NCA-11.052424 – NCERT Advisory – Smishing Alert: Fake Delivery Package Scam Threats

Introduction

In response to the escalating prevalence of fraudulent activities targeting individuals through deceptive delivery package scams, NCERT aims to address the critical need for heightened awareness and proactive measures to mitigate the risks associated with such malicious schemes. A notorious smishing (SMS phishing) scam claiming to be from Pakistan Post, and other courier service providers is still active, urging users to update their address via a malicious link to receive a delivery. This fake delivery package scam, a form of smishing attack, preys upon the widespread anticipation of receiving packages in today's digital shopping landscape, utilizing cunning tactics to coerce recipients into divulging sensitive personal information or inadvertently installing malware on their devices.

Understanding the Scam Operation

1. Initial Contact

a. **Deceptive SMS:** The scam commences with the receipt of an SMS purporting to originate from Pakistan Post. These messages often incorporate a tracking number or other ostensibly authentic details, striving to create an illusion of legitimacy.

b. **Impersonation:** Employing branding and language akin to genuine delivery services, the SMS is meticulously crafted to mimic official communication, thereby enhancing its credibility.

2. Deceptive Message

a. **Address Issue Notification:** The message typically asserts a discrepancy in the delivery address, prompting the recipient to update their information urgently to facilitate the receipt of the purported package. This manipulation fosters a sense of urgency and importance.

b. **Call to Action:** Enclosed within the message is a hyperlink urging the recipient to rectify the purported issue by clicking the provided link.

3. Malicious Link

a. **Phishing Website:** Upon clicking the link, recipients are redirected to a fraudulent website mirroring the appearance of legitimate delivery service

portals. This counterfeit site is ingeniously designed to harvest personal information.

b. **Malware Download:** Alternatively, recipients may be prompted to download a file, ostensibly related to the package delivery. However, this file harbors malicious software capable of clandestinely infiltrating devices, thereby compromising their security.

Target Audience and Mechanism

1. **Broad Demographic:** Scammers target individuals indiscriminately, capitalizing on the universal experience of ordering and anticipating package deliveries, irrespective of demographic attributes.
2. **Sense of Urgency:** Exploiting psychological triggers, such as urgency, these scams induce recipients to act hastily, thereby circumventing their usual cautious demeanor.
3. **Official Appearance:** By meticulously replicating the branding and communication style of genuine delivery services, perpetrators endeavor to instill trust and credibility in their deceptive messages.

Recommendations & Action Items

1. **Verify the Source:** Always authenticate the sender's phone number or email address, prioritizing consistency and familiarity. Exercise caution when confronted with messages from unfamiliar sources, particularly those containing typographical errors or irregular language.
2. **Avoid Clicking Suspicious Links:** Refrain from clicking links embedded within unsolicited messages; instead, access official websites directly by manually entering the URL into your browser. Hover over hyperlinks to discern their destination without clicking, scrutinizing for discrepancies or suspicious domains.
3. **Contact the Service Directly:** In the event of purported delivery issues, communicate directly with the delivery service via their authenticated contact channels to validate the legitimacy of the claim. Leverage the customer support resources available on the service's official website for further verification.
4. **Educate and Inform:** Share insights regarding prevalent scams with peers and family members to preemptively safeguard against potential victimization, emphasizing the pivotal role of awareness. Participate in community-driven initiatives or online forums aimed at educating and enlightening a broader audience about prevalent cyber threat.

5. **Leverage Security Software**: Ensure that your devices are equipped with updated security software capable of detecting and neutralizing malware and phishing attempts. Routinely update your operating system and applications to fortify your defenses against emerging vulnerabilities and exploits.
6. **Exercise Skepticism Towards Urgency:** When confronted with urgent requests, exercise prudence and deliberation, resisting impulsive actions prompted by heightened emotions. Independently corroborate the veracity of purported claims through alternative sources before responding to urgent solicitations.

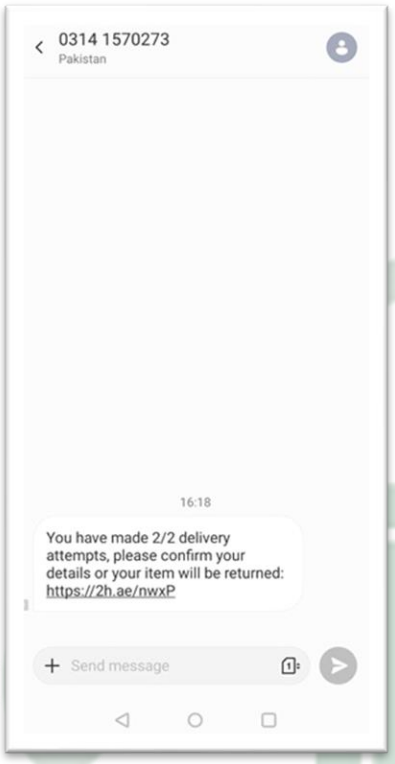
Additional Cautionary Note

It is crucial to remember that Pakistan Post or any other reputable courier delivery or postal service never requests online payments or address changes through SMS. Any reputed and credible courier delivery service never solicits online payments or initiates changes in your order through SMS, certainly not with a malicious link involved. Remain vigilant and exercise discretion when encountering such communications.

