

## **Une enquête internationale conduite par Gemalto souligne l'impact des failles de données sur la confiance et la fidélisation des consommateurs**

*Près des deux tiers des consommateurs ne souhaitent pas poursuivre leurs relations avec des sociétés dont les informations financières ont été piratées en raison d'une faille de données*

**Amsterdam, le 10 décembre 2015** – Près des deux tiers (64 %) des consommateurs dans le monde reconnaissent qu'ils ne sont nullement enclins à contacter ou à travailler à nouveau avec une société ayant subi une faille de leurs données impliquant le vol d'informations financières. Près de la moitié (49 %) expriment la même opinion lorsqu'il s'agit d'une brèche de données affectant des informations personnelles. C'est ce que révèle une enquête internationale récemment réalisée pour le compte de Gemalto (Euronext NL0000400653 GTO), leader mondial de la sécurité numérique, intitulée : « Broken Trust: 'Tis the Season to Be Wary » (Confiance rompue : soyons vigilants). Cette enquête a été réalisée auprès de 5 750 consommateurs dans sept pays : Allemagne, Australie, Brésil, États-Unis, France, Grande-Bretagne et Japon.

### **Constatations clés**

Les résultats de l'enquête sont d'autant plus révélateurs qu'à l'approche des fêtes de fin d'année, les consommateurs se font plus nombreux dans les magasins et les boutiques pour effectuer leurs achats. Six personnes sur dix (59 %) estiment en effet que la menace qui pèse sur leurs données personnelles s'accroît pendant les périodes de fête, et deux sur dix (18 %) estiment qu'elles peuvent être victimes d'une faille de données pendant cette période particulière de l'année.

### **Un faible niveau de confiance**

Seul un quart (25 %) des personnes interrogées jugent que les sociétés prennent suffisamment au sérieux la protection et la sécurité des données clients. Deux fois plus de personnes estiment que la responsabilité de la protection et de la sécurité de ces données incombe à la société (69 %) plutôt qu'au client lui-même (31 %). Parmi les personnes salariées interrogées, les deux cinquièmes uniquement (38 %) estiment que leur employeur prend les mesures de protection et de sécurité qui s'imposent en la matière.

### **Des consommateurs échaudés**

L'enquête fait également apparaître que 31 % des consommateurs ont déjà été affectés dans le passé par des failles de données. Quatre personnes sur dix pensent que les causes les plus probables conduisant à un incident de cet ordre ont pour origine la consultation d'un site frauduleux (42 %), le piratage par phishing (40 %), ou un clic imprudent sur le lien d'un site frauduleux (37 %). L'impact émotionnel des failles de données se traduit également par un sentiment d'appréhension à l'égard des sociétés, avec près d'un cinquième (19 %) des personnes craignant d'en être les victimes dans les douze à trente-six mois à venir.

90 % des consommateurs interrogés estiment que certaines applications et certains sites Web présentent un risque significatif pour la protection et la sécurité de leurs données personnelles. 55 % estiment que ce sont les sites de réseaux sociaux qui les exposent aux risques les plus notoires, et environ deux consommateurs sur cinq pensent que les contenus pour adultes et les appli/sites Web de type « Torrent » constituent le risque le plus sérieux pour la sécurité des données personnelles.

### **Une impatience croissante face à l'insécurité**

Environ un quart (23 %) des personnes interrogées ayant été victimes d'une faille de données ont envisagé dans le passé, ou envisageraient dans l'avenir, d'intenter une action en justice à l'encontre de la société impliquée dans l'exposition de leurs données personnelles. Près de la moitié (49 %) des personnes interrogées reconnaissent qu'elles intenteraient, ou envisageraient d'intenter, une action en justice à l'encontre des parties impliquées dans l'exposition de leurs données personnelles.

### **Privilégier une sécurité à double facteur**

Le consommateur n'est pourtant pas totalement exempt de responsabilité. Malgré les nombreux risques encourus, l'enquête montre également qu'une majorité (54 %) des personnes interrogées utilise le même mot de passe pour un grand nombre, voire la totalité, de ses comptes en ligne. Dans le cas des personnes interrogées qui utilisent souvent les réseaux sociaux, seul un quart (25 %) prend la peine d'utiliser une authentification à deux facteurs pour sécuriser l'ensemble des comptes. Parmi les personnes interrogées qui effectuent régulièrement des opérations bancaires en ligne ou via leur mobile, les trois cinquièmes environ (58 %) précisent que leurs banques utilisent une procédure d'authentification à deux facteurs pour sécuriser les transactions. Ces imprudences de comportement ne sont toutefois pas aussi répandues au sein de la grande distribution. Parmi les personnes interrogées qui utilisent activement des comptes de grande distribution, une sur quatre (25 %) précise que tous les sites Web / applications en ligne utilisés requièrent une authentification à deux facteurs pour assurer la sécurité des transactions.

