DALLA PARTE DEL CONSUMATORE
ASSOCIAZIONE NAZIONALE

Tel. 3470628721 – email: coordinamentoconsumatori@gmail.com

VADEMECUM "DALLA PARTE DEL CONSUMATORE" PER RICONOSCERE LE TRUFFE ON LINE E TUTELARSI DALLE STESSE

1.Nessuna Banca o Società (sia essa di gestione di carte di credito, sia essa di spedizione, ecc.) chiede, attraverso email, sms, whatsapp o telefonicamente i dati personali del cliente;

2.l'indirizzo dal quale proviene la mail fraudolenta non è quello ufficiale dell'Istituto di credito o della Società alla quale si vorrebbe attribuire e del quale viene riprodotto, spesso in modo perfetto, il logo;

3.l'oggetto della email è, spesso, generico, scritto in lingua inglese o appare come risposta ad una email precedente;

4.nella email fraudolenta, non viene, quasi mai inserito il nome e cognome del destinatario, ma sono utilizzati locuzioni standard come "Gentile cliente", "Egr. signore" ecc.;

5.nel testo della mail sono presenti errori di ortografia e di grammatica. Ad esempio: molte parole sono privi di accenti, di lettere o sono unite con quelle successive; l'italiano, in alcuni passaggi, è poco comprensibile;

6. Anche la formattazione del testo risulta poco precisa;

7. le mail (phishing), gli sms (smishing) e le telefonate (vishing) fraudolenti, nel proprio contenuto, paventano, qualora non si inseriscano i dati richiesti, un danno economico, il blocco del conto corrente, della carta di credito o di un pacco in attesa di consegna.

In altri casi, l'inserimento dei dati è richiesto per riscuotere vincite o beneficiare di offerte irrinunciabili;

8.le email, gli sms ed i whatsapp fraudolenti contengono l'indicazione di un link di rimando ad un sito che, sebbene spesso identico o molto simile a quello della Banca o della Società per le quali i truffatori si spacciano, non è, invece, quello ufficiale. Su tale link di rimando è bene, quindi, non cliccare;

9.spesso le email pervenute dai phisher ricadono tra la posta indesiderata;

10.per evitare di cadere vittima di una truffa informatica si consiglia di:

a)non aprire e cancellare immediatamente email, sms e whatsapp sospetti;

b)non intrattenersi in conversazioni telefoniche con soggetti/istituti/enti ed in particolare con coloro che richiedano di effettuare operazioni o inserire o fornire i propri dati personali e/o i propri codici di accesso;

c)non fornire mai i propri dati personali, codici di accesso ed informazioni private;

d)qualora si è, effettivamente, clienti della Banca o della Società della quale si è ricevuto telefonate, email, sms o whatsapp sospetti, telefonare o contattare, tramite i canali ufficiali, la detta Banca o Società;

11.qualora si sia rimasti vittime di truffe *on line*: bloccare, immediatamente, il proprio conto corrente e la propria carta di credito, comunicare l'accaduto al proprio istituto di credito e sporgere denunzia alla Polizia Postale.