Police issue advice to protect residents from cyber criminals

Posted on 12th September 2014 Print Download

Derbyshire residents are being encouraged to further protect themselves from cyber criminals following reports of 'fake payment' phishing emails.

The National Fraud Intelligence Bureau (NFIB) has recently received a number of reports about emails containing an attachment, which once opened, may infect the computer with a virus.

The email contains information about a transaction which appears to have been sent by a legitimate company. However, the email address of this company has been 'spoofed' and has actually been sent by a fraudster.

The email is sent to the victim with information regarding a fake transaction which has recently taken place and is often complete with an order number and payment details.

The email will state that more detailed information about the purchase can be found in the attachment. Once opened, this is likely to download a virus onto the computer.

Detective Constable Julie Wheeldon from the East Midlands Fraud and Financial Investigation Unit said: "Scams such as this are designed to play on your curiosity in order to get you to open the email attachment and infect your computer with a virus.

"These emails appear highly convincing and many people fall victim to the scam as they want to find out more about the transaction.

"If you receive one of these emails, do not open or download the attachment, delete it straight away and report it to Action Fraud."

Police are advising people to follow the below steps to help to protect themselves from falling victim to phishing email scams:

- Firstly, do not open attachments or click on links within emails unless you are sure that you know who has sent them;
- Ensure that your anti-virus software is up-to-date and performing regular scans;
- If you have not recently made an order with the company specified in the email do not open the attachment;
- Always check the legitimacy of the email. The NFIB suggests finding a telephone number for the company independently from the one suggested in the email as the phone number provided may be fake, or go straight to the suspect.

For information around frauds and scams visit the dedicated Stamp out Fraud in Derbyshire webpage at www.derbyshire.police.uk/stampoutfraud.

To report a fraud call Action Fraud on 0300 123 2040 or visit the website at: www.actionfraud.police.uk.

Below is an example of the email scam:

Thank you for using out services!

Your order #1170512135 will be shipped on 27.09.2014.

Date: September, 12, 2014. 10.34am

Price: £146.51

Payment method: Credit card

Transaction number: 56000F4NA65

Please find the detailed information on your purchase in the attached file

(order_2014_09_12_14_56_37_1170512135.zip)

Best regards,

*Sales Department ******

*Tel +07*********