FREEFORM DYNAMICS

In association with

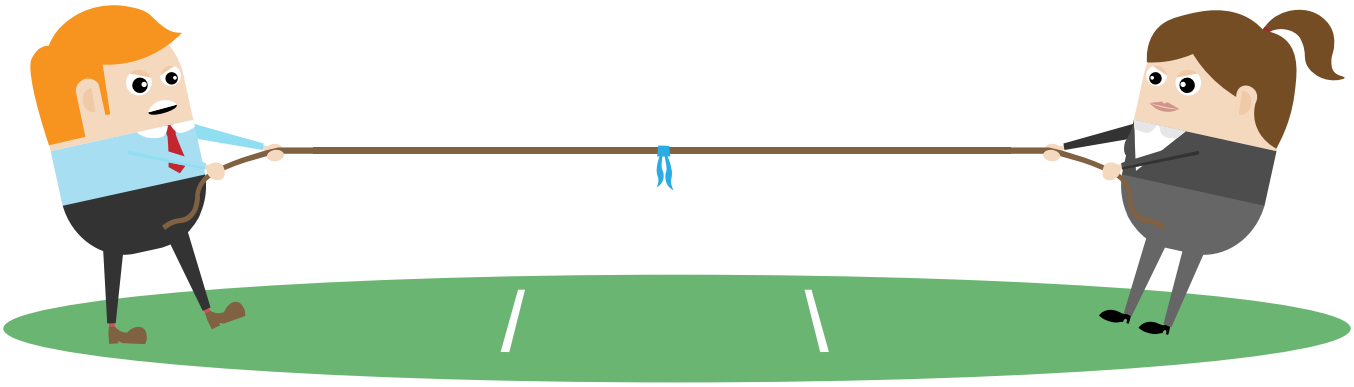
5APP

Safe & Secure Mobile Working

A no-nonsense guide to protecting you and your company

With the compliments of Freeform Dynamics and 5app

Tug of war between convenience and security



Convenience **Vs** Security

For many of us, our work life and social life are becoming intermingled. We can use our phones, laptops, tablets and USB sticks for business or pleasure and we like to use these devices for whatever we want to do at any given moment.

We don't want to return to the office or turn to a different computer, just to do 'work stuff'. We like the flexibility of working with whatever device is convenient at any moment, and there's no denying the benefit to our employers of this arrangement.

Did you know?

Data is more likely to be lost through mistakes and thoughtlessness than deliberate hacking or theft.

However, these same employers are probably more nervous than we are about this state of affairs. They usually have a great deal of control over all the boundaries of the organisation's IT system, except for mobile users and their devices. They fear that confidential information might fall into the wrong hands. After all, a serious breach could damage their reputation and lead to legal action and financial loss. Understandably, employers would prefer to remain in control of all of our business-related online activities.

At a personal level, you could suffer harm if someone stole or copied your address book, photos and other confidential information, even if you had a backup copy somewhere. However, that pales compared to the potential consequences for your organisation.

To a serious attacker, the most precious pieces of information you store are your access credentials to corporate and other IT systems, whether they're private networks or website login pages. Such a thief could wreak havoc simply by pretending to be you.

Did you know?

The best cyber-attacks from the bad guys' point of view are the ones you don't realise have happened until it's too late.

You are in the front line when it comes to your organisation's information security. If an attacker can exploit you, they will. We don't want to make you paranoid, but it does make sense to develop good security habits and behaviours that you maintain at all times. The hacker sees you as the weakest link, but that doesn't mean you need to prove them right.

What the bad guys want from you

At the lowest level, the 'prize' for stealing or finding your mobile computing device is a quick sale down the pub. At the next level, it's getting and exploiting your personal information. But, the big prize is using your credentials to get sensitive information out of your corporate computer system.

And who's to say that the buyer down the pub doesn't have one of the bigger prizes in mind?

The chart below shows what's likely to happen first as solid lines. The dashed lines show what may happen next.

The only good outcome is that you get your device back intact.

