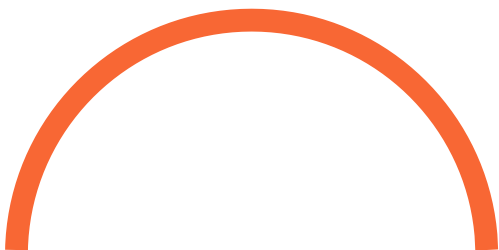




Android Enterprise Essentials

The SMB Mobile Security Masterclass.

Essential tips for keeping your business safer.

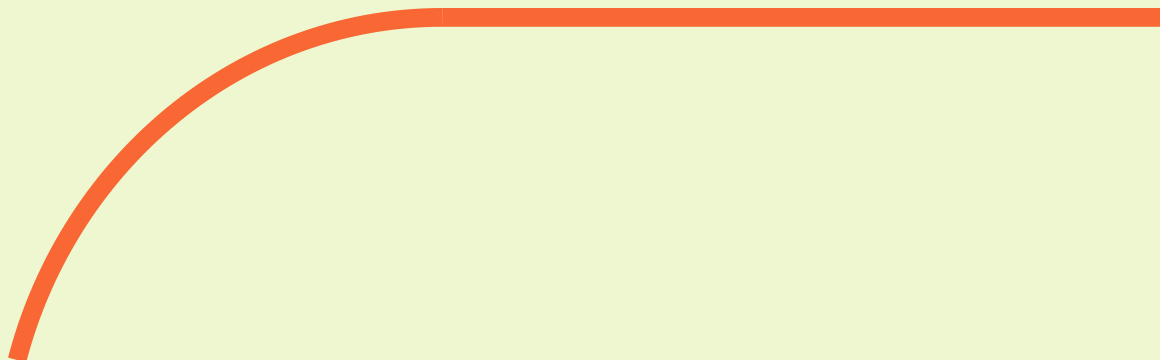


PARTNER LOGO HERE

android 

Table of contents

1.	<u>Introduction to mobile security</u>	03
2.	<u>Mobile security priorities for SMBs</u>	06
3.	<u>A simple way to protect your business</u>	11





Chapter 1

Introduction to mobile security

Introduction to mobile security

The mobile workforce: new opportunities for businesses ... and new risks

Mobile devices have revolutionized the way we work. Being able to access the data and apps we need for our jobs, no matter where we are, has been a welcome boost for productivity and flexibility. But since mobile devices are not as easily managed or secure as an office computer network, they can expose your organization to new threats.

Forty seven percent of companies have seen an increase in cyberattacks since the work from home shift¹. And the fact is, every single work mobile device is a direct link to your company's sensitive data. Relying on employees to keep their phones and tablets as secure as they need to be is a policy that is doomed to fail. Most workers are not only unaware of the security measures that need to be taken, just like all of us, they make mistakes. Through an innocent error or a misplaced device, they could unintentionally open your company up to a security breach.

Not-so-fun fact

**Nearly 1 in 4
cybersecurity
breaches are
caused by
human error²**



The Mobile Security Quick Quiz

Mobile security is expensive.

True False

Employees need training to work with a mobile security system.

True False

Mobile security is a lot of extra work for IT.

True False

Setting up a mobile security solution is complicated.

True False



Answer key

All of the above are false if you choose Android Enterprise Essentials. It requires no training for staff and won't drain IT resources. And at an estimated \$2 per device/month*, it's the simple and affordable mobile security solution that smaller companies have been looking for.

*Prices may vary by region and reseller. Please contact your reseller for specific pricing information available in your region.

But how bad can a mobile security breach be?

Security breaches can be devastating for any organization, but unfortunately small to medium-sized businesses (SMBs) are less able to absorb the high costs of one. After experiencing a breach, 10% of SMBs file for bankruptcy and 25% go out of business³.

The financial blows can come from all sides. Even if no money is stolen from the company, there is still the cost of shutting down while an investigation is underway, replacing devices, adding new security systems, paying fines, and compensating clients if private customer data is leaked.

On top of all that, there is the reputational damage to consider – losing the trust of valuable customers and partners who may feel that working with you is just too risky. In a Verizon survey, 69% of people said they would avoid a company that had suffered a data breach, even if it offered a better deal than competitors⁴.

