eGuide

Keeping Security in Hand

5 Dangerous Assumptions About Mobile Security Putting Your Organisation at Risk

Identity Experts

#1: Jailbroken Phones Are Safe

Jailbreaking mobile devices is still common, despite the practice being frowned upon by manufacturers. But there's more to risk than just Apple's ire.

To jailbreak a mobile device is to free it of the manufacturer's constraints, opening up opportunities to customise – which is why it's still an alluring past time for individuals and organisations.

Unfortunately, jailbreaking also puts users at great risk in the following ways:

- **Passwords and other secure information become vulnerable**
- **Dubious applications are able to talk to each other**
- **Apple push notifications (APNs) are faked, leading users to assume their device is secure**
- **Malware has access to the devices root, spreading an infection rapidly**

In short, it's worth thinking twice before trading security for a chance to customise your device.

KeyRaider

Back in November 2015, users of jailbroken iPhones became victims of the jailbreak malware called KeyRaider – which stole 225,000 Apple IDs, as well as thousands of certificates, receipts, and private keys

Source: Palo Alto Research Centre

#2: Public App Stores Are Safe

You're downloading an application via a public app store, so it's all safe, right? ...Right?

With so many apps on the market, it shouldn't be a surprise to find out that some of them are suspect when it comes to how secure they are, and yet we put a lot of trust into the app vetting process.

In reality, it doesn't matter whether or not an app does appear on the store – it should always be checked for security flaws, bugs, and malicious advertising scams.

The latter is a particularly potent method for getting users to divulge personal information or to download malware, as adverts can link to suspicious sites and other applications.

This is why it always pays to use a tool such as **Lookout** or some good old fashioned research before downloading applications that don't have the most stellar reputation for safety – it'll save you a lot of heartbreak in the long-run.

Apps, Apps, Apps

In the first quarter of 2019, there were 2.1million applications available on the Google Play Store and 1.8million on Apple, as well as 669,000 on Windows and 475,000 on the Amazon Appstore.

Source: Statista

#3: MDM is Enough

Mobile Device Management (MDM) is the passport that gets you over the border – but you still need someone checking cases on the other side.

That's to say that a lot of organisations think that having MDM in place is enough to secure their devices and keep employees out of harm's way. It's a great start, but really serves as a foundation upon which further measures must be built.

This is partially because Mobile Device Management is still a youthful technology, trying to adapt to the various challenges presented by the Bring Your Own Device (BYOD) workplace; it's also partially down to the fact that mobile devices are entirely different to PCs.

We have to re-approach everything we've learnt about security via PCs when it comes to mobile devices, and accept the fact that it requires a new approach. We'll talk more about these differences in the next two points, namely that:

- **Mobile devices are the new sweet spot for hackers**
- **Security features such as two-factor authentication need mobile phones**

Productivity Boost

According to research from Frost & Sullivan, using portable devices saves employees roughly 58 minutes a day, increasing productivity by 34%

Source: Frost & Sullivan via Samsung Insights

#4: Two-Factor Authentication is Enough

Two-factor authentication has become a widely popular security feature both in the workplace and at home – but is it enough?

In recent years, security measures have evolved beyond a simple email address and password to include additional factors – such as having a code arrive via SMS, or clicking a button in an email. Unfortunately, cyber threats have also evolved, and two-factor authentication isn't always enough to protect devices, especially when considering that mobile phones often *are* the second 'factor'.

Instead, multi-factor authentication (MFA) is recommended practice now, requiring users to provide further credentials based on 'factors' such as:

- **Location (GPS)**
- **Knowledge (security question)**
- **Inherence (biometrics)**
- **Possession (security token)**

State of Password Report

According to Yubico's most recent State of Password report, 69% of respondents share passwords with colleagues, while 57% have not changed their password behaviours, even after falling prey to phishing.

Source: Frost & Sullivan via Samsung Insights

#5: Mobile Devices Aren’t a Priority

When it comes to anticipating hackers and their priorities, many organisations still consider mobile devices to be less of a target than desktops.

Times have most definitely changed: data is now more valuable than oil, almost everybody has a mobile device within reach, and we’re even wearing advanced technology around our wrists now.

With a changing world comes changing priorities for those wanting to take advantage – the days of PCs being the main target for hackers is long gone. Security researchers have now identified smartphones in particular as a target, thanks to the wealth of data contained within – not to mention what else smartphones can help them to gain access to.

In short, if your organisation uses mobile devices – either in an organisational roll-out, or as part of a BYOD policy – then it pays to get serious about securing them, as they’re pretty high on hackers’ hit lists.

Dark Caracal

In 2018, a hacker group known as ‘Dark Caracal’ targeted international Android users via spyware, stealing hundreds of gigabytes of sensitive information.

Source: CSO Online

We’re Working with Lookout

As part of our ongoing commitment to empowering organisations through partner technology, we’ve started working with mobile security specialists Lookout.

Lookout are focused on shaping the mobile security industry, driven by finding creative and novel ways to meet and overcome their customers’ security challenges.

Every day, the Lookout team use their unique dataset to create insights, and use those insights to help shape their products. The products they build deliver value to customers and protect the privacy of end-users. Making the world safer as it becomes more connected is what drives life at Lookout.

Sharing our values of building trust, putting customers first, and a willingness to innovate, Lookout are a perfect fit for a partnership with Identity Experts.

To find out how Lookout can help your organisation to secure its mobile devices, get in touch with a member of our team.

Sales Contact:

Amy Stokes-Waters
AmyS@identityexperts.co.uk

Our Website: www.identityexperts.co.uk
Their Website: www.Lookout.com

Lookout