Génération Z et cyber sécurité

Leur rapport au numérique et aux données de santé à caractère personnel

APSSIS
Association pour la Promotion de la Sécurité des Systèmes d'Information de Santé

TREND MICRO™

INTERNET SAFETY KIDS by Trend Micro

NE VOUS POSEZ PLUS DE QUESTION QUANT À LEUR SÉCURITÉ

Les jeunes nés en même temps qu'Internet, appelés « Génération Z », sont 16 millions en France.
Le web est pour eux synonyme d'immédiateté, et de gratuité.
Ils partagent tout, trop peut-être.

Pour aider les jeunes et leurs parents, Trend Micro place son expertise au service des établissements scolaires en développant le programme « Internet Safety Kids ».
L'objectif : organiser des journées de sensibilisation sur les dangers d'Internet.

SWK • www.srwk-communication.fr

Pour en savoir plus :
www.trendmicro.fr/protegezvosenfants

INTERNET safety NIGHT

Préface

La tête dans le cyber, mais les pieds bien sur terre !

Je n'ai rien à cacher ! Pourquoi ? Parce que je n'ai rien fait de mal.

La génération Z née avec le cyberespace, qui a grandi un smartphone à la main et qui évolue, dans un monde devenu familier, au milieu des données numériques omniprésentes et des objets connectés bavards, imagine que ceux qui cachent des secrets sont ceux qui ont des choses à se reprocher. Elle n'est le plus souvent pas consciente que c'est précisément parce qu'on a des choses à cacher qu'on est un être humain, un citoyen, et pas un simple numéro, et que les informations qu'il convient justement de ne pas rendre publiques sont principalement celles sur soi-même.

Cacher ce que l'on fait est une chose parfois nécessaire, ne serait-ce que pour atteindre des objectifs qui nécessitent une certaine confidentialité tant que les buts fixés n'ont pas été atteints. Cette génération Z, face aux affaires d'espionnage si médiatisées, face aux harcèlements subis par des camarades, peut le comprendre facilement. Mais cacher ce que l'on est, ses paramètres biologiques, son état de santé, ses caractéristiques physiques qui sont non conformes à disons ce qu'on pourrait appeler un être humain nominal, ou plus généralement cacher « soi-même », pourquoi le ferait-on dans un monde où les complexes ont pour remède le partage d'informations avec le plus grand nombre pour discuter via les réseaux sociaux avec d'autres camarades qui ont peut-être les mêmes problèmes ou les mêmes avantages ?

Oui mais les jeunes oublient que les années passant, ce qu'ils ont révélé aujourd'hui persistera dans le cyberespace quand ils seront moins jeunes. Sont-ils conscients que sur l'Internet, ils ne peuvent compter ni sur le droit à l'oubli, ni sur le droit à l'anonymat, même s'ils pensent que des solutions techniques existent, même s'ils pensent que les lois apportent une protection sur leurs données à caractère personnel. Sont-ils conscients que l'Internet est une agora où tout s'entend, où tout se voit, où tout se retient, où les informations émises peuvent être utilisées contre l'émetteur ? Sont-ils conscients ces jeunes, que les discussions uniquement entre amis ne restent « entre amis » que si une attaque sur cette information ne rend pas inopérante la protection par mots de passe et autres moyens d'authentification, transformant dès lors les conversations privées en révélations publiques, desquelles beaucoup d'individus malveillants seront friands d'en prendre connaissance ?

Mais qui pourrait tirer parti d'une petite information sans importance, même si on regrette de l'avoir émise, noyée qu'elle est dans la masse gigantesque de données produites sur la toile à chaque seconde ? Là encore les jeunes se trompent. Toute information quel que soit son format, même si c'est ce qu'on appelle un signal faible, corrélée avec d'autres informations sur soi ou sur d'autres, peut conduire à des conclusions compromettantes et qui perdureront longtemps après. Les capacités de stockage combinées à la puissance de calcul et aux technologies du Big Data peuvent tirer parti d'informations anodines, mais corrélées à d'autres et sorties de leur contexte initial.

Alors que faire ? Conseiller aux jeunes de ne plus utiliser leurs PC, leurs smartphones, leurs tablettes, leurs montres connectées et autres moyens d'entrée dans l'Internet des objets ? Ce n'est plus possible, et certainement pas souhaitable, car les avantages apportés par un accès facile et immédiat à l'Information sont immenses et le numérique est devenu incontournable. Tout objet non connecté deviendra bientôt aussi bizarre que l'est aujourd'hui un téléphone noir en ébonite, une règle à calcul ou une 2CV Citroën.
Il convient d'éduquer les jeunes pour les aider à prendre conscience des dangers du cyberespace. Celui-ci doit rester ce pour quoi il a été conçu par les pionniers qui ont établi ses bases dans les années 60 : un espace de liberté, la disponibilité immédiate de données numériques qui peuvent être utiles et même indispensables si on garde un regard critique sur les informations trouvées. Tout ce qui est écrit n'est pas vérité, toute affirmation est contestable et on doit prendre de la hauteur.

Quant aux informations émises, en particulier sur ses données de santé, il faut bien faire attention de ne révéler que ce qui est nécessaire, en considérant qu'une donnée, une fois émise, ne pourra être effacée facilement de la toile et qu'elle pourra être utilisée dans un contexte autre que celui qui aura été prévu.

Gérard Péliks,
Expert en sécurité

Gérard Peliks préside l'atelier sécurité de l'association Forum ATENA, dans lequel il organise de grands évènements autour de sujets comme la cybersécurité, le futur de l'Internet et la cyberstratégie. Il coordonne l'écriture de livres collectifs sur la sécurité de l'information. Il est membre du conseil d'administration de l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information), membre de la réserve citoyenne de cyberdéfense de la gendarmerie nationale, et anime les « Lundi de l'IE » du Cercle d'Intelligence Economique du Medef Ile-de-France. Gérard Peliks est chargé de cours sur différentes facettes de la sécurité, dans le cadre de Mastères de l'Institut Mines -Télécom et du Pôle Léonard de Vinci.

Sommaire

Introduction

Confidentialité des données : le deal

Le service proposé, si possible gratuit, contre mes données personnelles.

Avec trois adolescents à la maison, le sujet du numérique prend souvent sa part dans les échanges familiaux. Chez nous, le choix de la liberté numérique a été acté depuis longtemps. Chacun dispose d'un PC librement connecté à Internet, d'un smartphone, de comptes Facebook, Twitter, Instagram et Snapchat, entre autres. Des applications de quantified-self accompagnent les activités sportives et parfois les phases de « régime alimentaire ». En contrepartie de cette liberté, ce sont les principes d'échanges, de pédagogie et de communication qui régulent les usages. Notre métier dans les technologies numériques nous permet de disposer d'un argumentaire solide et d'offrir à nos ados la cartographie des risques de la toile.

C'est lors des séquences d'échanges que j'ai rapidement fait le constat d'une certaine légèreté relative aux données produites sur Internet, qu'il s'agisse de photos, de vidéos, de textes ou de rapides commentaires. Ce que je croyais être un déficit de conscience n'est en réalité qu'un deal assumé entre un service proposé et son alimentation en données diverses. A la question : et si l'usage des objets connectés de santé et applications associées permettait aux compagnies d'assurances et aux mutuelles d'appliquer un bonus / malus tarifaire en fonction des données de comportement récoltées via les applications « sportives » ou « nutritives » ? La réponse est directe : quoi de plus normal. Si je prends soin de moi, il est logique que je contribue de façon minorée au système de soins, versus un assuré qui se laisse aller. Dont acte. Les assureurs qui se lancent dans cette voie auront donc des clients dociles. A la question : quid des données déposées durant des années sur les réseaux sociaux et autres plates-formes et qui constitueront, dans un futur proche, un « CV numérique » détaillé ? La réponse est à nouveau claire : à chacun de faire attention aux traces laissées, « il y aura une appli pour ça » et enfin, cette notion de transparence assumée. Après tout, chaque individu aura un passé ou « passif » sur le Web, et les comportements de l'adolescence, sauf excès manifeste, n'auront que peu d'impact sur l'entrée dans la vie professionnelle. Ces débats sont sans fin et la façon de penser de la nouvelle génération, baignée dans le numérique, transforme notre rapport assez traditionnel et conservateur, à la notion d'intimité, celle-ci devenant relative.

En mai 2015, souhaitant aller plus loin et étendre la discussion à un panel plus important d'adolescents, j'ai demandé au Lycée Robert Garnier de la Ferté-Bernard de m'accueillir, proposant de délivrer huit séquences de sensibilisation à la cybersécurité. En contrepartie, les étudiants ont accepté de répondre à un questionnaire de seize items, devant permettre de mesurer leur sensibilité à la confidentialité des données personnelles en général et de leurs données de santé en particulier. Je tiens à remercier le Lycée Robert Garnier, ses élèves, ses enseignants et son Proviseur adjoint, Monsieur Jean-Clovis POUNGUI, pour la qualité de leur accueil et de leur intérêt pour cette initiative de l'APSSIS.

C'est le résultat de ce projet qui est proposé dans ce document. Une fois les données recueillies traitées et mises en forme, nous avons demandé à des experts d'en prendre connaissance et de proposer leur analyse des résultats. Qu'ils soient remerciés de leur disponibilité.

L'APSSIS inscrit son action dans le processus d'acculturation de notre jeunesse, d'ores et déjà usagers d'un système de santé en pleine mutation technologique. Les conclusions de cette étude doivent nourrir notre réflexion et apporter quelques paramètres issus du réel à la conception traditionnelle que nous avons de la confidentialité. Il semble que le deal sera simple : la mise à disposition des données est par principe acquise, en fonction du bénéfice qu'apportera l'application collectrice. Nous serons tracés, géolocalisés et nos données intimes seront agrégées par des plates-formes privées, mais nous serons d'accord, car le retour sur investissement nous sera favorable. Il est également certain que la nouvelle génération prendra conscience de la valeur de ses données personnelles et décidera de les monnayer... Après tout, si la matière ce sont les données, ne serait-il pas légitime de rémunérer leur production ?

