Perché scansionare QR Code alla leggera non è affatto una buona idea

Il codice a barre noto come **QR Code** esiste sin dagli anni Novanta, tuttavia il suo utilizzo è sempre stato confinato a un ruolo relativamente marginale. O almeno lo è stato fino all'avvento della pandemia del 2020. A causa delle stringenti restrizioni igieniche, musei, ristoranti e spazi pubblici si sono trovati a dover sostituire qualsiasi supporto di consultazione fisico con una corrispettiva versione digitalizzata. Quest'ultima era spesso e volentieri veicolata attraverso i QR Code. Terminata la crisi, lo strumento è rimasto un punto stabile nella vita quotidiana del grande pubblico, eppure proprio la sua diffusione massiva si è accompagnata a una **crescente attività di cybercrime** ad esso associata.

Le restrizioni della fase pandemica hanno necessariamente innescato un'espansione del fenomeno della digitalizzazione, finendo con l'accelerare la diffusione di pratiche quali il lavoro in remoto, lo *streaming* e il graduale abbandono dell'archiviazione in formato cartaceo. Persino coloro meno familiarizzati con la tecnologia hanno dovuto imparare a destreggiarsi in un mondo che si sta rapidamente dirigendo verso una rivoluzione industriale informatica, con la conseguenza che il pubblico dei **consumatori di servizi virtuali** si è notevolmente ampliato. Secondo il rapporto dell'Internet Organised Crime Threat Assessment (IOCTA) redatto dall'Europol nel 2021, questa espansione ha attirato l'attenzione di criminali e truffatori, intensificando considerevolmente ogni possibile sfaccettatura del cybercrimine.

Secondo **John Fokker**, esperto di sicurezza informatica presso l'azienda Trellix, una delle tendenze in voga tra gli hacker è proprio l'utilizzo dei codici QR per condurre frodi e rubare dati, stratagemmi che nell'ambiente sono noti con il nome di ***phishing***. In una email inviata al *The New York Times* domenica 10 dicembre, Fokker ha lanciato un allarme: tra luglio e settembre 2023, la sua azienda ha rilevato almeno **60.000 casi di attacchi informatici** perpetrati attraverso l'abuso di codici a barre.

La segnalazione è stata presa seriamente dal Governo statunitense, con la Federal Trade Commission (FTC) che ha emesso immediatamente un comunicato al fine di consigliare ai cittadini di **diffidare dei QR Code sconosciuti e sospetti**. Una raccomandazione che peraltro era già stata diramata dall'FBI nel gennaio del 2022, quando dei truffatori avevano sostituito i QR Code sui parchimetri della città di Austin, riuscendo così a rubare i dati di pagamento di alcuni sventurati automobilisti.

Il *modus operandi* del *phishing* consiste nel fingere di essere una persona o un servizio legittimo al fine di indurre l'utente finale a fornire **informazioni sensibili** che altrimenti non si sognerebbe mai di condividere con degli sconosciuti. Questo inganno può manifestarsi sotto diverse forme, come ad esempio la simulazione di una mancata consegna di un pacco DHL, un'offerta di lavoro allettante o una richiesta d'aiuto da parte di un

ipotetico parente. Per quanto i QR Code abbiano preso piede solamente di recente, questo genere di truffa è consolidato sotto ormai da molto tempo. Basti pensare alle e-mail in cui i cybercriminali si spacciano per banche pronte a trasferire somme di denaro o ai finti SMS di sicurezza inviati da sedicenti portali di servizi.

Non esistono strategie definitive per contrastare efficacemente la diffusione dei codici a barre fraudolenti se non adottare un paio di precauzioni fondamentali: mantenere sempre aggiornato lo smartphone utilizzato per la scansione dei codici e **applicare un sano scetticismo**. È imperativo evitare di seguire i QR Code presenti all'interno di messaggi imprevisti o di email inattese, ma è anche opportuno diffidare di quelli rinvenuti in luoghi insoliti, quali graffiti o volantini anonimi. Tale diffidenza dovrebbe essere dunque estesa anche all'utilizzo di prese USB sconosciute, in particolare quelle delle centraline di ricarica dei cellulari presenti in luoghi pubblici come gli aeroporti e gli hotel: anche queste possono infatti costituire un accesso potenziale per malintenzionati che bazzicano l'ambito digitale.

[di Walter Ferri]