Digital Risk Protection Cases August 2025

An analysis of scam cases in Asia-Pacific, Australia and New Zealand.

About this report

This report presents a concise overview of key Digital Risk Protection (DRP) cases observed and investigated by the Group-IB APAC CERT team during August 2025. The aim of sharing this report is to provide valuable insights into the evolving threat landscape across Asia-Pacific (APAC) as well as Australia and New Zealand (ANZ); and highlights prevalent scam tactics and attack vectors.

While this report is shared freely to foster broader awareness and enhance collective cybersecurity, Group-IB DRP customers benefit from access to more in-depth and granular intelligence. Our dedicated analysts are also available to provide further detailed reporting and respond to specific queries from our DRP clientele, ensuring they remain robustly protected against sophisticated digital threats.

Cryptocurrency platform phishing campaigns

Target:

Users of a popular cryptocurrency platform.

Modus Operandi:

Threat actors send phishing emails with the subject “Migrate to [Platform] Wallet”, claiming a mandatory upgrade to self-custodial wallets due to “legal issues”.

The email instructs victims to download a legitimate app but provides a pre-generated recovery phrase – or ”seed phrase” – to set up a new wallet.

When the victim uses the provided phrase and transfers cryptocurrency to the ‘new wallet’, the threat actors gain full access to the funds because they already control the recovery phrase.

Deceptive Elements:

The emails appear to be from the platform but are sent from a third-party hosting provided with a shared IP address service, allowing them to bypass spam filters and security checks.

The attack is deceptive in how it reverses traditional phishing tactics by giving the user a recovery phrase which the attacker already controls, instead of stealing the user’s existing one.

Abuse of subdomains in shortened URLs for SMS phishing (smishing)

Target:

Residents who use a toll company's electronic billing system.

Modus Operandi:

Threat actors impersonate a toll company and send SMS messages, claiming the victim has an outstanding fee.

The SMS contains a shortened URL which directs the victim to a fake website showing the 'outstanding fee'.

The website then asks the victim to provide personal information and card details.

The shortened URLs use the "pse.is" domain which is registered under Picsee.io – a URL shortening service. Threat actors exploit the free 'Adjusted Subdomain' feacture of Picsee.io to create convincing and customized subdomains, making the malicious links appear trustworthy.

Deceptive Elements:

The use of a URL shortener which allows the customization of subdomains make the malicious link appear more legitimate.

The scam preys on victims' fear of penalties, which can be up to 10 times the amount owed.

Link injection via backdoor: Phishing site hosted on government website

Target:

Users of a leading e-wallet platform in APAC.

Modus Operandi:

The threat actor hosted a phishing page on a legitimate-looking subdirectory of a government-affiliated domain.

The page mimicked the login interface of a popular e-wallet platform to steal user credentials and financial information.

This is form of ‘directory abuse’ where attackers find an uploadable or writable folder on a server, plant malicious content, and use a deep path to avoid detection.

Deceptive Elements:

The phishing page was hosted on a real government site, which significantly increased the likelihood of a user trusting the link.

Attackers target deep directories because they are often publicly accessible and rarely monitored.

Fake job hiring scams

Target:

Job seekers.

Modus Operandi:

A fake job hiring website advertises remote freelance jobs with daily earnings.

The scam has two scenarios:

1. A WhatsApp company account asks the victim to fill out a form to register as an employee, requesting personal and banking information.
2. The victim is asked to join a WhatsApp group to observe how others complete assignments.

In the second scenario, the victim is asked to perform tasks to earn commissions, and promised free hotel stays. Eventually, the scammers ask the victim to transfer money for "registration fees" to a bank account.

Deceptive Elements:

The scam uses WhatsApp company accounts and group chats to create a sense of legitimacy. Scammers use social engineering tactics to build trust and pressure victims into transferring money.

When the victim joins the group, a "reward" message will appear, claiming that another user had earned their salary.

Fake job hiring scams

Target:

Individuals who have previously been scammed

Modus Operandi:

Scammers create impersonation accounts, often marked with blue verification ticks, to appear authentic. These fake Facebook profiles or pages frequently pose as lawyers or government ministries, leveraging the image of authority to gain trust.

They make false promises to help victims recover their lost funds.

