Réaction

Bruxelles, 14 juin 2021 – 08.00 heures

KBC réagit aux comptes-rendus des médias sur la fraude par hameçonnage (phishing)

Plusieurs médias se sont penchés aujourd'hui sur la fraude par hameçonnage (phishing) et ont fait référence à deux cas spécifiques liés à KBC. Ces dossiers font actuellement l'objet de procédures judiciaires. KBC ne souhaite pas mener de débats par voie de presse. Elle réserve ses arguments au tribunal, qui doit pouvoir statuer de manière objective et sereine. Par conséquent, KBC ne peut pas commenter en détail ces cas spécifiques. Elle peut seulement confirmer qu'elle a fait appel dans ces deux affaires.

KBC souhaite ici clarifier sa politique en matière de cybersécurité.

La cybercriminalité est omniprésente

La cybercriminalité connaît une croissance exponentielle et est devenue un véritable problème de société. Les fraudeurs ne se concentrent plus uniquement sur les canaux bancaires, mais abusent de plus en plus des marques de référence des entreprises et des services publics. La cybersécurité est aujourd'hui une responsabilité sociétale partagée. Des initiatives sont en cours au niveau sectoriel - en collaboration avec les opérateurs de télécommunications, le Parquet, la police, les pouvoirs publics et la justice, afin de lutter conjointement contre la cybercriminalité dans toutes ses dimensions et manifestations – mais les clients doivent eux-mêmes rester vigilants et conscients des risques potentiels de fraude. KBC renvoie à cet égard aux nombreuses actions de conscientisation de la clientèle relayées par différents médias (sociaux) et forums. KBC publie également des avertissements sur son site web.

La législation part du principe que les clients doivent eux aussi respecter un certain nombre de mesures et faire preuve d'une saine méfiance et d'une attention de tous les instants. En outre, le client a l'obligation légale d'informer la banque non seulement en cas de perte ou de vol de sa carte ou d'un autre instrument de paiement (p.ex. KBC Mobile), mais également dès qu'il sait ou soupçonne que ces instruments sont utilisés de manière illicite. Le tribunal a déjà estimé qu'un utilisateur de services de paiement ne peut plus prétendre ne pas connaître le phénomène du "phishing", qu'il doit se méfier lorsqu'il est contacté par des inconnus au sujet de ses affaires bancaires, et que la communication de codes constitue une négligence grave.

Les codes PIN, mais aussi les codes de réponse créés avec une carte bancaire et un lecteur de carte sont strictement personnels. Ils ne peuvent en aucun cas être transmis à des tiers - et encore moins à des étrangers - de quelque manière que ce soit.

KBC Cybersecurity : surveillance et accessibilité 24/7

KBC met tout en œuvre pour assurer le bon déroulement des transactions et pour prévenir autant que possible la cyberfraude. Etant donné que les criminels sont de plus en plus inventifs et qu'ils ont tendance à se professionnaliser, KBC ne souhaite pas divulguer d'informations sur les mécanismes de détection et de prévention qu'elle utilise, mais confirme qu'elle investit constamment dans des personnes et des moyens afin

d'assurer une surveillance intensive 24 heures sur 24. KBC parvient ainsi à protéger de nombreux clients contre la fraude, même s'ils n'en sont pas toujours conscients.

Secure4u, le service de cybersécurité de KBC, surveille activement toutes les transactions 24 heures sur 24 et 7 jours sur 7 afin de détecter les fraudes. Il est toujours accessible (y compris le week-end et les jours fériés) aux clients qui pensent être victimes d'une fraude. Grâce à cette surveillance poussée, KBC parvient à bloquer de manière proactive une grande partie des transactions suspectes et à alerter le client. 75% des virements frauduleux (chiffres Febelfin) ont pu être stoppés ou récupérés en 2020, un pourcentage qui s'applique également à KBC.

Et si le client est tout de même victime de phishing ?

Même dans les cas où le client est responsable, la banque parvient souvent à récupérer les avoirs et à les reverser au client, mais sans que cette démarche n'engage d'aucune façon sa responsabilité. Ces nombreux cas ne sont généralement pas rapportés par les médias, ce qui peut donner l'impression que les banques ne remboursent qu'à titre exceptionnel, ce qui ne correspond pas à la réalité.

KBC examine les plaintes pour fraude (digitale) sur la base de faits objectivement établis. Comment le client a-t-il été trompé? Quelles sont les mesures que le client a prises ou n'a pas prises? Le client aurait-il pu remarquer quelque chose de suspect au cours du processus de fraude? Le client a-t-il lui-même effectué des paiements à un fraudeur ou un fraudeur a-t-il eu accès à son application bancaire? Chaque cas est analysé individuellement sur la base des faits avant qu'une décision ne soit prise.

Pour des raisons de contexte et d'exhaustivité, vous trouverez ci-après quelques considérations juridiques:

La législation (article VII.38 du CDE) prévoit que l'"utilisateur de services de paiement" doit prendre les mesures raisonnables afin de préserver la sécurité de l'instrument de paiement et de ses données de sécurité personnalisées. Par ailleurs, le client a le devoir d'informer la banque non seulement en cas de perte ou de vol de sa carte ou d'un autre instrument de paiement (p.ex. KBC Mobile) mais également dès qu'il sait ou soupçonne raisonnablement que ces instruments sont utilisés de manière illicite.
Le non-respect de ces dispositions de sécurité constitue, le cas échéant et compte tenu des circonstances particulières du cas, une négligence grave de la part du client au sens de l'article VII.44 du CDE. Le payeur supporte par conséquent toutes les pertes liées à des opérations de paiement non autorisées s'il les a subies en agissant frauduleusement ou - que ce soit intentionnellement ou par négligence grave - en ne remplissant pas une ou plusieurs des obligations énoncées à l'article VII. 38.
Le juge considérera les faits d'une affaire de phishing à la lumière de la législation. Ce faisant, il appréciera le comportement de l'utilisateur des services de paiement par rapport au critère du comportement supposé d'un payeur normal et prudent - et ce dans les mêmes circonstances concrètes.

KBC Groupe SA
Avenue du Port 2 – 1080 Bruxelles
Viviane Huybrecht
Directeur Communication Corporate/ Porte-parole
Tél. 02 429 85 45

Service presse
Tél. 02 429 65 01 Stef Leunens
Tél. 02 429 29 15 Ilse De Muyer
Tél. 02 429 32 88 Pieter Kussé
Tél. 02 429 85 44 Sofie Spiessens
E-mail : pressofficekbc@kbc.be