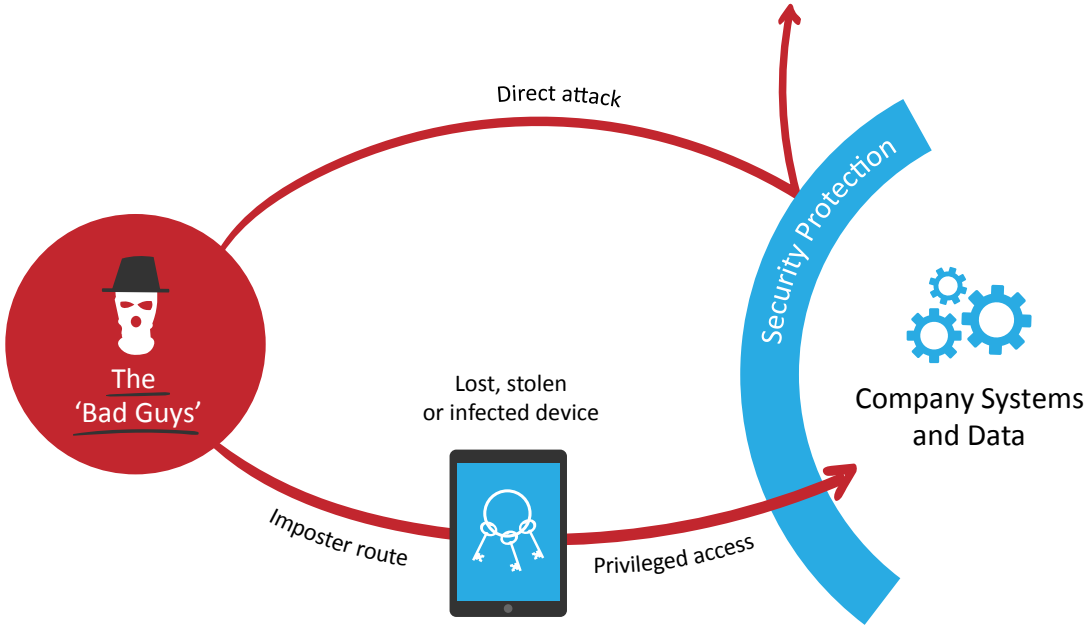
The low-level hacker might simply lift your email addresses and your personal details so they can send unsafe emails pretending to be you. If your photographs are 'interesting', they might try for a ransom in return for your device. Or they may try logging in to your social sites to cause you embarrassment.

On the other hand, the most serious hackers are extremely professional in their approach to stealing your employer's secrets as well as your valuables. They are often sponsored by organisations with very deep pockets such as nation states, organised crime groups or political activists. They can spend months planning their attacks to maximise their chance of success. In their case, success is getting the prized information on the one hand while, on the other, avoiding detection for as long as possible. Like a double agent from a James Bond film, their malware slides unobtrusively into your organisation's IT systems, often using your mobile device as a back door. Once inside, it covers its tracks and can send company secrets back to its owner for months, or even years, without being detected.

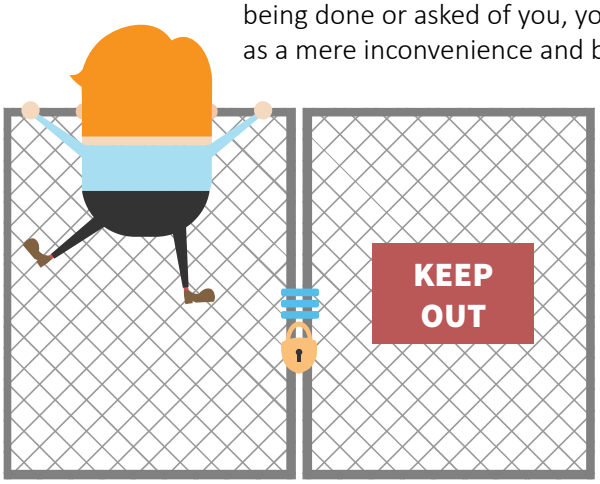
The hacker's best friend is the user that does something they shouldn't, like leaving their device unattended, clicking on a bad link in an email, downloading a dodgy email attachment or plugging in an innocuous-looking USB memory stick of unknown origin.

Why not just let IT take care of things?

Your IT team has probably built a pretty good shield around your organisation's IT systems. This will protect data held centrally from many direct attacks. But it can't guard against accidental security breaches caused by you as an authorised user, or deliberate attacks by imposters who use your device to masquerade as you.



Given this picture, it's important that you work with your IT folks, rather than against them, so let's take a minute to consider the world from their perspective. If you understand why certain things are being done or asked of you, you're less likely to dismiss an important security measure as a mere inconvenience and be tempted to look for a way past it.



When it comes to devices, while you would ideally want total freedom of choice, your IT team might restrict the types and even models of equipment that they will allow onto the network. This isn't because they are on some kind of control trip, it's because they are almost certainly better informed than you about which devices are safer, and which are more vulnerable to attack. Encouraging you to use familiar brands and models also makes it easier for them to provide support, which is in your interest, as well as theirs and your employer's.

