fair telecoms campaign **open message**

Possible ‘Banking Code of Practice for outbound communications by phone and email’

On 6 April 2017 we wrote to the BBA to raise concerns about the ease with which banking customers fall victim to scams, and fail to recognise true communications.

We had hoped to enter into discussions with the BBA and its members about the possibility of introducing a “Code of Practice” or protocol that would ensure that consumers were always able to distinguish between a genuine communication and a scam.

With the increased attention now being drawn to the issue of the “Approved Push Payment” scams, it is vital that consumers can feel free to dismiss ALL unexpected approaches by telephone. At the same time however, proper communications with customers and an appropriate level of trust must be maintained.

Our message included the outline of a possible Code of Practice, as a starting point for discussion, highlighting the features which would need to be covered.

We wrote:

“

Code of Practice?

Our initial suggestion is that a Code of Practice incorporating something akin to the principles laid out below should be adopted by BBA members.

- Bank business, which is private and therefore requires secure identification of the customer as the individual responding to the call, should NEVER be carried out during a call initiated by the bank. Customers have no secure means of verifying the identity of the caller.
- A telephone call, or text message, should ONLY advise the customer of the need, or a request, for them to take specific action. This could be a request for them to contact a particular representative of the bank.

  This contact must ONLY be invited to be made by using details (a telephone number, email address or branch address) known to the customer in some way, e.g. printed on a card, statement or correspondence, or obtained from a known website or directory.
- Contact details must NEVER be given in the course of a telephone call or text message. Similarly, there should be no specific direction about where the contact details may be found, e.g. a particular website URL.

  To avoid suspicion, any CLI used for the phone call must be the most widely recognised published number for the institution, as must any sender identity on a text message.
- To ensure confidentiality in respect of the nature of the call, it may be appropriate to identify the individual or department to be contacted by means of an anonymous extension number or some form of coded reference. (e.g. It may not be appropriate to tell an unidentified person responding to the call that the customer needs to speak with the “collections department”.)

”

With this open message now re-published and circulated, we hope that it will be possible to enter into meaningful discussions about such a code being devised and implemented by BBA members.

David Hickson

Tuesday, 19 November 2019