Getting set up for remote work

A short, but hopefully useful guide
by Desana

desana

Remote Tech

Computers

The core hardware of any remote workforce. Without them, remote working would simply not be possible.

As an entry point into your business, it's incredibly important to ensure that they're safe, secure and that they can be easily restored if the worst should happen.

It's easy to overlook some key aspects of managing your business's computers, but this will hopefully be a solid starting point.

Apple OS X

1. Set a strong password for your user account

   Change or reset the password of a macOS user account

2. Create and setup iCloud with your company email address

   Manage and use your Apple ID

3. Turn on FileVault

   This ensures that your hard drive's contents are encrypted so if your MacBook goes missing, the contents won't be accessible.

   Use FileVault to encrypt the startup disk on your Mac

4. Turn on Find My Mac

   If your MacBook is stolen, you can use Find My Mac to locate your Mac and lock it.

   If your Mac is lost or stolen

Microsoft Windows

1. Set a strong password for your user account

   Change your Microsoft account password

2. Create a Microsoft User with your company email address

   Create a local user or administrator account in Windows 10

3. Turn on BitLocker

   This ensures that your hard drive's contents are encrypted so if your laptop goes missing, the contents won't be accessible.

   Turn on device encryption

4. Turn on Find My Laptop

   If your laptop is stolen, you can use Find my Device to locate and lock it.

   Find and lock a lost Windows device

desana

Remote Tech

Mobile Phones

Your employees will either have a work provisioned mobile phone, or they may choose to use their own device to do what they need to do on-the-go.

Similarly to their laptops, it's incredibly important that your employees use their mobile devices as safely and securely as possible, whilst ensuring that should the worst happen to their devices, they'll still able to do their jobs.

These steps will ensure that your workforce's mobile devices are ready for remote work.

Apple iOS

1. Set a secure pin code and FaceID/TouchID

   Ensure your pin code is longer than 4 digits!

   Use a passcode with your iPhone, iPad or iPod touch

2. Create and setup iCloud with your company email address

   This should also be done during the initial setup, but if not:

   Set up iCloud on your iPhone, iPad, or iPod touch

3. Turn on iCloud Backup

   If ever your phone goes missing, you can get back up to speed again with a recent backup:

   How to back up your iPhone, iPad and iPod touch

4. Turn on Find My iPhone

   If your iPhone is stolen, you can use Find My iPhone to locate your phone, lock it and (optionally) wipe it.

   Set up Find My iPhone

Google Android

1. Set a secure pin code and biometric authentication

   Ensure your pin code is secure and longer than 4 digits!

   Set screen lock on an Android device - Android Help
   (NB: the guide above does not include fingerprint unlock but, if your phone includes it, you'll see "Fingerprints and Security" under "Privacy" in "Settings")

2. Add your company account to your device

   Add or remove an account on Android - Android Help

3. Turn on Backups

   If ever your phone goes missing, you can get back up to speed again with a recent backup:
   Back up or restore data on your Android device - Android Help

