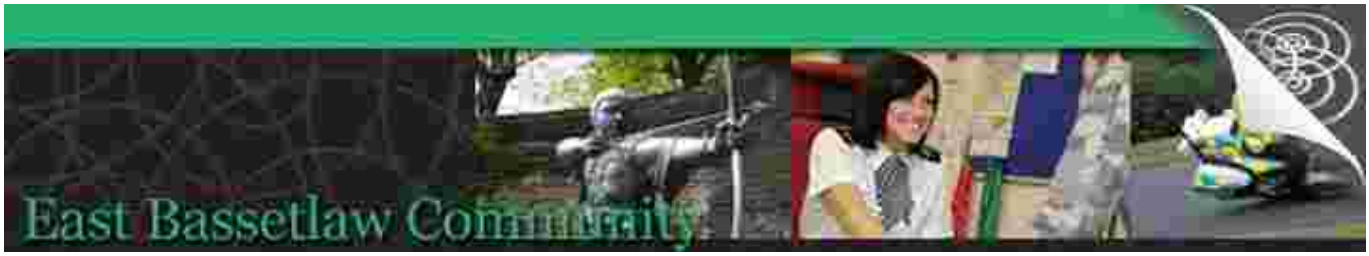

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Action Fraud is not an emergency service
dial 999 if you are in immediate danger.

Message sent by
Action Fraud (Action Fraud, Administrator, National) 26th May, 2017

Smishing – the term used for SMS phishing – is an activity which enables criminals to steal victims' money or identity, or both, as a result of a response to a text message. Smishing uses your mobile phone (either a smartphone or traditional non-internet connected handset) to manipulate innocent people into taking various actions which can lead to being defrauded.

The National Fraud Intelligence Bureau has received information that fraudsters are targeting victims via text message, purporting to be from their credit card provider, stating a transaction has been approved on their credit card.

The text message further states to confirm if the transaction is genuine by replying 'Y' for Yes or 'N' for No.

Through this method the fraudster would receive confirmation of the victim's active telephone number and would be able to engage further by asking for the victim's credit card details, CVV number (the three digits on the back of your bank card) and/or other personal information.

Protect yourself:

- Always check the validity of the text message by contacting your credit card provider through the number provided at the back of the card or on the credit card/bank statement.
- Beware of cold calls purporting to be from banks and/or credit card providers.
- If the phone call from the bank seems suspicious, hang up the phone and wait for 10 minutes before calling the bank back. Again, refer to the number at the back of the card or on the bank statement in order to contact your bank.
- If you have been a victim of fraud or cyber crime, please report it to Action Fraud at http://www.actionfraud.police.uk/ or alternatively by calling 0300 123 2040