ENQUÊTE CONSOMMATEURS 2018:

ATTITUDES ET COMPORTEMENTS A L'ÈRE DU PIRATAGE

INTRODUCTION

Les atteintes à la vie privée des consommateurs sont aujourd'hui des phénomènes récurrents. Ces failles de sécurité, comme le « snafu » Cambridge Analytica-Facebook et la fuite Google+, ont fait la une de l'actualité en 2018, avec pour toile de fond l'exposition d'informations personnelles de millions d'utilisateurs et une confiance ébranlée envers les grandes marques. De nombreux consommateurs se mettent à radicalement changer la façon dont ils interagissent en ligne avec les marques ; ils pensent que les entreprises doivent pleinement assumer la responsabilité de protéger leurs données. Ping Identity a interrogé plus de 3000 consommateurs aux États-Unis, au Royaume-Uni, en France et en Allemagne afin d'examiner leur attitude après un piratage de données et ainsi aider les entreprises à conserver la confiance et à anticiper les attentes de leurs clients.

RÉSULTATS CLÉS

- Une personne sur cinq (21 %) a été victime d'un piratage. Parmi elles, 34 % ont subi des pertes financières.
- Après un piratage de données, 78 % des utilisateurs envisagent de mettre un terme à leur relation avec la marque en ligne. En outre, près de la moitié (49 %) d'entre eux déclarent ne pas vouloir s'inscrire et utiliser un service ou une application en ligne si elles ont récemment subi un piratage de données.
- Plus de la moitié des consommateurs (56 %) ne veulent rien payer aux fournisseurs d'applications et de services en ligne pour une sécurité renforcée visant à protéger leurs informations personnelles.
- 59 % accordent la priorité à la protection de leurs informations personnelles lorsqu'ils interagissent avec une application ou un service en ligne, tandis que seulement 12 % accordent la priorité à une expérience utilisateur facile et confortable et 7 % à une interface personnalisée.

IMPACT D'UN PIRATAGE

À RETENIR

La grande majorité des personnes interrogées envisagent de mettre un terme à leur relation avec une marque après un piratage de données et placent la sécurité au cœur de leurs préoccupations. Plus de la moitié d'entre elles n'a pris aucune mesure pour sécuriser leurs données personnelles après un piratage. D'après les consommateurs, la sécurité relèverait donc de la responsabilité de l'entreprise plutôt que d'une responsabilité personnelle.

DONNÉES IMPORTANTES

- Une personne sur cinq (21 %) a été victime d'un piratage de données. Parmi elles, 34 % ont subi des pertes financières, dont 41 % entre 300 et 999 $.
- 78 % des consommateurs envisagent de mettre un terme à leur relation avec une marque en ligne (et 36 % envisagent de stopper toute relation avec la marque) s'ils ont récemment subi un piratage.
- Près de la moitié (49 %) d'entre eux déclarent ne pas vouloir s'identifier dans une application ou un service en ligne ayant récemment subi un piratage de données. Plus d'un tiers (37 %) accepteraient d'utiliser un service en ligne ayant récemment subi un piratage uniquement s'ils n'ont aucun autre moyen d'obtenir le service fourni.
- 47 % des utilisateurs ont changé la façon dont ils sécurisent leurs données personnelles suite à de récents piratages de données (tandis que 53 % n'ont pris aucune mesure). Voir Figures 1 et 2 ci-dessous.
- 54 % des personnes interrogées sont aujourd'hui davantage préoccupées par la protection de leurs informations

