The most **Frequently Asked Questions** about **Remote Working** and **Working from Home**

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

What is Remote Working?

Remote working is any work that's done away from your physical office. This is often referred to as telecommuting or **working from home**. The benefits of remote working often centre around being able to achieve success in your daily tasks without the need to commute to an office each day.

Whilst varying levels of remote employment existed before the pandemic in 2020, many workforces were forced to quickly adapt to allow more workers to work from home when lockdown rules came into effect.

As well as fully remote workers, many businesses have staff who have flexible working environments, such as office workers who still want to ensure they have a traditional desk in the office to maintain personal connections with colleagues and meet with clients via the traditional office environment.

Flexible working has long also been everyday working for workers who may not have the capacity to work from home on a full-time basis. This includes; legal professionals, field sales, building contractors, editorial freelancers, photographers and more.

Frequently Asked Questions about Working from Home

What cyber security risks do you face when working from home?

Sensitive Data Exposure - This applies to electronic devices, and physical paper documents/notes. Even family members should not be allowed to see Sensitive Data, and this would be a breach of GDPR. The best practice is to implement a Secure Storage Cabinet where all work items (devices, documents, notebooks etc.) can be kept.

Unauthorised Device Access - Even when working from home, your device must be locked whenever you leave it. Even though it may "only be family" that can see your screen, it is still a Cyber Risk.

Using the correct device - BYOD (Bring Your Own Device) is a common strategy amongst SMEs and WFH culture, However, if it is implemented it is important to ensure that work data and personal data are kept completely separate - if an Attacker gets your device, they may be able to gain further access to all the company information if it is not secure. The best practice is to use separate work and personal accounts and ensure strong, and unique passwords are used, in combination with Multi-Factor Authentication.

Frequently Asked Questions about Working from Home

How can I ensure my home router is secure?

The best way to ensure your router is secure is to change the default password that is supplied by your Internet Service Provider. When changing it, it is important to follow NCSC Guidance of combining 3 random words, letters, numbers and special characters, with a minimum length of 15.

For detailed information, read NCSC guidance here.

Do I need to use the cloud for backups?

No, you do not **need** to use the Cloud. Depending on business size and requirements, an acceptable solution may be to manually back up your business data to a physical storage device such as a hard drive. But this hard drive must be completely disconnected from the business network when not in use.

Frequently Asked Questions about Working from Home

Why do I need backups? How often should I be backing up my files?

Backups are one of the most effective defences against Malware Attacks because if you are the victim of one, and your data is encrypted by an Attacker, you effectively “ignore” the attack by reverting to your Backed Up data and start restoring business continuity from there.

There is no “one size fits all” approach for backups. The schedule will depend on business needs - some may require backups every 12 hours, but for others, it may be acceptable to back up every 24 hours. The most important aspect however is to make sure any Backups are stored separately from your business's network - either in the cloud or on a completely separate hard drive that is not network-connected.

Frequently Asked Questions about Working from Home

Why is important to keep your devices updated?

Do my apps need to be updated regularly?

Yes, all of your devices (computers, laptops, mobiles and tablets, etc) should always be kept up to date with the latest software. This is because the companies who provide the software (e.g. Microsoft) have security teams that search for vulnerabilities in their apps, and fix them before Attackers can take advantage. The longer you go without updating your apps, the more vulnerable you will be to an Attacker

Can I automate my device and application updates?

Yes - inside the settings of your device there will be an option to automatically update, all you have to do is select “Yes”. However, if you don’t want your device to update in the middle of work, you can also select “Working Hours” and this will tell your device to only install updates outside of that time

Frequently Asked Questions about Working from Home

Why is a Password Manager a safer way of storing passwords whilst working remotely?

Password managers take all of your passwords and store them in what is called a vault. However, when each password is put into the vault, the password manager will heavily encrypt its value so that it cannot be read by the naked eye. Then, the Password Manager will have you set an incredibly complex Master Password to access this vault (if you want to add/remove credentials from it). Finally, Password Managers have Two Factor Authentication (2FA) enabled by default, adding another layer of security by requesting you to input a code any time you want to access your secure vault.

What is a Bring Your Own Device (BYOD) policy?

BYOD is the concept of employees using their personally owned device(s) for work purposes. With BYOD, an organisation has ownership of the corporate data and resources that may be accessed or stored on a device, but the device itself is the property of the user.

Frequently Asked Questions about Working from Home

If you're using your own device for work, why could a Bring Your Own Device (BYOD) policy be useful for a business?

When employees use their own devices, if your budget is tight you don't need to buy any extra computers, screens, mobile phones, and tablets. Using personal devices is a preference for people who want to stay connected to both personal and work life and with home commitments such as childcare.

If staff are working remotely, your BYOD policy will ensure your team can stay connected without needing to carry multiple devices.

Within a well-structured BYOD policy, employees should feel more at ease with their day-to-day work and help to keep them working in your organisation.

Frequently Asked Questions about Working from Home

What are the benefits of a Working from Home (WFH) or Remote Working policy?

