-Fi (Public) Networks

Most workers will be working out their home where they should have already secured their own Wi-Fi. However, some may have to use unsecured public Wi-Fi networks (airport lounges, hotels, coffee shops, etc.), which are prime spots for malicious parties to spy on internet traffic and collect confidential information (more info **here**).

Where possible, one of the most secure ways to protect your company and sensitive information when working remotely is to 'hotspot' from your mobile phone.

Reporting Issues

For any staff who are going to be working remotely, they should be provided with initial and then regular feedback on how to react in case of problems. That means information on who to call, hours of service, and emergency procedures.

Should any staff member suspect they have fallen victim to such a scam or attack, ensure they are fully aware of the correct reporting/response procedures, and that they are encouraged to report it (without fear of repercussion or blame) to internal or external IT and your information security partner.

Physical Security While Working Remotely

Home Security

We should all be highly aware that this is "Security 101" however, if you bring your work computer home or tend to work remotely, and your home personal security hygiene isn't up to scratch, like locking your doors and windows at night, or when you leave the house, then your confidential corporate information could be seriously at risk.

Staff must observe the same information security rules at home as they do within the office. For example, screen locking their devices when away from the device, not allowing anyone access to their corporate devices, clean desk policy, not downloading any corporate documents or files to their personal devices or external drives, etc.

Never Leave Your Devices or Laptop in the Car

Another basic "Security 101" should be to remind staff never to leave any devices, especially their work computers or devices in a vehicle. It's a best practice to keep work laptops and devices on your person at all times while on the road. And the boot of your car is no safer. There may be criminals watching the parking lot from afar, waiting for their next victim. Putting valuables in the boot may make life a little bit easier in the short-term, but why take that chance?

Contact us to find out more about how to work securely when working remotely.

Cyber Audit TEAM

Cyber Audit Team is an independent Cyber Resilience Assessment and Managed Detection and Response Services provider.

The multi-disciplinary team of highly experienced industry specialists provide simplified end-to-end Information Security solutions as well as support and guidance to businesses of all sizes across various industries.

Cyber Audit Team
4 Helensvale Road
Helensvale QLD 4212
Australia

P: 1300 077 022

E: enquiries@cyberauditteam.com

W: cyberauditteam.com

Follow us on LinkedIn & Twitter
@cyberauditteam