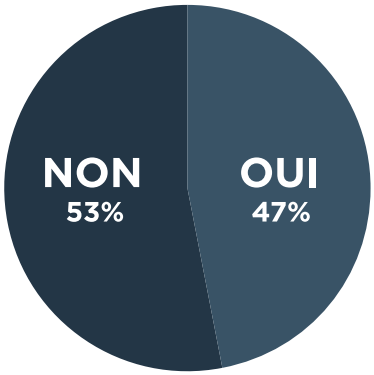

Figure 1

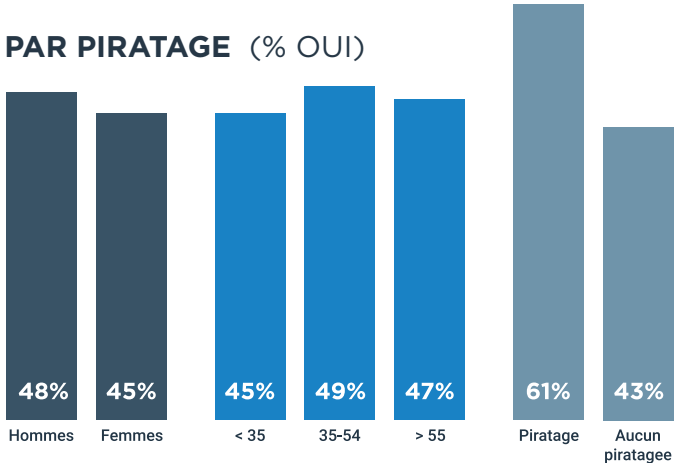

Figure 2

personnelles qu'il y a un an (2 % se déclarent moins préoccupées et 44 % déclarent que la situation leur semble identique à l'année précédente).

- Plus d'un quart (28 %) d'entre elles prévoient de changer la façon dont elles utilisent les réseaux sociaux pour se connecter après la révélation du cas Cambridge Analytica. Un tiers (32 %) ne changent pas la façon dont elles utilisent les réseaux sociaux pour se connecter après le cas Facebook/Cambridge Analytica.

QUI EST RESPONSABLE

À RETENIR

La majorité des personnes interrogées pensent que les marques ont pour obligation de protéger leur vie privée ; elles ne veulent pas payer plus pour la protection de leurs données personnelles. Alors que cette majorité ne veut rien payer aux fournisseurs de services/applications en ligne pour une sécurité renforcée, un quart seulement accepte de payer une petite somme. Par comparaison avec le nombre de personnes acceptant de payer pour garantir que leurs informations personnelles ne feront jamais l'objet d'un piratage (pas nécessairement à des fournisseurs de services et d'applications en ligne), leur volonté d'investir est légèrement plus élevée.

DONNÉES IMPORTANTES

- Plus de la moitié (56 %) des personnes interrogées ne veulent rien payer aux fournisseurs d'applications et de services en ligne pour une sécurité renforcée visant à protéger leurs informations personnelles ; un autre quart (24 %) ne veulent pas payer plus de 5 $ et 2 % acceptent de payer plus de 20 $. Voir Figure 3.

