



Question écrite de la députée Kattrin JADIN
À Madame Eva DE BLEEKER, Secrétaire d'Etat à la Protection des
consommateurs
concernant la lutte contre le smishing
- Bruxelles, le 2 décembre 2020 -

Madame la Secrétaire d'Etat,

Les fraudes bancaires par SMS, alias le smishing, sont en forte hausse depuis quelques mois. Cette fraude visant à extorquer de l'argent sur les comptes bancaires via des SMS ou des e-mails touche surtout les personnes n'étant pas habituées du digital qui tombe plus facilement dans ce piège.

Les victimes ne sont que rarement remboursées par leurs banques et la procédure est particulièrement longue car la règle des cas par cas est appliquée. Afin de protéger les consommateurs contre ce genre d'arnaque, il faut absolument trouver des solutions.

Madame la Secrétaire d'Etat, mes questions à ce sujet sont les suivantes :

- Quelles mesures seront envisagées pour lutter contre les fraudes bancaires par SMS ?
- En attendant, quels sont les possibilités pour se protéger à l'heure actuelle contre le smishing ? Quid des victimes ?

Je vous remercie, Madame la Secrétaire d'Etat, pour les réponses que vous voudrez bien m'apporter.

Kattrin JADIN

Réponse de la ministre :

La sensibilisation et la prévention sont essentielles dans la lutte contre le smishing. Différentes autorités publiques sont actives en la matière, telles que le Centre pour la cybersécurité Belgique, via son site safeonweb.be, et le SPF Économie.

Le SPF Économie met en garde contre le smishing via son site web et les réseaux sociaux.

Le SPF Économie aide également à diffuser les campagnes de sensibilisation et lance aussi ses propres campagnes. La campagne « Évitez les pièges » a ainsi été lancée le 11 septembre 2020. Son objectif est de sensibiliser la population à trois formes très fréquentes de fraude en ligne, y compris le smishing.

Nous allons poursuivre ces efforts et également prévoir une communication commune avec Febelfin au printemps.

Le meilleur conseil pour se protéger est de ne pas cliquer et de ne pas réagir au message.

Il est conseillé aux victimes de smishing de déposer un signalement sur le Point de contact. Si elles ont communiqué des données bancaires, il leur est recommandé d'appeler Card Stop et de prendre contact avec leur banque ou société de carte de crédit.

Si elles ont perdu de l'argent, il est également indiqué de faire une déclaration auprès de leur zone de police locale. Les faux messages, y compris les faux SMS, peuvent être transmis à suspect@safeonweb.be.

Dans le cas du smishing, la législation prévoit en fait depuis le 9 août 2018 deux cas dans lesquels la banque doit assumer la perte financière. Dans le premier cas, il s'agit des clients qui n'ont pas pu constater le paiement frauduleux avant qu'il n'ait lieu. La banque est ici obligée d'indemniser les pertes financières du client à condition que celui-ci ait respecté les conditions d'utilisation de la banque. Il doit signaler sans délai la perte, le vol ou l'utilisation abusive à la banque.

Le second cas concerne les clients qui ont effectivement pu constater l'utilisation abusive de l'instrument de paiement avant qu'un paiement n'ait lieu. S'il n'est pas question de négligence grave dans le chef du client, la banque doit assumer la perte financière, après déduction d'une franchise de 50 euros.

Les personnes ayant des réclamations concernant le remboursement par leur banque peuvent s'adresser à l'Ombudsman en conflits financiers.