BOLLO AUTO, phishing ai danni dell'ACI e degli automobilisti

MDC FVG: per proteggere i propri risparmi e non cadere nella trappola dei cybercriminali, si devono seguire alcune regole fondamentali di sicurezza informatica!

Lo **Sportello Truffe Online MDC FVG** ha appreso da **CERT-AGID**, il Computer emergency response team dell'**Agenzia per l'Italia digitale** - che, a pochi giorni dall'annuncio dell'esenzione del pagamento del bollo per un veicolo, nel 2027, e a determinate condizioni, il bollo auto torna protagonista in negativo con una campagna di phishing che sfrutta indebitamente nome, logo e grafiche dell'**ACI** "**Automobile Club d'Italia"** per indurre le Vittime a saldare una presunta morosità relativa al bollo auto!

L'allerta diffusa dal **CERT-AGID** di campagne di phishing sempre più sofisticate, capaci di riprodurre fedelmente la grafica e l'identità di Enti pubblici come **ACI** per carpire la fiducia dei Cittadini, conferma un fenomeno che **MDC** stà monitorando con la dovuta attenzione ed in questo caso specifico, **i Truffatori** non si limitano a sottrarre dati identificativi, come codice fiscale, targa e indirizzo, ma arrivano a richiedere gli estremi completi della carta di pagamento, un salto di qualità che espone le **Vittime** a un danno economico diretto e non solo a un rischio di trattamento illecito dei dati personali!.

Il **sito fraudolento**, ha segnalato CERT-AGID, è ospitato sui domini **acitalia[.]info e acitalia[.]click**, estranei ai canali istituzionali dell'**ACI**.

Il Portale riproduce una veste grafica riconducibile all'Ente e prospetta l'esistenza di un bollo auto annuale non pagato entro la scadenza, con conseguenti sanzioni amministrative e maggiorazioni per mora.

La prima pagina chiede alla vittima l'inserimento del codice fiscale e della targa del veicolo, con il pretesto di verificare lo stato del pagamento del bollo auto.

Il messaggio fa leva sulle possibili conseguenze del mancato pagamento, quali sanzioni, fermo amministrativo e limitazioni alla circolazione.

Dopo l'inserimento dei dati richiesti, il sito mostra una pagina dedicata alle "Informazioni di contatto", nella quale vengono raccolti nome, cognome, indirizzo email, numero di telefono e indirizzo di residenza completo di città, provincia e codice postale. Nell'ultima fase viene simulata una schermata di pagamento della sanzione, pari a € 15,87. La pagina riporta codice fiscale e targa precedentemente inseriti e richiede i dati completi della carta di pagamento: nome dell'intestatario, numero della carta, data di scadenza e CVV.

Il **Segretario MDC FVG**, D. Durì, evidenzia: ai Consumatori che, purtroppo, abbiano già inserito i propri dati sul sito fraudolento raccomandiamo di contattare immediatamente la propria Banca per bloccare la carta utilizzata, sporgere denuncia-querela e conservare screenshot e comunicazioni ricevute come prova tangibile!

Il pagamento del bollo auto avviene esclusivamente attraverso i canali ufficiali della **Pubblica Amministrazione**, con autenticazione SPID o CIE:

qualunque richiesta di dati personali o bancari al di fuori di questi canali ufficiali deve essere considerata, a prescindere dall'aspetto grafico del sito, un tentativo di carpire in maniera fraudolenta dati riservati e sensibili!.

Le ultime truffe in circolazione ineriscono campagne di phishing che utilizzano illegittimamente le denominazioni di piattaforme ufficiali tra le quali:

SEND, Servizio Notifiche Digitali, la piattaforma ufficiale di **PagoPA** utilizzata dalla Pubblica Amministrazione per inviare comunicazioni con valore legale ai Cittadini. L'allarme è stato lanciato dal CERT-AGID il 27/05 c.a. https://cert-agid.gov.it/news/nuove-campagne-di-phishing-a-tema-send/

Il **Pres. MDC FVG**, R.G. Englaro, sottolinea che, per proteggere i propri risparmi e non cadere nella trappola dei **cybercriminali**, si devono seguire alcune regole fondamentali di sicurezza informatica raccomandate dalle stesse Autorità:

- Non cliccare mai sui link ricevuti tramite Sms o messaggi di messaggistica istantanea, anche qualora l'indirizzo Url visualizzato possa apparire apparentemente verosimile.
- Non inserire dati sensibili o codici dispositivo relativi a carte di credito, prepagate o conti correnti su portali raggiunti tramite collegamenti esterni non verificati.
- Procedere all'eliminazione immediata del messaggio sospetto dal proprio dispositivo senza inviare alcuna risposta.

In caso di reali perplessità o per verificare l'effettiva presenza di pendenze tariffarie, il Cittadino deve utilizzare esclusivamente i canali di contatto ufficiali degli Enti preposti o, in alternativa, consultare i portali della Polizia Postale per monitorare le ultime segnalazioni di reati informatici sul territorio.

MDC FVG è impegnata in un'attività di monitoraggio, segnalazione e assistenza per queste nuove frodi

Invitiamo gli Utenti incappati in una truffa a segnalarla a

sportello_truffeonline@mdc.fvg.it

telefonando ai numeri 0432 490.180 – 040 977.6000 – 0434 169.7742

800-324.520