Forensic Analysis of GCash Cybersecurity Incidents

# 1. Executive Summary: The Dual Nature of Fintech Risk

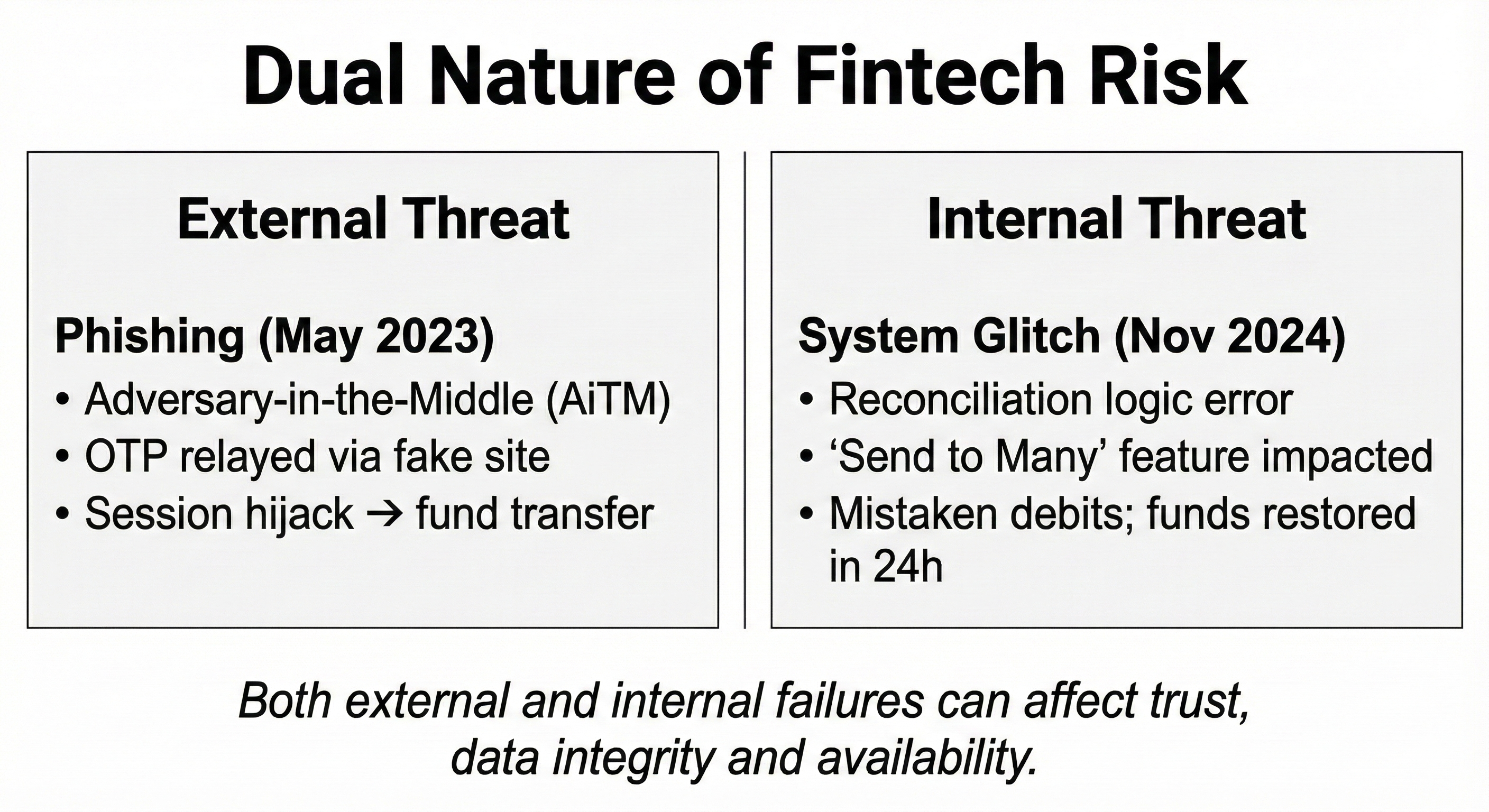
Mobile wallets **GCash** now play a central role in Philippine finance. As the leading platform, GCash processes massive volumes for tens of millions of users, making its security posture a matter of national stability. This report examines two pivotal events: (1) an external phishing campaign in May 2023 that used Adversary-in-the-Middle (AiTM) techniques to bypass SMS OTP, and (2) an internal reconciliation glitch in November 2024 linked to batch logic and the ‘Send to Many’ feature. Together, they show that both external social engineering and internal operational errors can disrupt integrity and availability.