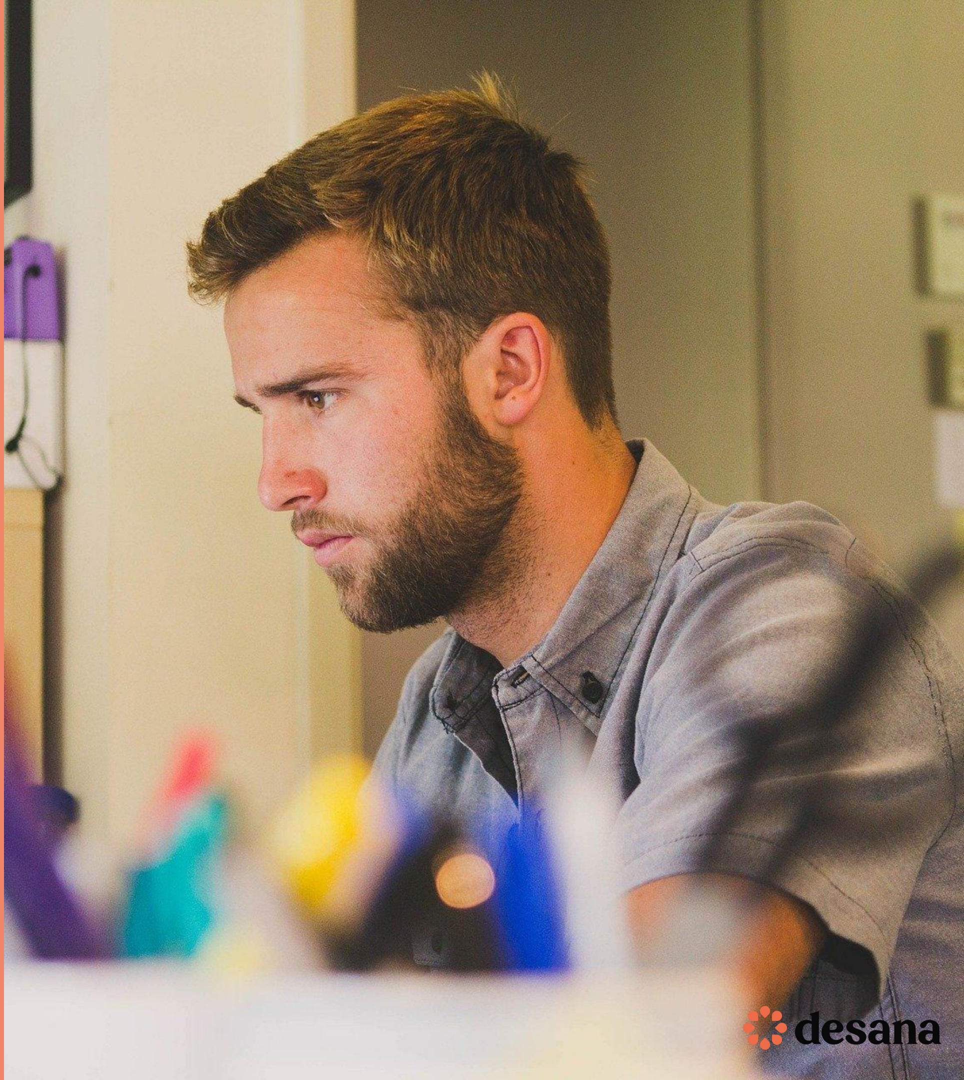
4. Turn on Find My Phone

   If your phone is stolen, you can use Find My Phone to locate and lock it.
   Be ready to find a lost Android device - Android Help

desana

Useful tools for remote work

Tried and tested tools to make the most of remote working



Useful Tools

Security

Two-Factor Authentication (2FA)

Security is really important when working outside of the office. Wherever 2FA is available, we recommend that it is actioned using tools like Authy. We like Authy because security tokens can be accessed even if staff lose their devices.

Procedure for Staff

1. Download Authy to your mobile and desktop https://authy.com/download/
2. Set up secure passwords / pin codes / fingerprint recognition following this guide
3. Set a strong backup password by following this guide. Make it memorable but, if you really think you might forget, write it down and store it securely at home.
4. Explore how to make Authy as secure as possible here

Alternatives: LastPass Authenticator, Microsoft Authenticator

⚠️ IMPORTANT ⚠️

DO NOT register 2FA through a text message or call for this reason.

If there's no option to use Authy (or similar), using just a secure password **without 2FA** can be more secure.

Password Manager

1Password is an example of how to manage team & individual passwords across organisations. It is advisable to generate unique secure passwords for every login and save them to a shared vault or to private vaults as appropriate.

Procedure for Admins

1. The team at 1Password have set up this helpful guide to get you started.

Procedure for Staff

1. Download the app for your laptop
2. Download the browser extension
3. Set your passwords to be super strong
4. Explore how to use 1Password for Mac and Windows
5. Download the iPhone or Android app

Alternatives: LastPass, Dashlane

Useful Tools

Business Continuity

Virtual Private Network (VPN)

What is a VPN?

A VPN allows your employees to access your internal network from a remote location. There are many VPN solutions around, but one of the most popular is OpenVPN.

Why OpenVPN?

OpenVPN provides a flexible way to secure your data communications, whether it's for Internet privacy, remote access for employees, securing IoT, or for networking Cloud data. It's particularly useful for remote work.

NB: some internet service providers may block a VPN from being used. Staff can contact their internet service provider (ISP) and this may be lifted if they explain that they will be using a VPN for work.

Procedure for Admins (this one's for the tech team)

1. Install OpenVPN access server or access via the cloud
2. Follow this quick guide to help get set up
3. Distribute your company's unique Connect Client access link to employees

Alternatives: Perimeter81, NordVPN

Procedure for Staff

This is very much dependent on the setup implemented, but this is a general usage:

Staff have the option to either Connect to the VPN via web browser using their login credentials or Login to the Connect Client.

When the user decides to login to the Connect Client they can download their user configuration files (client.ovpn) and use them to connect to the VPN with other OpenVPN Clients.

Useful Tools

Communication

Messaging

Slack is a great place to keep track of things day-to-day, for teams to connect & for files to be shared remotely. When you first get set up, take some time to get acquainted with creating different channels for teams to use!

Procedure for Admins

1. Get started here
2. There are lot of useful resources to get you up and running

Procedure for Staff

1. Download the relevant Slack app
2. Download the Slack mobile app from your relevant app store
3. You'll have an email invite from the team. Search for it and click the link.
4. Once in, set up 2FA using Authy. You may be prompted to give your phone number as a backup. Don't.

Alternatives: Google Hangouts, Microsoft Teams

Video Conferencing

Our prefered tool is Google Meet but there are plenty of other good ones out there. Zoom has been a particularly popular lately.

Procedure for Admins

1. Get started here

Procedure for Staff

1. Download the Zoom app
2. Get set up on the desktop client
3. Once in, set up 2FA using Authy
4. Start making calls

Alternatives: Google Hangouts, Skype