National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Phishing Scam – Facilitated Using Email Regarding "Cancelled Order" and "Tech Support" Alert

September 2017

CITY OF LONDON POLICE
Economic Crime Academy

To help prevent your business to counter fraud and/or obtain details of our available courses, please contact the City of London Police Economic Crime Academy via our website http://academy.cityoflondon.police.uk, or you can view our latest prospectus on http://academy.cityoflondon.police.uk/images/prospectus

PHISHING SCAM – FACILITATED USING EMAIL REGARDING "CANCELLED ORDER" AND "TECH SUPPORT" ALERT

The information contained within 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, bringing offenders to justice and increasing awareness of enablers currently being utilised by criminals.

ALERT CONTENT

The National Fraud Intelligence Bureau (NFIB) has received intelligence which suggests that fraudsters are continuing to evolve and exploit more ways to reach potential victims by using spam campaigns to distribute links that lead to fraudulent tech support websites.

They will invariably use spam emails by spoofing brands to get recipients to click suspicious links. The spam emails contain a link to fraudulent tech support pages that look like notifications from well known online retailers. The suspicious links attract customers by notifying them that their recent order has been successfully cancelled or amended.

Generally, the order number within the email is a hyperlink. The link leads to a message to call a hotline which warns victims about malware infection, license expiration and system problems. Victims will then call the provided hotline number and the fraudsters will ask victims to give them remote access to their devices to supposedly fix the problem. The fraudsters offer fake solutions and ask for payment in the form of a one-time fee or subscription to a purported support service.

A genuine company or organisation will only send an order cancellation email once you have instigated cancelling an order on the retailer's website. It is fairly easy to find out if you have cancelled an order by checking your account using a new browser window and going directly to the retailer's website.

PROTECTION / PREVENTION ADVICE

- Always be aware of your online order and where you have ordered it from.
- When receiving an email that is sent by an online retailer, always check that the punctuation, grammar and the spelling of the content within the email are correct. Poor spelling and grammar can indicate that the email could be fraudulent.
- If you have received a cancellation email by a retailer, take a look at the order number and compare it to the order number when you first ordered the product, or check your account for that website.
- If you do click on an order link and a pop-up window appears, you can open your computer's Task Manager (by pressing CTRL+SHIFT+ESC), select the browser under 'Apps', and click 'End Task'. This will let you close the browser or specific tabs even when there is a pop-up or dialog message.
- Don't give your bank account details or sensitive information to anyone who contacts you via any unsolicited email or phone call.
- If you have been affected by this, or any other type of fraud, report it to Action Fraud by visiting www.actionfraud.police.uk or by calling **0300 123 2040.**

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:	105435P
Review By:	Senior Analyst