

# THE 9 STEP GUIDE TO MOBILE DEVICE CYBER SECURITY

Practical advice for government agencies and private sector organisations following UK best practice recommendations

NUFFIELD TECHNOLOGIES

# CONTENTS


Introduction

The Cyber Security Challenge

Strategies for Hardened Security: Overview

1. Conduct a Mobile Device Risk Assessment

2. Procure Secure Devices

3. Keep Devices up to Date

4. Use Mobile Device Management

5. Follow Security Fundamentals

6. Create Secure Logins

7. Vet and Restrict Third-Party Software

8. Use Data Backup and Recovery

9. Manage and Educate Users

Checklist

Further Resources

About Nuffield Technologies

Contact Details

# INTRODUCTION

## ABOUT THIS GUIDE

This eBook provides an introduction to the steps you should take to securely deploy devices and protect your department or organisation.

Recommendations are based on best-practice advice from leading sources, including the UK government's National Cyber Security Centre.

Aimed at government bodies, the guide includes links to mandatory policies and guidelines – for instance, JSP 604 Defence Networks Governance for defence forces and contractors, and advice for local councils.

It also provides a useful introduction for private businesses that want to follow best practice and secure their future.

**Data Point:**

The famous WannaCry ransomware attack of 2017 cost the NHS £92m as a result of services lost during the attack and IT costs afterwards. (1)

1. WannaCry Attack



# THE CYBER SECURITY CHALLENGE

## THE SCALE OF THE PROBLEM

According to one report, if **cybercrime** was measured as a country it would be the third-largest economy in the world, behind only the USA and China. (1)

The size of the challenge is immense – and no one is immune. The public sector in particular is considered ripe for the picking by bad actors looking for financial gain. Also, hostile states actively target the UK's cyber infrastructure.

As a result, police forces, schools, the NHS and many more public organisations – and half of UK businesses (2) – are subjected to cyber security **attacks or breaches**.

### Mobile devices - a cyber security risk?

In particular, the growing use of mobile devices – and a labyrinth of different practices including bring your own device (BYOD), work from home (WFH) and blended working – present an opportunity for criminals.

In many cases, government agencies and businesses are simply not deploying devices with the correct security processes. This can lead to data breaches, financial and productivity loss, and legal consequences for breaking data protection and GDPR laws.

> In May 2024, the UK's Ministry of Defence experienced a major data breach, in which personnel information was hacked from a third-party payroll system. (3)



1. Scale of cyber crime
2. Half of UK businesses breached
3. Ministry of defence payroll system hack

# STRATEGIES FOR HARDENED SECURITY: OVERVIEW




## SO WHAT SHOULD YOU DO?

Combatting the problem is challenging and requires constant vigilance. Social engineering tactics such as phishing are becoming increasingly common – even IT novices can now purchase off-the-shelf 'phishing as a service' software to help launch attacks.

However, if you follow best practice advice you can deter the VAST majority of threats.

### The essentials of cyber security

In this 9 Step Guide to Mobile Device Cyber Security, we've summarised the essentials of device cyber security, taking UK government publications and websites as our primary sources.

We also recommend you investigate **Cyber Essentials**. This is the government-backed certification scheme that can help you maintain high security standards. If you're a business applying for government contracts, Cyber Essentials certification is a mandatory requirement.

Read on for our nine steps for mobile device cyber security.

> In August 2023, the Electoral Commission disclosed that its database had been breached, revealing the names and addresses of approximately 40 million people. (1)

1. Electoral Commission breach

# STEP 1

## CONDUCT A MOBILE DEVICE RISK ASSESSMENT

**Log hardware such as mobile computers and tablets and assign each user a risk profile.**

What increased threats may occur if you introduce or broaden the use of mobile devices? When you understand these threats, you can introduce measures to minimise the scale of the problem.

### Do this:

- **Log every device in your organisation** and its IMEI (International Mobile Equipment Identity) – for instance, 'Zebra Technologies TC58e 350163451934565'.
- **Log every user in your organisation,** including their name, their title and their department – for instance, Jackie Smith, Logistic Supply Specialist, Royal Logistic Corps.
- **Assign a risk score for each user** based on their role, the data they access and their access privileges – for instance, 'medium', based on a low/medium/high rating.

This information will help you track all devices, prioritise the highest security for the highest-risk individuals and properly manage your device estate.