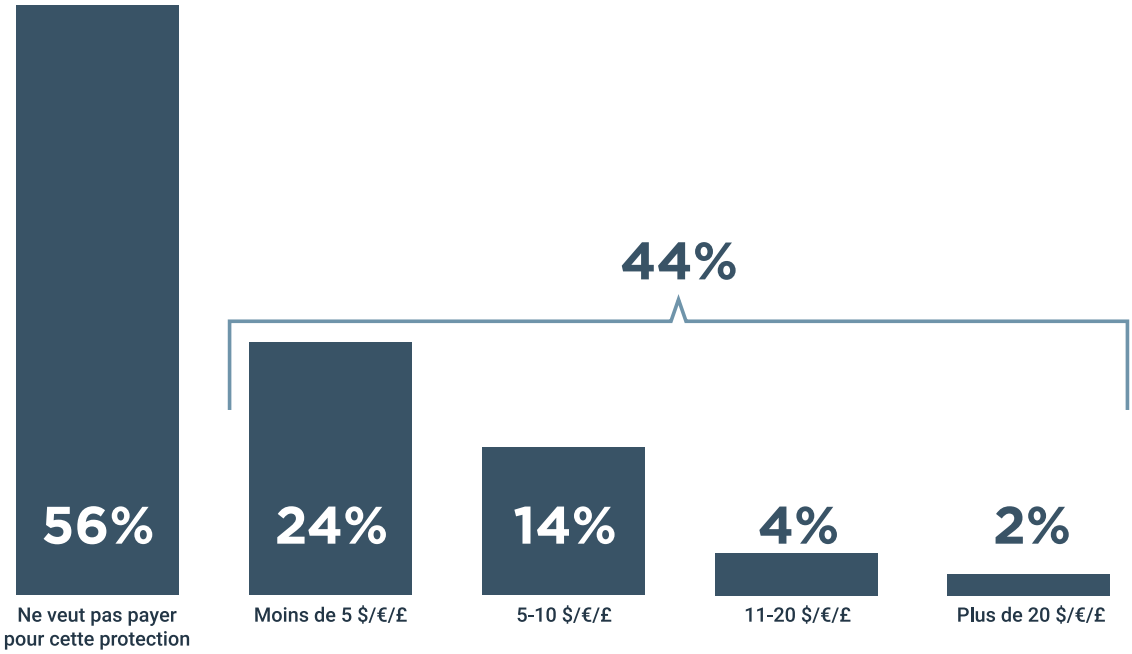

Figure 3

- 48 % des utilisateurs ne veulent rien payer pour garantir que leurs informations personnelles ne feront jamais l'objet d'un piratage ; 38 % acceptent de payer jusqu'à 49 $.

SÉCURITÉ CONTRE EXPÉRIENCE UTILISATEUR

À RETENIR

Les consommateurs déclarent accorder davantage d'importance à la sécurité qu'à une expérience utilisateur simple et personnalisée lors de l'interaction avec les marques, mais ils sont de plus en plus nombreux à choisir de se connecter à des sites web via leurs comptes de réseau social. L'importance des facteurs rapidité et simplicité dans le processus de connexion ne doit pas être sous-estimée, même si la sécurité a la priorité lors de l'interaction avec les marques.

DONNÉES IMPORTANTES

- 59 % accordent la priorité à la protection de leur identité et/ou de leurs informations personnelles lorsqu'ils interagissent avec une application ou un service en ligne ; 12 % accordent la priorité à une expérience utilisateur simple et confortable et 7 % à une interface personnalisée (22 % choisissent le coût [service gratuit plutôt que payant]). Voir Figure 4.

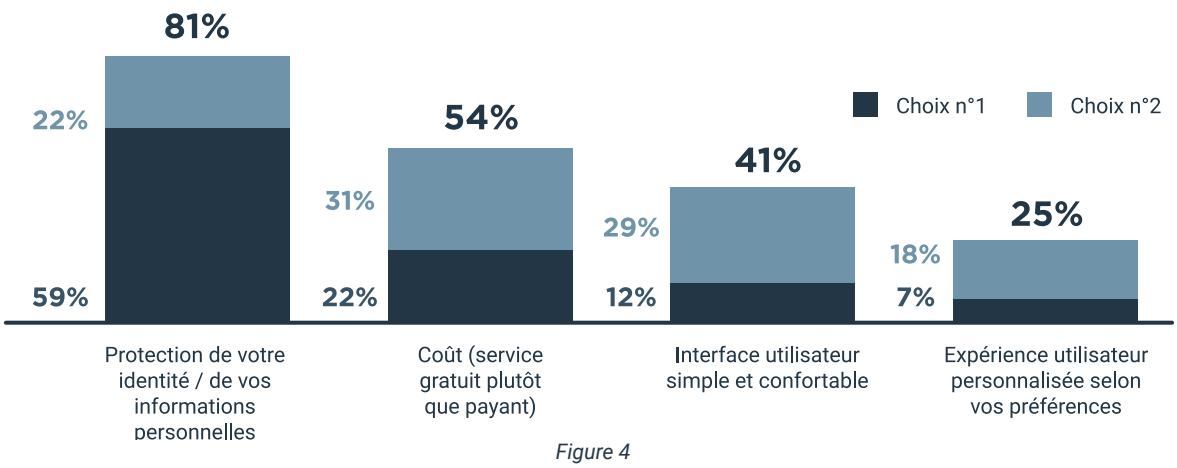

Figure 4

- Nom d'utilisateur et mot de passe restent la principale méthode de connexion pour 70 % des utilisateurs. 13 % des personnes interrogées utilisent l'authentification sociale comme principale méthode d'identification. Parmi celles qui s'identifient via leur compte de réseau social, 84 % procèdent ainsi parce que cette méthode est plus pratique (40 %) ou leur permet de gagner du temps (44 %).

