# IMPORTANT CYBERSECURITY NEWS: THREAT ACTORS EXPLOIT GOOGLE ADS AND PAYPAL NO-CODE CHECKOUT FOR PHISHING ATTACKS

## Vairav Cyber Security News Report

**Date: March 3, 2025**

**Vairav Cyber Threat Intelligence Team**


## Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

## EXECUTIVE SUMMARY

Security researchers have uncovered a sophisticated phishing campaign exploiting vulnerabilities in Google's advertising ecosystem and PayPal's no-code checkout system. Threat actors deploy fraudulent Google Search ads mimicking PayPal's branding, directing victims to malicious subdomains under **paypal.com**. These fraudulent pages, hosted on PayPal's legitimate infrastructure, trick users into calling fake customer support numbers, enabling credential theft and financial fraud. This attack highlights how cybercriminals weaponize legitimate platform features to bypass traditional security mechanisms, marking an escalation in social engineering tactics.

## INCIDENT ANALYSIS

The attack chain begins with Google Search ads impersonating PayPal's official support. Attackers exploit gaps in Google's Misleading Ad Design policy, which permits deceptive ads if the display URL and landing page share the same root domain. These ads lead victims to PayPal's no-code checkout system, which attackers manipulate to create fake payment forms embedded with fraudulent customer service contact details. Mobile users are at higher risk, as smaller screen sizes hide full URLs, making phishing pages appear more legitimate.

The infrastructure abuse is exacerbated by Google's January 2025 ad policy updates, which failed to detect these hybrid phishing pages. Additionally, PayPal's no-code checkout lacked automated detection of social engineering payloads, enabling attackers to insert fraudulent instructions directly into payment pages. As a result, attackers bypass traditional security tools and redirect victims to call scam numbers, leading to potential financial losses and credential theft.

In response, PayPal has temporarily disabled custom text fields in its no-code checkout pages and is implementing real-time NLP analysis to detect fraudulent support numbers. Meanwhile, Google has accelerated training ad detection models using adversarial machine learning to identify domain reputation hijacking tactics.