Another measure IT teams sometimes take is to restrict exactly how you can gain access to more sensitive systems and data. They may, for example, mandate the use of a particular mobile app, even when alternatives exist. Another common precaution is to disallow the use of apps altogether in relation to some types of data, forcing you to go through a web browser instead. The idea here is to prevent copies of data ending up stored locally on your device.

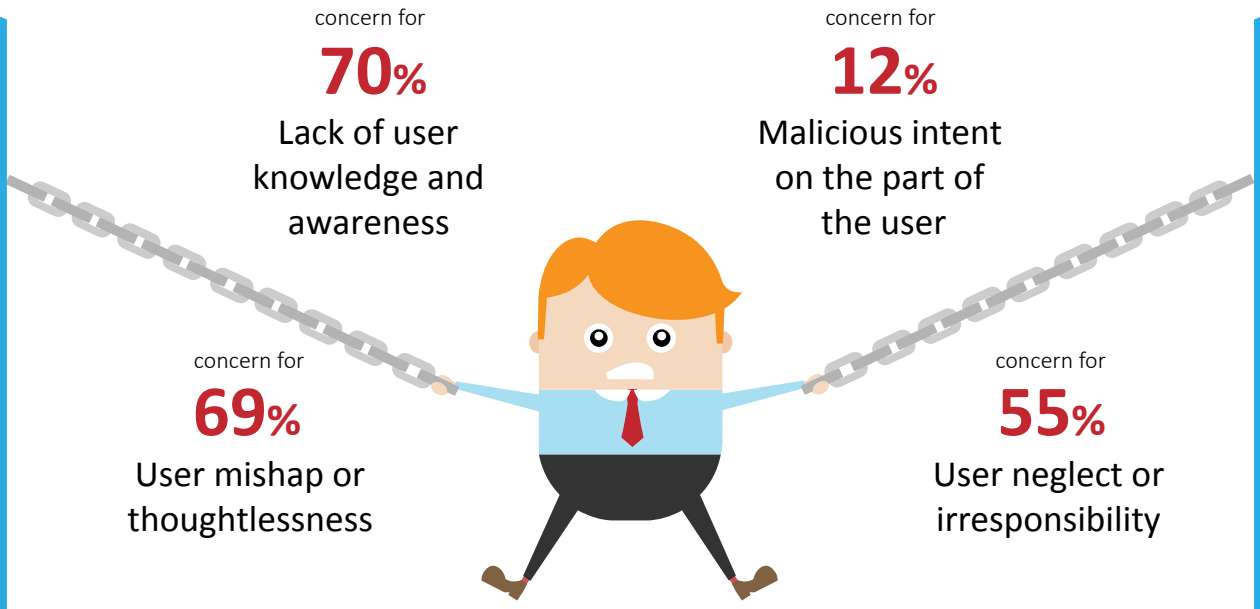
Whether it's these or other measures, it's important to accept that your IT team has put them in place for a reason. But also remember that they can't deal with all types of risks so you still need to play your part and avoid becoming the weakest link.

Did you know?

No technology measure, no matter how capable, can completely protect you from accidents or attacks.

How can you avoid becoming the weakest link in the security chain?

Cyber criminals are always looking for an entry point to an organisation's IT systems and an unaware user is a very weak link in the security chain. Here are some sobering statistics:



% of IT / BUSINESS PROFESSIONALS who consider these areas of exposure or uncertainty to be a concern in the mobile computing context.

Let's take a look at all the opportunities you have to protect yourself and your employer from attack.

Loss, theft and intrusion

In the event of theft, loss or even attempted compromise (when you've left your mobile device lying around) a good initial deterrent is a timeout lock. Set it for the minimum time you can live with. This means that every time it locks, you'll need to unlock it. But it also means the would-be information thief/intruder has to do this too. Another great measure is to encrypt your files (which basically scrambles them); this can often be done easily enough through your device settings. For both measures, make sure you use un-guessable key codes if asked for them. Finally, so you can get on with your life quickly in the event of loss or theft, make sure you back up your mobile device regularly.

Did you know?

The login credentials saved in mobile apps and your internet browser are often more valuable than data actually stored on your device.

Then you have airborne theft and compromise - people on the same network being able to see your files or intercept your transmissions. This is most likely when you are using a public Wi-Fi connection. Your company email is probably safe if it has been set up by IT, but think twice about typing passwords or sending/receiving sensitive information outside of this.