Figure 1. Dual nature of fintech risk: external phishing vs internal reconciliation glitch.

# 2. Strategic Context: The GCash Ecosystem and Attack Surface

GCash is a ‘Super App’ integrating banking (GSave), credit (GCredit), investments (GInvest), and lifestyle services. It relies on client-side controls (MPIN, device fingerprinting, biometrics), backend API gateways for real-time bank transfers and ledger updates, and multiple third-party integrations. Regulatory oversight by BSP and NPC enforces consumer protection and data privacy compliance. The platform’s scale and complexity enlarge its attack surface.

A diagram of a green scheme

AI-generated content may be incorrect.

Figure 2. Overview of the GCash ‘Super App’ ecosystem, integrations, and client security controls.

# 3. Incident I: The May 2023 Phishing Offensive (External Threat)

Attackers targeted online gamblers using social media lures (e.g., PhilWin promos). The phishing sites operated as real-time proxies between users and the legitimate service. Users entered mobile numbers and MPINs; the backend sent a real SMS OTP; the fake page prompted for the OTP and relayed it. Result: the attacker’s session was authenticated, leading to fund transfers to mule accounts. The core weakness was reliance on phishable SMS OTP without strong device/session integrity checks.

Key weakness: SMS OTP can be relayed; device/session integrity not verified

**AiTM Phishing Attack Flow (May 2023)**

Figure 3. AiTM phishing flow showing credential capture, OTP relay, and session hijack.

# 4. Incident II: The November 2024 System Reconciliation Glitch (Internal Threat)

On November 9, 2024, users reported repeated deductions (e.g., ₱2,000) due to a reconciliation logic error. Indicators point to the ‘Send to Many’ feature and a failure of transaction atomicity (ACID), allowing mistaken debits without corresponding transfer instructions. Response was rapid: detection, disabling of the feature, transparent communication with regulators, and full fund restoration within 24 hours—demonstrating mature incident management and business continuity.

A diagram of a company

AI-generated content may be incorrect.

Figure 4. Simplified schematic of reconciliation flow and where logic errors can cause repeated debits.

# 5. Framework Insights (Simplified)

MITRE ATT&CK (Mobile) helps describe attacker techniques (e.g., phishing, input capture, AiTM bridging, and user execution). OWASP Mobile Top 10 highlights authentication and communication weaknesses, code quality, and input validation risks. ISO/IEC 27001 emphasizes governance: change management, acceptance testing, incident response, and business continuity.

