

16.09.2025

Quanto sono pericolosi e-mail, SMS, WhatsApp & Co.?

Le varie applicazioni di messaggistica di uso comune comportano rischi diversi. Conoscendoli, questi strumenti si possono usare in sicurezza.

La posta elettronica, o più brevemente «e-mail», è uno dei servizi di messaggistica più utilizzati in assoluto. Oltre al testo, le «mail» possono trasportare vari contenuti, come immagini, elementi di pagine Internet e multimediali, nonché file allegati. Inoltre, il mittente può annotare vari metadati, come il suo indirizzo, l'oggetto, il livello di urgenza o una conferma di lettura.

Ciò fa sì che le e-mail siano pericolose su vari fronti. Il rischio maggiore deriva dai file allegati, i cosiddetti «attachment». Visto che in sostanza si può allegare a un'e-mail qualsiasi tipo di file, si possono spedire anche contenuti dannosi, come malware o documenti Microsoft (Word, Excel, ecc.) contenenti macro pericolose.

Un discorso simile si può fare per i link nelle e-mail, che possono portare l'utente su un sito Internet di phishing o su una pagina infetta da malware. Si può falsificare anche l'indirizzo del mittente delle e-mail (il campo «From» o «Da»), per far sembrare che il messaggio provenga da una persona o da un'istituzione fidata. **I link, gli allegati e il mittente andrebbero quindi trattati con grande prudenza.** Per lo più innocuo risulta essere invece il contenuto testuale effettivo («body») delle e-mail.

I servizi di messaggistica come WhatsApp, Telegram o Facebook Messenger sono in genere applicazioni proprietarie del rispettivo produttore, che seguono standard di sicurezza molto diversi tra loro. Non è quindi possibile una valutazione generale del livello di rischio. Poiché queste app permettono lo scambio di contenuti diversi come immagini, video, link o file allegati, come regola generale vanno seguite le stesse precauzioni delle e-mail.

Gli SMS (abbreviazione di «Short Message Service»), invece, sono relativamente innocui. Trattandosi di messaggi puramente testuali, non è possibile introdurre contenuti dannosi. Ciò non toglie che un link trasmesso via SMS possa condurre su un sito Internet dannoso. Attenzione però! Formati specifici come quelli sviluppati per iMessage di Apple o Samsung Message permettono la trasmissione di contenuti aggiuntivi di cui è difficile stimare il potenziale pericolo. Analogamente all'indirizzo del mittente delle e-mail, è possibile falsificare anche il numero di telefono di un SMS, cosicché il messaggio sembra provenire da una persona o un'azienda conosciuta. Questo vale anche per i messaggi WhatsApp.

Per tutti i tipi di messaggi la regola allora è questa: in caso di incertezze, non aprite link o allegati e non rispondete direttamente al messaggio, ma chiedete al presunto mittente di confermare l'invio e il contenuto tramite un altro canale. Per esempio potete comporre il numero di telefono ufficiale della persona, della banca o dell'azienda in questione.