



14ème législature

Question N° : 20908	De Mme Sandrine Doucet (Socialiste, républicain et citoyen - Gironde)	Question écrite
Ministère interrogé > PME, innovation et économie numérique		Ministère attributaire > Économie et finances
Rubrique > télécommunications	Tête d'analyse > Internet	Analyse > données personnelles. identifiants. campagne d'information.
Question publiée au JO le : 12/03/2013 Réponse publiée au JO le : 20/09/2016 page : 8407 Date de changement d'attribution : 31/08/2016 Date de signalement : 12/07/2016		

Texte de la question

Mme Sandrine Doucet attire l'attention de Mme la ministre déléguée auprès du ministre du redressement productif, chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, sur la question de la vulnérabilité des mots de passe sur internet. À la suite d'une étude réalisée par un cabinet de conseil, il y a quelques semaines, il serait avéré que 90 % des mots de passe enregistrés sur Internet pourraient être piratés. Les utilisateurs choisiraient, en effet, des identifiants trop courts ou trop simples, ce qui faciliterait les fraudes. En outre, de nombreux usagers d'internet disposeraient du même mot de passe sur plusieurs sites, que ce soit des réseaux sociaux, des sites marchands, voire leurs sites bancaires. Les risques encourus peuvent, ainsi, être très importants, allant du vol d'identité à la véritable fraude à la transaction sur des sites pouvant gérer des coordonnées bancaires. Tant les particuliers que les entreprises sont ainsi confrontés à ces nuisances, lorsque le manque d'efficacité de leur mot de passe n'est découvert que trop tard. Il semble, cependant, que les internautes ne soient pas assez alertés sur ces dangers et sur la manière dont ils pourraient diminuer les failles de sécurité rencontrées sur Internet. Elle souhaite donc savoir comment le ministère entend informer les consommateurs sur ces risques, afin que soient évités des accidents et que soient mieux protégées les données personnelles des usagers. Elle la remercie et la prie de bien vouloir la tenir informée des suites données à ce dossier.

Texte de la réponse

Il existe de nombreuses manières de s'authentifier auprès d'un service en ligne (mots de passe, cartes à puce, élément – token – sécurisé, etc.). Parmi celles-ci, la technique d'authentification par mot de passe souffre d'un certain nombre de faiblesses intrinsèques : « rejouabilité » aisée en cas de captation, facilité de transmission à des tiers, capacité pour les attaquants de deviner les mots de passe s'ils ne sont pas suffisamment robustes, etc. Le choix du mot de passe robuste et un niveau accru de vigilance au moment de son utilisation sont notamment très importants pour limiter les risques. Afin de sensibiliser nos concitoyens et nos entreprises et leur permettre de se poser les bonnes questions en matière de sécurité du numérique, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié de nombreuses recommandations adaptées à chaque public. On peut notamment citer : - un document dédié aux bonnes pratiques liées au choix et à l'utilisation des mots de passe : <http://www.ssi.gouv.fr/guide/mot-de-passe/> ; - un ensemble de documents et de recommandations à destination des citoyens : <http://www.ssi.gouv.fr/particulier/precautions-elementaires/> ; - un guide de bonnes pratiques à destination des PME : <http://www.ssi.gouv.fr/particulier/guide/guide-des-bonnes-pratiques-de-linformatique/> ; - le



guide « d'hygiène informatique » à destination de l'ensemble des entreprises : <http://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/>. Il importe que chacun, dans ses échanges au quotidien avec les citoyens et les entreprises, diffuse ces recommandations afin qu'elles puissent rapidement faire l'objet d'une large appropriation. L'adoption du règlement européen no 910/2014 relatif à « l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur », le règlement dit « eIDAS » favorisera par ailleurs l'harmonisation au niveau européen de ces pratiques. Comme l'indique la Stratégie nationale pour la sécurité du numérique présentée par le Premier ministre en septembre dernier, la France favorisera le renforcement des niveaux d'authentification sur les services en ligne. Enfin, le dispositif national d'assistance aux victimes d'actes de cybermalveillance, annoncé par la Stratégie nationale pour la sécurité du numérique, offrira dès le premier trimestre 2017 une plateforme numérique qui reprendra à destination des particuliers, des collectivités territoriales et des entreprises, les bonnes pratiques concernant les mots de passe.