PUBLIC ALERT

Easter and Eid al-Fitr Season Scams

1.0 Background

Easter is a major Christian festival that celebrates the death and resurrection of Jesus Christ. Eid al-Fitr is the first of two canonical festivals of Islam that marks the end of Ramadan, the Muslim holy month of fasting. Malicious actors have been observed to take advantage of the heightened commercial activity associated with festive seasons to perpetrate online scams. The Cyber Security Authority (CSA) has between January and March this year, received 194 cases of online fraud with a total loss of about **GH₵ 2,404,161**. The public is reminded to exercise caution and due diligence in their online activities.

2.0 Modus Operandi

- **Online Shopping Scams**: Malicious actors create fake online shops or impersonate existing businesses on social media pages, offering heavily discounted goods. Victims are enticed to send money for these deals but never receive the items.
- **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 members. 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 materialize.
- **Phishing Scams**: Malicious actors send unsolicited emails or messages claiming to be from a romantic partner, or a company offering deals associated with the festive season. These messages contain links or attachments that when clicked, install malicious software (malware), or steal personal information.

3.0 Recommendations

- Be cautious of unsolicited messages offering exciting or "too good to be true" deals connected to the festive season.
- Use a reputable online marketplace or retailer when purchasing items or gifts. Consider reviews and customer feedback before making an online purchase.
- Search engines can be manipulated to show misleading results. Check on the official website or with reliable sources to validate the contact details of the shop you are searching for.
- Insist on payment only after delivery and inspection and ensure that mobile money payments are made to wallets in the name of the online shop you are dealing with.
- Do not share personal information such as your Ghana card number, credit card information or bank account details with anyone.

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
March 28, 2024

Ref: CSA/CERT/MPA/2024-03/02