Protecting Public Transport Commuters from Social Media Phishing Scams

Executive Summary

Client	Major Public Transport Payment Provider
Industry	Public Transport & Digital Payments
Country	Singapore
Solution Implemented	Digital Risk Protection Services (DRPS)

In 2025, phishing scams impersonating a Singapore public transport payment provider surged across social media, luring commuters with fraudulent “unlimited travel” promotions and causing financial losses. To combat this, the organization deployed Digital Risk Protection Services (DRPS) to detect and remove malicious content proactively. Within the first year, multiple scam posts were taken down, helping protect commuters and strengthen trust in the national mobility ecosystem.

The Challenge

Phishing campaigns rapidly emerged across social media platforms using fake promotions designed to lure commuters.
Common tactics included:

- Fake ads promoting “unlimited travel” at extremely low prices
- Links redirecting victims to spoofed websites
- Requests for banking and payment credentials

Authorities issued public warnings urging consumers to verify promotions only through official channels.

Business Risks

Consumer Harm	• Commuters losing money to phishing scams • Growing public concern around digital payment safety
Reputational Damage	• Brand impersonation eroding customer trust • Rising complaints and negative sentiment
Regulatory Pressure	• As a regulated payment provider, the organization must demonstrate proactive fraud prevention and consumer protection

Why Digital Risk Protection Services (DRPS)
The organization adopted DRPS to:

- Continuously monitor social media and the open web for brand abuse
- Detect phishing campaigns and impersonation quickly
- Execute rapid takedown of malicious content
- Reduce fraud exposure and protect customers proactively

Deployment Overview

- Onboarding: Completed within one week
- Monitoring: Ongoing since September 2025

Key Actions

- Continuous monitoring for scam content impersonating the brand
- Identification of fraudulent social media posts and advertisements
- Coordination with platforms for takedown requests
- Ongoing risk visibility and reporting

Outcomes
Malicious social media content impersonating the organisation was successfully identified and removed, reducing the spread of phishing campaigns and preventing further victim exposure.

The initiative helped:

- Safeguard commuters from phishing attacks
- Reinforce trust in digital transport payments
- Support regulatory and risk management responsibilities

Further details about i-Sprint's products are available at www.i-sprint.com. To reach us, please email us at enquiry@i-sprint.com.