Mobile Device Management vs. Mobile Security App

MOBIVISOR

About us

IOTIQ GmbH has been providing innovative software solutions for various application areas since 2017. Our mission is to support companies of all industries and sizes in taking the path towards digitalization with the right tools at hand and the right partner at their side.
In a world that is mobile and constantly becoming more so, security remains the top priority. To ensure this, we have developed MobiVisor - the mobile device management system that is just right for you.

IOTIQ

Smartly Done.

1. What are the threats to mobile devices?

The security of mobile devices is a major concern for many organizations. As so-called end-points of internal networks, they are a popular target, along with desktop computers or laptops, for gaining access to networks and capturing valuable data.

Attackers use various methods to do this: viruses, malware and ransomware. Mobile devices cannot be attacked by "classic" viruses due to the structure of the operating system. Since on smartphones and tablets the components of the operating system are in individual packages, viruses cannot replicate themselves, as would be the case on computers. This provides a certain degree of protection – because the effort required to infect a smartphone with a virus does not justify the barely available gain.

Malware or ransomware, on the other hand, can also get onto mobile devices. One example is "smishing" (SMS phishing). In this case, a text is sent by a seemingly reputable provider, for example DHL or Amazon. The message often states that a package has been dropped and that the recipient should click on the link in the text to find out where the package is. If the link is clicked, either malware is installed directly on the device, or the user is prompted to enter data such as address, bank details or phone number.

This data is often sold on by the hackers. In other cases, the installed malware reads and can, for example, obtain payment data or passwords in this way. Ransomware, on the other hand, will render the device unusable by encrypting files, etc., so that access is no longer possible. This state continues until a ransom is paid.
In all cases, monetary damage is caused by both captured data or the ransom. In the worst case, companies can be sued for damages if their employees' data is lost.
Around 201 million attacks on mobile devices are registered worldwide every year - so the threat should not be underestimated.

2. What can be done to secure mobile devices?

The list of possible threats and the corresponding security measures is long.
Care should always be taken to ensure that the measures cover all levels.
It is not for nothing that people talk about the "onion approach" to mobile security.
Companies, in particular, should not rely on the knowledge of their employees with regard to the secure use of mobile devices - even if they have been extensively trained.

Below we have summarized common threats and how to defend against them:

SMS Phishing

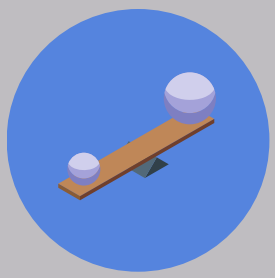
Ban incoming SMS as a matter of principle or ban them from unknown and 0800 numbers.
Alternatively, a secure messenger can be used.
These settings can be made, for example, via a mobile device management system (MDM).

Installing Harmful Apps

MDM can be used to reduce the number of apps available for download from the Playstore. It can be specified that only apps approved by the company can be installed.

Use of insecure Internet connections

Open Internet connections that are not protected by a password should always be avoided.
But to be on the safe side, an MDM can be used to specify that open Wi-Fi connections are not to be used.



Mixing work and private life

In some cases, employees are also allowed to use their own devices for work. This principle is called "bring your own device". Here, there should be no mixing of private data with work data.

Sharing sensitive data using insecure means of communication

This may concern attachments or data that is only for internal use. Passwords or similar information should generally never be sent via e-mail or chat. Chat programs intended for private use, such as WhatsApp, should also be avoided in the work context. Instead, use alternatives that are specially designed for secure communication within the company, e.g. MobiVisor Messenger.

3. What are mobile security apps good for?

Many smartphone and tablet users are familiar with the fact that the computer antivirus program comes with an accompanying antivirus program or antivirus app for the mobile device. But how useful are these apps and do they really help to fully secure the devices?
The opinions about it are actually divided. While some, mainly the smartphone providers themselves, affirm that the devices are optimally protected even without extra apps, on the other hand there are always voices of IT experts and providers of security software that claim the opposite.

Basically, however, you have to keep in mind what these apps can actually do and in which context they should be used.
For example, it is not advisable to use a mobile security app as the sole solution for securing devices. While every app asks for access permissions, in most cases these apps can at best display warnings. There is no intervention in the system to prevent access for malware.

In general, active prevention against threats is the most sensible security strategy, because it prevents malicious software and apps from getting onto the device in the first place. Accordingly, prevention can prevent greater damage.
However, in order to prevent effectively, the security system must be designed in such a way that sources of danger can be blocked. A security app usually cannot do this.

For example, the security app has access to the device's networks. As soon as the device wants to use an unsafe Internet connection, a warning is generated. But: the user can ignore this warning and use the insecure connection anyway. In the work context, this may not be possible.
The conclusion is that mobile security apps can increase the feeling of security - but ultimately only partially prevent careless behavior.

For example, if users receive a warning that a download link or similar is coming from an unsafe source, or if they are not aware of it, they will not be able to use it. If, for example, users are warned that a download link or similar comes from an insecure source or that Internet connections are not secure, this can certainly raise awareness of the threats to a certain extent and also prevent users from behaving carelessly.
In a private environment, this can make a lot of sense.

4. MDM - the better alternative?

Mobile Device Management (MDM) basically serves to implement corporate security policies in the mobile device fleet. On the one hand, it prevents sensitive company data from leaking to third parties, and on the other hand, MDM prevents improper use of company devices and thus shortened useful life.
Due to the great functionality of most MDMs, settings can be made in great detail. What can be used, how and by whom can be set even more decisively than via the system settings on the device itself.

This is a great advantage, because it also creates clarity in the responsibilities and authorities of the employees.
Of course, at first glance, MDM is not only more extensive, but also far more complicated than the simple installation of a mobile security app.
But one should always consider how costs and benefits balance out. A free security app will not provide the in-depth protection you hope for your mobile devices. While the MDM will take some time to install and set up, it will reliably avert the biggest threats to mobile security.

Would you like to learn more about mobile security?

Visit the blog of our mobile device management system MobiVisor! Just click here.

We would be happy to advise you personally!
Write us an e-mail at info@iotiq.de or contact us by phone at 0176/ 34110095