You should also keep Bluetooth switched off, or certainly 'non-discoverable', until needed because it can let attackers in. However, they would have to be within about ten metres. Check with your IT team if you're unsure of how to change Bluetooth settings.

Infections and leaks

The most common route to infection is for a cyber-criminal to send you an email that looks authentic or makes a 'too good to be true' offer. If the words in an email don't ring true, don't click on a link or open an attachment. If it's a stranger, it's easy to ignore. If it appears to come from a friend or colleague, still take care. Check the addresses that appear when you hover over the links, if they look odd, don't click. And certainly don't be sucked in to giving away any information even if it does look as if the bank or the tax authorities are writing to you. They wouldn't ask for anything of a sensitive nature via email.

USB memory sticks are a handy way to carry around large amounts of information. The first piece of advice is that if it's sensitive information "don't do it". If you really have to, then "encrypt it". While on the subject, hackers have been known to leave new-looking USB memory sticks in car parks, expecting they'll almost certainly be plugged in to a networked machine. If you find such a stick, even if it appears to be in its original wrapping, take it straight to the security or IT folk for investigation.

You may be tempted to use a generally available (and often 'free') cloud service for storing or sharing confidential information. Don't be tempted. Ask IT which services they regard to be safe.

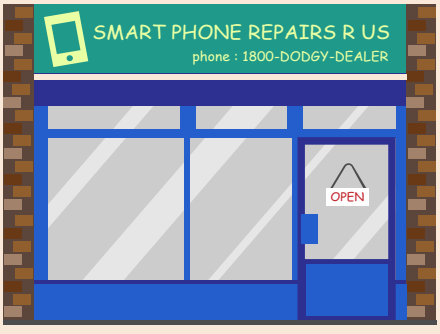
When doing anything confidential, make sure that no-one can be 'shoulder surfing'. Not only might they be snooping for inside information, they may be looking for usernames and passwords. They can watch (or film) keystrokes just as easily as they can read screens. And, although not really part of this briefing, be extra careful about what you do in public places, especially airport departure lounges, trains and aeroplanes. And that applies to speaking loudly and leaving paper and notebooks around when you nip to the loo. It's sad, but you do need to be a little bit paranoid if you ever work with sensitive information.

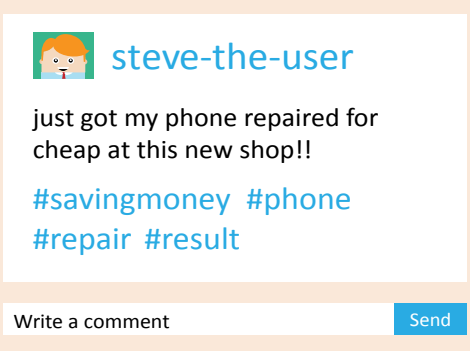
Repair and end of life

If your device needs a repair, you'll have to provide the passcode or swipe pattern so they can test it. Can you trust your repairer not to copy its contents, or worse? Best to see who your organisation recommends.

When it's time to replace your machine, you will migrate all the essential data to your new device. But, will you be diligent about deleting it from the old one? Does your company insist on professional memory wiping before you can pass it on?

Some companies would prefer simply to destroy redundant devices. But most people replace mobile phones while they still have a cash value, either to you or to, say, a charity. Make sure you know your company's policy.





Safe software

Don't disable or bypass in-built security measures in your device. They're there for a good reason. Some people 'jailbreak' or 'root' their mobile phones to be able to install unapproved software or, maybe, to sidestep some of their service provider's restrictions. Whatever the motive, you end up with a machine that can't be upgraded automatically with new security measures or, indeed, one that IT can't help with when things go wrong. As they are bound to do.

Acquire your apps from somewhere safe; either the firm's own app store or the device's recommended store (typically, Google, Apple or Microsoft.) Check whether any store you use is monitored and scanned for malware. Not all of them are. Alternative sites could offer free versions of paid-for programs. This may tempt you, but the chances are very high that the software will cause you problems. It's worth bearing in mind that a lot of free software sends information to its advertising partners, who automatically inherit any permissions you've granted to the publisher.

Employer guidelines

No-one should object to some basic safety rules, like "don't leave your device in an unattended car", "don't disable the password mechanism" or "don't use unapproved public cloud storage services for confidential information". Your organisation will give you DO and DON'T guidelines and it will explain the power it will expect over your devices in the event of loss, theft or compromise. It might ask you to agree formally to allow it to remotely access the device and destroy its contents. If it's a combined work/pleasure device this might alarm you. But, if you back up your personal data regularly, you'll feel more relaxed about signing such an agreement.

