BLOG POST

# Secure home working on personal IT

## Useful tips and resources for people using personal IT to work from home.

Rick C

In this blog post, I have collected together some useful tips and resources to help you set up your personal IT so that you can work from home securely.

This post is aimed at people new to home working, but the advice itself is not specific to the COVID-19 pandemic. If you use your own devices to connect to business systems, these ten tips will help protect your organisation and yourself from cyber attack.

### First things first

If your organisation has a policy in place for the use of personal IT, that is where you should start.

It's important to follow good practice when handling your organisation's information on your personal devices. This is true whether you're working on a mobile phone, desktop PC, or anything in-between. So, if your organisation has what's often known as a Bring Your Own Device (BYOD) policy, the advice below will just reassure you that things are in hand.

If there is no official policy, following these tips will help to keep your organisation's data and your personal devices secure.

If you're an IT administrator, you can also follow our guidance on how to prepare your organisation and staff to work from home.

## The tips

### Keep your devices up to date

Each of your devices - desktops, laptops, tablets and smart phones - will usually give you a notification to tell you when software or an app is ready to be updated. Don't ignore this message.

Install the latest software, firmware and application updates as soon as you can.

Updating (also known as 'patching') remains the most important thing you can do to protect a device, whether it's your organisation's or your own.

If possible, you should avoid using devices that can no longer be updated, as they will be at a higher risk of attack. If this is your only suitable device, discuss the situation with your employer. They may either accept the associated risks or supply you with an alternative device.

### Secure your accounts with strong passwords

Make sure that all your devices are password protected.

To help with this, we have advice on:

- the use of password managers
- choosing a strong PIN or password
- securing smartphones and tablets with a screen lock
- setting up two-factor authentication on your online accounts

### Only use approved software and collaboration tools

Before downloading any software or tools for work purposes, check that they are approved by your organisation.

You should only download apps for mobile phones and tablets from manufacturer-approved stores like Google Play or the Apple App Store. When using apps for conferencing follow the latest NCSC Guidance, introduced by this blog post.

Do not use any jailbroken devices or 'rooted' Android devices for work.

### Protect against viruses

Make sure you are running antivirus software on your desktop or laptop. The NCSC provides tips to help you understand how to use antivirus tools.

### Switch on your firewall

Firewalls help protect your computer when you’re connected to a network. Most popular operating systems, including macOS and Windows, now include a firewall. You should switch this on to help protect your device.

### Back up important data

Make sure that important files are backed up in case something happens to your device. If your organisation already provides you with access to cloud storage, you should use this. If not, you should speak to whoever handles your IT about setting something up.

You shouldn't back up your organisation's data to your personal storage spaces. This could easily happen without you realising though, so it's another topic for you to discuss with your IT department.

### Set up a separate account

Keep your work information separate from your family's by creating a separate account on your personal desktop or laptop. This will help to avoid any accidental access, or loss of sensitive information by family members.

### Protect your Wi-Fi

Enable password protection on your home Wi-Fi, if it isn't set up already.

Your IT department should be able to advise you on when, and how to use Virtual Private Networks (VPNs) to connect to secure workspaces.

### Watch out for phishing emails

To protect yourself from phishing scams you can follow our guidance on:

- spotting phishing emails
- making yourself a harder target
- taking action if you've clicked on a link or entered details

### Take our 'Stay Safe online' training

The NCSC's Stay Safe online interactive training is a good place to start building your security knowledge. The training covers how to:

- defend yourself against phishing
- use strong passwords
- secure your devices
- report incidents

## Regular checks

Once you have your IT set up so it works well for you, and keeps your organisation's data safe, you may be tempted to put a tick next to 'cyber security' on your to-do list.

That's OK, you've probably earned that. But it's important to regularly run though this list of tips, just checking everything is still as it should be. Your devices are up to date, your antivirus is reporting everything green and your backups are current.

If you're working to your organisation's BYOD Guidance, you should keep an eye out for changes in policy. Ultimately, however, it remains the responsibility of the organisation who employs you to manage the risks to its data when using BYOD solutions.

The NCSC also maintains sections on our website for small businesses, the self employed and individuals. These are kept regularly updated with useful cyber security information.

**Rick C**
**Cyber Risk Advisor, Digital Government Team**

**WRITTEN BY**

Rick C

Cyber Risk Advisor, Digital Government Team

**PUBLISHED**

18 May 2020

**WRITTEN FOR** ⓘ

Small & medium sized organisations

Individuals & families

Self employed & sole traders

**PART OF BLOG**

NCSC publications