A mobile device management (MDM) platform can help you with all of the above. (See step 4).

### Data Point:

HMRC revealed that 635 devices had been lost or stolen in 2023, including 387 mobiles, 244 tablets and4 USB drives. (1)

1. HMRC tablet theft

# STEP 2

## PROCURE SECURE DEVICES

**Choose a trusted provider that offers a long support window.**

When buying devices, device security takes precedence – **even over functionality.**

### Do this:

- **Buy from a trusted provider.** You should also research their supply chain. Have there been any concerning cyber-attacks on their – or their partners' – infrastructure?
- **Look for long support periods.** Only devices with regular system and security updates can be used safely. Find out how long your proposed devices will be supported for – this will help determine if they will provide a good return on investment.
- **Consider Android devices.** Using Android's open-source software, some manufacturers can extend support for up to 10 years, compared to five or less for iOS (Mac).
- **Consider zero-touch options.** Zero touch allows you to preconfigure items with the appropriate security straight out of the box. This is a time-saver – and security hardener.

### Data Point:

Some IT experts warn against buying devices from China, because they often come loaded with apps that **can send private data to third parties without consent**. (1) Many technology companies in China are partly state owned.

1. Chinese Android phone leaks

# STEP 3

## KEEP DEVICES UP TO DATE

**Automate updates and report on uptake to ensure compliance.**

A report (1) showed that 51% of respondents would prioritise keeping photos on a full device over making space for an essential OS update.

Don't let employees treat updates as a lifestyle choice.

### Do this:

- **Automate and mandate updates using your MDM.** This should include OS updates, browser updates and app updates. In cases where you can't update an app manually, ensure users are aware they must comply with update policies.
- **Monitor user compliance using your MDM.** Sometimes, users may be able to put off updates, or a device won't update until it is restarted. Monitor uptake of updates and alert non-compliant users accordingly.
- **Retire devices before security support ends.**

### Data Point:

Average smartphones receive security updates for three years, but specialist rugged provider **Zebra Technologies** can continue to support phones for as long as 10 years.

1. Prioritising photos over updates

# STEP 4

## USE MOBILE DEVICE MANAGEMENT

**Deploy an MDM to log and track devices and assign user-access privileges.**

With the increased rollout of devices in the workplace, it's crucial you take a methodical and organised approach to logging machines and user profiles. You can then assign privileges appropriately.

In the modern workplace, having no control won't cut it – you should use a mobile device management (MDM) platform. This can help you centrally manage, monitor and secure your machines.

### Use an MDM to:

- Assign users with privileges (for instance, which apps they can and can't access).
- Recover lost devices.
- Remotely wipe devices if security is compromised.
- Deploy security updates.
- Enforce good practice in your policies, such as screen locking after a period of activity.
- Roll out a safer bring-your-own-device (BYOD) policy by separating work from personal data. For instance, on Android you can use Work Profiles to keep work and personal information separate. For iOS, an MDM can separate corporate and personal data.

All of these functions can be undertaken remotely, at scale. The NCSC website offers detailed guidance on configuring most major platforms, as well as recommended policies.

### Data Point:

According to Mobiles.co.uk, the average UK adult has lost two smartphones. This adds up to 98 million smartphones since 2007. (1)

1. Smartphone losses

# STEP 5

## FOLLOW SECURITY FUNDAMENTALS

**Consider incorporating the Principle of Least Privilege (PoLP), Zero Trust and a virtual private network (VPN).**

Several key principles and policies should be at the heart of your mobile device security strategy.

- **Principle of Least Privilege (PoLP) -** Only give employees the bare minimum access they need to perform their roles – and nothing more. This means restricting access permissions and authorisations appropriately. Following this one rule will vastly harden your security.
- **Be a Zero Trust organisation -** Zero Trust eliminates the distinction between an internal 'secure IT space' and external threats – it assumes the bad actors are already in your network. With this mindset, every request for access is scrutinised with a 'default deny' security posture – until valid credentials are demonstrated. Find out more.
- **Use a virtual private network (VPN) -** A VPN creates a digital connection between a device and a remote server. This server encrypts your data and hides your IP address from potential hackers. It makes connecting to company servers much safer while working on a home or public network.

