PUBLIC ALERT

Brand Impersonation Scams Using Google Maps and Searches

1.0 Background

The Cyber Security Authority (CSA) has observed a growing trend in scams involving the impersonation of well-known brands and service providers, including Pizza Hut, Pizzaman/Chickenman, Hisense, Bel Aqua, Papaye, Burger King, etc. Using Google Map and Google Search, cybercriminals create fake business profiles or manipulating search results to trick the public into engaging with fraudulent phone numbers, websites, or addresses.

2.0 Modus Operandi

- Cybercriminals create or alter Google Maps business listings of popular companies, banks, hotels, airlines, courier services, and government agencies. The fraudulent listings include fake phone numbers, emails, and websites.
- When users search for a company's contact details or service information, they are presented with the fraudulent listing usually at the top of Google results, leading them to contact the cybercriminals instead of the legitimate business.
- The cybercriminals pose as customer service agents of the brands they represent and trick victims into sharing one-time passwords (OTP) or PIN's, which are used to withdraw funds from their mobile money wallets or make payments for goods and services they never receive.

3.0 Recommendations

3.1 For the Public

- Always cross-check contact details, including phone numbers, from the official websites of institutions instead of relying solely on Google Search or Maps.
- Treat top search results with caution; fraudulent listings may appear above legitimate ones, particularly paid "Ad" results. Scammers pay to have their fraudulent links appear at the very top.
- Avoid sharing sensitive information, including PINs and OTPs online.
- If you encounter fake business listings or contacts on Google Maps, report them directly through Google's reporting tools and notify the CSA.

3.2 For Institutions/Businesses

- Regularly search for your brand online, including Google and Google Maps to identify fraudulent listings or fake websites.
- Proactively share verified contact details on official websites, social media, and other trusted platforms
- Monitor reviews and comments online, especially on social media handles for mentions of fraud, as this is often a sign of impersonation.
- Institutions are encouraged to acquire official toll-free numbers (e.g., 0800 XXXX) that can be centrally managed and mapped to their various branches, ensuring consistency and trust. Alternatively, organisations may acquire dedicated number ranges and actively publicize them to the public as their official contact lines.

The CSA has a 24-hour Cybersecurity/Cybercrime Incident Reporting Point of Contact (PoC) for reporting cybercrimes and for seeking guidance and assistance on online activities; Call or Text – **292**, WhatsApp – **0501603111**, Email – report@csa.gov.gh .

Issued by the Cyber Security Authority
August 29, 2025
Ref: CSA/CERT/MPA/2025-08/02