How to Secure Remote Work in 2021

In recent years, there was no real need for robust and secure remote work infrastructure. As a result, the sudden global shift to a work from home (WFH) way of life left many businesses unprepared for running their operations remotely. This presents a real problem as even the slightest vulnerability can be [easily exploited by cybercriminals](https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/).

Working remotely, when managed incorrectly, can leave an organisation particularly susceptible to cybercrime. This, however, is unnecessary; the use of some additional security measures, regular virus scans and secure employee practices can ensure that your business remains protected from cyberattacks when working out of the office.

# Typical security issues working from home

From popular virtual desktop infrastructure (VDI) applications like Microsoft Azure and Citrix to Office 365 and Google Suite applications, [more work is being completed online](https://review42.com/remote-work-statistics/) than ever before. And as remote work is so heavily dependent on these online applications, working from home without the internet would be impossible. Therein lies the issue - as [1 in 13 web requests lead to malware](http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?), the chances of an organisation's data being compromised are greater when working at home than when accessing private networks in offices.

The following common weaknesses in the WFH approach lead to the greatest cybersecurity vulnerabilities:

## Lack of security within home networks.

Typically, in an office, devices are connected to each other on a private network and connected to the internet (or external networks) through a firewall. Without those provisions, it is possible that your network traffic could be monitored, personal data could be stolen and attackers could gain illegal access to your organisation.

At the minimum, a strong (not-default) password should be used when connecting to a wireless router but, ideally, the use of [VPNs (virtual private networks)](https://us.norton.com/internetsecurity-wifi-how-does-a-vpn-work.html) and [firewalls](https://usa.kaspersky.com/resource-center/definitions/firewall) should be used as well. VPNs establish a safe connection between you and the internet so that your data is encrypted through a virtual tunnel and your IP address is hidden from cybercriminals, thereby preventing unwanted intrusions. Firewalls offer further protection from incoming data by blocking malicious files before they enter your device.

An even greater threat is the use of public wifi networks; connecting to the internet through a wireless router which is not password protected and open to the public (like those in cafes) is very dangerous due to the ease with which cybercriminals can connect to your device through that public network. As the users connected to public networks cannot be regulated, it is recommended that no business activity is conducted on such open networks.

## Multiple devices lead to more vulnerabilities.

As homes lack the IT infrastructure commonplace in offices, it is understandable that employees would make use of multiple devices to get their work done. Typically, a mobile device may be used as a hotspot, a tablet may be used as an external monitor or a personal computer may be used for video conferencing. Regardless of the situation, accessing company data from more than one device increases the weaknesses in the organisation's cybersecurity as it is [unlikely that those ancillary devices are suitably protected](https://www.cyberdb.co/cybercrime-is-moving-towards-smartphones-this-is-what-you-could-do-to-protect-your-company/).

Any device which is used to connect to an organisation is at risk of cyber-attacks; naturally, the more devices each employee uses, the chances of a successful attack increase. Although a company laptop may be well protected, other devices, like smartphones, are less secure and cannot provide the same level of security. For example, cybercriminals may be able to infiltrate your organisation through a compromised smartphone which has a malicious app installed; [there exists many fake mobile applications](https://www.zdnet.com/article/mobile-security-these-seven-malicious-apps-have-been-downloaded-by-2-4m-android-and-iphone-users/) which may seem harmless but are able to secretly harvest personal data, passwords and even take recordings using your camera.

## Disaster recovery is not implemented at home.

In the office, IT support staff are often on hand to deal with any technical issues immediately. When daily operations are spread across many locations, providing such services can be nightmarish to manage - it can be impossible to recover from a data breach, theft or corruption when working remotely. Hence, implementing procedures to avoid such disasters is crucial; these should cover regular, encrypted online backups, antivirus software updates and frequent password changes.