Vincent TRELY
Président de l'APSSIS

Méthodologie

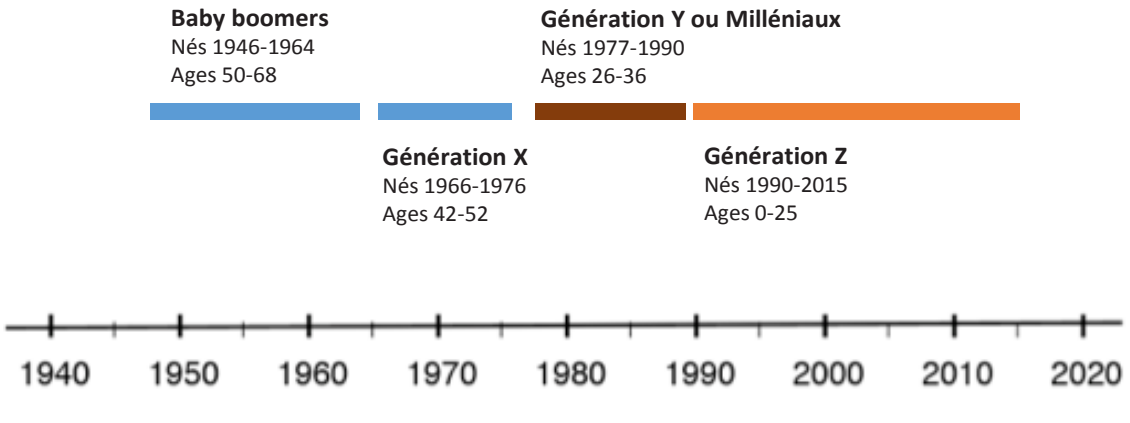
L'étude a été réalisée par l'APSSIS sur la base d'un questionnaire en 16 points auprès de 204 jeunes (107 filles et 97 garçons) scolarisés en classe de Seconde au Lycée public de La Ferté Bernard (Sarthe) le 2 juin 2015.

Voir Questionnaire brut en annexe.

Génération Z : qui sont-ils ?

Ils sont nés après 1990 et ont moins de 20 ans. Ils sont nés connectés et mobiles. La Génération Z représente 16 millions d'individus en France. Cette génération « selfie » ne rime pas avec « selfish », bien au contraire, mais avec « réseau ». Le digital pour eux, c'est le partage, une culture de l'immédiateté, de l'accessibilité et de la gratuité.

Pour cette jeune génération, les applications et le web sont des outils. Ils ont toujours vécu au milieu des appareils connectés. L'évolution est dans leur usage : de Facebook à Snapchat en passant par Twitter, chaque application ou site web a sa propre utilité. Le web social est pour eux le moyen de se construire une image et un réseau. Et ils savent quel type d'information partager selon le canal utilisé.



Leur environnement est fait d'objets connectés, de big data, de GAFA, d'homme augmenté, de télémédecine ou encore d'impression 3D... Ils sont entourés de données, les leurs et celles des autres, qu'ils partagent parfois sans mesure.

L'APSSIS fait le point sur cette Génération Z et son rapport à la confidentialité, au partage de données et en particulier celles liées à la santé. Comment ces adolescents voient-ils Internet, le partage des données, la confiance et la confidentialité ?

La Génération Z est-elle en train de réinventer la notion de confidentialité ?

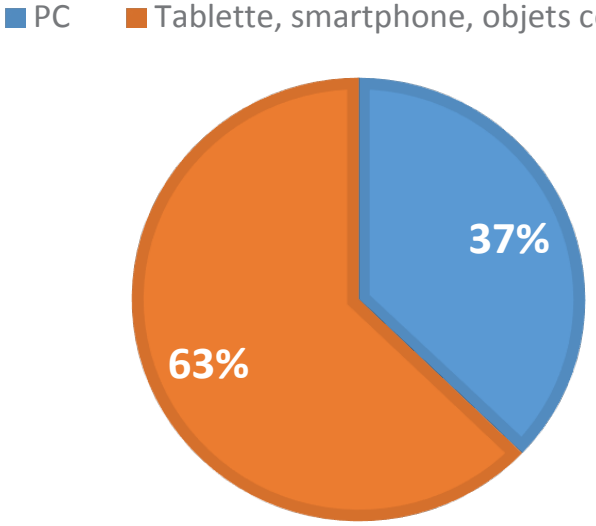
1

A quoi sont-ils connectés et comment ?

© aey - Fotolia

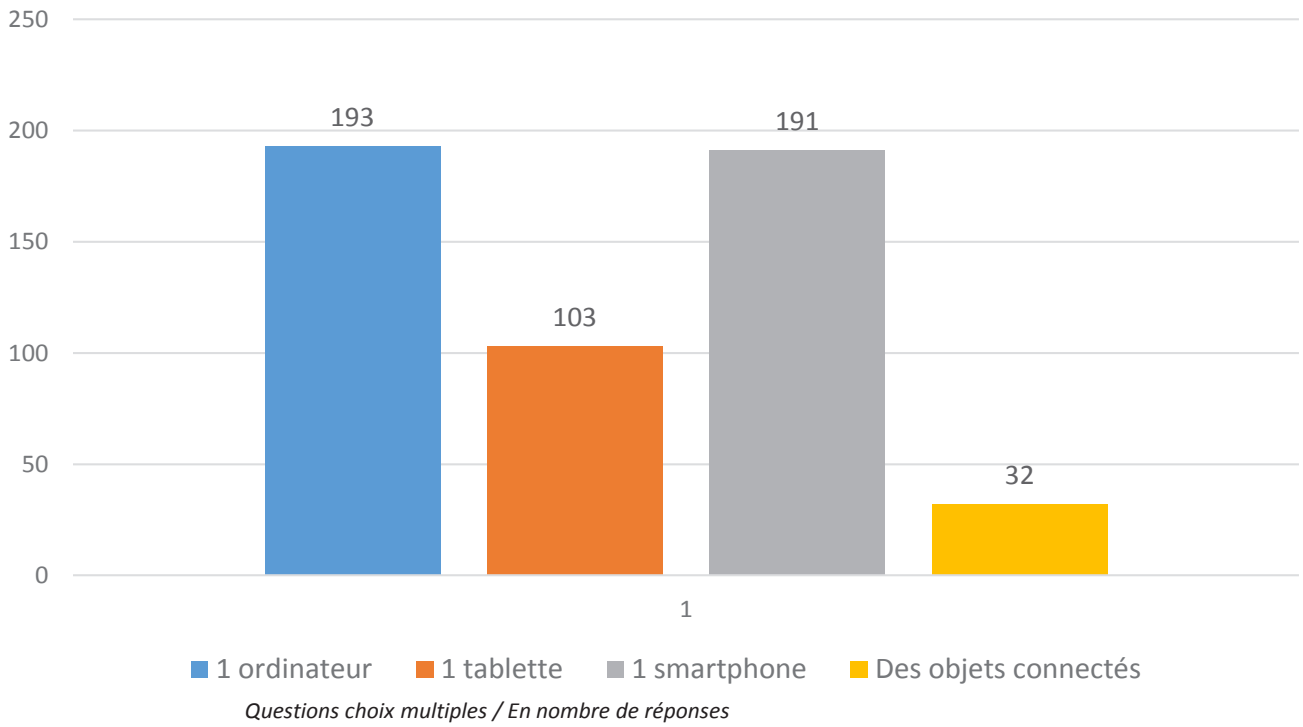
L'accès à Internet en mobilité privilégié par les adolescents (Q1)

Par quel(s) moyen(s) êtes-vous connectés à Internet ?
Questions choix multiples



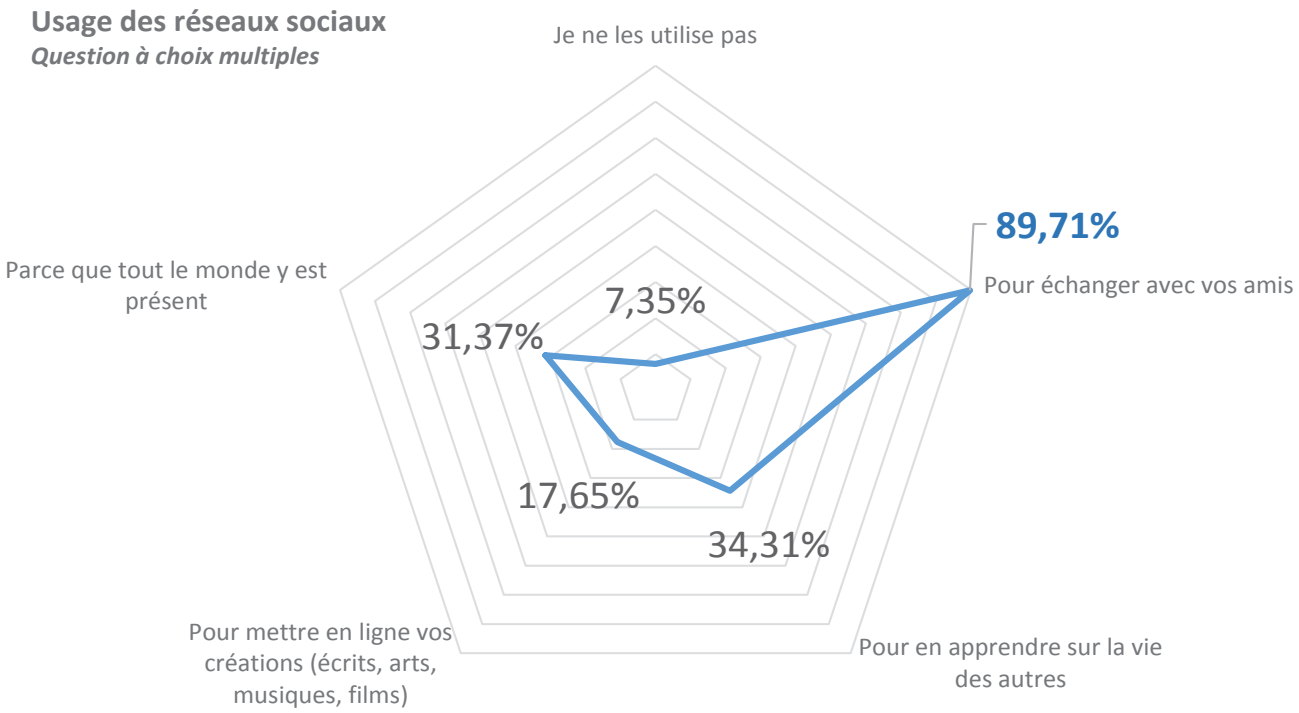
Internet en mobilité : Smartphone, tablette et objets connectés sont largement utilisés pour se relier au web.

Le smartphone autant utilisé que le PC, le premier permettant de préserver un peu son jardin secret, contrairement au PC familial. Ils sont peu nombreux à mentionner les objets connectés… Est-ce parce que finalement le smartphone est déjà un objet connecté via un panel d'applications ?
Selon une étude menée par *Gartner et l'Idate,* **on peut estimer que le nombre d'objets connectés en circulation en 2020 à travers le monde se situera entre 50 et 80 milliards**.



