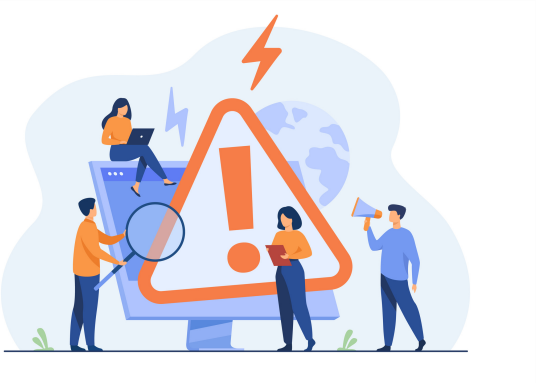
COME DIFENDERSI

- **nessuna banca chiede mai dati riservati né tramite telefono, né tramite email né attraverso un sms.** Se qualcuno, anche presentandosi come un operatore della nostra banca dovesse chiedere tali informazioni, si tratta di un tentativo di frode, quindi non fornirle a nessuno;
- **non rispondere mai a e-mail, sms, chiamate o chat da call center in cui vengono chiesti i codici personali** (utenza, password, codici di sicurezza, dati delle carte di pagamento, codici otp);
- **non cliccare sul link** contenuto nelle e-mail sospette; se per errore dovesse accadere, non autenticarsi sul sito falso, chiudi subito il web browser;
- **non dare mai i propri dati riservati,** né tramite telefono, né email né sms.



CONTATTI

Adiconsum Marche

Via Ragnini 4 - 60127 - Ancona

Tel. 0712832101

ACQUISTI ONLINE E TRUFFE SUI SISTEMI DI PAGAMENTO

Ormai siamo soliti usare gli strumenti digitali per svolgere molte operazioni e in qualunque luogo ci troviamo, ma questa comodità rischia di esporci a molti rischi informatici spesso poco conosciuti.

Ecco perché è necessario conoscere in maniera approfondita le diverse truffe costantemente in atto e quali sono i comportamenti da seguire per evitarle e difendersi.

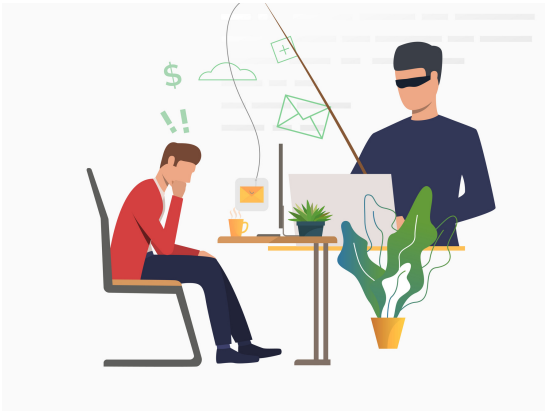
ADICONSUM MARCHE

Associazione di Promozione Sociale

Acquistare online spesso è conveniente e più comodo; tuttavia le truffe sono sempre dietro l'angolo, soprattutto in relazione ai **pagamenti online.**

Generalmente, infatti, su internet gli acquisti vengono effettuati con carte di credito e i malintenzionati sono sempre in agguato per carpire i nostri dati e le nostre credenziali e quindi poi svuotarci il conto corrente.

I rischi maggiori sono legati ai tentativi da parte di truffatori di carpire, attraverso artifizi o raggiri, i nostri dati riservati (dati della carta di pagamento, utenza, password, codici di accesso e/o dispositivi).



LE PRINCIPALI TIPOLOGIE DI TRUFFE

PHISHING

La truffa "base" è il phishing: consiste nell'invio di una ***mail*** che sembra provenire in tutto e per tutto dalla propria banca, che generalmente ha un contenuto preoccupante, ad esempio può esserci scritto che il nostro account è bloccato, oppure che è necessario aggiornare i propri dati, e contiene un link sul quale ci invitano a cliccare. Cliccando sul link veniamo indirizzati ad una pagina internet che sembra in tutto quella della nostra banca ma è un sito falso dove viene richiesto di inserire i nostri dati riservati come il numero della carta, la nostra password numero di cellulare o altro. Facendolo stiamo comunicando ai truffatori i nostri dati riservati per accedere o al nostro conto online o per utilizzare la nostra carta di credito.

SMISHING

Molto simile al phishing, ma in questo caso il messaggio truffaldino non viene inviato per email ma attraverso un ***SMS*** sul nostro cellulare. Occorre fare molta attenzione perché in molti casi il messaggio si mette in coda agli altri che ci sono già pervenuti dalla nostra banca e quindi sembra in tutto e per tutto provenire effettivamente dal nostro istituto di credito ma non è così.
In questo caso si parla di ***SMS Spoofing***, una tecnica con la quale i truffatori sono in grado di mascherare il numero reale dal quale il messaggio è stato inviato e farlo apparire nel nostro cellulare come se il mittente fosse la nostra banca. Anche in questo caso in genere c'è un link su cui cliccare, oppure siamo invitati a chiamare il numero indicato, o ancora ci viene chiesto di inserire il nostro numero di cellulare sul quale poi veniamo richiamati dai truffatori.

VISHING

Questa tipologia di phishing avviene tramite ***chiamata telefonica*** da parte di un frodatore che si finge un operatore della nostra banca: anche in questo caso con varie scuse, come aiutarci a fare un aggiornamento, o bloccare un tentativo di frode in atto, cercano di convincerci a comunicare i nostri dati riservati che poi i truffatori utilizzeranno per fare operazioni con il nostro denaro.

LA TRUFFA DEL PACCO IN GIACENZA

Un tipo di truffa recente è "truffa del pacco": consiste nella ***ricezione di messaggi***, sia scritti sia vocali, che ci avvisano dell'arrivo di un pacco o del ritardo della sua consegna e ci invitano a premere un link per risolvere il problema e contattare un operatore.
Cliccando quel link si apre una pagina dove ci vengono chiesti dati personali e sensibili che i truffatori utilizzeranno per accedere al nostro conto corrente e per utilizzare le nostre carte di pagamento.