SaronnoNews

False multe da pagare via SMS, la truffa che imita SEND e pagoPA arriva anche in provincia di Varese

Tomaso Bassani · Friday, September 4th, 2026

Un **SMS che sembra spedito dal proprio Comune**, il numero di targa già citato nel messaggio, un link per "consultare i dettagli" di una multa che nessuno ricorda di aver preso. È lo schema di una campagna di phishing **segnalata dal CSIRT Italia**, la struttura dell'Agenzia per la cybersicurezza nazionale, e finita anche nelle segnalazioni che **circolano tra i lettori in provincia di Varese**.

L'alert descrive **una truffa veicolata via SMS** che sfrutta in modo improprio **i riferimenti grafici e testuali di SEND**, il Servizio Notifiche Digitali, e di pagoPA, per rendere credibile la richiesta di pagamento di una sanzione inesistente.

Come funziona l'inganno

La forza della truffa sta nel **riprodurre passo passo un iter amministrativo plausibile**. Il messaggio arriva da un mittente generico riconducibile a un "Comune" e segnala una presunta infrazione collegata alla targa del destinatario, invitando a consultarne i dettagli tramite un collegamento esterno. La prima pagina, costruita graficamente per somigliare a un servizio istituzionale, chiede di inserire il numero di targa per verificare eventuali verbali o sanzioni amministrative non saldate.

Subito dopo compare il dettaglio della finta violazione del Codice della Strada: velocità rilevata, margine di tolleranza, limite consentito, entità del superamento, data dell'infrazione, importo della sanzione e spese di notifica. Nel caso analizzato dagli analisti **la cifra richiesta era di 44,40 euro, comprensiva di sanzione ridotta e presunte spese di notifica**: un importo basso, unito alla riduzione per il pagamento entro cinque giorni, che serve a creare urgenza e ad abbassare la soglia di attenzione. Il terzo passaggio raccoglie i dati dell'intestatario del veicolo, cioè nome e cognome, indirizzo, comune, provincia, CAP, telefono e mail: **informazioni che possono essere riutilizzate per successive frodi** mirate o per tentativi di furto d'identità.

Solo alla fine la vittima viene portata su **una finta pagina di pagamento con il logo SEND** e i **richiami grafici a pagoPA**, dove vengono chiesti i dati della carta. A quel punto il rischio è la compromissione dello strumento di pagamento, con transazioni non autorizzate o riutilizzo dei dati su altri circuiti fraudolenti.Il dominio malevolo individuato dal CSIRT è notificheadigitali.org, molto simile nella forma a un indirizzo istituzionale ma senza alcun legame con la pubblica amministrazione.

Non è un episodio isolato. Già a fine maggio il CERT-AGID aveva individuato diverse campagne che sfruttavano il nome di SEND, la piattaforma di PagoPA per le comunicazioni con valore legale, con falsi solleciti di pagamento per sanzioni stradali che facevano leva su importi precisi, numeri di pratica e scadenze imminenti. L'associazione Codici, che ha rilanciato l'allarme, ricorda che SEND non sollecita pagamenti tramite mail ordinaria o SMS e non rimanda a siti di terze parti per il pagamento.

Cosa fare (e cosa non fare)

Le indicazioni del CSIRT sono poche e nette. Diffidare di SMS, mail o messaggi che chiedono il pagamento urgente di sanzioni o notifiche amministrative, soprattutto se accompagnati da scadenze ravvicinate o dalla minaccia di maggiorazioni. Non aprire i link ricevuti con messaggi inattesi, anche quando il mittente sembra un ente pubblico o un Comune. Verificare sempre il dominio del sito prima di inserire dati personali o finanziari. Accedere ai servizi pubblici solo dai canali ufficiali, digitando l'indirizzo a mano nel browser o usando le app istituzionali. Non inserire i dati della carta su pagine di cui non si è certi. **Chi si accorge di aver già inserito i propri dati su una pagina sospetta dovrebbe contattare subito la banca o l'emittente della carta** per valutare il blocco dello strumento di pagamento e tenere sotto controllo i movimenti non riconosciuti.