Questions choix multiples / En nombre de réponses

Génération réseaux (Q2)



Seuls 7,35% des adolescents interrogés répondent ne pas utiliser les réseaux sociaux. Rien d'étonnant pour cette génération, pour laquelle le partage sur le web est naturel. **C'est la génération réseaux.**

98% des lycéens ont un compte Facebook[1]. Mais ils commencent à délaisser ce réseau social (jugé « ringard ») au profit d'autres plateformes telles que Snapchat, Twitter, Instagram, WhatsApp, Vine, Pinterest …

(1)http://www.netpublic.fr/2013/03/pratiques-numeriques-des-jeunes/

Réseaux et mobilité : une génération omni connectée !

Que les jeunes de la Génération Z favorisent l'accès à Internet via leurs appareils mobiles n'a rien d'étonnant, notamment lorsque l'on sait que l'adolescent moyen reçoit son premier téléphone à 11 ans (source Médiamétrie). Pour cette nouvelle génération, née avec les écrans, la prise en main d'un smartphone, d'une tablette ou d'une console de jeu est instinctive. Et cela a contribué à transformer leur vie quotidienne, leurs relations sociales, leur façon de communiquer, leurs loisirs, leur accès à la culture ou encore leur manière d'apprendre.

Autant utilisé que le PC pour se connecter à Internet, le smartphone ne sert pas franchement à téléphoner, comme l'a montré une récente étude du Credoc (« La diffusion des technologies de l'information et de la communication dans la société française » -2012). En effet, l'adolescent moyen, entre 12 et 17 ans, envoie 381 SMS par semaine. Très consommatrice d'Internet, la génération Z passe en moyenne 13h30 par semaine sur le web (enquête Ipsos d'avril 2015). Et plus de 50% des utilisateurs surfent la nuit.

Un rapport du PISA[(1)] étudiant le lien entre présence et utilisation des nouvelles technologies à l'école et performance des élèves, montre que les jeunes de plus de 15 ans, passant plus de six heures sur Internet, sont particulièrement susceptibles de développer des comportements problématiques à l'école (retards, absentéisme,…).

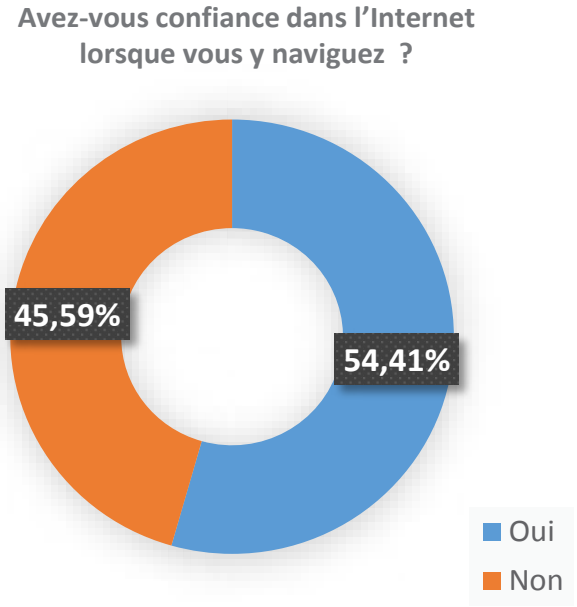
(1) OECD (2015), Students, Computers and Learning : Making the Connection, PISA, OECD Publishing
http://dx.doi.org/10.1787/9789264239555-en

2

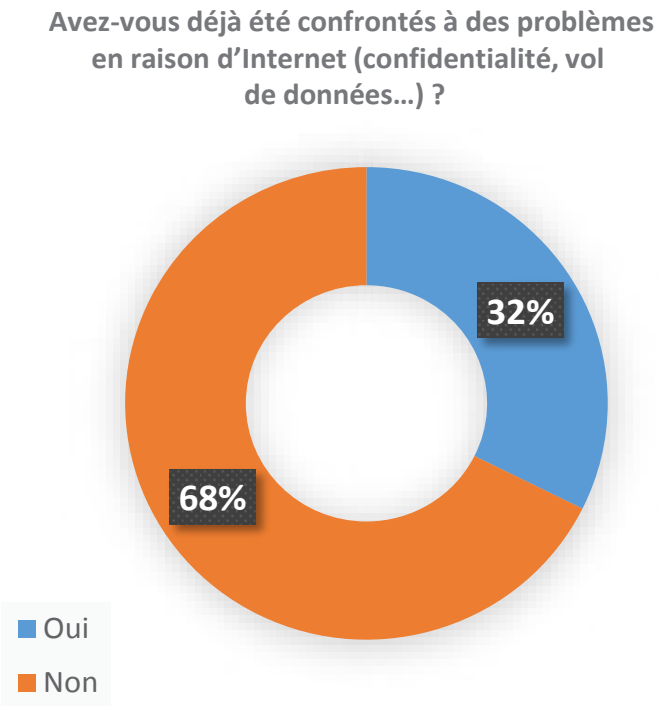
Internet et la confiance

© djvstock - Fotolia

La génération Z fait-elle confiance à Internet ? (Q11&6)



54,41% des jeunes interrogés déclarent faire confiance au réseau. Le faible écart entre les réponses positives et négatives, collectées dans le cadre de l'enquête, montre bien qu'ils ne sont pas complétement rassurés et qu'ils ont malgré tout une certaine conscience des dangers.



Confidentialité, vols de données personnelles ou harcèlement moral **: 32% des jeunes interrogés** déclarent avoir déjà vécu une expérience de ce type.

Selon l'Association e-Enfance, 25% des 8-17 ans disent avoir déjà été victimes d'insultes ou de rumeurs sur Facebook.

Les adolescents ne font pas franchement confiance à Internet, ont déjà connu des problèmes (harcèlement moral, vol de données, etc.) à cause des réseaux et pourtant 92% des 8-17 ans utilisent leur véritable identité sur Facebook et y livrent des informations personnelles. *(Source Association e-Enfance)*

Il faut rappeler que les adolescents harcelés sur les réseaux ont 3 fois plus de risques de faire une tentative de suicide que les autres. Peut-on considérer qu'il puisse s'agir d'un nouveau risque de santé publique?

La CNIL a d'ailleurs engagé un programme de sensibilisation auprès des jeunes « *Protège ta vie privée sur Internet* » afin d'aider à développer les bonnes pratiques dans l'usage d'internet et des réseaux sociaux.

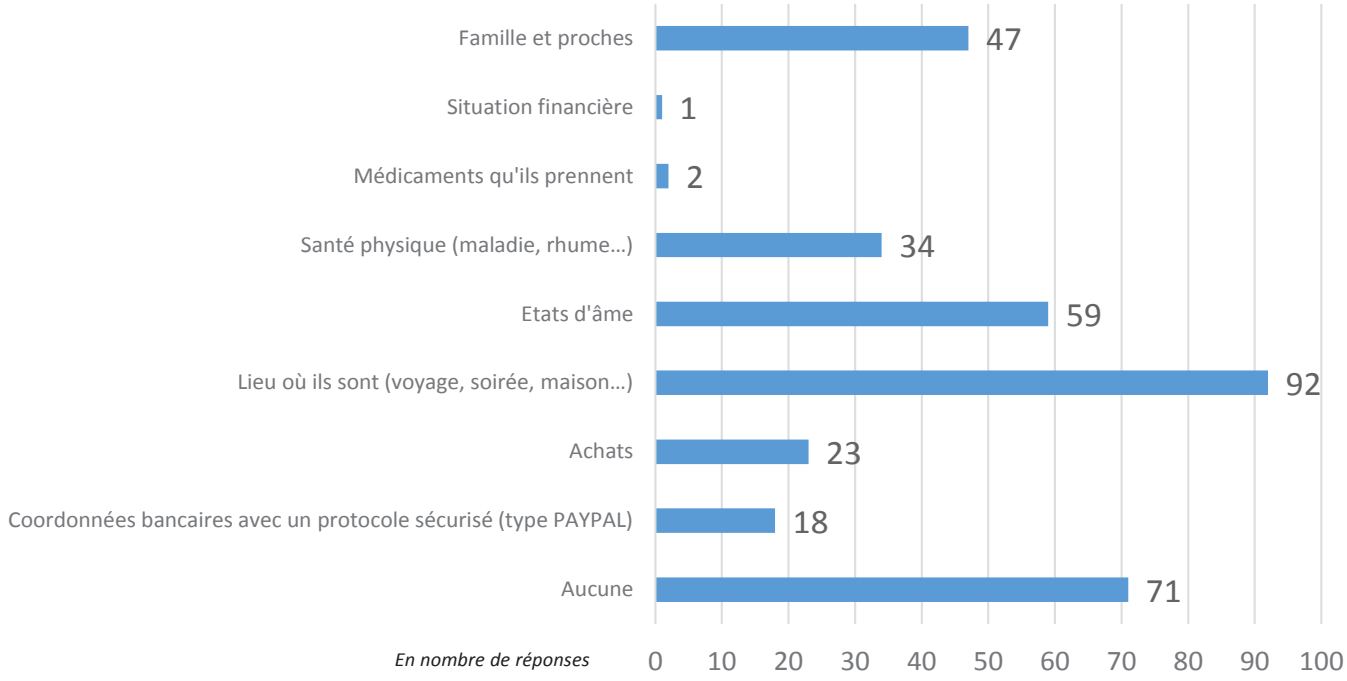
Il s'agit pour les adolescents de **prendre conscience de ce qu'est une donnée et du caractère personnel de celle-ci.**

3

Quel rapport aux données à caractère personnel ?

Leurs informations personnelles largement partagées sur les réseaux
(Q3)

Quels types d'informations diffusez-vous sur les réseaux sociaux et autres plates-formes (forums, sites spécialisés, sites d'achats…) ?

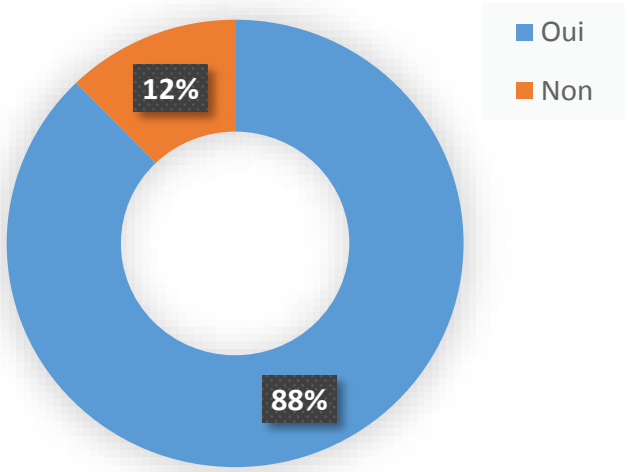


Les réponses le confirment, les adolescents partagent de nombreuses données intimes et personnelles sur les différents réseaux qu'ils fréquentent. Du lieu où ils se trouvent en passant par leurs achats ou encore leur santé, il s'agit d'informations relevant du domaine privé, qu'ils n'hésitent pas à publier.