Did you know?

Storing business data in consumer cloud services designed for saving your photos and music could expose both you and your company to legal action.

Make sure you read and understand all security warnings and notices that are issued from time to time. You can't push them to one side to read later – you know you never will.

Report anomalies

Finally, be sure to report odd behaviour to the security team. If your mobile device starts behaving strangely – lots of ads or popups, decreased battery life, slower performance than usual, unexpected crashes, etc – then it could be that malware is at work inside. If available on your device, use antivirus software and scan periodically to root out anything that might have sneaked in unnoticed.

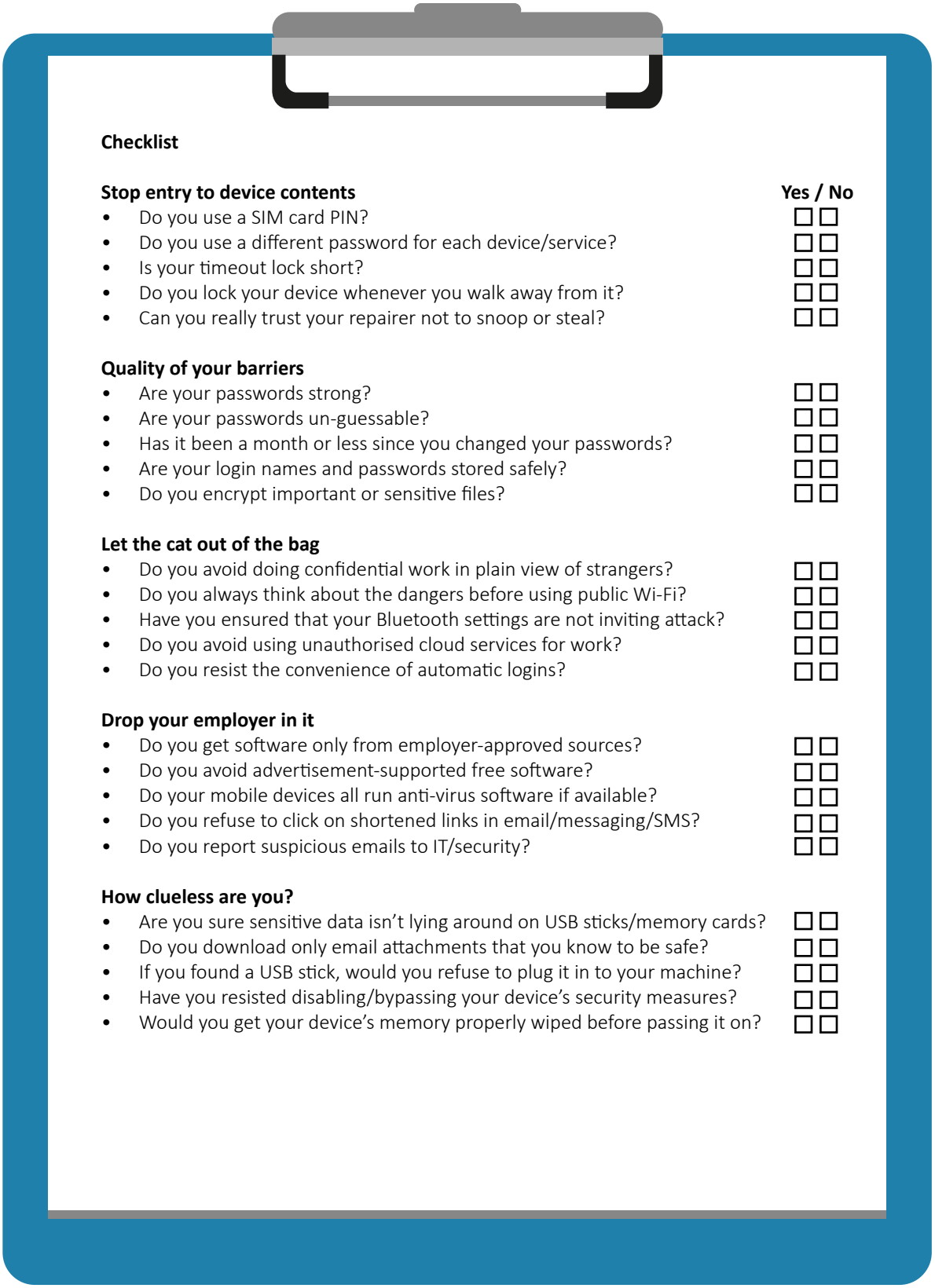
You also need to report a loss, theft or compromise immediately you discover it so the IT team can take swift action. At this stage, it doesn't matter whether you've followed the rules to the letter – maybe you just couldn't resist putting that silly game on for your kids, or whatever – the important thing is to prevent further damage.

