PUBLIC ALERT

ONLINE SHOPPING SCAM – BLACK FRIDAY DEALS

1.0 Background

"Black Friday" marks a period in the shopping season where retailers offer significant discounts and promotions to buyers. The Cyber Security Authority (CSA) anticipates a surge in online shopping scams and urges citizens to conduct due diligence when shopping online. The CSA recorded a total of 266 cases of online shopping fraud from January to October 2025, with monetary losses of over GHS 600,000.

2.0 Modus Operandi

- **Brand Impersonation:** Scammers mimic known brands on search engines such as Google and then use optimisation techniques to manipulate search results to list their contact information at the top. Unsuspecting victims, after engaging these scammers, make advance payments for products or services which they never receive. The scammers proceed to block their victims after receiving payments.

- **Fake Online Shops:** Scammers create online profiles, especially on social media, to sell non-existent goods and services at too-good-to-be-true prices. After making advance payments to mobile money wallets of the scammers, which usually do not bear the names of the supposed shops, victims are blocked and do not receive what they paid for.

- **Phishing Schemes:** Scammers trick online shoppers into disclosing sensitive information such as credit/debit card information or account passwords by luring them via email, WhatsApp message, or SMS, to click on links that lead to legitimate looking but fraudulent shopping sites.

3.0. Recommendations

- Check via official websites or reliable sources to validate the contact details of shops/businesses rather than relying solely on search engine results. Additionally, check user reviews to verify the reputation of the contact.
- Limit shopping to reputable and well-known online stores and exercise caution with unfamiliar shopping sites.
- Be cautious of phone calls, emails or messages promising deals that seem too-good-to-be-true.
- Insist on payment after delivery and inspection of products.

The CSA has a 24-hour Cybersecurity/Cybercrime Incident Reporting Point of Contact (PoC) for reporting cybercrimes and receiving guidance/clarification on suspected scams. Contact us via Call or Text – 292, WhatsApp – 0501603111 or Email – report@csa.gov.gh.

Issued by the Cyber Security Authority
November 28, 2025

Ref : CSA/CERT/MPA/2025-11/01