# Best WFH practices to implement

To lower the risks of a successful cyberattack and secure your organisation remotely, the following are the best practices to implement:

* **Fortify how your employees connect to your business.** Employees should ensure that their private wifi routers are password protected and they should ideally connect to the internet through a VPN service. The default password on the router should be reset and a strong alphanumeric password should be used if using a smartphone as a wireless hotspot.
* **Invest in powerful antivirus software.** All devices used by employees for work should be protected by a unified antivirus software package. By seeing that the antivirus applications are updated regularly to account for new threats, most cyberattacks can be blocked before any damage is done and contained in the event of a successful breach.
* **Take extra precautions to guarantee impermeable defences.** Although encryption is a must-have when transmitting sensitive information over the internet, it should also be strongly considered for standard emails, messages and video conferences. While firewalls provide a barrier between your devices and malicious software online, [encrypting communication adds an extra layer of protection](https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537) - even if data is stolen, it is worthless in its encrypted state. This can be extended to video-conferencing - if virtual meetings are not encrypted, at least ensure that guests can only enter the meetings with passwords to prevent unwanted users from gaining access.
* **Distribute company-owned devices.** If it can be afforded, issuing employees with devices that are to be used for work only and are equipped with all the required security software, full control can be taken over your organisation’s cyber defences.
* **Prioritise backing up files in a centralised location**. Backups are crucial for data recovery and can be the difference between your business being inoperational for a few hours or a few months. Backups are only effective when made regularly, in a secure, online location - these backups should be as well protected as the original files and should be easily accessible to those working remotely.

# Essential staff training

Beyond installing hardware and software crucial to maintaining your business’s cybersecurity, it is important to train your employees in basic practices that will ensure their safety when working from home. This may include training on:

* **Password protection**. Employees should never recycle passwords (i.e. use a single password for more than one account) as a breach of one account could lead to compromising many accounts. Next, passwords should be at least 6 digits long, containing a combination of upper and lower case letters, digits, and special characters; note the capitalisation of the first letter and ending the password with ‘!’ are common and should be avoided. Employees should be forced to reset their passwords at least twice a year and the “remember my password” feature on online applications should never be used. Two-factor authentication, whereby two passwords of different types (e.g. a password and a pin code) are required to log in, is recommended as a way to further secure employee accounts.
* **Common online threats**. Although the types of threats online are diverse, cyber-attacks are often found in a few common areas. [Phishing and email scams](https://www.phishing.org/what-is-phishing) are common causes of malware entering a system - employees should be suspicious of emails from unknown senders, emails without a subject, emails which do not address the employee by name, and particularly emails that require a link to be followed or an attachment to be downloaded. Next, employees should keep their webcam covered when not in use as it is easy for a cybercriminal to illegally [gain access to it and monitor you and your surroundings undetected](https://www.kaspersky.com/resource-center/threats/webcam-hacking). Lastly, browser add-ons should be kept to an absolute minimum - extensions used for shopping or social networking can easily collect data about your browsing history which can be used against you.
* **Security at home**. The physical security found in offices is often absent in homes. Therefore, it is important that employees log out of devices when they are not in use, keep their devices locked away overnight/ over the weekend, and restrict other family members from using work devices.

# The SentryBay Solution

[SentryBay](https://www.redite.co/products) is trusted worldwide by banks, firms and governments to secure remote access, WFH software and web browsing. By wrapping online tools, remote access solutions, and software as a service (SaaS) applications in advanced security layers, the [SentryBay Armored Browser](https://4462bf0ddbe0d0da40e1e828ebebeb11.cdn.ilink247.com/ClientFiles/reditereskin/Redite4.1/Company/Documents/Armored%20Secure%20Browser%202020.pdf) provides real-time protection against a diverse array of threats including malware, keylogging, screen capture and phishing. By using the Armored Browser with SentryBay’s patented data scrambler, all data entered and transmitted online is completely protected from theft and your devices are kept secure from external threats.

Through the easy-to-use management portal, SentryBay will complement and secure your existing remote work setup, ensuring that you and your organisation are protected and kept safe online 24/7.