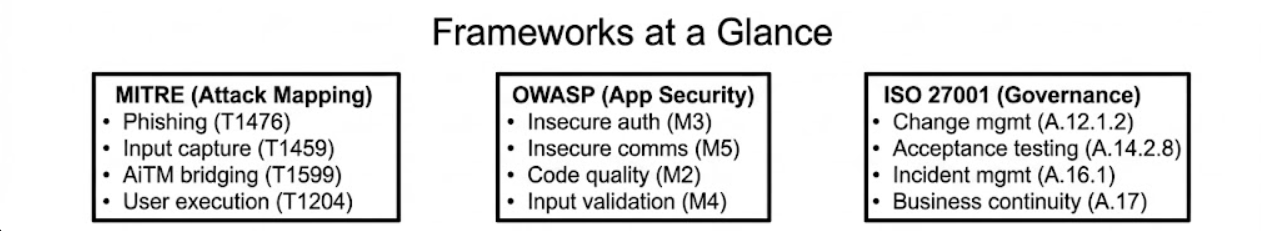


Figure 5. High-level summary of MITRE, OWASP, and ISO 27001 focus areas relevant to the incidents.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident Component** | **Forensic Evidence / Observation** | **MITRE ATT&CK (Mobile) Mapping** | **OWASP Mobile Top 10 (2024) Mapping** | **ISO 27001:2022 Control Mapping** |
| **Gambling Lure** | Users targeted via "PhilWin" / "TapWin1" ads.3 | **T1476 (Phishing):** Delivery via social media links. | **M5 (Insecure Communication):** Interaction with untrusted endpoints. | **A.7.2.2 (Security Awareness):** Failure of user education regarding safe browsing. |
| **Fake Login Page** | Spoofed UI capturing Mobile Number & MPIN.3 | **T1459 (Input Capture):** Harvesting credentials. | **M1 (Improper Credential Usage):** Entry of secrets into untrusted forms. | **A.9.4.2 (Secure Log-on):** System allowed access via spoofable static credentials. |
| **OTP Bypass** | Attackers relayed OTP in real-time.4 | **T1621 (MFA Request Generation):** Triggering SMS. **T1599 (Network Boundary Bridging):** AiTM Proxy. | **M3 (Insecure Authentication):** Reliance on phishable SMS OTP. | **A.9.4 (Access Control):** Weakness in authentication strength (MFA implementation). |
| **Fund Transfer** | Money moved to East West / AUB.13 | **T1499 (Financial Theft):** Unauthorized transfer. | **M10 (Insufficient Cryptography):** Transaction signing did not verify device location/integrity. | **A.16.1 (Incident Management):** Detection of anomalous flows to specific banks. |
| **Ledger Error** | "System reconciliation" caused deductions.5 | **N/A** (Not adversarial). | **M2 (Inadequate Supply Chain):** Internal code quality failure. | **A.12.1.2 (Change Management):** Failure to test batch script updates. |
| **Feature Glitch** | "Send to Many" feature malfunction.2 | **N/A** | **M4 (Insufficient Input Validation):** Logic error in batch processing inputs. | **A.14.2 (Security in Development):** Flawed acceptance testing for specific features. |
| **Denial of Hack** | GCash/BSP statements ruling out breach.12 | **Defensive Tactic:** Reputation Management. | **N/A** | **A.5.19 (Supplier Relationships):** Managing public trust and transparency. |
| **Refunds** | Restoration of funds in 24h.11 | **Defensive Tactic:** Remediation/Recovery. | **N/A** | **A.17 (Business Continuity):** Effective resilience and data restoration. |
| **Defense Upgrade** | Implementation of "Double Safe" (Face ID).8 | **Mitigation:** Stronger MFA. | **Remediation for M3:** Implementing biometric binding. | **A.9.4.2 (Secure Log-on):** Upgrading to biometric standards. |

Table 1 : Comparative Framework Matrix: The Mapping

# 6. Defensive Evolution: From SMS to Biometrics (‘Double Safe’)

Following the 2023 phishing wave, GCash accelerated rollout of biometric ‘Double Safe’ logins with selfie liveness checks. This shifts authentication from ‘something you have’ (SIM/OTP) to ‘something you are’ (biometrics), reducing phishing success and strengthening session integrity on new device logins.

A comparison of a comparison of a comparison of a comparison of a comparison of a comparison of a comparison of a comparison of a comparison of a comparison of a comparison of a comparison of a comparison of

AI-generated content may be incorrect.

Figure 6. Before/After comparison: SMS OTP vulnerabilities vs. biometric ‘Double Safe’ benefits.

## 6.1 The "Double Safe" Mechanism

Following the phishing wave, GCash moved to eliminate the dependence on SMS OTPs, which GXI executives explicitly acknowledged "has been exploited by some fraudsters".8

* **The Implementation:** The new feature requires a **Selfie Scan (Liveness Check)** for any new device login.
* **Cybersecurity Logic:** This shifts the authentication factor from "Something You Have" (the SIM/OTP, which can be relayed) to "Something You Are" (Biometrics).
* **Framework Impact:**
* **MITRE:** This effectively mitigates **T1599 (AiTM)**. A phishing site cannot easily capture a 3D liveness check and relay it to the app in real-time without sophisticated, high-latency deepfake injection tools that are currently rare in mass-market attacks.
* **OWASP:** This closes the **M3 (Insecure Authentication)** vulnerability gap.

## 6.2 ISO Certification as Maturity Indicator

In 2024, GCash achieved dual certification for **ISO/IEC 27001:2013** (Information Security Management) and **ISO/IEC 27701:2019** (Privacy Information Management).18

* **Significance:** This certifies that GCash has moved beyond ad-hoc security measures to a systematic, risk-based approach. The certification audit by the British Standards Institution (BSI) validates that their processes for **Risk Assessment (A.8.2)**, **Access Control (A.9)**, and **Cryptography (A.10)** meet global standards.

**Context for 2024 Incident:** The fact that the November 2024 incident was *contained* and *reversed* quickly is likely a direct result of the Incident Management processes (A.16) put in place to achieve this certification.

# 7. Conclusion

The May 2023 incident exposed limitations in SMS-based authentication against AiTM, while the November 2024 glitch revealed the importance of rigorous change management and testing. Together they underline that resilience demands both stronger external defenses and tighter internal controls, supported by governance frameworks and continued user education.  
  
