SAFE COMMUNICATION WITH

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.

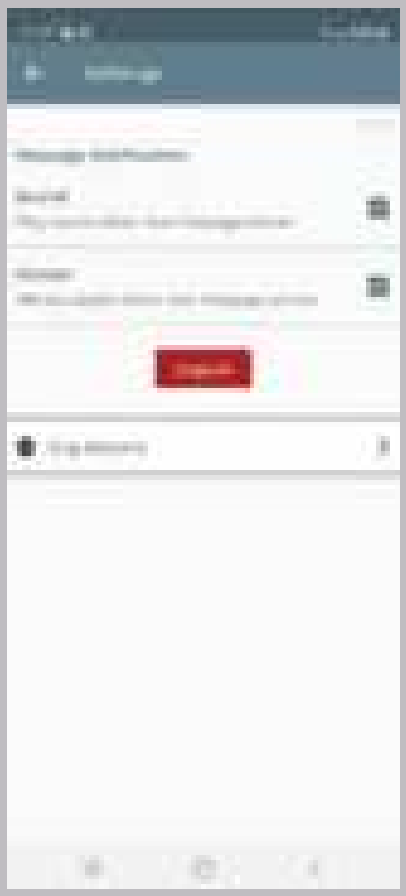
Smartly Done.

FACTORS TO CONSIDER

Most commonly, companies use public chatting networks like SMS, MMS, WhatsApp, Skype, Telegram, WeChat, Line, or social media applications such as Facebook or LinkedIn to keep in touch with employees. One main safety concern is that the data in those apps is mostly hosted on American servers. The US actually has fewer data protection rules than others, such as countries belonging to the EU.

Furthermore, the popularly known apps listed above do not provide sufficient protection for the user. They allow users to communicate with anyone in their personal contact list, ignoring corporate vigilance. They do not provide a corporate-specific contact list for conducting teamwork. Internally, one should create a policy list determining which apps can be used by whom and during which time periods. Although apps like Instagram and Facebook may serve as an inspiration, especially for creative tasks, multiple contacts with anyone are highly likely to distract employees and may spoil their concentration on business-related issues. Here, MobiVisor supplies you with its' extension MobiVisor Messenger to support direct and group messages in the company.

If you change your device and download MobiVisor Messenger on the new device, you don't need to worry about your past conversations. They are backed up and can be seen in the new device as well.



If you notice that something is wrong with the app and some of the features do not operate smoothly, bug reports will direct you to what the problem is and how it can be fixed.

This is an example of what the message screen looks like. You can send and receive any type of media, document, video, and audio.

MobiVisor Messenger is especially reliable since it secures messages with encrypted infrastructure via SSL/TLS. In contrast to other chatting apps, images, files, texts and documents can be restricted, as then no one can copy-and-paste or forward those items. Even if a device is lost, the content of messages can be deleted remotely so that no one can view them when finding or viewing the device. Since the device can be put into lost mode, strangers are then prevented from using it entirely and accessing company data.

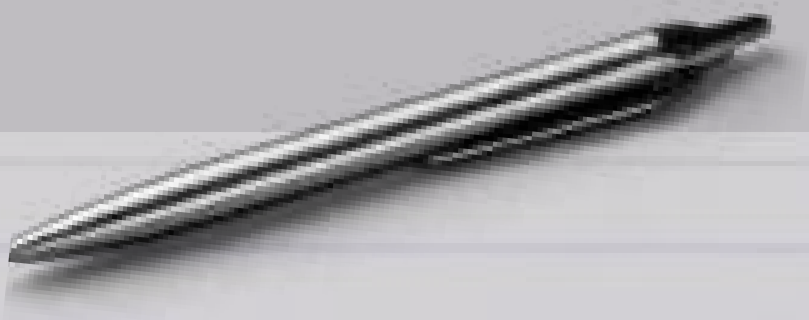
COMMUNICATION CHALLENGES

Data breaches

Forwarding messages or copy-and-pasting text into another chat might signal data breaching. In most cases; data and information that is produced in relation to company tasks belong to the company and not to the employee. This difference is important, because an action as little as sending information to a private email address to get back to later may be a breach of the company's data strategy.

Unauthorized access

It needs to be clear that some messages are confidential within certain departments, between employees, or in the communication between the company and outside parties. There cannot be a chance that people or institutions not related to the company can gain access to messages. This happens more easily than most of us can imagine: you need only forget to remove the intern from the group chat or remove their access to shared files.