Selon une étude Pew fondation de 2012, 94 % des jeunes déclarent poster des photos d'eux-mêmes et 71% mentionnent dans leur profil le nom de leur école et la ville où ils résident, voire indiquent leur adresse mail (53%) et leur numéro de éléphone portable (20%).

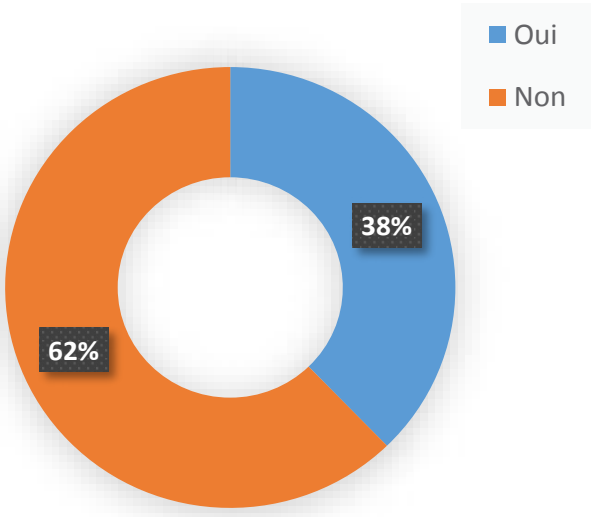
Les adolescents savent qu'Internet conserve toutes leurs données mais ce n'est pas si important ! (Q12&13)

Savez-vous que tout ce que vous écrivez, publiez (photos, vidéos) ou enregistrez sur les services Internet (Facebook, Twitter, Instagram…) est conservé à vie sur Internet ?



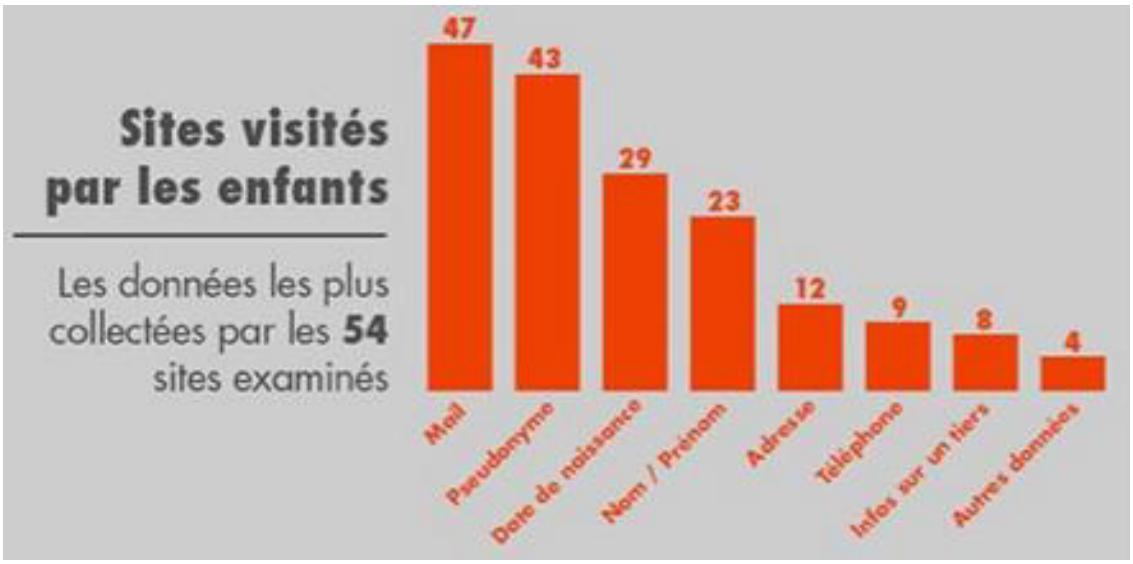
Tout ce qu'ils écrivent, publient (photos, vidéos) ou enregistrent sur les services Internet (Facebook, Twitter, Instagram…) est conservé. Ils le savent (88%), et le risque élevé que ces données soient stockées à vie sur Internet ne semble pas poser de problème à la majorité d'entre eux (62%).

Finalement, est-ce important que ces données soient conservées à vie quelque part ?



Et les sites ne se gênent pas pour collecter leurs données !

29 autorités dans le monde ont mené un audit pour vérifier le respect des règles de protection de la vie privée par les sites internet consultés par les enfants. Le résultat montre que leurs données personnelles sont insuffisamment protégées.



http://www.cnil.fr/linstitution/actualite/article/article/vie-privee-des-enfants-une-protection-insuffisante-sur-les-sites-internet

Source Institut Montaigne – Big Data et Objets Connectés, faire de la France un champion du numérique

Finalement que savent-ils de la protection des données personnelles?

Les adolescents interrogés ont exprimé à plusieurs reprises leur inquiétude quant à la protection des données sur le web. D'ailleurs, lorsqu'ils achètent en ligne (56%), ils accordent de l'importance à la sécurité des données bancaires (67%). On peut donc estimer qu'ils comprennent les enjeux de la protection des données personnelles.

D'ailleurs, toujours selon l'Etude Pew Fondation (2012), 92% des adolescents déclarent maîtriser les paramètres de confidentialité pour protéger leurs données (et in fine de leur réputation) vis-à-vis des autres utilisateurs.

Pourtant, une étude RSA/IFOP de janvier 2013 réalisée auprès d'enfants de 11 à 17 ans, montre que 49% des répondants pensent que sur Facebook, les paramètres de confidentialité empêchent les informations personnelles d'être diffusées à des personnes inconnues ou non identifiées.
Ce n'est évidemment pas le cas !

Protéger ses données personnelles, c'est aussi protéger sa réputation en ligne, et rester dans la légalité.

Etude RSA/IFOP de janvier 2013

L’avis de l’expert

Cédric Cartau

Responsable Sécurité des Systèmes d’Information et CIL au CHU de Nantes

Cédric Cartau est chargé de cours à l'Ecole de Hautes Etudes en Santé Publique (EHESP). Il réalise également des audits de systèmes d'information (www.siconcept.fr) pour le compte d'établissements publics ou privés dans différents secteurs d'activité. Il a publié à ce jour plusieurs ouvrages aux Presses de l’EHESP, et le dernier aux éditions Eyrolles (« L'informatique de santé », coauteur, Eyrolles, 2015).

L’hypermnésie est une pathologie désignant la capacité d’une personne à se souvenir d‘absolument tout ce qu’elle a vu, entendu, dit, écrit, et cela depuis sa petite enfance. On ne dénombre que quelques cas à l’échelle mondiale (moins de 10 selon certaines sources) et à chaque fois les patients vivent très mal cet état : temps considérable passé chaque jour à se remémorer les évènements passés, impossibilité de faire le tri dans les souvenirs, intégration sociale quasi-inexistante.

Ce qui frappe dans les chiffres de cette étude, c’est que le caractère hypermnésique de l’Internet ne semble émouvoir personne. Or, qui peut dire ce qu’il fera dans 20 ou 30 ans, surtout à l’adolescence ? Qui peut dire si, dans quelques décennies, l’adolescent d’aujourd’hui qui poste des photos d’une fête arrosée sur son compte Facebook ne briguera pas un mandat électoral, la direction d’une grande entreprise du CAC40, ou un poste à responsabilité dans un service marketing mondial ? Et alors à ce moment, nul doute que les équipes du candidat concurrent fouillerons le Web à la recherche d’éléments compromettant la candidature du malheureux. Science-Fiction dites-vous ? Que nenni, les études en Sciences Politiques démontrent que plus une démocratie est « avancée », et plus lors d’une campagne électorale les candidats passent de temps à se dénigrer mutuellement plutôt que d’évoquer des questions de fond.

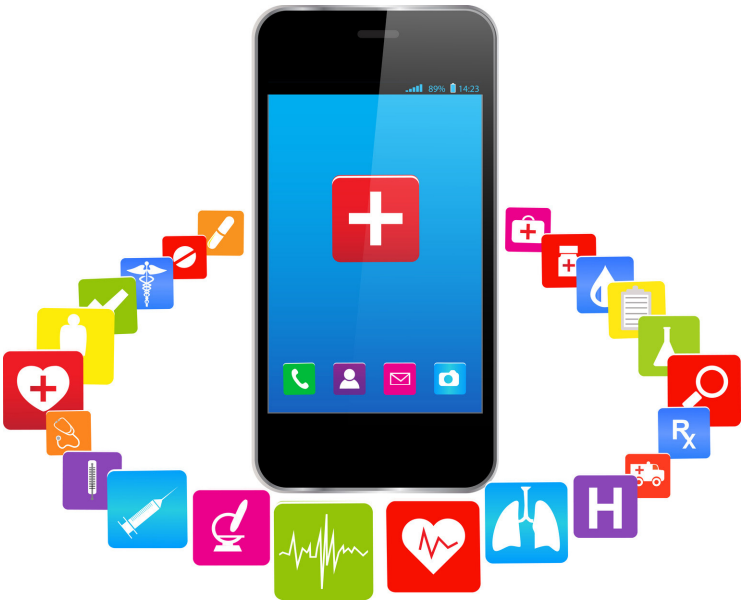
Le second point marquant de l’étude est la distorsion entre les deux réponses : 88% des adolescents interrogés affirment être conscients que le Web n’oublie rien, mais seuls 62% admettent que cette hypermnésie pose problème. Il faudrait être en mesure de croiser les populations, mais nul doute que pas mal de répondants ont une attitude étrangement contradictoire.

La capacité d’oubli d’une société est une des conditions du lien social. N’est-ce pas Voltaire qui en son temps réclamait le « droit de pouvoir se contredire ». Si une parole lancée peut vous être renvoyée au visage jusqu’à la fin des temps, plus le droit de changer d’avis, plus le droit de rien affirmer, plus de vie sociale. Dans le troisième épisode de la terrible série TV anglaise Black Mirror, chaque citoyen s’est fait implanter un enregistreur vidéo relié à sa rétine, et les personnages se repassent en boucle leurs meilleurs moments de vie. Le héros finit par abandonner toute vie sociale après avoir découvert les petits mensonges de ses collègues et relations.

