# PROTECTING THE DATA ON YOUR SMARTPHONES / MOBILE DEVICES

As individuals, we use our smartphones and mobile devices (ie: laptops and tablets) every day for a variety of casual uses but as business leaders we're using them in ways that are key to how our businesses run. Your devices are likely the source of the majority of your and your business's information and data, and keeping it all secure is paramount.

If your device is lost, broken, stolen or hacked in any way then this will have an immediate and likely detrimental effect on your business. And not just for yourself - the same goes for any employees you have. Many companies have bring-your-own-device policies with their employees, and almost all will be using their smartphones for work-related uses too (even if it's just emails).

Security threats related to personal devices are among the greatest that businesses currently face and so knowing the risks about how to protect yourself to help negate these things happening will be of immeasurable benefit.

Here's some top tips to help you protect the data on your smartphones and mobile devices and those within your business:

- Have a security policy for all people within your business which covers personal device use. Identify the risks,what can be done to negate the risks, and whose responsibility it will be (with overall responsibility always being taken by the business leader(s) within the organisation). Remember that this should cover both technical *and* user issues / risks.
- Ensure that all mobile data is backed up regularly. Hard-drives are useful but can similarly be lost or damaged, and backing up across more than one is ideal if this is the option you go for. Ideally use a secure cloud service (though avoid personal accounts and ensure a business account is created and used).
- Turn on automatic updates on all the apps and software you use - many of the updates will be security updates! This really is one of the best defenses and one that so often gets missed. If automatic updates aren't available for your devices, apps, software, etc. then ensure that you have regular reminders to check for updates.
- Ensure that all devices are protected with passwords or pins (or both!), and even biometrics where possible.
- Ensure that encryption is always turned on where possible - this will provide a lot less to worry about if your device is lost or stolen.
- Install anti-malware apps / software.
- Ensure that both you and your staff are aware of cyber threats - regular training is key as this is an evolving threat. There are free online training courses available from the government (please see the link at the end of this guide) tailored for small businesses, they usually only take about an hour to complete.
- Use a Password Manager. This will help you keep note of your passwords in a secure way rather than them being available in a document on your device(s).

- If possible, use a VPN when outside of your office. Free public WiFi hotspots are one of the most common ways in which people can be vulnerable to cyber attacks. These networks can be interfered with and so cyber criminals are increasingly using these networks. Using a VPN service (personal or corporate) can help to minimise this risk and will ensure that your users' traffic is secure while they are using a device on these networks.
- Always download trusted apps and software - ie: do your research before hitting 'download'.
- Never click on suspicious links (no matter how tantalising that celeb gossip might sound!).
- **And definitely, 100% do not use the same password for everything!**

There's a wide variety of cyber-security risks for smartphone and mobile device users today, and these risks aren't going anywhere - in fact, they're likely to continue to increase.

Protect your smartphone, your mobile devices, your information and data, and therefore you and your business by implementing these simple measures.

**The government's National Cyber Security Centre (NCSC) have a lot of useful guides, training and more on their website: [https://www.ncsc.gov.uk/collection/](https://www.ncsc.gov.uk/collection/)**

*Save trees, save paper. Please consider the environment before printing this document.*

**BETTER
BUSINESS
NETWORK**