Consiglio Nazionale
Geometri e Geometri Laureati

presso
Ministero della Giustizia

Serv. **FS** Area **1 – DG**
Rif. del
Allegati

Ai Signori Presidenti dei Collegi Geometri e GL

Ai Signori Presidenti dei Comitati Regionali Geometri e GL

Ai Signori Consiglieri Nazionali

Alla Cassa Geometri

LORO SEDI

Oggetto: Segnalazione Aruba S.p.A. – Tentativi di frode e furto identità SPID

In relazione ad una segnalazione pervenuta da Aruba S.p.A., afferente al disconoscimento dello SPID a seguito di furto di identità subito da alcuni professionisti, si riporta la seguente informativa finalizzata a prevenire il verificarsi di casi similari.

"Si evidenzia anzitutto che la problematica riguarda la modifica dei dati di contatto dell'identità SPID, effettuata tramite un raggiro ai danni dell'utente da parte di una falsa assistenza Aruba.

Le casistiche più ricorrenti sono:

- *Il cliente viene contattato telefonicamente dal numero fisso 0575/0505 riconducibile al contatto di assistenza Aruba (abbiamo rilevato contatti anche dal numero di cellulare. 3793584261). Chi contatta il cliente si spaccia per "operatore di Aruba" e utilizzando svariate scuse/motivazioni convince il cliente a farsi comunicare il codice OTP ricevuto sul cellulare;*
- *il cliente riceve un'email da un finto indirizzo di Aruba nella quale gli viene comunicato che l'identità SPID sta per scadere anticipandogli che sarà*

necessario utilizzare il suo OTP e che verrò chiamato dal numero 0575/0505 per ricevere assistenza; Il cliente viene contattato e come riportato nel punto precedente arrivano a carpire il suo codice OTP. Possono utilizzare altre svariate scuse/motivazioni: un presunto rinnovo, una presunta scadenza della password, un avanzamento del livello di sicurezza dello SPID, ecc.;

- *il cliente riceve un'email da un finto indirizzo di Aruba tramite il quale viene invitato ad accedere a un URL che non appartiene ad Aruba (anche se può sembrare). Su questo sito gli viene richiesto di inserire login, password e codice OTP SPID: il cliente accede e inserisce i dati, ma trattandosi di un sito fraudolento, i truffatori acquisiscono tutte le informazioni necessarie per rubargli lo SPID. Questa attività può essere ulteriormente supportata da una telefonata da parte di un falso operatore di Aruba che influenza il cliente nell'eseguire tali operazioni.*

I messaggi che hanno portato i clienti ad essere vittime di queste truffe sono stati inviati dalle caselle ***aruba.spidstaff@blu.it***, ***arubastaffdigitale@virgilio.it****".*

Alla luce di quanto sopra esposto, si ritiene opportuno ribadire l'importanza di non comunicare in nessun caso, attraverso canali telefonici, le proprie credenziali di accesso e(o) i codici OTP.

Si raccomanda altresì di verificare attentamente che ogni comunicazione provenga effettivamente da Aruba e non da indirizzi e-mail sospetti o riconducibili ad altri domini (ad esempio Gmail, Virgilio, Blu, ecc.).

Occorre inoltre prestare la massima attenzione prima di inserire eventuali codici OTP, accertandosi di operare esclusivamente all'interno del pannello web ufficiale di Aruba, previa accurata verifica sia dell'indirizzo URL del sito, sia della coerenza grafica della pagina visualizzata.

Con preghiera di voler assicurare la massima diffusione della presente comunicazione, si porgono cordiali saluti

IL DIRETTORE GENERALE

(Dr Avv. Francesco Scorza)

/ga