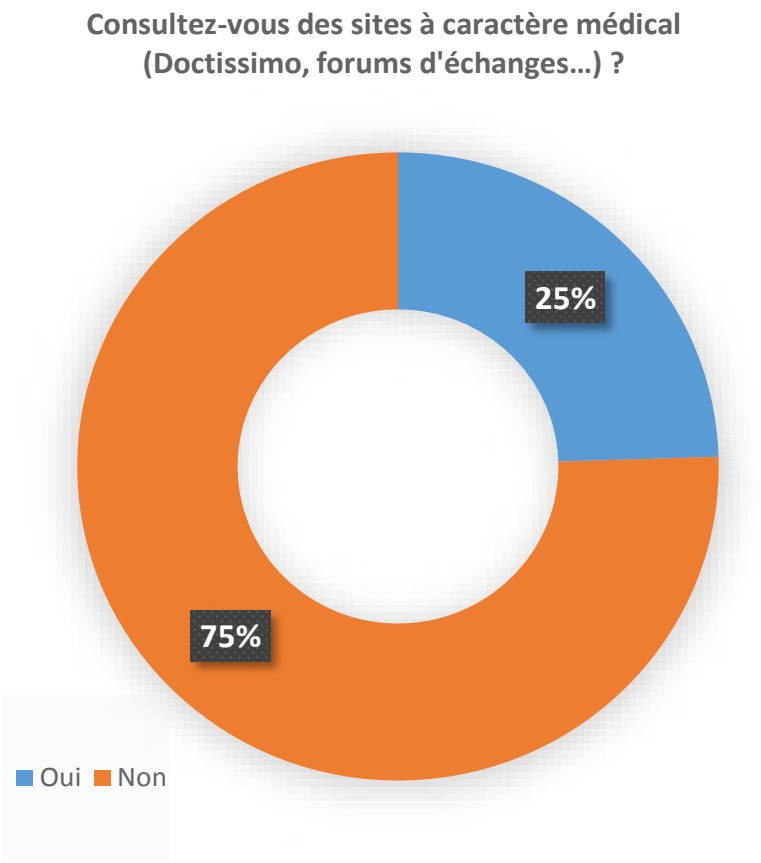
C’est peut-être cela l’enfer.

4

Quel rapport aux données médicales personnelles ?



Une question santé, et c'est Internet qu'ils consultent... (Q9)

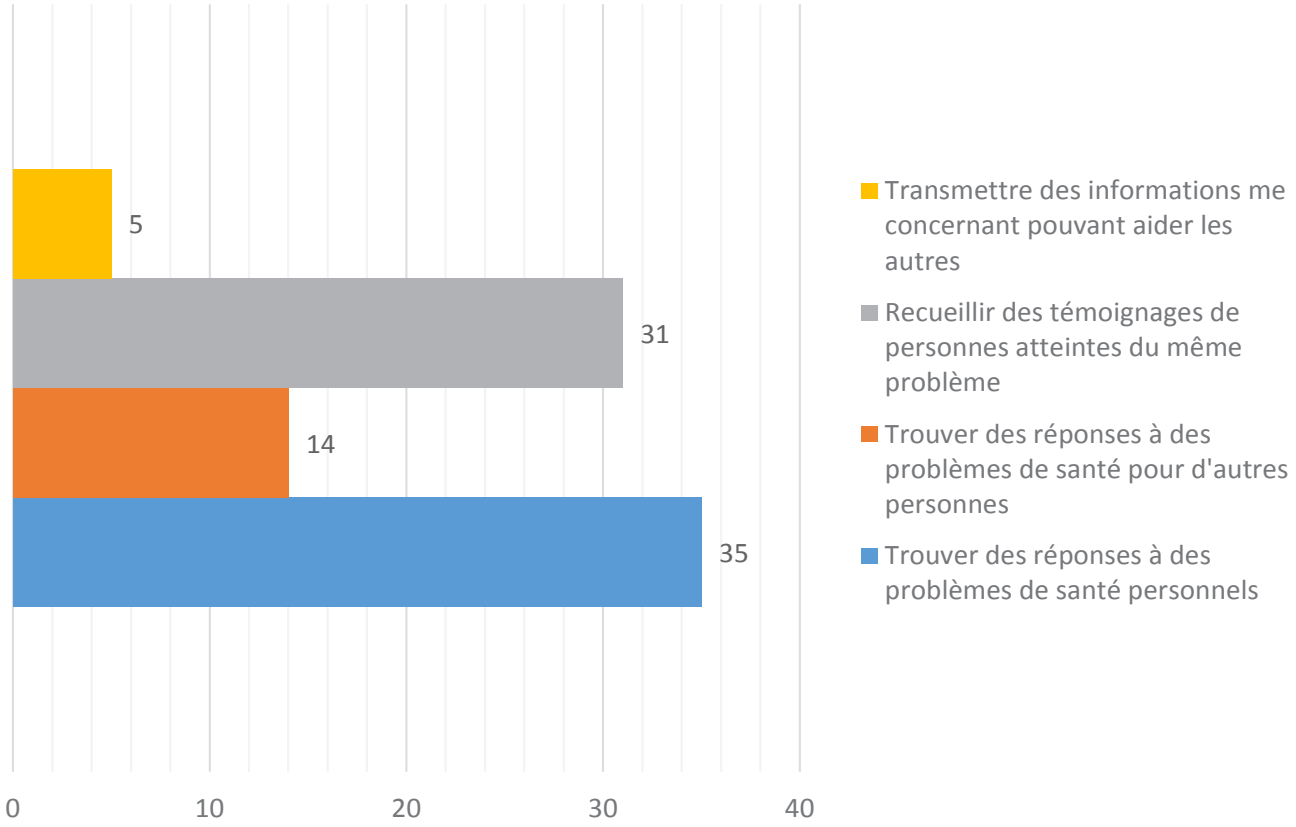


Ils ne sont que 25% à indiquer qu'ils consultent les sites à caractère médical.

Au final, ils sont plus nombreux, car comme le montre une enquête réalisée en 2013 par l'Institut National de Prévention et d'Education pour la Santé, « *Ta santé et ton bien-être sur internet* », les adolescents procèdent à leurs recherches directement via des mots clés dans le moteur de recherche. Ils sont d'ailleurs plus de 80% à estimer que les informations ainsi récoltées sur le net sont « crédibles ».

Et si plus de 50% d'entre eux vérifient qui est la personne ou l'institution qui diffuse l'information sur internet, l'autre moitié le fait rarement, voire jamais. Enfin, seuls 40% d'entre eux savent ce qu'est un site de santé labellisé.

… avec comme principale intention d'y trouver des informations et des réponses sur leurs problèmes de santé (Q10)

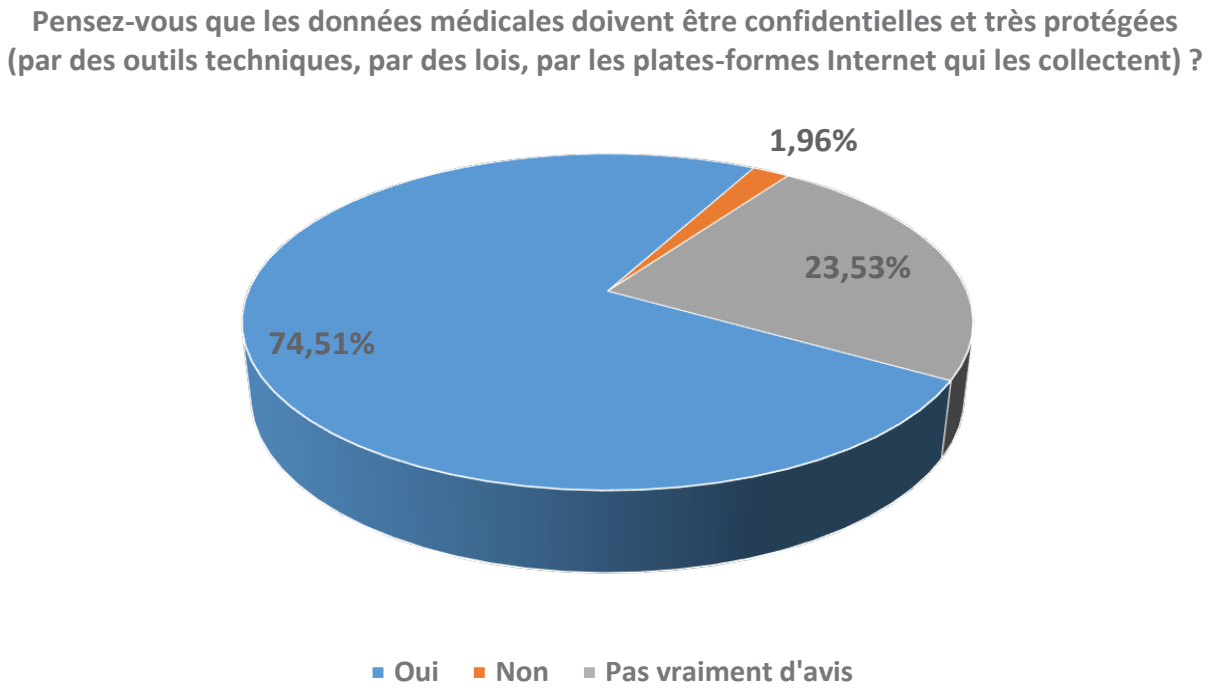


En nombre de réponses

Pour un adolescent, il n'est pas toujours facile d'interroger ses parents ou son médecin de famille pour parler de ses préoccupations de santé (tabac, stress, sommeil, poids, sexualité, déprime…). Internet s'avère donc l'endroit idéal pour « googler » son mal et trouver des informations.

Mais qu'en est-il des cookies et autres outils de traçage et d'identification utilisé par ces sites ? Quelles informations personnelles et médicales sont ainsi potentiellement utilisées ? Qui lit les fameuses conditions générales d'utilisation ?

