

IVG

Banda di cyber truffatori svuota i conti di decine di liguri grazie a sms falsi e telefonate

di G.M.

26 Novembre 2020 - 12:20



Liguria. Messaggi riferiti a carte bloccate, prelievi non autorizzati o all'aggiornamento dell'app dell'istituto bancario. Al loro interno alcuni link che rimandavano a siti clonati delle banche stesse. **Sms** apparentemente innocui e **simili in tutto e per tutto a quelli che si ricevono comunemente dalle banche**, ma ad inviarli erano dei cyber truffatori che ingannavano i correntisti riuscendo così a farsi rilasciare dati personali e, soprattutto, le password.

Lo avevamo raccontato qualche mese fa riportando la truffa subita da alcuni clienti di **Banca Carige** e di **Intesa San Paolo**. Si chiama tecnica dello *smishing-vishing*, una nuova frontiera dell'ormai noto phishing, con la quale un gruppo di quattro persone è stato scoperto e denunciato dalla polizia postale della Liguria e dai colleghi della Campania. Attraverso lo stratagemma i cyber truffatori **erano riusciti a sottrarre** dai conti di diversi istituti bancari operanti in Italia **da un minimo di 300 a un massimo di 55 mila euro**.

Un'altra tecnica utilizzata era quella del **raggiro telefonico**, *vishing* appunto, che consisteva nel contattare la potenziale vittima tramite una chiamata telefonica nella quale un finto operatore di banca, attraverso raggiri e argomentazioni capziose, la persuadeva

a **fornire i codici dispositivi del proprio rapporto finanziario.**

“Queste frodi - spiega la polizia - hanno avuto un **incremento notevole nel periodo pandemico** che stiamo vivendo, in quanto, in ragione del contingentamento degli accessi fisici alle filiali, i rapporti telefonici con le banche da parte dei clienti si sono intensificati”.

Dalle attività tecniche sono emerse inoltre la sfacciataggine e la convinzione di restare impuniti dei **criminali i quali in alcuni casi hanno apostrofato e insultato i frodati** con frasi del tipo: **“Ti abbiamo fregato”** o **“Sei stato un ciambellone”**.

La Polizia Postale e delle Comunicazioni attraverso le periferiche Sezioni Financial Cyber Crime si è prefissata l’obiettivo di colpire in maniera selettiva questa specifica attività criminale denominata **“Alias”**, che sta mietendo numerose vittime in ogni contesto sociale e geografico, provocando danni per milioni di euro.

Le regole d’oro per non abboccare.

- Non “cliccare” sui link inviati tramite e-mail o sms sospetti;
- Verificare sempre l’autenticità della pagina dell’istituto bancario.
- Non fornire alcuna credenziali di accesso/codice otp via telefono o sms.
- Effettuare la scansione del dispositivo con un antivirus aggiornato.
- Modificare le credenziali di accesso ai servizi on-line in caso di accessi sospetti.