PUBLIC ALERT

Valentine's Day Scams

1.0 Background

Valentine's Day is an occasion when people show their affection for others by sending gifts or items with messages of love. Malicious cyber actors also use the celebration to defraud unsuspecting victims through various schemes. Of the total losses recorded for 2023, at least **GH₵ 3,558,940** was lost through online shopping and romance scams. The Cyber Security Authority (CSA) is by this alert reminding the public to exercise caution and due diligence in their online activities.

2.0 Modus Operandi

- **Shopping Fraud:** Malicious actors create fake websites or online shops or impersonate existing businesses on social media, offering heavily discounted packages and items. Victims are enticed to send money for these items which they never receive, or they receive in substandard forms.
- **Brand Impersonation**: Malicious actors create fake business listings or profiles with their contact details on Google Maps mimicking legitimate businesses or brands and use search engine optimization techniques to manipulate search results for the targeted brand to divert legitimate inquiries to the scammers' contact numbers. After the unsuspecting victims engage and pay (usually to a mobile money wallet) for products, the scammers block them from making further contact, and the expected delivery does not materialise.
- **Phishing Scams:** Malicious actors send unsolicited emails or messages claiming to be from a romantic partner, or a company offering Valentine's Day deals. These messages contain links or attachments that when clicked, install malicious software (malware), or steal personal information.
- **Romance Scams:** Malicious actors create fake online profiles to deceive victims into believing they are engaging in a trusting relationship. They use the relationship to persuade the victims to send money, provide personal and financial information, or purchase items for them.

3.0 Recommendations

- Be cautious of "too good to be true" deals on Valentine's Day packages or gifts.
- Use a reputable online marketplace or retailer when purchasing Valentine's Day gifts. Look for reviews and customer feedback before making an online purchase.
- While search engines provide convenient access to information, they can also display manipulated or misleading results. Check on the official websites or with reliable sources to validate the contact details of shops rather than relying solely on search engine results. Also, check user reviews for hints on the reputation of the contact.
- Be alert for fake online shops and hyped adverts, especially on Facebook, Instagram, and Telegram. In most cases, request a physical location to enable you to validate the legitimacy of the business.
- Insist on payment only after delivery and inspection.

3rd Floor, NCA Tower
KIA, 6 Airport By-pass Rd, Accra | Digital Address: GL-126-7029 | Tel: 0303 972530, 0303 972531
E-mail: info@csa.gov.gh | Website: www.csa.gov.gh

- Be wary of unsolicited messages or emails claiming to be from a romantic partner, especially those that make requests for money or other sensitive information.
- Do not share personal information such as your Ghana card number, credit card information, or bank account details with anyone.
- Ensure that mobile money payments are made to wallets in the name of the online shop you are dealing with.

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 – **050 160 3111**, Email – report@csa.gov.gh.

Issued by the Cyber Security Authority
February 7, 2024

Ref: CSA/CERT/MPA/2024-02/01

3rd Floor, NCA Tower
KIA, 6 Airport By-pass Rd, Accra | Digital Address: GL-126-7029 | Tel: 0303 972530, 0303 972531
E-mail: info@csa.gov.gh | Website: www.csa.gov.gh