National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Set-Top Box Fraud Alert

May 2017

SET-TOP BOX FRAUD ALERT

The content of this alert is based on information gathered by the National Fraud Intelligence Bureau (NFIB). The purpose of sharing this information with law enforcement partners and key stakeholders is to assist in preventing/ detecting crime, bring offenders to justice and increase awareness of enablers currently being utilised by criminals.

ALERT CONTENT

The NFIB identified a new fraudulent trend that may impact the general public in relation to set-top boxes infected with malware intended to steal user's details to commit fraud.

Safeguarding the public from illegal streaming services via set-top boxes is vital to the UK economy, the Creative Industry and the many people employed in the industry. There are 'set-top' boxes imported from various foreign jurisdictions that are enabled so people can view illegal content.

We are aware that set-top boxes, although perfectly legal in their own right, are repeatedly adapted by criminals to unlawfully receive TV channels protected by intellectual laws.

The set-top boxes can come with many common features the person purchasing may be unaware of, such as sites offering access to copyright infringing material and access to illegal sites. The set-top boxes may also contain infected malware that is disguised as something as innocent as a play button and is unknowingly initiated by the user; potentially impacting other electronic devices. The users will normally have used some personal details when setting up the set-top box, which could be used to defraud them. Consequently, what may appear to be a bargain for the consumer may quickly turn into a genuine problem by loss of personal data and or money.

PROTECTION / PREVENTION ADVICE

- Only purchase set-top/streaming boxes from recognised outlets.
- Contact your bank if you notice any suspicious transactions on your accounts.
- When signing up to websites/internet services, use a password or PIN you have not used elsewhere.
- Enable 2-Factor Authentication on your important accounts (i.e. email/banking/social media).

FEEDBACK

The NFIB needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following NFIB feedback survey through: https://www.surveymonkey.com/r/FeedbackSDU. This should take you no more than 2 minutes to complete. If you have other feedback or additional information that you would prefer to provide by email please send to NFIBfeedback@cityoflondon.pnn.police.uk.

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998.

The cover sheets must not be detached from the report to which they refer.

Protective Marking:	**NOT PROTECTIVELY MARKED**
FOIA Exemption:	NO
Suitable for Publication Scheme:	NO
Version:	V.1
Storage File Location:	NFIB
Purpose:	Fraud Alert
Owner:	NFIB Management
Author:	11990q
Review By:	103939P