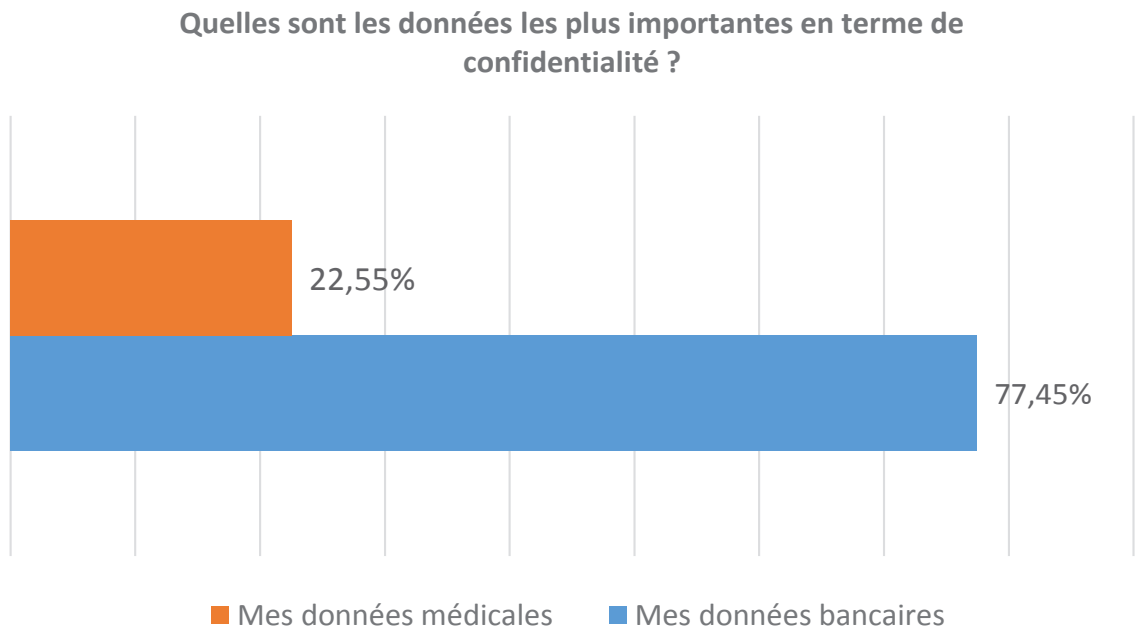
Ils ont conscience que la protection de leurs données médicales est nécessaire (Q15)



Informés des risques de fraude au paiement en ligne, ils voient naturellement un risque vis-à-vis d'autres données qui pourraient être sensibles, telles que des informations médicales les concernant. 74,5% considèrent que les données médicales doivent être protégées.

A noter que 23,5% n'ont pas d'avis sur la question.

Mais paradoxalement, leurs données personnelles médicales leur semblent moins confidentielles que leurs informations bancaires (Q14)



Depuis de nombreuses années, l'information dans le domaine du risque de fraude au paiement en ligne a été largement diffusée et les affaires de piratages ont été très relayées. Aussi, les familles sont sensibilisées à ces risques.

Ce n'est pas encore vraiment le cas des données personnelles de santé. Celles-ci sont considérées par la Loi Informatique et Libertés comme des données sensibles et bénéficient d'un régime de protection plus strict. Mais, encore faut-il savoir ce qu'est concrètement une donnée médicale.

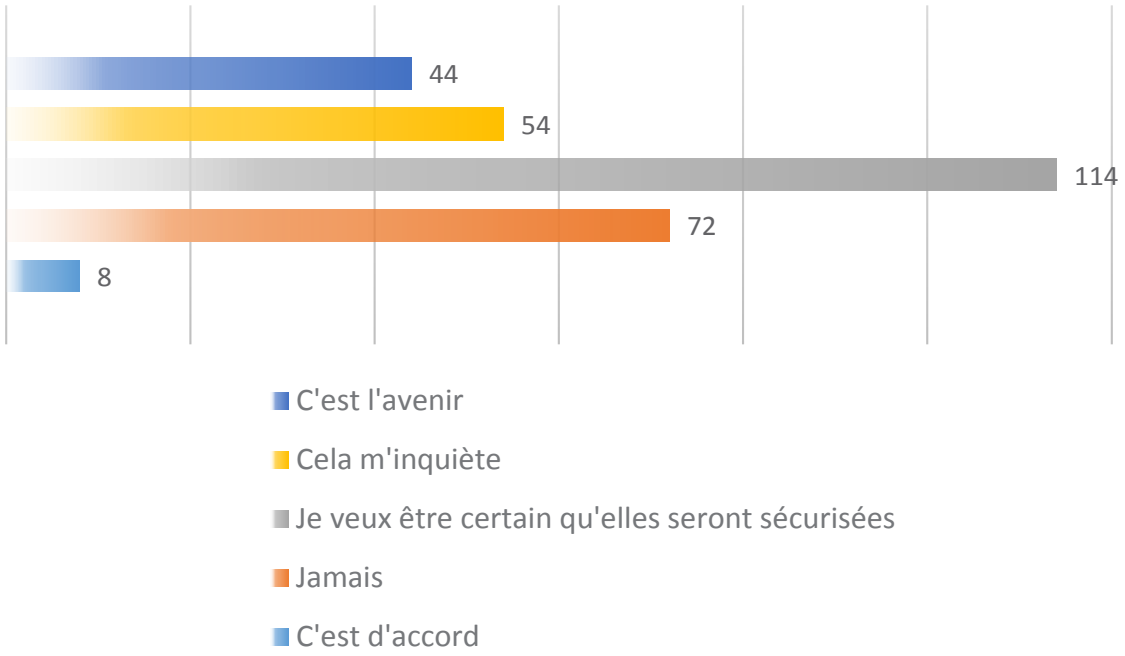
La question posée au panel « *Entre vos données bancaires (comptes, situation) et vos données médicales (traitements acné, contraception, pathologies particulières), quelles sont les plus importantes en terme de confidentialité ?* », il y avait bien la notion de données personnelles médicales. Est-ce parce qu'ils ne sont pas encore confrontés de manière directe au système de santé, qu'ils semblent ignorer la notion de confidentialité de ces données ?

Finalement, ne portons-nous pas un regard sur ce sujet, empreint de craintes propres à notre relation au numérique alors que nos enfants, baignant dans le digital, voient ce changement de paradigme comme une opportunité de transformer le système de santé, de mieux prendre soin de soi et de se soigner, de faire avancer la science grâce au partage des données ?

Et ils sont prêts à en laisser l'accès
(Q4)

Donner à des sociétés l'accès à vos données médicales afin qu'elles vous proposent des services et des solutions personnalisées (comme des objets connectés de santé qui suivront votre activité) :

Questions à choix multiples / En nombre de réponses

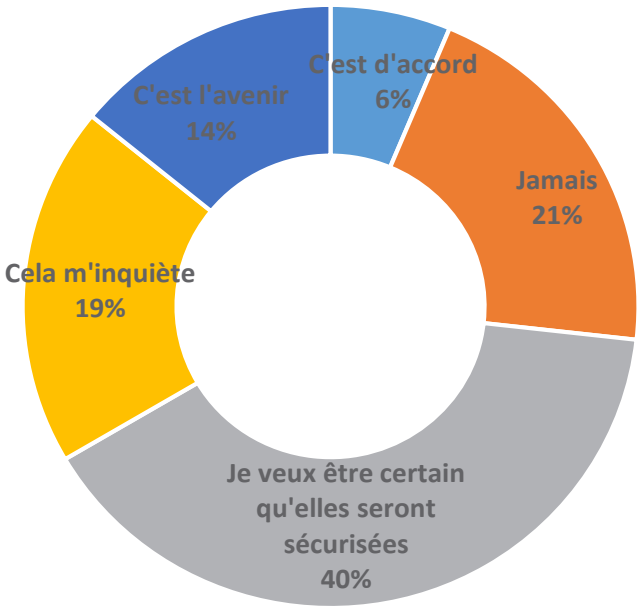


Plutôt inquiets et sensibles à la sécurisation de leurs données, ils sont néanmoins, en grande majorité, prêts à donner accès à leurs données de santé.

Il n'est donc pas difficile d'imaginer qu'ils vont probablement contribuer à transformer la relation patient / médecin / assureur en adoptant une démarche proactive, puis prédictive en ce qui concerne leur santé.

Notamment à leur mutuelle ou assurance (Q5)

Par exemple, que votre Mutuelle ou votre Assureur aient accès à vos données de santé afin de moduler les tarifs (moins cher pour celui qui fait du sport et qui mange correctement) ?



Dans un rapport datant de 2012 réalisé par *Abi research,* les applications liées à la santé et au sport devraient augmenter sensiblement d'ici 2017 passant de 21 millions en 2011 à 169,5 millions en 2017.

Malgré des craintes relatives à la sécurisation de leurs données, les adolescents sont en majorité plutôt d'accord avec le principe de partager leurs données de santé avec leur mutuelle ou leur assureur au travers des applications qui les collecteront et ce, dans la perspective d'obtenir des tarifs adaptés à leur cas particulier. Seuls 21% déclarent s'y refuser.

Le quantified-self comme base de calcul ?

Ces adolescents sont de futurs assurés prêts pour une petite révolution. Cette approche, basée sur la connaissance et la traçabilité de soi qui émerge rapidement avec le quantified-self, ne constitue-t-elle pas au fond une sérieuse remise en cause de notre système de santé basé sur le partage des risques ? Il s'agit donc, au travers de ce nouveau rapport aux données médicales personnelles, de l'émergence d'un système basé non plus sur le partage mais sur la responsabilisation de chacun. Et peut-être que cela pose aussi les bases d'une médecine prédictive et personnalisée.

L’avis de l’expert

Damien Bancal

Journaliste et spécialiste du cyber crime

Journaliste, spécialiste des problématiques du cyber crime et de la cybersécurité depuis plus de 25 ans. Auteur des blogs zataz.com et datasecuritybreach.fr. Auteur et coauteur de 6 livres dont "Pirates & hackers sur Internet" (Ed. Desmart) ou encore "Hacker, le 5ème pouvoir« (Maxima). Intervenant pour la Licence professionnelle Collaborateur pour la Défense et l'Anti-Intrusion des Systèmes Informatiques (CDAISI) de l'Université de Valenciennes. Officier réserviste Cyber Défense Gendarmerie Nationale.

Pour croiser de nombreux adolescents dans les lycées et collèges dans lesquels j'interviens pour les former à la bonne gestion de leur identité, réputation et sécurité numérique, j'ai rapidement découvert qu'ils n'avaient pas une, mais plusieurs vies binaires. Des vies 2.0 évoluant aux grès des modes, des amourettes et autres classes scolaires croisées. Ma méthode est simple pour les faire parler. Le jour de mon intervention -j'en réalise une cinquantaine par an dans les établissements français-, je leur communique toutes les informations que j'ai pu collecter sur eux. Avec leur autorisation, je les présente à l'ensemble de la classe. Bien évidemment, je n’affiche que les informations qui ne nuiront pas à la réputation déjà fragile des adolescents volontaires. Autant dire que des dents grincent : photos, messages privés, achats, captures écrans, applications utilisées... Ils diffusent tout et n'importe quoi. Dans la majorité des cas, ils le font sans réfléchir, pensant que seules leurs interlocuteurs privilégiés (amis, camarades de classe, famille) étaient leurs uniques destinataires. Une démonstration adaptée à leur âge, leurs ricanements, leur fausse assurance. Cela fonctionne à merveille. Ils comprennent que leur journal intime, celui qu'ils cachent sous leur oreiller dans leur chambre, ils ne le jetteraient pas dans la rue, et espère que personne ne le lise. Alors pourquoi le faire sur le web ?