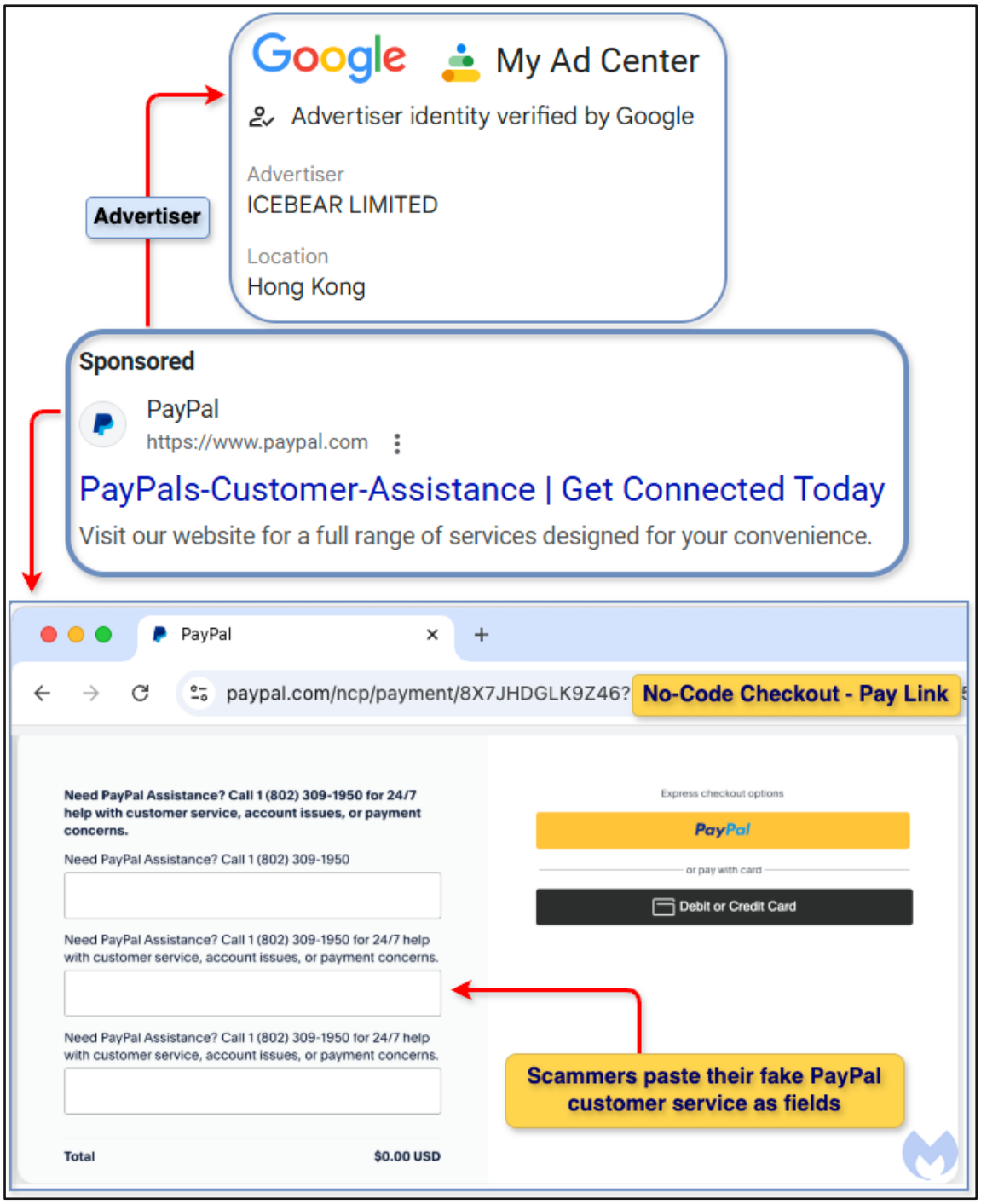


*Figure 1: No-code checkout abuse*

## INDICATORS OF COMPROMISE (IOCS)

**URL**: *hxxps[:]//urlscan[.]io/result/3ea0654e-b446-4947-b926-b549624aa8b0*

**Malicious PayPal Payment Links:**

- *hxxps[://]www[.]paypal[.]com/ncp/payment/8X7JHDGLK9Z46*
- *hxxps[://]www[.]paypal[.]com/ncp/payment/7QUEXNXR84X3L*
- *hxxps[://]www[.]paypal[.]com/ncp/payment/BHR4AMJAPWNZW*

- *hxxps[://]www[.]paypal[.]com/ncp/payment/FTJBPVUQFEJM6*
- *hxxps[://]www[.]paypal[.]com/ncp/payment/2X92RZVSG8MUJ*
- *hxxps[://]www[.]paypal[.]com/ncp/payment/D8X74WYAM3NJJ*

**Scammers' Phone Numbers**:

- *1-802[-]309-1950*
- *1-855[-]659-2102*
- *1-844[-]439-5160*
- *1-800[-]782-3849*

## RECOMMENDED ACTIONS

To mitigate the risk posed by Lotus Blossom's espionage activities, organizations should:

**For Enterprises**

- Monitor transaction payloads for phone numbers or unusual text strings in payment pages.
- Implement cross-channel verification via OAuth 2.0 before processing sensitive user requests.
- Enhance client-side URL validation using strict public IP checks to detect unauthorized redirects.

**For End Users**

- Avoid calling phone numbers embedded in PayPal payment pages—use official support channels.
- Bookmark PayPal's official site instead of relying on Google Search ads.
- Use ad blockers that filter sponsored results to reduce exposure to fraudulent ads.

As of now, Google has removed 63% of identified malicious ads, but researchers warn that similar attacks could soon target YouTube and Gmail infrastructure. Organizations and individuals must remain vigilant as cybercriminals continue adapting their techniques

## RESOURCES

https://cybersecuritynews.com/hackers-abused-google-and-paypals-infrastructure/

https://www.malwarebytes.com/blog/scams/2025/02/paypals-no-code-checkout-abused-by-scammers

## CONTACT US

**Vairav Technology Security Pvt. Ltd.**

**Cyber Defender from the land of Gurkha**

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com