CSO Chief Security Office

LLOYDS BANKING GROUP

Urgent: Brokers are targets for cyber criminals. Action is required.

LBG has seen a significant increase in cyber-attacks, being exploited for very large sums of money by criminals; this is a direct threat to you, your Brokers, and our customers.

Here are two recent Broker examples: *

Example 1 - Fake Login Page

A single business email account was compromised through a phishing attack involving a fake login page. The adviser entered credentials into the false site but quickly reported the incident.

Following review by our forensics team we were comfortable that no vulnerabilities were exploited, no data was exfiltrated, and there was no lasting impact to ourselves or Brokers services. The event was contained and closed with no concerns.

Example 2 – Remote Access 'Scareware' Attack via Fake Microsoft Support

The Broker was tricked by a scareware pop-up while visiting a restaurant website, which falsely claimed the device was infected and prompted a call to a fake Microsoft support number.

The threat actor gained remote access to the laptop during the call, locked down the device, and ended the session. The laptop was rendered unusable and later securely destroyed.

Following review by our forensics team we were comfortable that no vulnerabilities were exploited, no data was exfiltrated, and there was no lasting impact to ourselves or Brokers services. The event was contained and closed with no concerns.

How can a Broker protect their business:

Multi-factor Authentication

- MFA is a second line of defence.
- It is easy to use but makes any potential attack harder for criminals.
- Ask an IT provider, or search security settings, to set up MFA.

Broker's must:

- Never use the same password in different places.
- Be ultra cautious entering the firm's password into any website, checking the website address carefully.
- Ask customers to call directly on a known number to confirm any changes or concerns about payment requests.
- Report any cyber-attack immediately so we can provide support and initiate a thorough investigation.

Get government funded support:

- Visit NCSC.gov.uk
- Search 'Funded Cyber Essentials NCSC' for funding and support to get your company cyber security accredited.
- The sections on the NCSC site have further advice.

Kind regards,

Security Education and Awareness

Chief Security Office

*Examples are representative of real cases. Some details have been changed for privacy.