Question écrite de la Députée Kattrin JADIN
à Monsieur Mathieu MICHEL, Secrétaire d'État
chargé de la Digitalisation et de la Protection de la vie privée
concernant le phénomène d'hameçonnage
- Bruxelles, le 23 mars 2022 -

Monsieur le Secrétaire d'État,

Récemment, trois hommes ont été jugés devant le tribunal correctionnel de Liège d'une affaire de fraude aux SMS. Les sommes extorquées sont colossales, près de 2 millions d'euros. Cette technique de fraude est en extension au sein de notre pays, et ce, malgré les différentes campagnes menées.
Les techniques sont multiples, SMS, appels, mails, liens, … de quoi perdre les victimes.

Monsieur le Secrétaire d'État, mes questions à ce sujet sont les suivantes :

- L'hameçonnage est un phénomène grandissant qui touche toutes catégories de personnes, comment nous positionnons-nous actuellement ?
- Ne serait-t-il pas opportun de se pencher d'avantage sur les problèmes inhérents à la protection des données personnelles ?
- Combien de plaintes en la matière ont-elles été déposées ces 5 dernières années ?

Je vous remercie, Monsieur le Secrétaire d'État, pour les réponses que vous voudrez bien m'apporter.

Kattrin JADIN

Réponse du Secrétaire d'État :

1. Nous sommes tous les acteurs de notre sécurité numérique. Aujourd'hui, le champ d'action de ceux qui volent des données, va de la vulnérabilité humaine à des mesures technologiques de pointe. Nous devons ensemble tout mettre en œuvre pour enrayer ce phénomène et cela passe essentiellement par de la sensibilisation et de l'information.

   L'hameçonnage, ou phishing est une forme d'escroquerie qui se manifeste sous différentes formes : par e-mail, par sms ou même par téléphone. Ce phénomène est répandu dans le monde entier. Il n'y a aucune raison de supposer que nous, en Belgique, sommes plus souvent visés.

   Bien que la vigilance des citoyens porte de plus en plus ses fruits, le phishing continue de faire de nombreuses victimes. En 2020, la police fédérale a constaté une augmentation de 204 % du nombre de victimes de phishing par rapport à 2019, avec un total de 7502 signalements. En 2020, les cybercriminels ont effectué 67 000 transactions frauduleuses, pour un montant net total de 34 millions d'euros. En outre, il s'avère que 12 % des Belges n'ont jamais entendu parler du phishing. Chez les jeunes, ce pourcentage atteint même les 30 % (Febelfin, 2021).

2. En sensibilisant le public, on assure une meilleure protection des données personnelles. La stratégie de lutte contre les malwares repose en effet principalement sur la sensibilisation des utilisateurs.

   Plusieurs mesures préventives peuvent être ainsi prises pour éviter la propagation des malwares et assurer ainsi une protection des données :

   a. ne pas télécharger d'applications mobiles dont le développeur n'est pas clairement identifié,
   b. ne jamais télécharger une application via un hyperlien reçu via un SMS suspect,
   c. s'assurer que les autorisations qu'une application demande sur l'appareil sont conformes à l'objectif de l'application,
   d. ne jamais diminuer la sécurité de son appareil à la demande d'une application, et
   e. s'assurer que toutes les applications et logiciels d'un appareil sont mis à jour avec les derniers patchs de sécurité.
   f. installer un bon anti-malware à jour et activer la protection en temps réel.
   g. Si un utilisateur est infecté par ce malware, désactiver les applications qui ont des privilèges de gestion, puis désinstaller ces applications en mode « sans échec »(safeboot) et réinitialiser son appareil aux paramètres d'usine.

3. Le CCB a créé une adresse mail vers laquelle le citoyen peut envoyer des messages suspects, qu'il s'agisse d'e-mails ou de SMS : suspect@safeonweb.be (verdacht@safeonweb.be ; suspekt@safeonweb.be, suspicious@safeonweb.be) Via ces adresses mails, il est possible de faire bloquer les liens suspects dans ces messages.

   En 2021, le CCB a reçu 4,5 millions de messages suspects provenant d'alertes de citoyens (soit en moyenne plus de 12 000 messages par jour). Il a ainsi été en mesure de notifier plus de 1,4 millions de sites Internet frauduleux à Google et à Microsoft, qui les ont bloqués. En 2020, les chiffres étaient encore de 3,2millions de messages reçus par le CCB et 667.000 sites bloqués.

   De même, le CCB envoie en moyenne 25 000 redirections par jour vers une page sécurisée après des clics par des utilisateurs belges sur des liens malicieux. Si une personne vient à cliquer sur le lien malicieux, elle recevra un message d'alerte clair lui signalant de ne pas surfer sur cette page. De cette manière, chacun peut contribuer à un environnement numérique sécurisé.