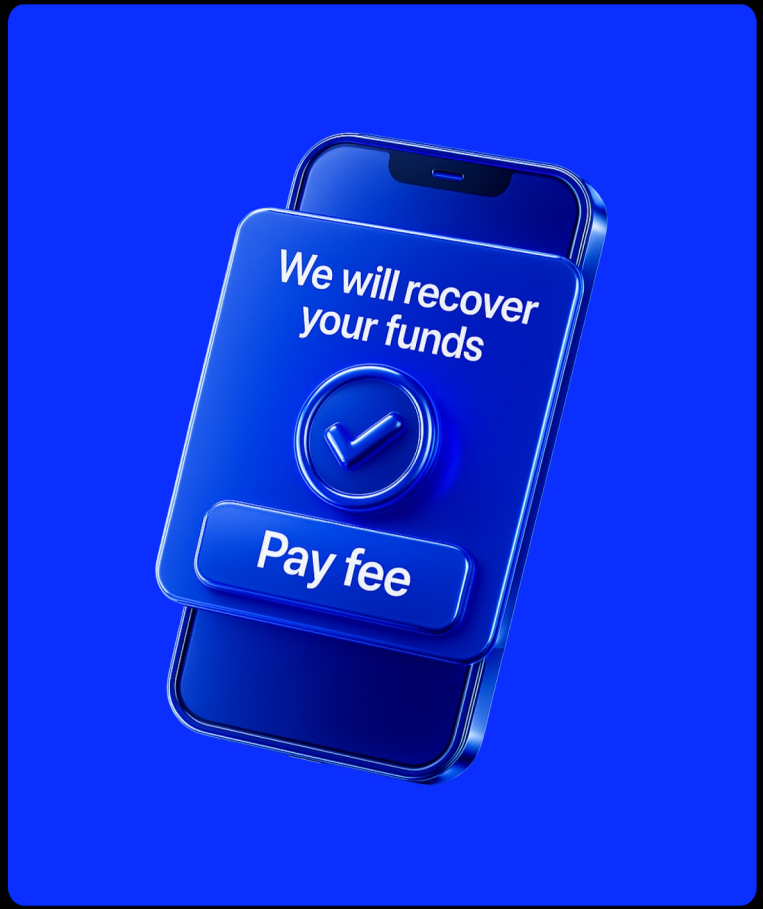
Instead of recovering funds, the scammers ask for an upfront payment or fee, scamming the victim again.

Deceptive Elements:

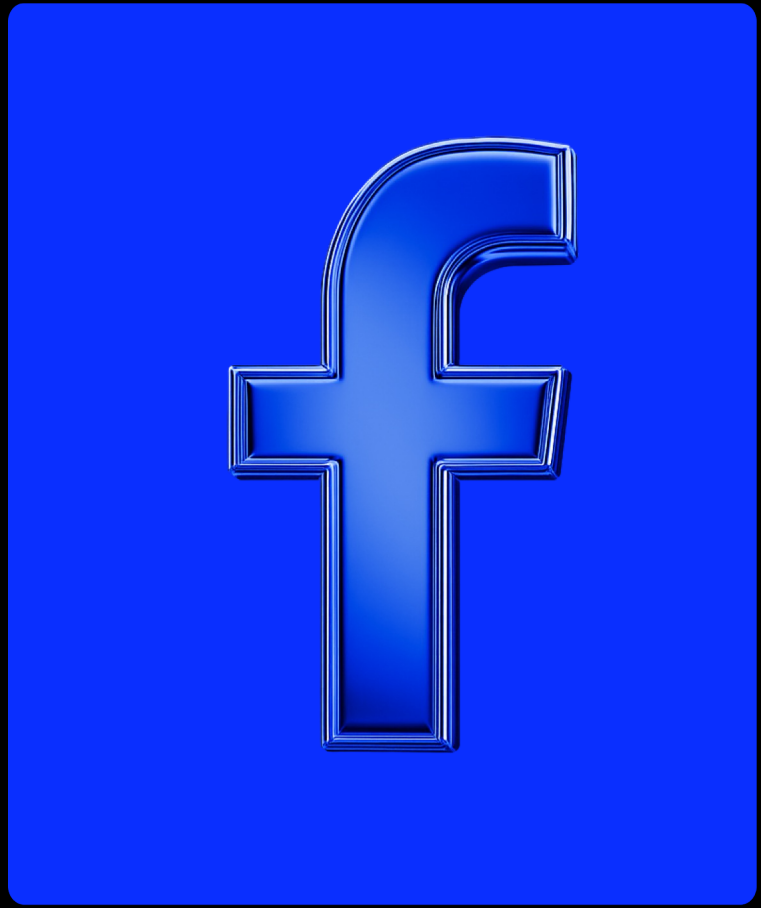
The use of verification ticks and fake comments under impersonated accounts make the profiles seem authentic.