### Data Point:

In 2021, a disgruntled former employee of the South Georgia Medical Center in the USA downloaded patient data to a USB drive the day after quitting, then **leaked this data**. The reputational damage was devastating. (1)

1. Disgruntled employee hack

# STEP 6

## CREATE SECURE LOGINS

**Use tools such as biometrics, MFA and 2FA, strong passwords and password management software to help secure access.**

One report suggests 81% of security breaches are caused by weak, compromised or reused passwords. (1) Yet many people still insist on using passwords that have cyber criminals rubbing their hands together, such as 'guest' and '12345678'. The results can be devastating.

### Do this:

- **Use biometrics such as a fingerprint or facial scan** to unlock phones. At the minimum, use a six-digit PIN code.
- **Use multi-factor authentication (MFA)** or two-factor authentication (2FA) for accessing sensitive data or systems.
- **Enforce strong passwords.** Mandate strong, memorable passwords using the 'three random words' technique – such as 'rocktentfoxglove'.
- **Use password management tools** to securely store and manage passwords.

### Data Point:

When the UK government's National Cyber Security Centre – otherwise a trusted and excellent source for security advice – was found to have used the code '1234' on internal doors, the nation's press swooped. DON'T follow this example. (2)

1. Weak passwords
2. NCSC entry code

# STEP 7

## VET AND RESTRICT THIRD-PARTY SOFTWARE

**Consider the pros and cons of third-party apps and take a structured approach to app permissions management.**

'By using this app, you agree to give XYZ Company control of your phone and access to your camera, microphone and conversations.' Are you happy with ceding this level of control and security for a 'handy tool'?

### Do this:

**Decide if an app is permissible**

- Consider your business need versus the permissions asked for and the data implications of those permissions.
- Investigate the app's reputation and any past security issues.
- Consider geopolitics. Does this app, or could it, emanate from a hostile state?

**Create an allow or deny list**

- Your MDM will help you tightly control access to apps on devices.
- An allow list – 'only these apps are permissible' – is the least time-intensive to incorporate: you simply need to list only those apps people are allowed to use. However, it is restrictive. Also, if users want a new app to be added, it will require approval from the IT team.
- A deny list – 'don't use these apps' – may provide more freedom and flexibility, but it requires maintaining a list of suspicious apps. This can be time-consuming.

Most security accreditations (including Cyber Essentials) mandate that you maintain a list of allowed apps.

### Data Point:

On 16 March 2023, the UK government banned the social media app TikTok on its devices. The US and Canadian governments, and the European Commission, have a similar policy. (1)

1. TikTok ban

# STEP 8

## USE DATA BACKUP AND RECOVERY

**Enforce a structured data backup and recovery policy to minimise disruption in the event of a cyber attack.**

Whether it's caused by a cyber breach, a hard drive failure or human error, losing data can be devastating. Follow these best-practice principles.

### Do this:

- **Decide which data you need to back up.** This is likely to include documents, emails, contacts and calendars.
- **Use the 3-2-1 principle for backing up data,** which is considered best practice and is most likely to ensure you avoid a disaster.

  **3 -** Keep three copies of your data – the original data on your primary device and two copies.

  **2-** Use two different storage devices. For instance, an external hard drive, a flash drive or cloud storage.

  **1 -** Maintain one backup off site, to prevent data loss due to a local disaster. Typically, this will be a remote cloud storage option.
- **Regularly test your backups** and the recovery process.

### Data Point:

Nearly half (48%) of UK small-and-medium-sized businesses have lost company or customer data in the past five years, something which has cost them, collectively, over £5bn since 2019. (1)

1. Company data losses

# STEP 9

## MANAGE AND EDUCATE USERS

**Introduce awareness and learning programmes to keep your people informed and compliant.**

PoLP, strong passwords, VPNs and other methods discussed in this ebook help, but your biggest defence against criminals is a cyber-aware workforce.

### Do this:

- **Educate your teams.** Some specialist cyber security providers offer in-house tuition, reminders, and gamified training to test awareness and resilience.
- **Beware social engineering attacks such as phishing**, where bad actors gain the trust of a target and manipulate them to give up logins, data or money. This is by far the biggest form of cyber attack or breach (it accounts for over 80% according to the UK government (1) ) and you must educate your teams accordingly.
- **Create a joiners and leavers policy**. Introduce a structured process so that new employees have access to secure equipment on joining, and leavers' authorisations and logins are revoked.