*« La médiatisation des failles de données massives survenant de temps à autre n'incite nullement les consommateurs à faire confiance aux mesures de protection des données censées être assurées par les sociétés, grandes ou petites », explique Jason Hart, vice-président et directeur de la Technologie en charge du pôle Protection des Données, chez Gemalto. « Le fait que les salariés eux-mêmes n'ont pas le sentiment que leurs employeurs prennent avec le sérieux qui s'impose la protection de leurs données personnelles, constitue un indéniable signal d'alarme. Soit les entreprises doivent renforcer leurs mesures de sécurité, soit elles doivent communiquer plus efficacement avec leurs clients si elles ont déjà mis en place de telles mesures »*

*« Avec la collecte de quantités de plus en plus importantes de données clients, et compte tenu de la diversité croissante de nos interactions numériques, il est clair qu'il y a de plus en plus d'informations stockées en ligne relatives à nos activités habituelles, à notre profil et à nos goûts personnels », poursuit Jason Hart. « Cette enquête prouve que l'état d'esprit actuel en matière de sécurité des données doit évoluer. Cela concerne aussi bien les entreprises que les consommateurs, qui doivent adopter des mesures de sécurité avancées, comme l'authentification à deux facteurs. Sinon, un nombre croissant de consommateurs s'éloignera des entreprises ne prenant pas suffisamment au sérieux la protection des données, pour se rapprocher d'entreprises et de commerces en qui ils pourront avoir confiance. »*

#### A propos de l'enquête

Gemalto a mandaté Vanson Bourne, spécialiste indépendant des études de marchés de technologies, pour réaliser l'enquête sur laquelle repose ce compte rendu. 5 750 consommateurs ont été interrogés en octobre et novembre 2015. 1 500 entretiens ont été réalisés au États-Unis, 500 au Brésil, et 750 dans chacun des pays suivants : Allemagne, Australie, France, Grande-Bretagne et Japon. Afin d'être qualifiés pour répondre à cette enquête, les consommateurs devaient utiliser activement des sites de banque en ligne/mobile, des comptes de réseaux sociaux ou des comptes en ligne pour la grande distribution.

#### **Références complémentaires**

- [Customer Loyalty and Data Breach Report](#)
- [Customer Loyalty and Data Breach Infographic](#)

À propos de Gemalto

Gemalto (Euronext NL0000400653 GTO) est le leader mondial de la sécurité numérique avec un chiffre d'affaires 2014 de 2,5 milliards d'euros et des clients de premier plan dans plus de 180 pays.

Dans un monde numérique de plus en plus interconnecté, Gemalto aide à établir des relations de confiance mutuelle. Des milliards de personnes à travers le monde veulent un mode et un cadre de

vie plus agréables et intelligents. Ils veulent être libres de communiquer, acheter, voyager, faire des transactions bancaires, se divertir et travailler – à tout moment et en tous lieux - de façon agréable et sûre. Dans ce monde mobile et numérique en évolution rapide et constante, nous donnons aux entreprises et aux administrations les moyens d'offrir une large gamme de services numériques pratiques et sûrs en sécurisant les transactions financières, les services mobiles, les « clouds » publics et privés, les systèmes d'e-santé, l'accès aux services d'e-gouvernement, l'« Internet des objets », et les systèmes de billettique et de transports.

Notre portefeuille unique, qui s'étend des logiciels cryptographiques embarqués dans une variété d'objets du quotidien, à nos plateformes de back-office extrêmement robustes et évolutives pour l'authentification, le cryptage et la gestion des identifiants numériques, est mis en œuvre par nos équipes qui assurent un service de niveau mondial. Présent dans 46 pays, Gemalto emploie plus de 14 000 salariés travaillant depuis 99 bureaux, 34 centres de personnalisation et de données et 24 pôles de Recherche et de Développement logiciel.

Pour plus d'informations, visitez nos sites

[www.gemalto.com/france](http://www.gemalto.com/france), [www.justaskgemalto.com](http://www.justaskgemalto.com), [blog.gemalto.com](http://blog.gemalto.com), ou suivez @GemaltoFrance sur Twitter

#### **Relations presse Gemalto :**

Philippe Benitez  
Amérique du Nord  
+1 512 257 3869

[philippe.benitez@gemalto.com](mailto:philippe.benitez@gemalto.com)

Peggy Edoire  
Europe et CEI  
+33 4 42 36 45 40

[peggy.edoire@gemalto.com](mailto:peggy.edoire@gemalto.com)

Vivian Liang  
Grande Chine  
+86 1059373046

[vivian.liang@gemalto.com](mailto:vivian.liang@gemalto.com)

Ernesto Haikewitsch  
Amérique latine  
+55 11 5105 9220

[ernesto.haikewitsch@gemalto.com](mailto:ernesto.haikewitsch@gemalto.com)

Kristel Teyras  
Moyen-Orient et Afrique  
+33 1 55 01 57 89

[kristel.teyras@gemalto.com](mailto:kristel.teyras@gemalto.com)

Pierre Lelievre  
Asie-Pacifique  
+65 6317 3802

[pierre.lelievre@gemalto.com](mailto:pierre.lelievre@gemalto.com)