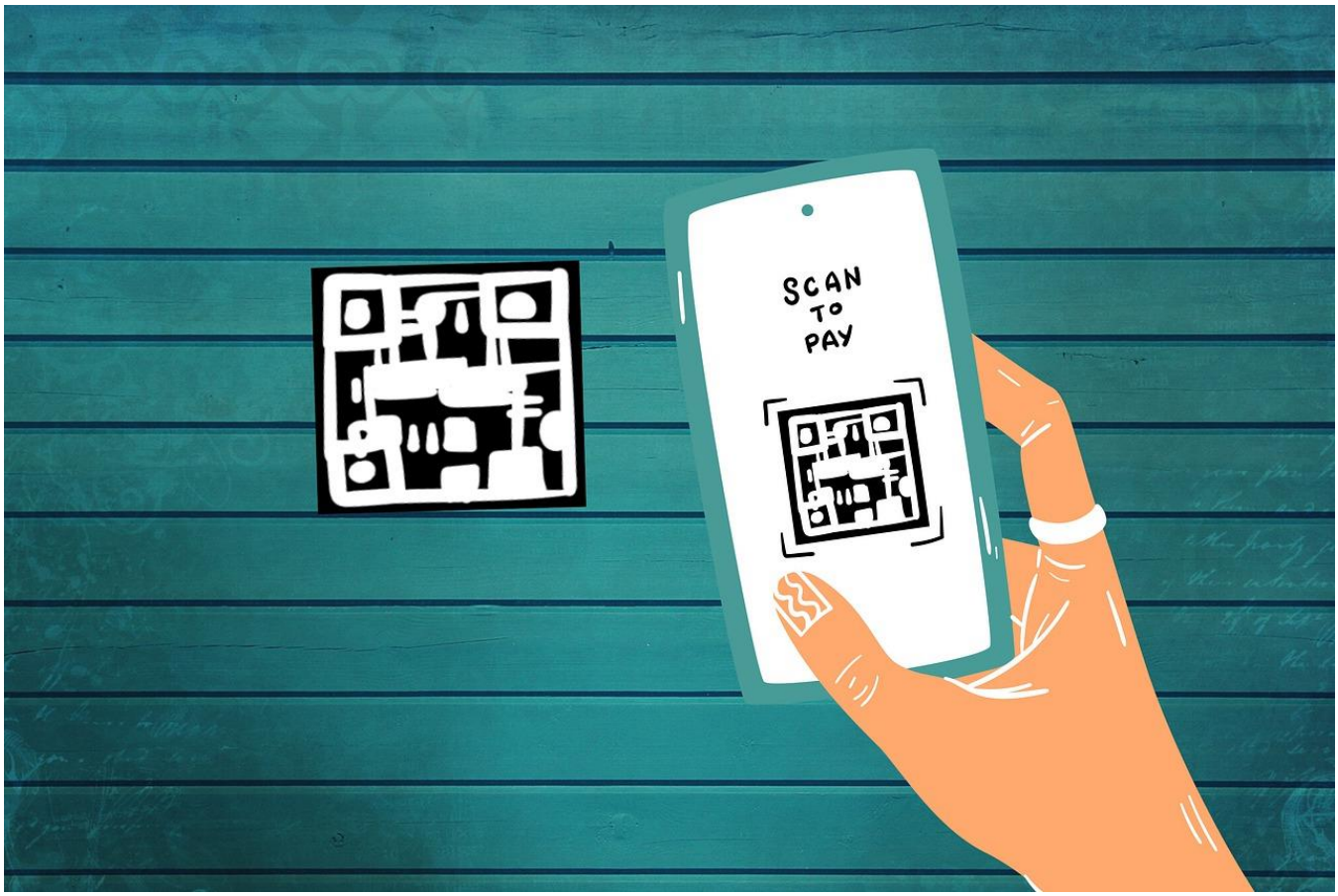
QRishing: attenzione alla nuova truffa digitale

I malviventi sfruttano i codici QR-code per sottrarre dati sensibili e credenziali di carte e conti



Parma, 26 ottobre 2022 – Le **truffe bancarie online** si stanno evolvendo, e ora utilizzano un nuovo sistema per carpire i dati sensibili dei malcapitati cittadini: il cosiddetto "***QRishing***". Questo raggiro si aggiunge alle ormai note tecniche di "*phishing*" (e-mail fasulle inviate, ad esempio, a nome della banca), "*smishing*" (sms ingannevoli inviati nella chat autentica della banca) e "*vishing*" (telefonata di un falso operatore bancario), a causa delle quali Confconsumatori si è ritrovata ad assistere, negli ultimi tempi, numerosi cittadini vittime di truffe.