Empreinte digitale et reconnaissance faciale sont appréciées mais leur utilisation reste anecdotique.

Les technologies émergentes comme l'utilisation des empreintes digitales ou de la reconnaissance faciale pour l'identification gagnent en popularité, mais la disparition des mots de passe n'est pas pour demain. Il convient donc d'informer les consommateurs sur les avantages de l'identification biométrique.

- 51 % pensent que les technologies d'identification comme les empreintes digitales et la reconnaissance faciale sont plus fiables que le couple nom d'utilisateur mot de passe (40 % pensent que leur fiabilité est équivalente). Seules 10 % des personnes interrogées utilisent la technologie biométrique (empreinte digitale et reconnaissances faciale) comme principale méthode d'identification, probablement parce qu'il s'agit d'une technologie émergente qui n'est pas proposée par la majorité des plates-formes.

SPOTLIGHT: RÉPARTITION PAR ÂGE

MOINS DE 35	PLUS DE 55
Confiance envers les marques relativement élevée • 53 % ont confiance ou pleinement confiance en la capacité des fournisseurs de services et d'applications à protéger leurs informations personnelles.	**Confiance envers les marques relativement faible** • 27 % seulement ont confiance ou pleinement confiance en la capacité des fournisseurs de services et d'applications à protéger leurs données personnelles.
Plus insouciants envers leurs données personnelles sensibles • 54 % acceptent de saisir leurs coordonnées bancaires sur un site web ou dans une application mobile.	**Protègent mieux leurs données personnelles sensibles** • 41 % acceptent de saisir leurs coordonnées bancaires sur un site web ou dans une application.
Plus susceptibles de subir des pertes financières suite à un piratage de données • 41 % ont subi des pertes financières suite à un piratage de données.	**Moins susceptibles de subir des pertes financières suite à un piratage de données** • 27% ont subi des pertes financières suite à un piratage de données.
Plus susceptibles de dépenser davantage pour garantir la protection de leurs données personnelles • 42 % ne veulent pas payer plus cher des applications et services en ligne pour une sécurité renforcée visant à protéger leurs données personnelles. • 37 % ne veulent rien payer pour garantir que leurs données personnelles ne feront jamais l'objet d'un piratage. • 42 % acceptent de payer entre 1 et 49 $ pour garantir que leurs données personnelles ne feront jamais l'objet d'un piratage.	**Moins susceptibles d'investir davantage pour garantir la protection de leurs données personnelles** • 75% ne veulent pas payer plus cher des applications et services en ligne pour une sécurité renforcée visant à protéger leurs données personnelles. • 62% ne veulent rien payer pour garantir que leurs données personnelles ne feront jamais l'objet d'un piratage. • 32% acceptent de payer entre 1 et 49 $ pour garantir que leurs données personnelles ne feront jamais l'objet d'un piratage.
Après Cambridge Analytica, Facebook Connect perd un nombre important d'utilisateurs, tous âges confondus. • 37 % éviteront d'utiliser Facebook Connect pour s'identifier dans des applications et services en ligne. Dans une moindre mesure par rapport à l'ancienne génération, Facebook Connect perdra tout de même un tiers de sa clientèle.	**Après Cambridge Analytica, Facebook Connect perd un nombre important d'utilisateurs, tous âges confondus.** • 56% éviteront d'utiliser Facebook Connect pour s'identifier dans les applications et services en ligne.
Plus ouverts en matière d'adoption des technologies biométriques • 46 % utilisent la biométrie (empreinte digitale ou reconnaissance faciale) pour s'identifier dans les applications et services en ligne.	**Moins ouverts en matière d'adoption des technologies biométriques** • 13% utilisent la biométrie (empreinte digitale ou reconnaissance faciale) pour s'identifier dans des applications et services en ligne.

