



How to set up a remote desktop

How to use a remote desktop, best practices and important things to consider

Remote access is a must-have for today's businesses, especially smaller ones aiming to stay agile and connected.

It brings a host of business benefits, like flexible working, reduced office costs, seamless collaboration, improved productivity, and can even attract top talent.

Here's all you need to know about setting up and securing a remote desktop connection, as well as some important things to remember.

1. Setting up remote access:



Choose your remote desktop software: Pick one that fits your needs and budget, keeping in mind the features, cost, and compatibility.

There are free and premium options available, though no-cost tools might have limited or basic features.



Install your software: Follow your software provider's instructions and install it on both the computer you want to access (the host) and the device you'll use to connect (the client).

Make sure both devices meet the software's system requirements.



Get connected: Enable remote connections in the system settings on your host computer.

Open the remote desktop software on your client device, enter the hostname or IP address of the host computer (you can find this in the network settings), and log in with the host computer's details.



Test your connection: Carry out a few tests from your preferred locations to make sure everything's working.



Disconnect safely: Always disconnect properly from the remote session to prevent unauthorised access.

2. Keep your connection secure:



Use strong passwords: Make sure your team creates and regularly updates strong, unique passwords.



Enable two-factor authentication (2FA): Add an extra layer of security to prevent unauthorised access.



Update software regularly: Keep your remote desktop software and antivirus programmes up to date to patch any vulnerabilities.



Limit access: Make sure only authorised people have access to sensitive information or data.



Consider a VPN: Using a Virtual Private Network (VPN) encrypts your connection for extra security, especially when accessing your remote desktop from public or shared networks.

3. Get the best performance



Tweak your system settings: Adjust settings on both your client and host devices to get the best performance – like lowering the display resolution or turning off unnecessary features.



Get a strong internet connection: Make sure your wi-fi is fast and reliable to prevent lag and dropouts.



Check your security settings: Check your firewall and antivirus programmes are set up to allow remote desktop traffic.

4. Stay compliant



Follow regulations: Make sure your setup complies with data privacy regulations, especially if you're handling sensitive information.



When in doubt, ask: If you're unsure about compliance, always speak to a legal expert for guidance.

5. Keep it simple



Choose simple software: Go for remote desktop software that's intuitive and easy for everyone to use.



Train your team: Make sure everyone knows how to use the remote desktop tools and how to troubleshoot common issues.



Think ahead: Choose a remote desktop solution that can grow with your business so you're ready for whatever comes next.

Need a little more help in choosing the right tool or have questions about setting up?

Speak to our V-Hub Digital Advisers for personalised 1-2-1 support.