Endpoint-security consists of many layers:

1. ***Signature Comparisons:*** *Tests each virus' signature (code) and compares it to a set of known viruses.*
2. ***Machine Learning Verification:*** *Prepares the system's behaviors for defense in case of cyber threats.*
3. ***Behavioral Analysis:*** *Uncovers any unusual behavior in the system and determines whether it's malicious.*

Undefined contact list

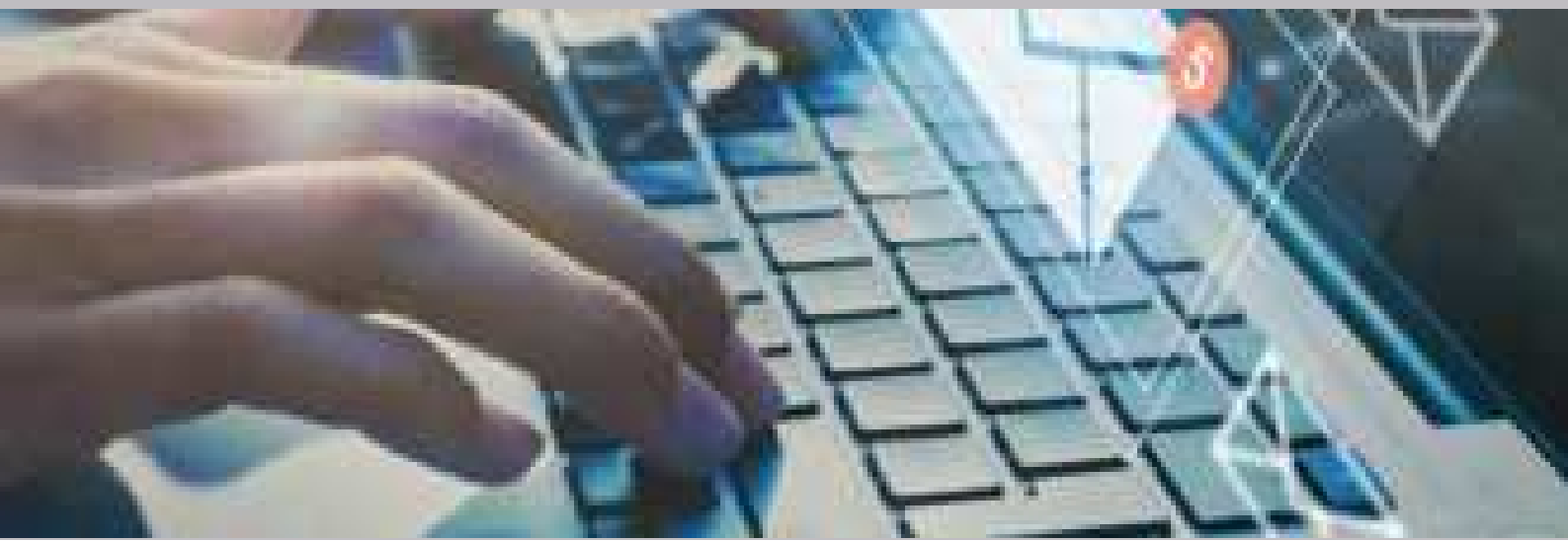
Sometimes employees' email accounts are terrorized by advertisements, application notifications and more. This occurs because nearly all commercial websites and apps require email accounts to create a membership. Their unnecessary emails may be counted as a threat as long as they keep popping up in the central mail inbox.

Using open-public chatting apps

Apps like WhatsApp, Line, WeChat and Telegram may be harmful in terms of the protection of data. Using express mail services like Gmail, Outlook, etc. is also not advised. As mentioned above, they keep the data mostly on American servers which have less strict data protection laws.

Internal Forwarding

Sometimes employees may forward documents, accidentally or intentionally, to the wrong person. For example, data about costs, benefits and salaries might be are expected to be sent to the finance department of the company. However, some might deliver it to the marketing department.



Liability for emails

Companies can spread viruses, worms, or any type of malware to other companies via email. Sometimes they spread them unintentionally if another company has previously transmitted a virus to them and they are not aware of it.

Spam

If messages can be sent to anyone in the personal contact list and if no special contact list is created for company matters, the content of the communication network may be leaked. Separation between work contacts and personal contacts can be achieved by containerization (the division between work profile and private profile on one device).

Solutions

- Establishing clear communication privacy policies so that each employee follows its' rules.
- Encrypting the written text as well as video conferences with complex passwords including touch ID, face ID, etc.
- Training plays an important role to improve security awareness among the employees, employers, and companies.
- Cloud computation, meaning data backups will save you in case of a stolen/lost/broken device.
- App monitoring keeps employees away from engaging in public chatting networks such as WhatsApp, WeChat etc., and establishing personal contact with somebody out of the office.

- Controlling email distribution plays an important role to make sure that data will be sent directly to the right official.
- Securing emails via SSL (Secure Socket Layer) which means an encrypted link between a client and a server.
- Blocking email access from unauthorized devices.
- Restricting email access to only company-approved devices.
- Uncovering unmanaged devices that try to access corporate emails.
- A Qualified Electronic Signature is legally binding and valid in terms of secure communication about paperwork when documents need to be shared and signed across borders. A digital signature can be used in emails, installation packages, application updates, etc.

Do you want to know more?

Do you have questions about how MobiVisor and our extensions work, or are you unsure whether MobiVisor MDM fits your company and its challenges?

We are happy to assist you with advice and support! Just contact us by phone or e-mail.
We would also be happy to arrange a personal presentation appointment with you and provide you with a test environment of MobiVisor without obligation.

Toni Voß
toni@iotiq.de
+49 1578 3020995

Saskia Riechers
saskia@iotiq.de
+49 176 1500 6080