Come difendersi dalle truffe su WhatsApp

Autore: Daniela Baudino
Fonte: Città Nuova

Si sono moltiplicati i messaggi che, giocando sulla buona fede, invitano a cliccare su dei link per compiere una certa azione. Sono messaggi Scam, vere e proprie truffe online da cui bisogna imparare a difendersi.

Spesso succede così: più uno strumento prende piede nell'uso quotidiano delle persone, più prima o poi finisce per diventare il luogo dove spargere truffe (abbinate spesso alla dinamica della "catena di Sant'Antonio"), nella speranza che qualcuno prima o poi abbocchi. È successo con le email qualche anno fa. Poi con Facebook. E ora è il turno di **WhatsApp**. In questi ultimi tempi, infatti, **si sono moltiplicati i messaggi che**, giocando sulla buona fede di tanti, **invitano a cliccare su dei link per compiere una certa azione**. Questo fenomeno, che viene chiamato **Scam**, rappresenta un vero e proprio tentativo di truffe online, che sfrutta i sistemi di comunicazione istantanea per diffondersi più facilmente. **I messaggi Scam** Esistono tre diverse tipologie di messaggi Scam. Ci sono quelli più **"innocui"**, dove solitamente il messaggio ricevuto contiene **grandi promesse di sconti (esagerati) con un link da cliccare** che porta ad una pagina che sembra essere quella di chi propone l'offerta, in cui ci viene chiesto di inserire i nostri dati, e poi di condividere a nostra volta il messaggio. **Lidl, Ferrero, Ryanair** sono solo alcune delle tante aziende "usate", a loro insaputa, per questo genere di truffe. Quello che può succedere una volta cliccato il link è **l'attivazione di un servizio a pagamento** (meteo, oroscopi o quant'altro) oppure, se abbiamo inserito **la nostra email**, che questa – o il nostro indirizzo fisico di casa - **venga utilizzata per inondarci di messaggi pubblicitari**. La seconda tipologia di messaggi è quella con cui veniamo **avvisati di fantomatiche multe da pagare per altrettante non specificate connessioni illegali o il sempre-verde ritorno a pagamento di WhatsApp** (vale anche per altri servizi gratuiti). In questo caso i link riportano a pagine che richiedono i nostri dati bancari o di effettuare il pagamento: se proprio abbiamo ceduto alla tentazione di cliccare sul link, non diamo però i nostri dati bancari e meno che mai paghiamo quello che ci viene chiesto. In comune questi messaggi hanno la **trappola psicologica della scarsità di tempo** necessaria per poter "approfittare" della promozione o per pagare quanto dovuto, che come nelle normali pubblicità ci induce ad agire di impulso, senza ragionare sul messaggio e il suo contesto. Il consiglio è, inevitabilmente, quello di **non farci allettare da messaggi che ci offrono premi o ci spaventano** con richieste che potrebbero anche sembrare legittime, e di **non cliccare sui link** contenuti in questo genere di messaggi, **anche se ci arrivano da conoscenti**. Vale la pena ricordare che le grandi aziende non si servono del passaparola per ottenere da noi dei soldi e le offerte che lanciano devono trovarsi specificate anche un canale istituzionale. **La truffa del "prestito"** La terza tipologia è quella più pericolosa: riceviamo un messaggio che sembra provenire da un nostro conoscente, che ci comunica di essere all'estero e di aver smarrito il portafoglio o di essere stato derubato, chiedendoci un piccolo prestito per poter sostenere delle spese. Spesso sui social network siamo invitati a inserire tutta una serie di dati personali, che lì per lì non ci sembra pericoloso lasciare. Esistono però dei cybertruffatori che con un po' di pazienza riescono ad ingannare gli altri, fingendosi ad esempio un'altra persona per ottenere altre informazioni decisamente più appetibili, come i nostri dati bancari. La truffa "del prestito" ha un'architettura molto semplice: il cybercriminale sceglie una vittima su Facebook, scorre la lista dei suoi amici e ne sceglie uno, di cui si salva la foto. Con questa foto creerà un account falso, su Messenger, su Telegram o, se è riuscito a risalire al numero della vittima, anche su WhatsApp. A questo punto contatterà l'utente-vittima spacciandosi per l'utente-esca e, fingendosi in difficoltà, chiederà l'aiuto economico al povero malcapitato. Che, vedendosi recapitare una richiesta da un conoscente, abbasserà le sue difese e potrebbe anche inviare denaro al finto-amico. **Come comportarsi?** Semplice: se dovessimo

ricevere un messaggio in cui qualche conoscente ci chiede dei soldi (pratica diffusa anche attraverso le mail!), verifichiamo personalmente con lui, attraverso altri mezzi, se davvero ci ha fatto quella richiesta. E solo in questo caso diamo seguito all'invio di denaro. **Qualche consiglio (che vale anche per i messaggi ricevuti via email) Non clicchiamo mai su link che ci arrivano via WhatsApp o attraverso altri strumenti simili che ci promettono offerte spropositate o ci imputano multe**: anzi, questo è proprio il campanello d'allarme che c'è qualcosa che non va.

- In caso di offerte, **verificare sempre che quella specifica offerta sia presente anche sul sito** dell'azienda che le offre.
- Nessun servizio (Poste, Paypal, banche...) richiede di inviare nuovamente i propri dati attraverso le email.
- **Farsi aiutare da Google**: digitare nel motore di ricerca una parte del testo ricevuto. Se è una bufala o una truffa, troveremo sicuramente tra i primi risultati i siti specializzati nel loro rilevamento.