Les consommateurs estiment que la protection de leurs données personnelles revient aux entreprises

	Les consommateurs estiment que la protection de leurs données personnelles revient aux entreprises

Les consommateurs sont de plus en plus conscients des risques de sécurité en ligne, mais tiennent les entreprises responsables de la violation des données. Tel est le constat dressé par Gemalto qui, pour parvenir à ce résultat, a interrogé 9 000 consommateurs en Australie, au Benelux, en France, en Allemagne, en Russie, aux Émirats Arabes Unis, en Arabie Saoudite, en Inde, au Japon, au Royaume-Uni et aux États-Unis. Au final, estiment ces derniers, 70% de la responsabilité de la protection et de la sécurisation des données des clients doit être attribuée aux entreprises, et 30% de cette responsabilité doit leur revenir.
Pourtant, moins d'un tiers des consommateurs interrogés (29%) pensent que les entreprises prennent très au sérieux la sécurisation de leurs données personnelles. Cela fait écho à la crainte du vol des données personnelles qui s'accentue : 58% des personnes interrogées pensent qu'elles seront les futures victimes d'un vol de données.
Plus de 4,8 milliards de données enregistrées ont été exposées depuis 2013, le vol d'identité étant le principal type de brèche de données. Il représente en effet 64% de l'ensemble des failles de données recensées.

Des comportements à risque
Si les répondants se montrent conscients des menaces auxquelles ils sont exposés en ligne, seulement une personne sur dix (11%) pense qu'aucune application ni aucun site Web ne peut présenter un quelconque risque direct pour eux. Ils ne semblent pour autant pas être enclins à adopter un changement d'attitude lorsqu'ils sont en ligne. Ainsi, 80% des répondants utilisent les médias sociaux, même si 59% d'entre eux pensent que ces réseaux présentent un grand risque. 87% utilisent les services bancaires en ligne ou mobiles, même si 34% estiment être vulnérables face aux cybercriminels. Ils sont également plus susceptibles de faire des achats en ligne pendant les périodes commerciales très chargées comme le « black friday » et Noël (2% d'augmentation en ligne contre -2% de baisse en magasin), bien que 21% d'entre eux admettent que la cybercriminalité augmente beaucoup pendant ces périodes.

Les attitudes des consommateurs face aux violations de données
Près de six consommateurs sur dix (58%) pensent qu'ils seront victimes d'une attaque à un moment ou à un autre, d'où la nécessité pour les organisations de se préparer aux conséquences pouvant être causées par de tels incidents. La majorité des utilisateurs en ligne prétendent qu'ils cesseraient d'utiliser un site de vente en ligne (60%), un site de banque en ligne (58%) ou un média social (56%) si l'un d'eux venait à subir une brèche. De même, 66% déclarent qu'ils seraient peu enclins à rester en contact avec une entreprise victime d'une attaque au cours de laquelle leurs données personnelles et financières auraient été volées.

Impact des violations de données sur les consommateurs
L'étude révèle également que l'utilisation frauduleuse d'informations financières a touché 21% des consommateurs, tandis que d'autres ont été victimes de l'utilisation frauduleuse de leurs données personnelles (15%) et de vol de données d'identité (14%). Plus d'un tiers (36%) de ceux ayant été exposés à une violation, attribuent celle-ci à un site Web frauduleux. Le clic sur un mauvais lien (34%) et le phishing (33%) sont les principaux pièges dans lesquels les consommateurs sont tombés. Concernant l'origine des attaques, plus d'un quart (27%) a attribué la violation à un échec des solutions de sécurité des données de l'entreprise.

Le manque de mesures de sécurité influe sur la confiance des consommateurs
Le manque de confiance des consommateurs pourrait s'expliquer par l'absence de mesures de sécurité efficaces mises en œuvre par les entreprises. Pour les services bancaires en ligne, le mot de passe reste encore la méthode d'authentification la plus courante – 84% des services bancaires en ligne et 82% des services bancaires mobiles y ont recours, suivi par des méthodes de sécurité avancée pour les transactions (respectivement 50% en ligne et 48% pour les services mobiles). Des solutions comme l'authentification à deux facteurs (43% en ligne et 42% sur mobile) et le chiffrement des données (31% en ligne et 27% mobile) viennent compléter le tableau.
Des résultats similaires peuvent être observés dans le retail, avec seulement 25% des répondants ayant des comptes clients en ligne affirmant que l'authentification à deux facteurs est utilisée sur toutes les applications et sites Web, et sur les réseaux sociaux, et 21% utilisent l'authentification pour toutes les plates-formes. Seulement 16% des personnes interrogées ont admis avoir une compréhension complète de ce qu'est le chiffrement de données….[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les consommateurs estiment que la protection de leurs données personnelles revient aux entreprises