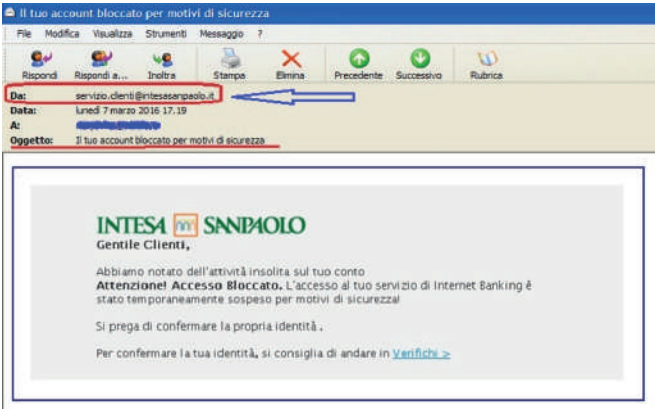
LE FRODI ONLINE HOME-BANKING NELL'ERA DEL COVID-19

I consigli utili di MDC

Ente Terzo Settore

MOVIMENTO DIFESA del Cittadino

Il Phishing cos'è e come difendersi



Secondo gli ultimi dati della Polizia Postale durante l'emergenza pandemica causata dal COVID-19 il maggior utilizzo di telefoni, e -mail, PC e smartphone per i contatti con la propria banca ha comportato un aumento delle truffe di cui quelle denunciate sono state 98mila.
Particolarmente insidioso è il cosiddetto phishing una particolare tipologia di truffa che si realizza via internet attraverso messaggi di posta elettronica ingannevoli.

Una e-mail **solo apparentemente** proveniente da banche o società di carte di credito invita riferendo problemi tecnici anche legati alla pandemia a fornire i propri dati riservati per l'accesso ai servizi di home banking e come spiegato dalla Polizia Postale solitamente nel messaggio, per rassicurare falsamente l'utente, è indicato un collegamento (link) che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati. In realtà il sito a cui ci si collega è stato artatamente allestito identico a quello originale. Qualora l'utente inserisca i propri dati riservati, questi saranno nella disponibilità dei criminali.
Altro pericolo è rappresentato dai cosiddetti "financial malware" o "trojan banking" allegati ai messaggi di posta elettronica con file in formato .doc; .pdf; .exe.

Una volta aperti questi veri e propri virus si installeranno sul PC o smartphone per carpire i dati finanziari ed attraverso il cosiddetto "keylogging" entrare in possesso delle chiavi di accesso ai vostri account di posta elettronica o di e-commerce.

Gli Istituti di Credito o le Società che emettono Carte di Credito non chiedono mai la conferma di dati personali tramite e-mail ma contattano i propri clienti direttamente per

tutte le operazioni riservate. Diffidate delle e-mail che, tramite un link in esse contenute, rimandano ad un sito web ove confermare i propri dati.

• **Verificate** sempre che nei siti web dove bisogna immettere dati (account, password, numero di carta di credito, altri dati personali), la trasmissione degli stessi avvenga con protocollo cifrato.

• **Controllate,** durante la navigazione in Internet, che l´indirizzo URL sia quello del sito che si vuole visitare, e non un sito *"copia"*, creato per carpire dati.

• **Installate** sul vostro computer un filtro anti-spam.

• **Controllate** che, posizionando il puntatore del mouse sul link presente nell´ e-mail, in basso a sinistra del monitor del computer, appaia l´indirizzo Internet del sito indicato, e non uno diverso.

Ente Tutela Cattore
MOVIMENTO DIFESA del Cittadino

Il Vishing e le telefonate truffa per carpire i codici bancari e delle carte di credito

Parallelamente, il procacciamento di codici “one-time”, token virtuali e password "avviene mediante il ricorso all'insidiosa variante “vocale” del phishing, il cosiddetto “vishing”. Finti operatori bancari o di società emittenti carte di credito chiamano riferendo anomalie nella gestione del conto corrente o della carta chiedendo di attivare non meglio precisate misure di sicurezza. In realtà il truffatore ha solo bisogno di farsi comunicare il “codice di conferma” per una transazione finalizzata a sottrarre il denaro alla vittima. Anche in questo caso il consiglio è semplice: **non rivelare mai a nessuno, via telefono come via social o via mail, i nostri dati più sensibili, le nostre password dispositive, i PIN o i nostri codici di accesso.**

Il Movimento Difesa del Cittadino con i propri sportelli territoriale ed on line continuerà a supportare i consumatori, soprattutto se anziani, al fine di tutelarli da Smishing ed altre tipologie di raggiri bancari.

Attività di interesse generale ETS finanziate ai sensi art. 67/DL 19.5.2020 n.34 - Avviso n.3/2020