ARTICOLO 3 - DICEMBRE 2020 – GENTILE CLIENTE L'ACCESSO AL SUO CONTO E' STATO LIMITATO

"Gentile cliente, l'accesso al suo conto è stato limitato. Sblocchi la sua utenza alla seguente: http://bit.ly/2rCnL92"

Se hai ricevuto un messaggio analogo ovvero altro dal contenuto similare sei stato vittima di una tentata e si spera, non consumata, truffa.

Il reato è quello che del c.d. *pishing*, ovvero, il tentativo di rubare i tuoi dati di accesso al conto bancario che si sta anche tramite SMS.

Ciò che non si deve in alcun modo fare è cliccare sul link riportato nel contenuto nell'sms che rimanda ad un sito creato apposta per rubare i dati inseriti. Si tratta di un sito "civetta", con la stessa grafica del portale web della banca, ed i malfattori riescono così ad ottenere i dati sensibili.

E' bene diffidare sempre da messaggi e comunicazioni con cui vi si chiede la compilazione di *form* ovvero di accedere a *link*ove comunicare i vostri dati personali al fine di evitare la sospensione del conto corrente. Nessuna banca o istituto di credito invia SMS per tale scopo, anche perché, nel caso in cui siate correntisti, li possiede già.

Talvolta,alla richiesta di cliccare su un link e digitare nome, cognome e codice cliente viene fatta seguire, dopo poche ore, una telefonata da un numero identico al numero verde del *call center* della banca e, con la scusa di bloccare operazioni sospette, i truffatori riescono a violare il conto online e farsi accreditare somme di denaro: l'interlocutore dall'altro capo della lineaè proprio il vostro truffatore.Ricordate, i numeri verdi si possono solo chiamare, dal numero verde non si può chiamare!

Analoga truffa in danno agli utenti consumatori ha coinvolto di recente anche una nota catena di elettronica.

Il cliente veniva avvisato tramite sms di un tentativo di contatto non andato a buon fine per la necessità di segnalare un trasferimento sospeso. Anche in questo caso, il messaggio conteneva un link che naturalmente non portava al sito della catena di elettronica ma ad una pagina web che emulava quella originale con logo, layout e colori molto simili a quella originale. All'interno del collegamento fraudolento si trovava un *form* da compilare con i propri dati proprio per ottenere il sospeso non ancora arrivato a destinazione.

Tentativi di *pishing* sono stati realizzati anche utilizzando il nome del noto gigante del mercato Amazon da cui provenivano messaggi promettenti l'abbonamento ad Amazon Prime in regalo celanti in realtà il tentativo di impossessarsi dei dati di accesso all'account Amazon attraverso un collegamento ipertestuale non ufficiale e fraudolento.

Il piano truffaldino risultava in questo caso ancora più ingegnoso: l'sms Amazon arrivava personalizzato con tanto di riferimento al proprio nome di battesimo.

Il fatto che gli hacker di turno conoscano questa preziosa informazione è verosimilmente dovuto al fatto che le vittime erano già state coinvolte in precedenti campagne di spam.

Diffida sempre dei messaggi con cui, anche attraverso la promessa di servizi gratuiti, viene richiesto di comunicare dati sensibili poiché dietro di essi si nascondono sempre hacker: l'unica cosa da fare è quella di ignorare e cancellare l'sms oppure, per qualsiasi dubbio, rivolgersi agli operatori della vostra banca o del soggetto da cui da cui risultano prevenire i messaggi.

In caso di sospetta truffa sul proprio conto corrente notificate immediatamente dell'accaduto il vostro istituto di credito, fornendo tutti i dettagli e le prove del caso. Inoltre, se la truffa è stata fatta online, informate la Polizia Postale.

La vittima di una truffa online può sporgere denuncia presso la Procura della Repubblica che agirà aprendo un apposito fascicolo per truffa online ai danni del soggetto denunciante.

Nel caso di truffa su Internet la Polizia di Stato ha messo a disposizione dei cittadini una speciale forma di denuncia: la denuncia *online*, da effettuarsi direttamente dal web collegandosi al sito istituzionale della polizia.

Si tratta di una procedura più rapida rispetto alla denuncia ordinaria.Occorre fornire le proprie generalità, gli estremi di un documento d'identità e dare il proprio consenso al trattamento dei dati personali.

Al termine il sistema rilascia una ricevuta elettronica e un numero di protocollo con il quale la vittima può recuperare la pratica presso l'ufficio di Polizia di Stato prescelto.

E' importante sapere che questa procedura non sostituisce la denuncia vera e propria ma rappresenta soltanto il primo step della procedura di presentazione della denuncia per reati telematici. Infatti, la vittima di truffa online dovrà necessariamente recarsi presso un ufficio di polizia per eventuali integrazioni e per dare valore legale all'operazione iniziata via Internet.

Se non si vuole sporgere denuncia, né su internet né all'ufficio della Polizia è comunque possibile segnalare il sito web, la mail o la pagina web alla Polizia Postale, utilizzando il sito web della Polizia Postale mediante la compilazione degli appositi moduli.

Avv. Chiara Zardi

ufficio legale Assoutenti Lombardia

Progetto realizzato nell'ambito del Programma generale di intervento della Regione Lombardia con l'utilizzo dei fondi del Ministero dello sviluppo economico. Ripartizione 2018