Considering the possible fallout, protecting yourself from a mobile security breach isn't just a precaution, it is vital to the future of your business.

\$200,000

Average cost of a data breach⁵



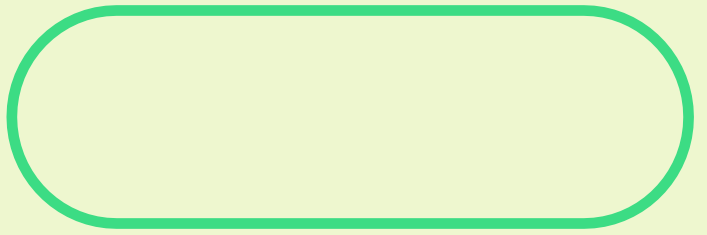
Case study

Security breaches can come with big fines

Even with all their resources, it took the hospitality company, Marriott, four years to notice a massive data breach that disclosed the personal and financial information of 339 million guests. Since regulators established that there weren't sufficient safeguards in place to protect this sensitive information, they were fined £18.4m.

Find out how to protect your business now.

[Skip to Chapter 3](#)



Chapter 2

Mobile security priorities for SMBs

Mobile security priorities for SMBs

Smaller businesses and security breaches

You may believe that it's mainly larger organizations that fall victim to security breaches and targeted attacks, but unfortunately that isn't true. More than one in four data breaches in 2020 involved small businesses⁶.

SMBs are particularly vulnerable as they often don't have the budget for in-house experts who can educate employees as well as set up and manage sophisticated security systems. In fact, 43% of SMB owners have no digital defense plan whatsoever⁷.

An unprotected business is an easy target. Sensitive information like customer payment data, lucrative intellectual property and confidential personal information are a goldmine for criminals who can use them for scams and identity theft. SMBs may be smaller fish, but they can also be easier to catch.

How protected is your business? Take the quiz.

Do all your employees have screen locks on their devices?

Yes No I don't know

Can you protect your company data if a device is lost or stolen?

Yes No I don't know

Are your company devices encrypted by default?

Yes No I don't know

Can you block your employees from downloading unsafe apps?

Yes No I don't know

Calculate your total

For every "No" or "I don't know", you get one point. If you have any points, your business is open to a security breach. Two points or more means your business is at high risk.

We're only human, after all

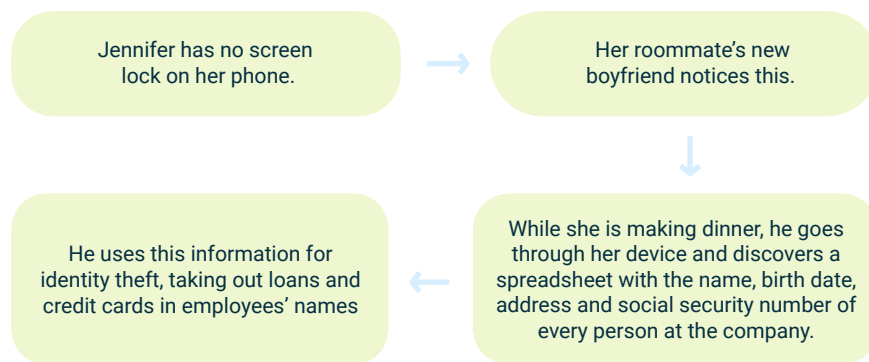
You might be surprised to learn that cybercriminals aren't the only security threat to your business. Your employees are too – their actions can have costly consequences. Simple mistakes and lost or stolen devices leave the door wide open for a data breach. And 40% of information workers say that they ignore or go around their company's security policies because it's a more efficient way of getting their work done⁸. Here are just a few ways your employees can put your business at risk:




No screen lock

A shocking 1 in 10 smartphone users don't have a screen lock⁹. That means that if a device is left unattended even for a short time – nevermind lost or stolen – whoever comes across it can access anything on it, from emails and calendars to sensitive company and employee data. In the wrong hands this could be used to steal from and scam employees, partners, and your company.

