This is a message sent via The Neighbourhood & Home Watch Network (England & Wales).
This information has been sent on behalf of Action Fraud (National Fraud Intelligence Bureau)

(Please do not reply directly to this email, please use the Reply button at the bottom of this message)

Message sent by

Action Fraud (Action Fraud, Administrator, National)

Current spam email campaigns are trying to infiltrate or infect email accounts by pretending to come from either Adobe or LinkedIn Support. The emails from LinkedIn claim 'irregular activities have prompted a compulsory security update'. With the Adobe emails attempt to direct the user to the latest updates

Phishing is an attempt by a fraudster to steal valuable information by pretending to be a company that you know and use. It relies on people to think the message is genuine. Victims are initially sent an email that will have either a link to a website, or contain an attachment. What the fraudsters want you to do is click on the link or attachment so that they can steal valuable information from your computer, like your bank account or credit card details

Protect yourself:

- Look at who the email is addressed to – many will say "Dear user" or "Dear valued customer" and will not be addressed directly to you.
- If there are images included in the email they may be of a poor quality but will try to look like the company they are trying to represent.
- The message may have a few spelling mistakes.
- Do not click on the link supplied. Instead, go to the relevant website and log in from there.

IF YOU NEED TO REPORT A FRAUD, PLEASE CALL ACTION FRAUD ON 0300 123 2040 OR USE THE ACTION FRAUD REPORTING TOOL, VIA THE ACTION FRAUD WEBSITE - http://www.actionfraud.police.uk/. PLEASE DO NOT REPLY TO THIS EMAIL IF YOU NEED TO REPORT A FRAUD OR ANY OTHER CRIME.