**Risk 1: Social Engineering Susceptibility (High)**

* **Observation:** The success of the "PhilWin" campaign proves that a significant portion of the user base is vulnerable to psychological manipulation.
* **Evidence:** Users willingly entered MPINs into non-GCash domains.10
* **Framework:** MITRE T1476 (Phishing).
* **Remediation:** Removal of clickable links in all official SMS and emails 19 to train users that *no* legitimate link will ever come via text.

**Risk 2: Batch Processing Logic Fragility (Medium/High)**

* **Observation:** The "reconciliation" glitch indicates that the backend systems responsible for balancing ledgers are prone to logic errors during high-volume or specific feature execution ("Send to Many").
* **Evidence:** Unauthorized deductions of P2,000 without user interaction.17
* **Framework:** ISO 27001 A.12.1.2 (Change Management).
* **Remediation:** Implementation of automated **Chaos Engineering** and **Canary Deployments** for all ledger-impacting scripts.

**Risk 3: Supply Chain/Third-Party Ecosystem Risk (Medium)**

* **Observation:** The attack vector utilized the brand trust of gambling sites (PhilWin) to target users. While GCash cannot control these sites, their existence creates a "gray zone" of risk.
* **Evidence:** Attackers used "tapwin1.com" as a launchpad.3
* **Framework:** ISO 27001 A.5.19 (Supplier Relationships).

**Remediation:** Aggressive **Threat Intelligence** monitoring to identify and take down domains mimicking GCash or associating heavily with GCash logos for fraudulent purposes.

# 8. References

1. Senate probe into recent GCash system glitch, e-wallet phishing scams sought, accessed December 2, 2025, <https://mb.com.ph/2024/11/14/senate-probe-into-recent-g-cash-system-glitch-e-wallet-phishing-scams-sought>
2. GCash Restores Funds After Technical Glitch, Suspends 'Send to Many' Feature, accessed December 2, 2025, <https://fintechnews.ph/64932/e-wallets/gcash-unauthorised-transfers/>
3. NPC confirms GCash incident caused by phishing attacks - Philippine News Agency, accessed December 2, 2025, <https://www.pna.gov.ph/articles/1202151>
4. OTP Fraud Prevention: E-Snatching Scams and How to Stay Safe - Remote Staff, accessed December 2, 2025, <https://www.remotestaff.ph/blog/e-snatching-otp-fraud-philippines/>
5. GCash says customer funds safe amid technical issue, no money was lost - InsiderPH, accessed December 2, 2025, <https://insiderph.com/gcash-says-customer-funds-safe-amid-technical-issue-no-money-was-lost>
6. PROSPECTUS - Ayala Corporation, accessed December 2, 2025, <https://ayala.com/app/uploads/2023/05/Ayala-Corporation-Prospectus-dated-May-3-2023-1.pdf>
7. GCash becomes first Philippine fintech to secure dual ISO Certifications for Information Security and Privacy Management - adobo Magazine, accessed December 2, 2025, <https://www.adobomagazine.com/brand-business/gcash-becomes-first-philippine-fintech-to-secure-dual-iso-certifications-for-information-security-and-privacy-management/>
8. GCash to roll out 'double authentication' feature | GMA News Online, accessed December 2, 2025, <https://www.gmanetwork.com/news/money/personalfinance/852490/gcash-to-roll-out-double-authentication-feature/story/>
9. GCASH - Compromised? : r/phinvest - Reddit, accessed December 2, 2025, <https://www.reddit.com/r/phinvest/comments/12m0prp/gcash_compromised/>
10. NPC Concludes Investigation on Unauthorized GCash Transactions, accessed December 2, 2025, <https://privacy.gov.ph/npc-concludes-investigation-on-unauthorized-gcash-transactions/>
11. GCash glitch triggers BSP probe: All funds restored, but concerns remain - Manila Bulletin, accessed December 2, 2025, <https://mb.com.ph/2024/11/11/g-cash-glitch-triggers-bsp-probe>
12. Statement on GCash Incident - Bangko Sentral ng Pilipinas Media and Research Press Releases, accessed December 2, 2025, <https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=7314>
13. NPC: Phishing attacks, not hacking, behind GCash fiasco - News - Inquirer.net, accessed December 2, 2025, <https://newsinfo.inquirer.net/1774207/npc-phishing-attacks-not-hacking-behind-gcash-fiasco>
14. Unauthorized GCash transactions caused by phishing attack – NPC | Philstar.com, accessed December 2, 2025, [https://www.philstar.com/headlines/2023/05/25/2268833/unauthorized-gcash-tra](https://www.philstar.com/headlines/2023/05/25/2268833/unauthorized-gcash-transactions-caused-phishingattack-npc)