La majorité des parents ne savent pas que leurs enfants n'ont pas un, mais des espaces Facebook. Mon record, pour une jeune Lilloise de 12 ans : 14 comptes différents. Des espaces ouverts à la suite du piratage d'un précédent, d’une fermeture forcée par les adultes, ou l'envie de changer de vie 2.0. Et elle n’avait que 12 ans ! Que les parents cessent de se voiler la face. Les adolescents utilisent plusieurs réseaux sociaux alors que les adultes de la famille ont bien du mal à en comprendre un seul. Dangereux ? Oui et non ! Non, car rassurant de regarder nos "mômes" se créer leur monde, se familiariser avec les us et coutumes de la société. Inquiétant car la masse d'informations qu'ils distillent, de compte en compte, de réseau en réseau, sans ne plus pouvoir les effacer pourraient remplir leur chambre en à peine quelques semaines. Des données leur appartenant, mais aussi celles d'amis, de connaissances, de la famille. Découvrir des photographies de la maison familiale sur des réseaux sociaux n’amuse pas les parents. Mais trop tard !

Les bonnes pratiques pour protéger leur vie privée sur Internet ? Ils les connaissent parfaitement. Il suffit de parler avec eux pour s'en assurer. Les pratiquent-ils ? Ils essaient, tant bien que mal. Ne pas donner son identité, se créer des groupes privés sur les réseaux sociaux, ils n'hésitent plus. Mais l'outil est fourbe, demande réactivité, culture de l'image et du paraître. Bilan, ils continuent de parler de leur vie privée, de diffuser des documents pouvant être sensibles sur les pages "privées" créées sur Facebook, sur Twitter. Je ne parle même pas de la grande mode des montres connectées qui leur permet d'échanger les kilomètres parcourus ou les rythmes cardiaques, leurs activités extrascolaires ou encore des très modes « *Hello Siri* » ou « *Ok Google* » qu’ils distillent à partir de leur smartphone. Retrouver leurs voix et leurs recherches vocales dans les serveurs d’Apple et de Google, les amusent beaucoup moins.

Pour les faire réagir, l'une de mes techniques est simple. Je leur montre le cheminement d'une photographie qu'ils ont pu diffuser. Leur expliquer que ce simple document peut finir sur un site malveillant, pour adulte ou n'ayant strictement aucune affinité avec leur vie réelle.

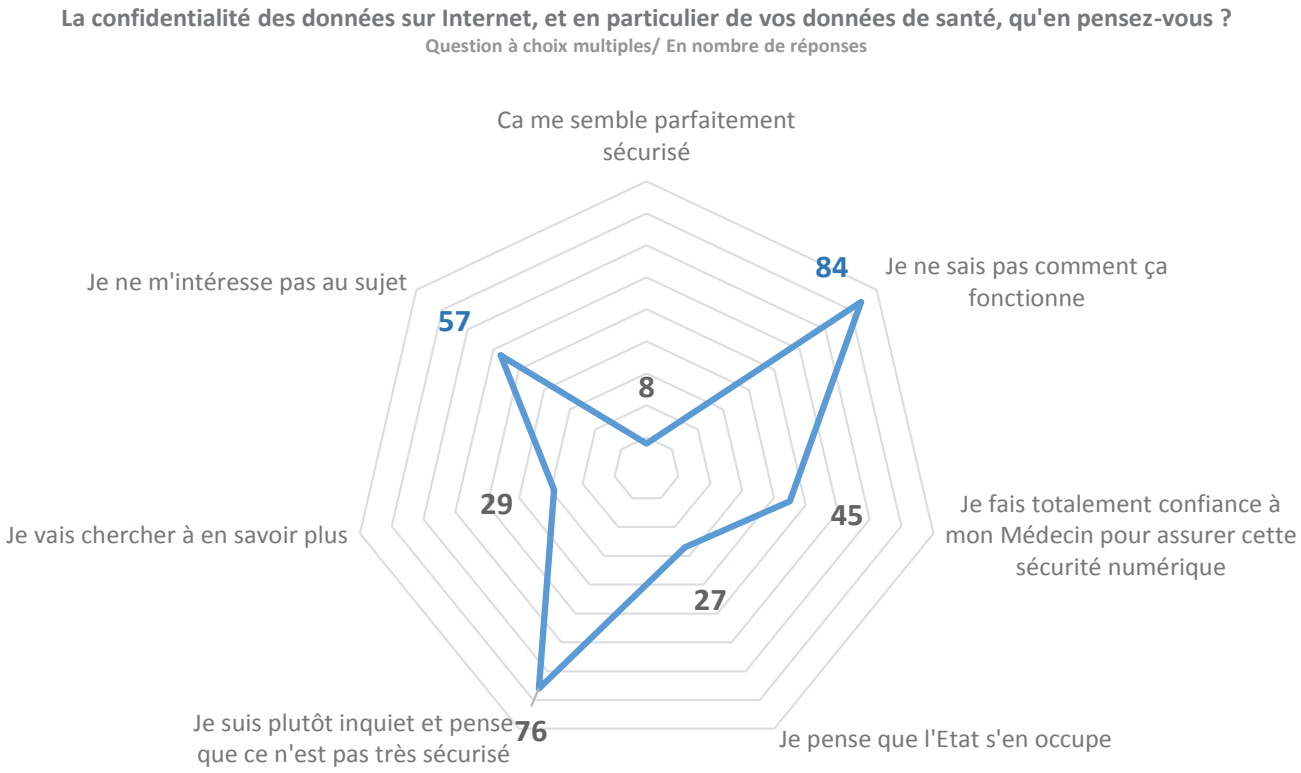
Il suffit, par exemple, d'utiliser Google Image, d'y proposer la photographie et de contempler le moteur de recherche proposer des dizaines de réponses différentes. Autant dire qu'ils comprennent très vite les débordements possibles, surtout si l'information volée par ces tiers peu ragoûtants étaient d'une toute autre nature qu'un simple cliché de vacances.

Se sécuriser, ils comprennent. Sécuriser leurs données, ils y pensent. Leur santé, soyons honnête, ils s'en moquent, sauf si cela touche à leur apparence : cheveux, boutons, ... Il est d'ailleurs intéressant de leur demander s'ils savent où sont stockées leurs données sauvegardées par leur montre connectée. Les adolescents que j'ai pu croiser (tous) pensaient que ces informations n'étaient stockées qu'à leur poignet.

5

Vous avez dit confidentiel ?

La confidentialité des données médicales personnelles en question
(Q16)



Les réponses des adolescents illustrent le cœur de la problématique pointée par cette enquête : la notion de confidentialité des données à caractère personnel et en particulier médical est mise à mal.

Omni connectée, la génération Z semble manquer de repères en ce qui concerne la protection des données médicales personnelles. Le manque d'information sur le fonctionnement de la protection de ces données génère de l'inquiétude chez les adolescents. Pensant se reposer sur le médecin et sur l'Etat pour s'en occuper, ils n'ont pas la curiosité d'en savoir plus sur la façon dont ils seraient impliqués dans le processus ou dans la manière de développer de bonnes pratiques.

La Génération Z va-t-elle contribuer à faire évoluer la notion de confidentialité ?

Quel sera le pacte que la génération qui vient établira avec l'écosystème numérique ? C'est tout l'enjeu des 50 ans qui viennent.

Dans une récente étude du Figaro(1), les adultes se positionnent, et expriment leurs premières exigences en matière de données personnelles de santé. Alors qu'un Français sur deux considère que la santé connectée est une menace pour le secret médical(3), en 2017, 1 utilisateur de smartphone sur 2 aura installé au moins une application dédiée au bien-être ou à la santé(2).

L'étude l'a montré, les jeunes de la Génération Z, de par leur nature digitale, n'envisagent pas le rapport aux données personnelles et la notion de confidentialité de la même manière que leurs parents. En cela, ils vont certainement contribuer à initier un nouveau pacte de confiance numérique, et contribuer à la transformation numérique de notre système de santé.

La confidentialité devient alors toute relative, contextuelle. Si une application, un service m'apporte un vrai plus, alors je peux accepter de donner accès à mes données médicales, ce ne sera pas un problème. Finalement, au-delà de casser les codes de la confidentialité, ne seront-ils pas les acteurs d'une prochaine uberisation, celle des données de santé ?

L'APSSIS suivra de près l'évolution des usages et de cette nouvelle manière de concevoir la confiance et la confidentialité, dont les enjeux sont grands pour l'avenir de notre système de santé.

Une nouvelle rencontre est d'ailleurs prévue au mois de mai 2016 avec les élèves du Lycée Robert Garnier, et leur concours permettra de faire évoluer et d'enrichir ce premier travail.

(1) Source le Figaro: http://www.lefigaro.fr/secteur/high-tech/2015/10/08/32001-20151008ARTFIG00013-les-francais-moins-reticents-a-partager-leurs-donnees-personnelles-sous-conditions.php
(2) Source : *Mobile Health Market Report 2013-2017* par Research2Guidance, mars 2013
(3) Source : Baromètre sante 360, Odoxa, janvier 2015.

A propos de l'APSSIS

Fondée en 2010, l'APSSIS a vocation à **promouvoir la sécurité des Systèmes d'Information de Santé**.

En 2011, le premier Congrès National de la Sécurité des Systèmes d'Information de Santé du Mans positionnait l'Association comme acteur majeur de la SSI santé, regroupant professionnels de santé, médecins, DSIO, RSSI, industriels, éditeurs, chercheurs, directeurs généraux d'établissements de Santé autour d'un objectif simple : créer et animer un **Think Tank pluri professionnel** dédié à la réflexion sur la sécurité de l'écosystème numérique de santé. Le congrès de l'APSSIS se tient tous les deux ans au Mans, sa quatrième édition se déroulant les 4, 5 et 6 avril 2016.
L'APSSIS assure la promotion des outils élaborés par les Instances Nationales : ANSSI, DGOS, puis ASIP Santé. Elle aide les professionnels en charge de la Sécurité des SI de Santé et ses adhérents à appréhender avec simplicité le corpus documentaire mis à disposition.

Depuis 2011, l'APSSIS est **prestataire de formation**, et propose des séminaires de sensibilisation à la SSI Santé, ainsi qu'à l'usage des guides et outils proposés par les Instances.

