How to Protect Your Corporate Data in a Work From Home Environment

The global pandemic has seen a complete shift in standard workplace practices. For both countries that are entering new lockdowns and countries which are easing their restrictions, businesses around the world have all been forced to embrace a distanced approach to getting work done. And whilst some organisations are [edging back towards the typical office lifestyle](https://edition.cnn.com/interactive/2020/health/reopening-coronavirus/work.html), many companies may [continue to operate remotely](https://www.forbes.com/sites/rachelsandler/2020/08/27/heres-when-major-companies-plan-to-go-back-to-the-office/#6f6c9b43361c).

As some businesses may reap the rewards of lower operational costs when Working From Home (WFH), they must consider the risks associated with spreading their workload across many external networks, devices and locations as well. Usually, when working in an office, cyber threats are well blocked and mitigated as the robust, enterprise-grade cybersecurity software used by businesses only needed to protect an internal server, network and the devices connected within the building. Now, [WFH has introduced more weaknesses into companies’ cyber defences](https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html) through the employees’ use of their own weaker networks, less-protected endpoint devices and public internet.

Simply, the dangers of data theft and corruption increase when files are shared and accessed remotely. Especially at times like these, where on-site assistance may be limited, the damage done in the event of any form of cyber attack could not only cost a business money, time and clients but could bring the organisation to a complete standstill.

The following guide covers the most basic Do’s and Don’ts of remote working when it comes to ensuring your data stays safe while outside the office.

# The Do’s of WFH Security

**Make use of Virtual Private Networks (VPNs).**

[Virtual Private Networks](https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html) allow for secure, remote connections to an existing company network. A VPN service is an excellent way of keeping data in transit protected from external threats as it connects a user securely to a network through the internet. When a device connects to a VPN, all data transmitted travels through an encrypted connection over the internet; this means that the data is protected from man-in-the-middle attacks as all information sent through a VPN is obscured to outsiders.

This additional security layer not only encrypts the data sent between users and applications, but it hides the users’ IP addresses and geographical locations as all that is discernible from the outside is the IP address of the VPN server (which can be repeatedly bounced around the world).

**Invest in powerful antivirus.**

It has never been more crucial for all devices in your organisation to be protected by robust and well-trusted antivirus software. Cybercriminals are deploying more and more intelligent attacks each day, and without strong firewalls, virus scans and anti-spyware programs, your organisation is completely defenceless. Employees may feel relaxed at home and may let their guard down - as an organisation, you should regularly remind your personnel of the risks online, encourage them to be vigilant of strange device behaviour, and enforce mandatory antivirus policies.

**Increase password security.**

In the safety of their own homes, employees may not be too concerned about the importance of strong passwords. To ensure the best password ‘hygiene’, passwords should be reset regularly (in the case that a password becomes compromised) and should consist of both lowercase and uppercase letters as well as digits and symbols (e.g. #$%?!). Two-factor authentication, whereby two different forms of identification (passwords or PINs) are required before access is granted, is strongly recommended. In these times, maintaining secure password backups would be wise in the event that an employee may be unable to access/ share critical information if they become sick.

**Make use of secure file sharing.**

Enforcing a company-wide policy for secure file sharing will guarantee a better chance of protection from intrusive attacks, than when employees make use of various software platforms and sharing methods. Files need to be stored on the cloud not only to support remote work but also to be more reliably protected. In most cases, critical data should be cloud-based as creating copies and storing files locally on employee devices presents the perfect opportunity for cybercriminals to access that information if the endpoint device is [not as well-protected as the cloud-base](https://www.infoworld.com/article/3316637/how-the-cloud-has-made-you-more-secure.html).

**Increase home router security.**

Home routers can be a significant weakness when it comes to the protection of business data. If the routers that employees use at home are insufficiently protected, it becomes far easier for cybercriminals to gain access to an organisation’s network. To increase the security of the routers used out of the office, ensure that their default passwords have been reset to something stronger, the password security is set to at least WPA2 and the router’s software is updated.

**Maximise physical security.**

Home offices do not likely enforce the same physical security standards seen in typical workplaces like keycards, biometric entry and pin-locked doors. Just because employees are working from, does not mean these security measures should be forgotten, however. While high-level security measures would be challenging to install in all homes, employees should make the best effort to keep their work property safe. This may be through locking doors, storing files in a safe or hiding their devices at night.

# The Don’ts of WFH Security

**Don’t open emails from unknown senders**

Cybercriminals are relying on the fact that employees may be less vigilant while working from home to gain illegal access to private data through emails infected with malware. A [cyberattack may present itself covertly as an email](https://www.phishing.org/what-is-phishing) from a colleague with a seemingly normal attachment. This attachment, when opened, could instantly infect a device with a dangerous virus. Employees should be sure that they recognise the sender of an email before they open any attachments. The same goes for opening links and downloading software from unrecognised sources.

**Avoid sharing external hard drives and using public WiFi**

The only way to be sure that an external hard drive or USB stick is infected with a virus is to insert it into a device and run a virus checker - by the time that this happens, it's usually too late and the virus would have already infected the device. For this reason, it is best to avoid inserting any type of external device into your hardware; instead make use of secure, cloud-based file sharing. Additionally, public wifi networks should be avoided at all costs - working at a coffee shop may seem appealing, but those networks are insufficiently protected.

**Prohibit family use of devices used for work.**

Although challenging when living with family members, young and old, it is important to prohibit unauthorised people from using your work devices. When more than one person makes use of the same device (which contains sensitive documents and is connected to a company network), it becomes significantly more difficult to monitor and protect against cyber threats. Any organisation would struggle to protect against the wide array of threats that can come from the addition of non-employee use like children’s games, online shopping, streaming and torrenting.

The [SentryBay Armoured Client](https://redite.co/armoredclient) package (which includes the Armored Browser) can be used to ensure maximum data security and privacy when working remotely. At [Redite](https://redite.co/home), we recommend this service as it provides an airtight line of defence which includes the encryption of browser data, anti-keylogging and protection against man-in-the-middle attacks all in addition to robust anti-virus software. SentryBay can be configured to meet all virtual-work needs through the protection of applications like Microsoft Office and remote access solutions like Windows Virtual Desktop.

Glossary:

Malware → malicious software designed specifically to cause damage to electrical devices.

Man in the middle attacks → when a cybercriminal intercepts data sent between two users who are unaware that the data in transit has become compromised.