The false promises make it difficult for victims to walk away.

As soon as new members join these groups, scammers pose as fellow ‘victims’, asking about their experiences while sharing fabricated recovery stories of their own. This creates a false sense of solidarity and trust, making their so-called recovery methods appear credible.



Facebook Marketplace scams



Target:

Online sellers on social media and e-commerce platforms.

Modus Operandi:

Scammers comment on a seller's post or send a direct message, expressing interest and asking to move the conversation to Line messenger.

The scammer invites the seller to a group chat with other members who are also believed to be threat actors.

The conversation is diverted from the sale of the product to convincing the seller to invest or register on a fake online platform related to trading, cryptocurrency, or gambling.

In some cases, the scammer directly asks the victim to transfer money to a mule account for "registration fees".

Deceptive Elements:

The scammers use social engineering tactics to redirect the conversation from a legitimate sale to a fraudulent investment opportunity. The group chat is filled with other scammers who act as members to lend credibility.

Delivery courier scams

Target:

Individuals who have recently ordered a package.

Modus Operandi:

The victim receives a text message from a courier claiming a wrong package was delivered.

The scammer offers to assist with a refund and sends a QR code for processing.

Scanning the QR code redirects the victim to a mobile banking app, prompting them to pay an amount exceeding the package's value.

If the victim's balance is insufficient, a new QR code is sent with a payment amount that matches the victim's balance, leading to the transfer of all their savings.

Deceptive Elements:

The scammer has precise details about the ordered items, suggesting possible collusion with a corrupt delivery courier, a delivery service employee, or the seller. This detailed information makes the scam more convincing.

E-Wallet 'Money Pocket' Tasks Scam

Target:

The target of these scams are e-wallet users, particularly social media users attracted by quick rewards such as cashbacks or vouchers. Victims are often persuaded to share sensitive information, including Identity Card (IC) pictures and selfies, or to make deposits with the expectation of unlocking larger withdrawals.

Modus Operandi:

The modus operandi begins with scam posts on platforms like Facebook that redirect victims to newly registered external domains.

Scammers contact victims via Messenger or WhatsApp, guiding them through simple online tasks and showing fake balances or testimonials.

To access the supposed earnings, victims are pressured to deposit money and submit IC photos for “verification,” trapping them in a cycle of deposits and blocked withdrawals.

Deceptive Elements: Threat actors use branded visual assets, professionalized messaging, and falsified payout evidence to establish credibility. They rotate short-lived, obfuscated domains to evade detection and deploy psychological tactics such as small initial “returns” to build trust. In parallel, they harvest personally identifiable information via fake compliance checks, exposing victims to identity theft, account takeover, and financial loss.

Malware Disguised as Service App

Target:

Citizens using national social security services through a mobile application.

Modus Operandi:

A malicious Android APK disguised as a government social service app is being distributed through social engineering channels such as SMS and chat applications, bypassing official app stores.

Once installed, it presents fake forms that capture sensitive personal information, including names, birthdates, ID card images, and financial details. The stolen data is encrypted with hardcoded keys and transmitted to attacker-controlled servers.

Deceptive Elements:

The malware mimics the legitimate social security services mobile application.

Victims lured into downloading it via direct links shared through SMS, chat applications, and other social engineering channels.

Convincing interface exploits trust in government services to trick users into entering sensitive information.

Rewards Redeem Smishing targeting SEA and ANZ

Target:

These Smishing Campaign Templates target various business groups across South-East Asia (SEA) as Australia and New Zealand (ANZ) in the telecommunication, banking and airline sectors.

Modus Operandi:

Scammers send SMS messages claiming that reward points will soon expire and ask victims to click a link. The link opens a phishing website, but the content can only be accessed if three conditions are met:

- A specific path file is used. e.g. /[country abbreviation], /rewards
- Users are connected via an in-country network.
- A mobile user agent is detected. Using Desktop will redirect the resource to Google.com

These campaigns show two main patterns: they use the same website design (same stylesheet) with localized content.

Deceptive Elements:

The smishing messages are sent to real customers of the targeted company, making the scam more convincing.

The phishing websites are designed to look neat, detailed, and visually appealing, giving the impression of an official site.

The websites include several interactive features such as phone number entry, instruction pages, redeem pages, and online forms, which make them appear legitimate and trustworthy.

Fight Against Cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785