BNP PARIBAS

ASSEMBLEE GENERALE

19 mai 2020

QUESTION ECRITE POSEE PAR MONSIEUR PHILIPPE FERRAS

Question :

J'ai compris que le piratage informatique des comptes des clients de la BNP a fortement cru ces derniers temps, ma question s'adresse aussi bien aux gestionnaires de la BNP-France qu'aux experts comptables et commissaires aux comptes qui certifient la sincérité des comptes qui nous sont présentés.
Je voudrais avoir les renseignements chiffrés suivants en m'attachant uniquement aux comptes de particuliers en France :

- ***Combien (en nombre et en montant global) de comptes courants (hors piratage de cartes de crédit) ont fait l'objet de piratage en 2018, 2019 et ces 3 premiers mois de 2020 ;***
- ***La BNP est-elle inquiète de ce phénomène qui met gravement en question la sécurité de ses services informatiques ?***
- ***Combien de comptes piratés ont été rétablis par la banque sur simple constatation du client que son compte avait été indument débité (nombre et valeur) ;***
- ***Combien ont été rétablis après intervention du Médiateur (nombre et montant) en 2018 et 2019 ;***
- ***Combien sont aujourd'hui en discussion entre le client et la banque ;***
- ***Combien sont actuellement à l'examen du médiateur (nombre et montant) ;***
- ***Combien de dossiers judiciaires ont été conclus en donnant raison au client et combien à la banque en 2018, en 2019 et ces derniers temps ;***
- ***Combien sont aujourd'hui en phase judiciaire (nombre et valeur) ;***
- ***Combien a été provisionné par la banque pour ce type de risques en 2018 et combien a été consommé ; même question pour 2019 ;***
- ***Quelles investigations spécifiques ont été menées par les auditeurs et commissaires aux comptes sur ces différents chiffres et sur ces différentes fraudes.***

Réponse du Conseil d'administration :

BNP Paribas met tout en œuvre pour assurer le meilleur niveau de sécurité des moyens de paiement et outils digitaux liés. Pour cela, nous nous appuyons sur un dispositif de gestion du risque opérationnel robuste (contrôles, outils de détection, audits indépendants,…) et une équipe d'experts en sécurité et de lutte contre la fraude digitale.

L'accès à l'espace sécurisé en ligne de nos clients ainsi que la réalisation des opérations nécessitent une authentification forte (clé digitale, sms) conformément à la réglementation.

En 2019, nous avons constaté une forte intensification des campagnes de phishing dans tous les secteurs, dont bancaires.

Cette typologie de fraude consiste à générer une campagne massive de mails aux clients usurpant l'identité des Banques. Ce mail contient un lien dirigé vers un site simulant celui de la Banque. Le parcours du client sur ce site illégitime va permettre au fraudeur de collecter des informations clients (identifiant, mot de passe, etc….) puis de détourner des fonds après s'être connecté à l'espace sécurisé du client. Les fraudeurs sont particulièrement inventifs pour tromper la vigilance des utilisateurs à des fins malveillantes.

Le préjudice déploré découle bien des manœuvres d'un tiers et non d'une défaillance des applications et des outils mis à disposition par BNP Paribas. Dans le cadre de nos relations clientèle, nous étudions bien entendu chaque cas de fraude pour apporter systématiquement une réponse personnalisée.

Par ailleurs, pour les cas les plus complexes, le Médiateur peut également intervenir.

Face à ces menaces croissantes et afin de protéger nos clients, BNP Paribas adapte en permanence son dispositif.

Ainsi des mesures concrètes ont été prises pour renforcer la sécurisation des opérations et sensibiliser les clients à ce type de fraude :

- Bandeaux d'alertes sur le site MaBanque et l'application MesComptes (depuis mai 2019),
- Envoi d'un mail de confirmation d'ajout de bénéficiaire demandant au client de vérifier s'il est bien à l'origine de l'opération (depuis juin 2019),
- Plusieurs campagnes de mails de sensibilisation anti-Phishing à destination des clients (septembre, novembre 2019),
- Campagnes de sensibilisation sur les réseaux sociaux (octobre 2019),
- Insertion de messages d'alertes afin d'améliorer le niveau de vigilance des clients lors des opérations d'ajout ou de modification de bénéficiaires, par clé digitale ou SMS (depuis novembre 2019),
- Poursuite de la suppression des sites de phishing (62 000 en 2019 après 17 300 en 2018).

Pour rappel, voici les conseils que nous pouvons donner à nos clients :

- Ne jamais cliquer sur des liens contenus dans des emails qui semblent suspects, ne pas ouvrir les pièces jointes et supprimer ces emails sans y répondre. BNP Paribas n'enverra jamais à ses clients de lien direct vers une page leur demandant de saisir leurs identifiants et code secret ;
- Ne jamais communiquer par téléphone ou par email des données confidentielles ou un code. BNP Paribas ne demandera jamais à ses clients de transmettre leurs identifiants, numéros de téléphone, mot de passe ;
- Accéder uniquement aux comptes via le site ou l'application BNP Paribas et s'identifier avec le bouton « Accéder à mes comptes » situé en haut à droite. Privilégier l'usage d'un favori enregistré dans le navigateur pour se connecter à son espace sécurisé ;
- Contrôler l'url du site : les pirates changent en général le domaine internet de premier niveau (« .net » au lieu de « .com » par exemple) et reproduisent le site tel quel. Noter que le domaine internet de BNP Paribas utilise l'extension « .bnpparibas » et non « .com » ou « .net » ;
- Ne jamais valider une opération initiée par un tiers ;
- Protéger son matériel informatique des malwares qu'il s'agisse d'ordinateur ou de smartphone. BNP Paribas donne tous les conseils nécessaires à la protection de ces matériels sur le site mabanque (https://mabanque.bnpparibas/), onglet « conseils sécurité et bonne pratique ».