POINT CLÉ : RÉPARTITION PAR PAYS

Adeptes du partage :

Plus susceptibles de partager leurs données personnelles avec les marques que ceux d'autres pays, notamment :

- Numéro de sécurité sociale (16 % USA contre 9 % France, 6 % Allemagne, 4 % Royaume Uni)
- Numéro de carte de crédit (40 % USA contre 36 % France, 26 % Royaume Uni, 13 % Allemagne)

Gros acheteurs — de services, pas de sécurité :

- Les Américains payent plus pour des applications et des services en ligne (ex. Spotify, Netflix, etc.), que dans les autres pays (62 % payent pour des services/applications aux USA contre 53 % Royaume Uni, 49 % Allemagne, 47 % France).
- Les Américains sont les moins disposés à payer pour mettre leurs informations personnelles à l'abri d'un piratage de données (36 % USA contre 46 % Allemagne, 54 % Royaume Uni, 60 % France).

Faible niveau de confiance :

- Les Français sont les moins convaincus de la capacité des fournisseurs de services et d'applications à protéger leurs données personnelles (38 % seulement font confiance/pleinement confiance aux fournisseurs contre 48 % USA, 48 % Royaume Uni, 42 % Allemagne).

Moins susceptibles de subir un piratage :

- Les consommateurs au Royaume-Uni (15 %) sont moins susceptibles de subir un piratage de données qu'aux USA (27 %), en France (21 %) ou en Allemagne (17 %). Toutefois, parmi les utilisateurs ayant subi un piratage de données, 42 % ont essuyé des pertes financières (contre 24 % aux USA, 38 % en Allemagne et 43 % en France).

Ne veulent pas payer plus pour la sécurité :

- Les utilisateurs au Royaume-Uni sont les moins disposés à payer plus cher des applications/services en ligne pour une sécurité renforcée visant à protéger leurs données personnelles (64 %) contre les utilisateurs en France (61 %), en Allemagne (52 %) et aux USA (48 %).

Abandon de Facebook Connect :

- Les Allemands adoptent une position plus dure lorsqu'il s'agit de changer leurs comportements suite à Cambridge Analytica. 50 % d'entre eux n'utiliseront plus Facebook Connect pour s'identifier dans les applications et les services en ligne suite à cette attaque (contre 42 % USA, 41 % France et 39 % Royaume Uni).

CONCLUSION

Les piratages de données et les problèmes de confidentialité sont plus omniprésents que jamais et les marques courent le risque de perdre des clients, et au final de voir leurs revenus baisser, si la sécurité n'est pas au centre de leur stratégie. Étant donné que la majorité des utilisateurs ne veulent pas payer pour une sécurité renforcée visant à protéger leur identité en ligne, les entreprises doivent les protéger par défaut. De même que les consommateurs attendent des marques qu'elles fournissent des expériences personnalisées et conviviales, les entreprises doivent comprendre la valeur et l'importance d'une stratégie solide de gestion des identités et montrer aux consommateurs les mesures prises pour garantir la sécurité de leurs identités en ligne.

Pour en savoir plus sur la manière dont la gestion des accès et des identités peut vous aider à protéger les données personnelles de vos clients, rendez-vous sur pingidentity.fr.

MÉTHODOLOGIE

Ping Identity a demandé à MarketCube de réaliser une enquête auprès de 3264 consommateurs aux États-Unis, au Royaume-Uni, en France et en Allemagne, âgés d'au moins 18 ans et qui utilisent au moins un de ces sites ou services en ligne : distribution, banque, films/TV, musique, services publics, voyages ou applications de type Uber/Lyft. Par ailleurs, les participants à l'enquête ont dû saisir au moins l'un des éléments suivants sur un site web ou une application au cours des 12 derniers mois : adresse, date de naissance, numéro de téléphone, numéro de carte de crédit, coordonnées bancaires, numéro de sécurité sociale ou numéro de permis de conduire. La répartition géographique des personnes interrogées est la suivante : USA - 1004, Royaume Uni - 753, France - 754 ; Allemagne - 753. L'enquête a été réalisée en ligne entre le 21 et le 25 mai 2018. La marge d'erreur est plus ou moins 1,7 pour cent.

#3375 (FR) | 11.18 | v001