How it could happen



How it could be prevented

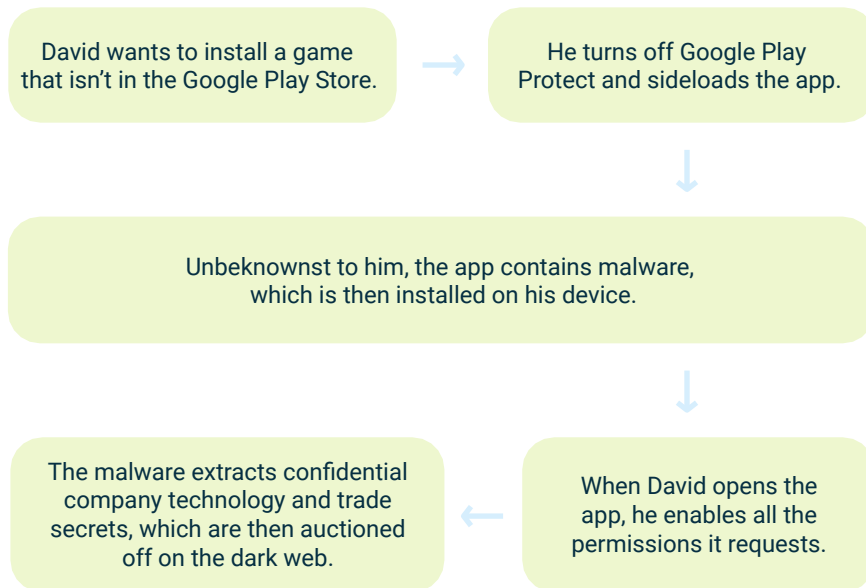
 **Mandatory, automatic screen locks for all employees.**



Downloading malware

Malware is short for “malicious software” – programs that are specifically designed to disrupt or gain unauthorized access to a computer or mobile device. Employees can inadvertently install malware like viruses, worms, ransomware, and Trojan horses by sideloading unverified apps or clicking on spam links. In 2020, 52% of organizations experienced a malware incident on a remote device¹⁰.

How it could happen



How it could be prevented

- Google Play Protect, Google’s anti-malware system, should be turned on at all times.
- Restrict employees from installing apps from unknown sources.
- Make sure mobile devices have the latest updates and security patches installed.
- Educate employees about the dangers of malware.

Case study

A Trojan horse heist

Construction company PATCO lost approximately \$350,000 after Trojan horse malware was installed on one of their systems. The thieves used it to steal online banking credentials and make transfers from the organization’s accounts. On top of the theft, the business was also hit with thousands of dollars in overdraft fees from their bank.

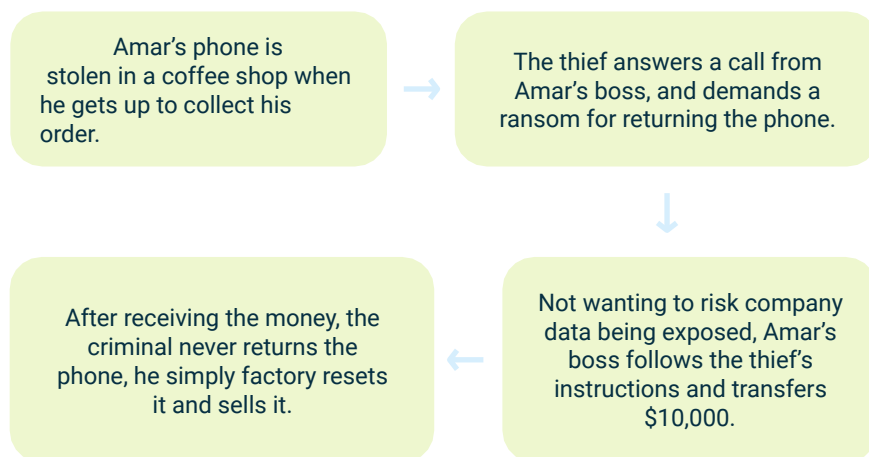


A lost or stolen device


Since we tend to have our devices with us all the time, there are endless opportunities for them to be misplaced or stolen. Loss or theft of smartphones and laptops were involved in 20% of security breaches globally¹¹.

Since the beginning of the pandemic, 48% of organizations have reported that attacks on compromised or stolen devices have increased¹². Often, the data on a device is more valuable than the cost of the actual hardware. Criminals can use the information they find for illegal activities or demand a ransom for returning the device.

How it could happen



How it could be prevented

 **Being able to remotely wipe a device prevents anyone from stealing your data or demanding a ransom.**



Case study

One missing phone, one year of problems

The managing director of an electronics manufacturing firm had his phone stolen on a business trip to China. Soon after, vendors began receiving fraudulent emails from his account with invoices requesting payments. It was almost a year before the company finally managed to put an end to the scam.