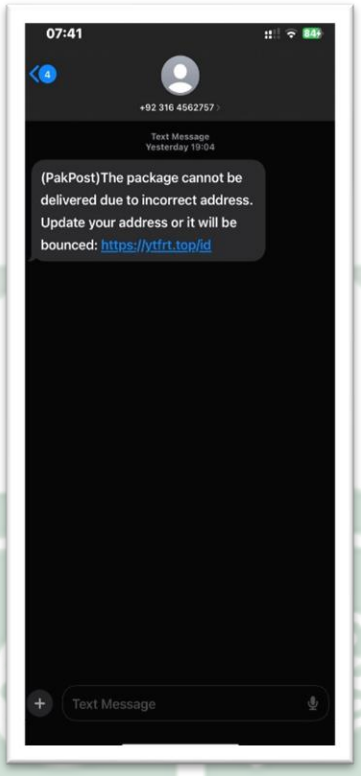
Conclusion

NCERT advises individuals to remain vigilant against the persistent threat of fake delivery package scams, particularly those masquerading as communications from reputable courier services like Pakistan Post, TCS, Leopard, and FedEx. Despite ongoing warnings, these deceptive messages continue to target unsuspecting recipients. It is imperative for individuals to prioritize awareness and adopt proactive measures to safeguard against potential victimization. By comprehensively understanding the tactics employed by scammers and adhering to best practices for verification and security, individuals can significantly mitigate the risks associated with such fraudulent schemes.

Annex

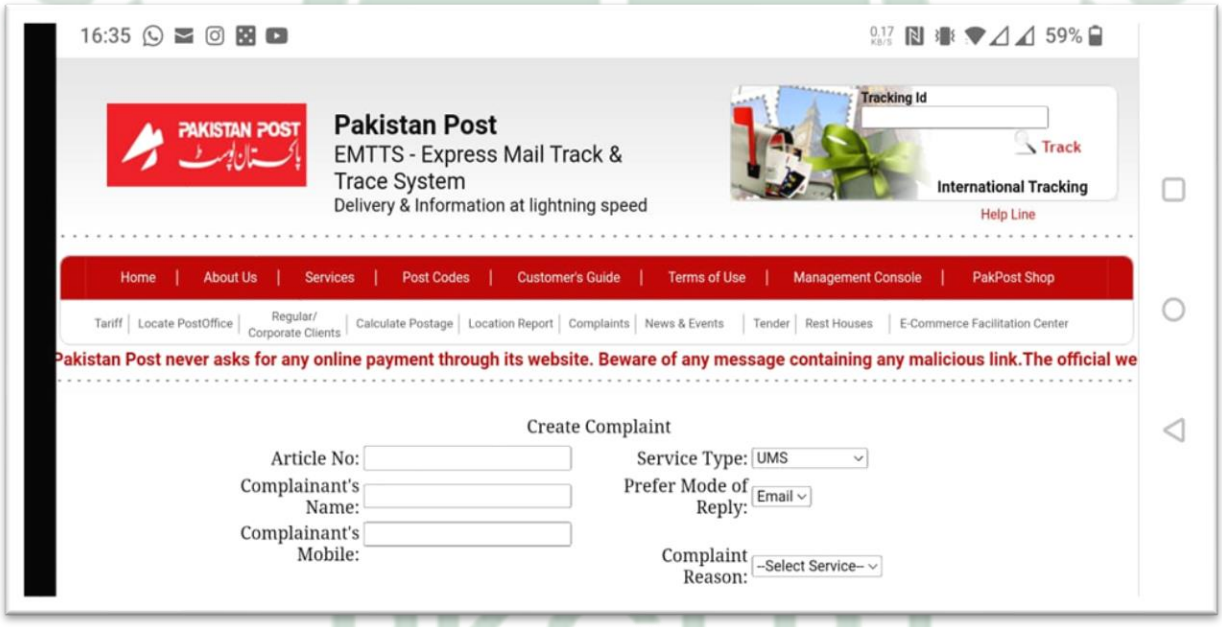


The Deceptive SMS 1
Containing a Malicious Link



The Deceptive SMS 2
Containing a Malicious Link

The Counterfeit Website 1



The Counterfeit Website 2