And always report suspicious emails beyond the normal spam, especially if you spot a recurring pattern. Better to report them, even if it leads nowhere, than fail to do so and then find it was a sign of trouble brewing.

In a world where the threats change daily, you really are the first line of defence for your organisation. Don't be its weakest link.

The importance of an honest and informed assessment

Ask yourself these questions to see how well you protect yourself and your organisation when using a mobile device. If you answer 'no' to any of them, you could be a danger to yourself and your employer. Change is simple enough, so why not highlight any areas where you're not up to scratch and do something about them?



Checklist

Stop entry to device contents	**Yes / No**
• Do you use a SIM card PIN?	☐☐
• Do you use a different password for each device/service?	☐☐
• Is your timeout lock short?	☐☐
• Do you lock your device whenever you walk away from it?	☐☐
• Can you really trust your repairer not to snoop or steal?	☐☐
Quality of your barriers	
• Are your passwords strong?	☐☐
• Are your passwords un-guessable?	☐☐
• Has it been a month or less since you changed your passwords?	☐☐
• Are your login names and passwords stored safely?	☐☐
• Do you encrypt important or sensitive files?	☐☐
Let the cat out of the bag	
• Do you avoid doing confidential work in plain view of strangers?	☐☐
• Do you always think about the dangers before using public Wi-Fi?	☐☐
• Have you ensured that your Bluetooth settings are not inviting attack?	☐☐
• Do you avoid using unauthorised cloud services for work?	☐☐
• Do you resist the convenience of automatic logins?	☐☐
Drop your employer in it	
• Do you get software only from employer-approved sources?	☐☐
• Do you avoid advertisement-supported free software?	☐☐
• Do your mobile devices all run anti-virus software if available?	☐☐
• Do you refuse to click on shortened links in email/messaging/SMS?	☐☐
• Do you report suspicious emails to IT/security?	☐☐
How clueless are you?	
• Are you sure sensitive data isn't lying around on USB sticks/memory cards?	☐☐
• Do you download only email attachments that you know to be safe?	☐☐
• If you found a USB stick, would you refuse to plug it in to your machine?	☐☐
• Have you resisted disabling/bypassing your device's security measures?	☐☐
• Would you get your device's memory properly wiped before passing it on?	☐☐

Things to remember

If you're in a tearing hurry and have time to read only one part of this report, please read this. It's the quickest of quick reminders of things to watch out for. If you want more information, the rest of this document provides not only details of what each of these DOs and DON'Ts means, but also background to the dangers that you and your organisation face. It also gives you a handy assessment checklist to keep you on the straight and narrow.

DO

Learn about mobile security issues and remedies

Think and check before clicking, downloading or connecting

Ensure your data is encrypted wherever practical

Cooperate with your IT and digital security people

Take responsibility for your personal and work mobile security

DON'T

Install software if you are unsure of its origin and safety

Leave your mobile device unlocked

Reveal your logins and other access credentials

Use WiFi or Bluetooth without appropriate safeguards

Use public cloud services for confidential information

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better informed investment decisions.

For more information, and access to our free research library visit www.freeformdynamics.com

About 5app

At 5app, we love simple and straightforward. Our goal is to help employees overcome their 'data overload' and find what they need, when they need it.

We understand the challenges mid-market companies face when trying to embrace a mobile enabled workforce. The consumerization of IT has resulted in the perennial problem of a 'digital overload'. So many apps to choose from, so many ways to find and store content. This is a major problem for data security, and a massive headache for IT.

We offer businesses a unique solution. Utilising our mobile application management background and adding into the mix our ability to curate and share all types of digital content, online and offline, The Digital Hub can help you achieve a simple and straightforward digital strategy. With our user centric approach employees will find the Digital Hub intuitive to use, easily finding what they need whenever they need it, without IT having to manage complex MDM solutions.

Our background as a company is steeped in the mobile world and we want to help organisations of all sizes embrace the benefits of mobile technology to create happy and effective workforces.

For more information please visit www.5app.com