Reaction

Brussels, 14 June 2021 – 8 a.m.

KBC reacts to media reports of phishing scams

Several media outlets today highlighted the issue of phishing fraud and explicitly referred to two specific cases in which KBC is involved. These cases are currently the subject of judicial proceedings. KBC does not wish to debate this in the media and will instead reserve its arguments for the court, which must be able to deliver an objective and reasoned verdict. For this reason, KBC cannot comment in detail on these specific proceedings, rather it can only confirm that it has lodged an appeal in both cases.

KBC wishes to clarify its policy in this area.

Cybercrime is everywhere in society

Cybercrime is a widespread phenomenon which has developed into an issue for society as a whole. Scammers no longer focus purely upon banking avenues, but rather increasingly abuse the trust placed in the recognised names of public and private institutions. This of course makes online security today a shared social responsibility. This is why there are already initiatives underway at sector level in cooperation with telecom companies, public prosecutors, police, government and judicial authorities in order to jointly tackle cybercrime in every shape and form – which does not diminish the fact that customers must also remain alert and aware of possible risks of fraud. In this regard KBC would like to indicate the many warnings published across a variety of (social) media and forums highlighting this type of fraud so that customers are made aware. KBC also publishes these kinds of messages on its website.

The law presupposes that customers must themselves respect a number of rules and maintain a healthy degree of suspicion and vigilance. Furthermore, the customer has not only the legal obligation to inform the bank should their card or other method of payment (e.g., KBC Mobile) be lost or stolen, they must do so from the moment they learn or suspect that these methods are being used unlawfully. It has already been ruled, for example, that users of payment services can no longer claim to have no knowledge of the phenomenon of 'phishing', that they must view contact from strangers regarding banking matters with suspicion, and that sharing PIN and response codes is very much an act of gross negligence.

Both PINs and response codes created with a bank card and card reader are strictly for personal use. Under no circumstances may they be passed on to third parties - let alone strangers - in any way whatsoever.

KBC Cybersecurity: 24/7 monitoring and accessibility

KBC makes every effort to ensure that transactions take place securely and that cyberfraud is prevented to the greatest extent possible. Criminals grow increasingly inventive and professional, however. As a result, KBC cannot provide any information regarding the detection and prevention methods it employs, but notes that continuous investment is made into material and human resources so that intensive monitoring can take

place around the clock. This is how KBC's preventative measures successfully protect a great many customers from fraud even if they perhaps remain unaware of the fact.

Secure4u, KBC's cybersecurity service, actively monitors all transactions 24/7 to detect fraud. It is available 24/7 to any customers who suspect that they are the victim of fraud (even on weekends and public holidays). Thanks to this extensive monitoring, KBC manages to proactively stop a large proportion of suspicious transactions and alert customers. It was possible to stop or recover 75% of fraudulent transfers in 2020 (Febelfin figures), and this percentage also applies to KBC.

What if the customer has fallen victim to phishing?

In many cases where the customer is liable, the bank still manages to recover the funds and pay them back to the customer, but this is separate from any liability. Many such cases are rarely reported in the media if at all, which sometimes creates the false perception that banks only repay in exceptional circumstances. In practice, this is not the case.

KBC always examines complaints relating to (digital) fraud on the basis of the objectively established facts. How was the customer misled? What actions did the customer take or fail to take? Could the customer have noticed something was going on at certain points in the fraud process? Did the customer make payments to a fraudster themselves, or did a fraudster gain access to their online banking service? The facts are always analysed on case-by-case basis before any decision is made.

For context and completeness, a few legal considerations:

The relevant legislation (Article VII.38 WER) stipulates that the 'payment service user' should take all reasonable measures to ensure the security of their payment method and their personal security details. In addition, the customer has a duty to inform the Bank not only in the event of loss or theft of their card or other payment method (e.g., KBC Mobile) but also to do so as soon as they know or reasonably suspect that such instruments are being used unlawfully.
Failure to comply with these security provisions constitutes, where applicable and considering the specific circumstances of the case, gross negligence on the part of the customer within the meaning of Article VII.44 WER. The payer shall therefore bear all losses relating to unauthorised payment transactions if they have incurred them by acting fraudulently or – whether intentionally or through gross negligence – by failing to fulfil one or more of the obligations set out in Article VII.38.
The court will therefore assess the facts of a phishing case concretely in light of the law. In doing so, the court will also judge the payment service user's behaviour against the assumed behaviour of a normal, careful payer – and this in the same concrete circumstances.

KBC Group NV
Havenlaan 2 – 1080 Brussels
Viviane Huybrecht
General Manager
Corporate Communication /Spokesperson
Tel. + 32 2 429 85 45

Press Office
Tel. + 32 2 429 65 01 Stef Leunens
Tel. + 32 2 429 29 15 Ilse De Muyer
Tel. + 32 2 429 32 88 Pieter Kussé
Tel. + 32 2 429 85 44 Sofie Spiessens
E-mail: pressofficekbc@kbc.be

KBC press releases are available at www.kbc.com or can be obtained by sending an e-mail to pressofficekbc@kbc.be

Follow us on www.twitter.com/kbc_group
Stay up-to-date on all innovative solutions