Chapter 3

A simple way to protect your business

A simple way to protect your business

Right-sized security for outsized threats

Making sure your devices are secure is just as important as locking the door to your office building on the way out. But for years there has been no easy way for small to medium-sized businesses to set up this important line of defense. Cost has often been a prohibitive factor – half of SMBs have less than \$5,000 budgeted for IT security and almost a third have less than \$1,000¹³. Companies have had to choose between expensive, resource-intensive mobile device management that may be too complex for their needs or limited-to-no protection.

With new risks emerging daily, businesses need an easy way to keep data and assets secure – one that doesn't require time-consuming management from IT or negatively impact employees' productivity. This is exactly why Android Enterprise Essentials was built.

Android Enterprise Essentials: Automatic and affordable data protection by Google.

Essentials was designed and built by the Android team at Google, creators of device management and security tools for the world's largest organizations. They leveraged their extensive experience to create a scalable, affordable mobile security solution, perfectly suited to the needs of SMBs.

The service is extremely easy to set up, use and manage, requiring no additional training for employees. Essentials policies are applied automatically, as soon as you take the device out of the box, and even small companies can afford it, with an estimated purchase price of just \$2/device/month*.



Simple, automatic security



Instant set-up and easy management



Excellent value

Need more granular controls?

For organizations that want more mobile security options and customizable solutions for their business models, there is



¹³ Untangle, 2018.

*Prices may vary by region and reseller. Please contact your reseller for specific pricing information available in your region.

7 features for stress-free security

With Essentials, all policies are enforced out of the box and are always-on, without any action or configuration by IT. Protecting your business couldn't be simpler. Especially with these powerful security features:

1. Enforced screen lock

Every device has a mandatory screen lock to prevent unauthorized access to company data. These can easily be reset remotely by IT should an employee forget their passcode.

2. Wipe devices remotely

If a device is lost or stolen, personal and company data can be deleted remotely with a few clicks.

3. Always-on malware protection

Google Play Protect provides malware protection and constantly runs in the background, scanning and verifying more than 50 billion apps every day.

4. Prevent sideloading of apps

Essentials makes it impossible for employees to download potentially unsafe apps from outside the Google Play Store.

5. Enforce persistent policies even if a device is factory reset

Devices remain secure and critical data safe, even after a factory reset – no intervention by the company is necessary.

6. Data encryption

If a device falls into the wrong hands, there is a second layer of protection to keep company data safe.

7. Manage all devices via a streamlined portal

All devices can be viewed and managed from a user-friendly portal, which IT will most likely only access if a device is lost or stolen.



Case study

A compromised email account can be costly

Small business, Wright Hotels, lost over \$1 million after cybercriminals gained access to the owner's email account. They impersonated him in messages to the bookkeeper, requesting money transfers from the company's account to their own in China. By checking his Outlook calendar, they could easily see when he would be busy in meetings, giving them plenty of time to organize the transfer and then delete all correspondence.

Make staying safe a habit

Essentials is an excellent way to make mobile devices more secure, but you can also do your part to protect your business and data by following these simple tips.

- Don't use unsecured public WiFi networks.
- Use strong, unique passwords for all your accounts.
- Don't share your work device with family or friends.
- Back up data regularly.
- Keep your apps and operating system up-to-date.
- Educate employees on mobile security risks.

Easy for employees. Easy for IT. Easy for SMBs.

Mobile security has never been so simple. It only takes a minute to get started, with instant set up, and simple management as you scale.

- 1.** Sign up for Android Enterprise Essentials at the point of sale.
- 2.** Instant deployment – just open the box and employees are ready to go.
- 3.** View and manage all your devices from one centralized, easy-to-use portal.
- 4.** Take immediate action from anywhere if any devices are lost or stolen, or if an employee forgets their PIN.

Invest in some peace of mind

Get started today.
Discover how Essentials can help protect your devices and data at an affordable price.

For more information visit
android.com/enterprise/essentials

Congratulations!

You have completed the **SMB Mobile Security Masterclass**.
Now you have the power to defend your work data, devices, and your business.

You can find out more about
Android Enterprise Essentials [here](#).

