

16.09.2025

Just how dangerous are e-mails, texts, WhatsApp and co.?

The various messaging apps in use today all carry their own, different inherent risks To be aware of them means you can use them safely.

Electronic mail, or e-mail for short, is simply one of the most widely used messaging services around nowadays. Next to text, “mails” can include different content such as images, website and multimedia elements plus file attachments. In addition, senders can include a variety of metadata, for instance their return address, subject line, urgency level or read receipts.

Accordingly, e-mails present various risks. The biggest one is posed by any file attachments. Since you can basically include any number of files in a mail, it is possible to smuggle in malicious content this way, too, for instance malware or Microsoft documents (in Word, Excel etc.) containing dangerous macros.

The same goes for e-mails containing links. These could lead to a phishing website or one infected with malware. Even e-mail sender addresses (data contained in the “from” field) can be faked so that it looks like a message originates from a trusted person or institution. **You should therefore always handle any links, attachments and senders with great care.** The one thing considered largely harmless nowadays is the actual text content (body) contained in e-mails.

Messenger services such as WhatsApp, Telegram or Facebook Messenger are usually proprietary apps of the provider concerned, who apply totally different security standards in turn. It is therefore impossible to provide a general risk assessment. Since these apps allow you to send a variety of content such as images, videos, links or file attachment, you should basically apply the same safety measures you use with e-mails.

Short Message Service messages, “SMS” for short, pose few risks in comparison. As they are text-only messages in their original format, there is no chance of introducing any malicious content. However, links contained in an SMS can still lead to a malicious website. Caution though! Provider-specific formats such as iMessage by Apple or Samsung Message could contain additional content where it is difficult to judge their risk potential. Similar to e-mail sender addresses, you can also fake the phone number of a text sent, so that it appears to originate from a well-known person or company. This actually also applies to WhatsApp messages.

The same goes for all types of messages: If you are unsure, don’t open any links or attachments and don’t reply to the message received directly, but ask the purported sender to confirm they actually sent it and what it contained, using a different channel of communication. You could for instance call them via the official telephone number of the person, bank or company involved.