L'APSSIS a publié en juillet 2014, le premier Vademecum des Objets connectés.

Annexe

APSSIS

Association pour la Promotion de la Sécurité des Systèmes d'Information de Santé

QUESTIONNAIRE 16 QUESTIONS – 5 Minutes – Rapport à la confidentialité des données et aux usage de l'Internet – Lycée Robert Garnier – Mardi 2 Juin 2015

INTRUCTIONS :
Remplir AGE, SEXE, CLASSE pour les besoins de l'étude. Le questionnaire est anonyme.
Répondre aux 15 questions.
Merci de votre participation !

AGE : **SEXE** : Masculin ☐ Féminin ☐ **CLASSE** : 2 ☐ 1 ☐ TER ☐

QUESTION 1 – Plusieurs réponses possibles
Par quel(s) moyen(s) êtes-vous connectés à Internet :
1 ordinateur ☐ 1 tablette ☐ 1 Smartphone ☐ Des Objets connectés ☐

QUESTION 2 – Plusieurs réponses possibles
Vous utilisez les réseaux sociaux :
Je ne les utilise pas ☐
Pour échanger avec vos amis ☐
Pour en apprendre sur la vie des autres ☐
Pour mettre en ligne vos créations (écrits, arts, musiques, films) ☐
Parce que tout le monde y est présent ☐

QUESTION 3 – Plusieurs réponses possibles
Quels types d'informations diffusez-vous sur les réseaux sociaux et autres plates-formes (forums, sites spécialisés, sites d'achats…) ?
Aucune ☐
Vos coordonnées bancaires avec un protocole sécurisé (type PAYPAL) ☐
Des informations sur vos achats ☐
Des informations sur le lieu où vous êtes (voyage, soirée, maison…) ☐
Des informations sur vos états d'âme ☐
Des informations sur votre santé physique (maladie, rhume…) ☐
Des informations sur les médicaments que vous prenez ☐
Des informations sur votre situation financière ☐
Des informations sur votre famille et vos proches ☐

QUESTION 4 – Plusieurs réponses possibles
Donner à des sociétés l'accès à vos données médicales afin qu'elles vous proposent des services et des solutions personnalisées (comme des objets connectés de santé qui suivront votre activité) :
C'est d'accord ☐ Jamais ☐ Je veux être certain qu'elles seront sécurisées ☐
Cela m'inquiète ☐ C'est l'avenir ☐

QUESTION 5 – Plusieurs réponses possibles
Par exemple, que votre Mutuelle ou votre Assureur aient accès à vos données de santé afin de moduler les tarifs (moins cher pour celui qui fait du sport et qui mange correctement) :
C'est d'accord ☐ Jamais ☐ Je veux être certain qu'elles seront sécurisées ☐
Cela m'inquiète ☐ C'est l'avenir ☐

QUESTION 6
Avez-vous déjà été confrontés à des problèmes en raison d'Internet (confidentialité, vols de données personnelles, piratage ou harcèlement moral) ? Oui ☐ Non ☐

QUESTION 7
Effectuez-vous des achats en ligne (seul ou avec vos parents) ?
Oui ☐ Non ☐ Rarement ☐

QUESTION 8
Accordez-vous de l'importance au niveau de sécurité du site lors du paiement (lecture du contrat, outil de sécurité de la transaction utilisé…) ? Oui ☐ Non ☐ Rarement ☐

QUESTION 9
Consultez-vous des sites à caractère médical (Doctissimo, forums d'échanges…) ? Oui ☐ Non ☐

QUESTION 10 – Plusieurs réponses possibles

Si Oui, pour quelles raisons ?

Trouver des réponses à des problèmes de santé personnels ☐

Trouver des réponses à des problèmes de santé pour d'autres personnes ☐

Recueillir des témoignages de personnes atteintes du même problème ☐

Transmettre des informations me concernant pouvant aider les autres ☐

QUESTION 11

Avez-vous confiance dans l'Internet lorsque vous y naviguez ?

Oui ☐ Non ☐

QUESTION 12

Savez-vous que tout ce que vous écrivez, publiez (photos, vidéos) ou enregistrez sur les services Internet (Facebook, Twitter, Instagram…) est conservé à vie sur Internet ? Oui ☐ Non ☐

QUESTION 13

Finalement, est-ce important que ces données soient conservées à vie quelque part ?

Oui ☐ Non ☐

QUESTION 14

Entre vos données bancaires (comptes, situation) et vos données médicales (traitements acné, contraception, pathologies particulières), quelles sont les plus importantes en terme de confidentialité ?

Mes données bancaires ☐ Mes données médicales ☐

QUESTION 15

Pensez-vous que les données médicales doivent être confidentielles et très protégées (par des outils techniques, par des lois, par les plates-formes Internet qui les collectent) ?

Oui ☐ Non ☐ Pas vraiment d'avis ☐

QUESTION 16 – Plusieurs réponses possibles

La confidentialité des données sur Internet, et en particulier de vos données de santé, qu'en pensez-vous ?

Ca me semble parfaitement sécurisé ☐

Je ne sais pas comment ça fonctionne ☐

Je fais totalement confiance à mon Médecin pour assurer cette sécurité numérique ☐

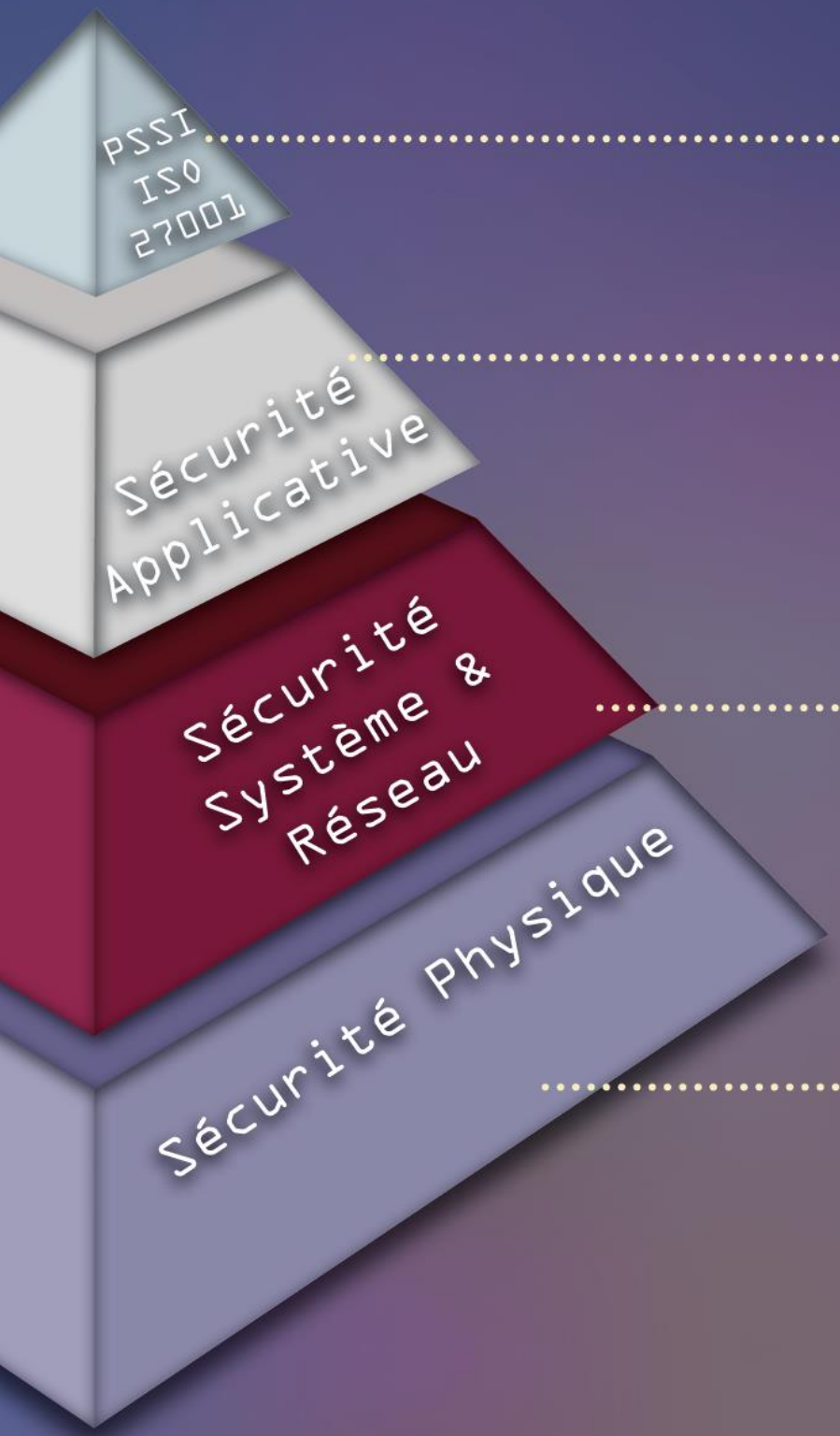
Je pense que l'Etat s'en occupe ☐

Je suis plutôt inquiet et pense que ce n'est pas très sécurisé ☐

Je vais chercher à en savoir plus ☐

Je ne m'intéresse pas au sujet ☐

Votre sécurité, notre métier



PSSI ISO 27001
- Audit de sécurité
- Définition de la PSSI

Sécurité Applicative
- Détection – Analyse – Remédiation des vulnérabilités Web et Mobiles
- Processus sécurisés de développement
- Formations Sécurité applicative – APPSCAN – IBM JAZZ ...

Sécurité Système & Réseau
- Audit Systèmes et Réseaux
- Wifi sécurisé – Portail captif
- Pare-feu Palo Alto
- Prévention cyber-squatting – SQUATMON.com
- Logs Management – Cloud privé Openstack
- Formations SIEM – QRADAR

Sécurité Physique
- Sécurité des bâtiments
- Vidéosurveillance – Intégration contrôle d'accès et alarmes
- Formations et e-learning

ABLOGIX spécialiste en sécurité du système d'information
OPTIMISE vos processus et politique de cyber-sécurité
SÉCURISE vos applications, vos systèmes & réseaux et vos bâtiments

Fournisseur de services et produits en Sécurité

www.ablogix.fr

ABlogiX - 72110 Saint-Célerin - Tél. : 02 44 68 35 16 - contact@ablogix.fr @ABlogiX

FLASHEZ CE CODE

APSSIS

84 rue du Luart
72160 Duneau

www.apssis.com

APSSIS
Association pour la Promotion de la Sécurité des Systèmes d'Information de Santé