### Data Point:

According to Forbes, (2) new employees are a soft touch for phishing campaigns and are actively targeted by criminals. In fact, bad actors use AI tools to scan LinkedIn for individuals posting about new roles. Once they find a promising new starter, they begin a campaign of deception...



1. Phishing prevalence
2. Forbes article

# CHECKLIST

## ESSENTIALS FOR DEVICE SECURITY

**1. Conduct a Mobile Device Risk Assessment**
Log hardware such as mobile computers and tablets, and assign each user a risk profile.

**2. Procure Secure Devices**
Choose a trusted provider that offers a long support window. Retire devices before security support ends.

**3. Keep Devices up to Date**
Automate updates and report on uptake to ensure compliance.

**4. Use a Mobile Device Management System**
Deploy an MDM to log and track devices, and assign user-access privileges.

**5. Follow Security Fundamentals**
Consider incorporating the Principle of Least Privilege (PoLP), Zero Trust and a virtual private network (VPN).

**6. Create Secure Logins**
Use tools such as biometrics, MFA and 2FA, strong passwords, and password management software to help secure access.

**7. Vet and Restrict Third-Party Software**
Consider the pros and cons of third-party apps and take a structured approach to app permissions management.

**8. Use Data Backup and Recovery**
Enforce a structured data backup and recovery policy to minimise disruption in the event of a cyber attack.

**9. Manage and Educate Users**
Introduce awareness and learning programmes to keep your people informed and compliant.

## Further Resources - Useful Links

**The National Cyber Security Centre (NCSC)**
The UK government's online portal for general advice and guidance. Your essential resource for best practice.

**The National Cyber Security Centre: Device Security Guidance**
Specific advice from the NSCS regarding device security.

**The National Cyber Security Centre: Public Sector Portal**
Cyber security guidance for public sector organisation employees.

**Government Cyber Security Policy**
A referral point for all government bodies to check they are complying with mandatory rules around mobile device management. Also a useful reference point for private organisations.

**Cyber Essentials: The Government-Backed Accreditation Body**
Follow Cyber Essentials to integrate robust cyber security and get universally respected accreditation. Mandatory for government contractors.

**Security of Government Devices: A Parliamentary Debate**
Hansard's transcription of the parliamentary debate: Security of Government Devices. An insight into one of the most recent cyber security debates, which includes the ban on TikTok.

## Government Bodies' Specific Advice

**JSP 604 Guidance for Defence Networks Governance.** Specific advice for the nation's highest security environment. Used across the Ministry of Defence.

**The Local Government Association 360 Framework.** A resource for councils to help explore and improve their cyber security culture.

# ABOUT NUFFIELD TECHNOLOGIES

## WE DEPLOY DEVICES SECURELY

Established in 2001, Nuffield Technologies solves device procurement and software development challenges for commercial and public-sector clients.



We help highly regulated sectors in the UK purchase and deploy tough devices securely and safely. Our clients include Boeing, The Ministry of Defence and many other public and private sector organisations.

We partner with Zebra Technologies, a rugged device provider that offers more hardened security for organisations above and beyond that offered by other device manufacturers.

We also work alongside Zebra to provide tailored device cyber security solutions for public sector clients.

# DEFENCE FORCES DEVICE SECURITY

## CASE STUDY

In 2020, Nuffield Technologies, in partnership with Zebra Technologies, helped a large defence organisation deploy devices in environments with limited WiFi coverage.

To meet these challenges, we created a unique security layer for the Android OS. Deploying both Android Enterprise features and Zebra Technologies' software tools, the solution, called ASP, provides a method for operating devices securely offline.

Device hardening, file transfer and remote updates could all be delivered offline using existing defence networks and connecting to the host system via USB.



Read more about the case study **here**.

# DISCLAIMER

None of the advice in this eBook is definitive or exhaustive. You should use it as a starting point for your investigations, and research further recommendations and compliance guidance for your sector or industry.

Nuffield Technologies takes no responsibility for any actions organisations take as a result of advice contained in this eBook. Always undertake your own due diligence.



NUFFIELD TECHNOLOGIES

**Nuffield Technologies**
42 High Street, Poole Dorset
BH15 1BT, United Kingdom

hello@nuffieldtechnologies.co.uk
01202 122670
www.nuffieldtechnologies.co.uk