IL QRISHING – Il "*QRishing*" ha l'obiettivo di sottrarre credenziali e dati sensibili dei conti correnti attraverso i codici "*QR-Code*", cioè quelle immagini quadrate con moduli neri su fondo bianco che vediamo sempre più frequentemente su riviste e giornali o che troviamo incollate su molte vetrine di ristoranti e musei. Tali codici rappresentano l'evoluzione dei più noti e datati "codici a barre" e, inquadrati attraverso lo schermo di uno smartphone, **permettono di aprire le porte a siti web, a contenuti multimediali, ma anche di**

effettuare pagamenti tramite app della propria banca. L'aumento dei codici QR ha indotto i *cyber* criminali a inventarsi una nuova tipologia di frode digitale che si basa sulla **modifica o sostituzione di un *QR-Code***: l'utente che scansiona il codice viene dunque **diretto verso un indirizzo internet differente** da quello verso cui credeva di essere condotto. Tramite link malevoli o contraffatti, senza rendersene conto la vittima viene "aggredita" nei propri dati personali suscettibili, che possono poi essere utilizzati da parte dei criminali informatici.

COME ACCADE? – Le tecniche più frequenti attraverso le quali vengono diffusi falsi *QR-code* in grado di trarre in inganno le potenziali vittime sono:

- la **sovrapposizione di una guaina trasparente sopra ai codici originali**: questa tecnica si verifica soprattutto in luoghi considerati sicuri dalle vittime. La conseguenza di questo senso di sicurezza è la percezione che la scansione del codice QR proposto dal locale, dal negozio e in generale dal luogo di fiducia, sia esente da rischi;
- l'**utilizzo di marchi di aziende note**: per ingannare gli utenti il criminale informatico utilizza un codice malevolo che fa riferimento a un marchio reale, simulando una pubblicità, ad esempio attraverso un volantino o un manifesto, creato ad hoc;
- l'**utilizzo di buoni sconto**: sfruttando il fatto che gli utenti sono molto più propensi ad aprire i codici QR che offrono sconti, i criminali inseriscono codici malevoli in finti buoni a nome dei principali marchi online.

Il pericolo che nasconde il *QRishing* deriva dalla tranquillità e dalla frequenza con cui gli utenti inquadrano codici QR, senza fare in tempo ad accorgersi di essere stati indirizzati verso pagine web truffaldine.

COME TUTELARSI? – Ecco dunque alcuni consigli:

- Osservare il **formato** dei codici QR: il principale attacco *QRishing* viene compiuto incollando sopra un codice QR originale uno fasullo;
- Chiedersi **chi ha generato quel codice** QR: codici generati da applicazioni sicure, che svolgono una specifica funzionalità e non portano a siti in cui vengono richieste informazioni personali sono certamente meno pericolosi di codici esposti pubblicamente, nel mondo fisico o virtuale, che portano a siti in cui viene richiesto l'inserimento di informazioni personali;
- Attenzione a **URL abbreviati**: se si utilizza un browser mobile, attraverso cui non è possibile fare un controllo, è meglio evitare di aprirli;
- Installare **applicazioni di sicurezza** anche sui propri dispositivi mobili: a differenza dei browser desktop, infatti, che chiedono all'utente se vuole entrare in siti non sicuri, i browser mobili di solito espongono l'utente a rischi maggiori.

Confconsumatori, pertanto, ritiene di rendere un servizio utile ai propri associati e a tutta la cittadinanza in genere, suggerendo di prestare particolare attenzione quando si compie un gesto ormai naturale come puntare l'obiettivo della fotocamera del proprio cellulare su un *QR-Code*. La tipologia di truffa che si sta diffondendo, infatti, essendo ancora poco conosciuta, rischia di colpire in modo indiscriminato molte persone. Per ulteriori informazioni e assistenza è possibile rivolgersi agli sportelli di Confconsumatori: www.confconsumatori.it/gli-sportelli-di-confconsumatori/.