Giving employees access to a hybrid working environment will give them the option to work comfortably from their home office. This may be especially useful when offering remote work on a flexible basis for employees with childcare needs, medical appointments or when having work done at home.

Spending long periods travelling to work each day can be a strain for all of us, especially with train strikes and cold, wet weather during the autumn and winter months. Remote workers can often feel more motivated and organised when working without a commute, with many workers using their commute time to talk walk and exercise before and after work.

With more staff working remotely many businesses in the UK have made cost-savings through reduced reliance on large offices and reduced staff turnover. Staff can often find increased motivation in a role which has introduced flexible hours and then be more comfortable to stay in a job and progress.

Frequently Asked Questions about Working from Home

What key things should be covered in a Working from Home (WFH) or Remote Working policy for a business?

Explain why you've created the policy and which members/teams it applies to. For example, you may want to clarify whether the remote worker policy is in effect only temporarily.. Specify whether your contractors, part-time employees, interns and new hires are covered by this policy, or if it only applies to existing full-time employees who have been with your company for at least six months.

If your business is entirely remote, there may be some eligibility criteria you'll want to include; will employees need to live within a certain distance or can they move anywhere in the UK?

Outline who is working from home and when. For instance, your remote work policy may state that people in client-facing roles can only work from home three days per week. You can also create other criteria rules, such as those who have passed their probation can work remotely.

Some roles aren't suited for remote work; employees who need certain equipment, access documents available only in the office or regularly interact in person with clients. If there are broad categories of positions that are not eligible for remote work, remember to list them in your policy.

Frequently Asked Questions about Working Remotely

Why isn't public wi-fi secure when working remotely?

You may be unaware that an innocent trip to a coffee shop may have threats lurking in the background of their public Wi-Fi network.

Public wi-fi is common in most locations when working remotely, we all frequently connect to them to check our emails or social media without thinking twice. Whilst your local cafe owner may believe they're providing free wi-fi to try and keep you in-store to buy that extra slice of cake, chances are the security on these networks is minimal or nonexistent.

A Man-in-the-Middle (MitM) attack is a form of eavesdropping. When your laptop or phone connects to the Internet, data is sent from your device to the website, and security vulnerabilities can allow an attacker to get in between these transmissions and "read" them. Your data could be no longer private and shared amongst a criminal network.

If a public wi-fi router hasn't got encryption, the information being sent from your laptop/phone to the wi-fi router could be intercepted. There's also no way you can tell if a public wi-fi spot has got the necessary encryption.

Frequently Asked Questions about Working Remotely

Why isn't public wi-fi secure when working remotely? (cont)

Attackers way look to slip malware onto your computer without you even knowing through public wi-fi. If attackers know of a software vulnerability they may use a busy public location to write code and target a specific vulnerability, and then inject the malware onto your devices through a public wi-fi network.

Wi-Fi snooping is what it sounds like. Cybercriminals can buy special kits and devices to eavesdrop on Wi-Fi signals. This technique can allow the attackers to access everything that you are doing online — from viewing whole webpages you have visited (including any information you may have filled out while visiting that webpage) to being able to capture your login credentials, and even hijack your online accounts.

Rogue public wi-fi networks trick victims into connecting to what they think is a legitimate network because the name sounds reputable. Say you're staying at the Hotel Easy and want to connect to the hotel's Wi-Fi. You may think you're selecting the correct one when you click on "HotelEassy," but you haven't. Instead, you've just connected to a rogue hotspot set up by cybercriminals who can now view your sensitive information.

Frequently Asked Questions about Working Remotely

Is public wi-fi more secure than a mobile hotspot?

The biggest threat to free Wi-Fi is for a hacker to position themself between you and the wi-fi point. So instead of talking directly with the wi-fi router, you'll be sending your data to the hacker, who might exploit this data.

Using a phone hotspot can increase your security, your mobile connection is secured and private as you would be making a phone call or using your phone to browse the internet. Most phones now are using 5G networks which use 256-bit AES encryption, this blocks fake mobile network transmission sites (referred to as stingrays) and encrypts your phone's ID during transmissions.

Frequently Asked Questions about Working Remotely

What is a Virtual Private Network (VPN)?

Virtual Private Networks (VPNs) allow businesses and organisations to provide secure connectivity between devices, especially useful if staff work remotely.

Why would using a VPN help secure your laptop/phone/tablet when working remotely?

VPNs are encrypted network connections, that allow remote employees to securely access your company's services. VPNs are one way to guarantee the security of 'data in transit' across an untrusted network, if you have offices in multiple locations you can use VPNs to provide access to your remote users for any corporate email and file storage services.

Talk to us

Whether you just want informal advice, to learn more about staying secure when working remotely or our services and membership. We are happy to help.

Get in touch with our expert team who can help you on your journey towards cyber resilience.

CALL US: 0161 706 0940

INFO@NWCRC.CO.UK

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

info@nwcrc.co.uk
www.nwcrc.co.uk