ENQUÊTE CONSOMMATEURS 2019 :

CONFIANCE ET RESPONSABILITÉ À L'ÈRE DE LA MAUVAISE UTILISATION DES DONNÉES

INTRODUCTION

La confidentialité et la sécurité des données occupent une place de plus en plus importante au sein de l'expérience en ligne moderne. Au niveau mondial, on bombarde les consommateurs avec des gros titres sur la mauvaise utilisation généralisée des données, pourtant les failles de sécurité à grande échelle continuent à se développer. Pour mieux comprendre comment cet environnement mouvementé affecte les relations des consommateurs avec leurs fournisseurs de services, mais aussi le comportement des consommateurs en matière de sécurité en général, Ping Identity a récemment interrogé plus de 4 000 personnes aux États-Unis, au Royaume-Uni, en Australie, en France et en Allemagne.

Les résultats montrent que les consommateurs n'ont plus confiance dans la capacité des entreprises à protéger leurs informations en ligne, et qu'ils sont prêts à tenir ces organisations pour responsables des failles de sécurité et autres atteintes à leur confiance, telles que le non respect de la confidentialité de leurs données. Mais les consommateurs présentent aussi un manque général de compréhension des risques auxquels ils sont exposés, et une connaissance limitée des bonnes pratiques à suivre pour protéger leurs données en ligne. Cet état d'esprit et les actions contradictoires les exposent au risque d'être au final moins protégés.

RÉSULTATS CLÉS

- **81 % des personnes interrogées cesseraient de s'engager avec une marque sur le web à la suite d'une fuite de données,** soit un peu plus qu'en 2018 (78 %), dont 25 % qui cesseraient d'interagir totalement avec cette marque.
- **63 % des personnes interrogées ont déclaré qu'une entreprise est responsable de la protection des données des utilisateurs,** y compris lorsque les utilisateurs sont victimes de phishing ou utilisent des connexions Wi-Fi non chiffrées.
- **Plus de la moitié (55 %) des personnes interrogées ont déclaré qu'une entreprise qui partage leurs données personnelles sans leur autorisation a plus de chances que tout autre scénario de les dissuader d'utiliser les produits de cette marque,** même plus qu'une fuite de données (27 %).
- **Près de la moitié (47 %) des personnes interrogées ont déjà laissé quelqu'un d'autre utiliser leur mot de passe pour accéder à un service de divertissement ou de e-commerce.** De plus, près d'un quart (24 %) de ce groupe a déclaré qu'ils sont susceptibles de réutiliser ces mêmes mots de passe de sites de divertissement ou e-commerce pour un site pouvant contenir des informations plus personnelles, comme une messagerie électronique ou un compte en banque.
- **65 % des personnes interrogées sont frustrées par leurs expériences de connexion,** ce qui n'est pas surprenant si l'on considère que le même pourcentage de personnes a eu son compte bloqué plusieurs fois en un an. Cette frustration pousse à agir : Un tiers (33 %) des personnes interrogées ont cessé d'utiliser un terminal, une application ou un service ou ont laissé un mauvais commentaire à la suite d'une expérience de connexion peu pratique.

LES CONSOMMATEURS TIENNENT LES ENTREPRISES POUR RESPONSABLES DE LA SÉCURITÉ DE LEURS DONNÉES

À RETENIR

Au cours des dernières années, la sécurité des données est devenue une préoccupation majeure pour les consommateurs. Aujourd'hui, les gens considèrent que les entreprises sont les seules responsables de la protection de leurs données et n'hésitent pas à leur demander des comptes. Les fuites de données poussent de plus en plus les gens à modifier leurs relations avec les entreprises ayant été affectées, et un nombre croissant de personnes se désengagent totalement à la suite d'une fuite. Les résultats ci-dessous montrent à quel point une fuite de données peut dissuader des clients potentiels de s'engager avec une marque, affectant ce faisant le chiffre d'affaires de cette entreprise.

DONNÉES IMPORTANTES

PRÉOCCUPATIONS CROISSANTES EN MATIÈRE DE SÉCURITÉ

- 49 % des personnes interrogées ont déclaré qu'elles étaient davantage préoccupées par la protection de leurs informations personnelles aujourd'hui qu'il y a un an, tandis que 49 % sont aussi inquiètes que l'année dernière.

- C'est aux États-Unis que le pourcentage d'anxiété est le plus élevé, car 60 % de personnes sont indiqué être plus inquiètes que l'année dernière, contre moins de 50 % dans les autres pays.

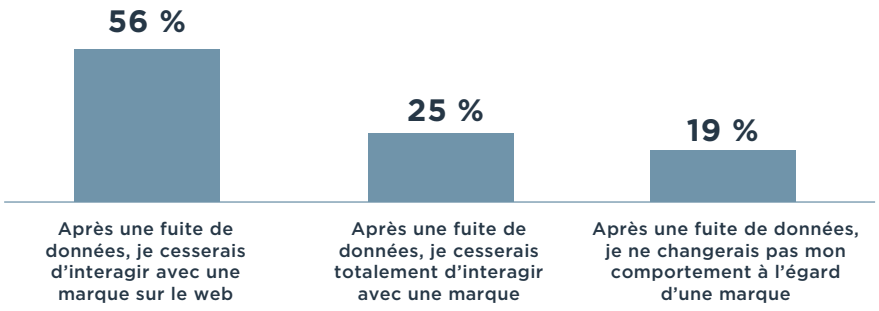
LES ENJEUX SONT ÉLEVÉS POUR LES ENTREPRISES PIRATÉES

- 63 % des personnes interrogées ont déclaré qu'une entreprise est **toujours** responsable de la protection des données des utilisateurs, y compris lorsque les utilisateurs sont victimes de phishing ou ont des pratiques non sûres telles que des connexions wifi non chiffrées ou la réutilisation de mots de passe. Dans bon nombre de ces cas, les entreprises seront tenues pour responsables y compris si elles n'auraient rien pu faire pour l'éviter.

- Seulement 14 % des personnes interrogées seraient prêtes à s'inscrire à et à utiliser une application/un service à la suite d'une fuite de donnée.

- 81 % cesseraient de s'engager avec une marque sur le web à la suite d'une fuite (3 % de plus qu'en 2018), et 25 % cesseraient simplement tout type d'interaction.

Que feriez-vous à une marque ayant subi une fuite de données ?



LES QUESTIONS DE SÉCURITÉ ET DE CONFIDENTIALITÉ DES DONNÉES AUGMENTENT LE MANQUE DE CONFIANCE DE LA PART DES CONSOMMATEURS

SÉCURITÉ = PROTÉGEZ-MOI

Ne laissez pas les gens voler mes données.

CONFIDENTIALITÉ = RESPECTEZ-MOI

Ne vendez pas et ne partagez pas mes données sans mon consentement.

À RETENIR

La confiance dans la capacité des entreprises à protéger les données personnelles et la vie privée est en déclin. C'est aux réseaux sociaux que l'on accorde le moins de confiance, mais les services financiers et les entreprises du secteur de la santé, qui détiennent les données les plus précieuses, ont également leurs lots de cyniques en matière de sécurité. Le fait que l'on n'accorde pas plus de confiance aux banques est assez surprenant, compte tenu de la réputation qu'elles ont d'être à la pointe de la sécurité. Pour ce qui est des entreprises du secteur de la santé, il est probable que les attaques par demande de rançon affectant les hôpitaux tirent la confiance des consommateurs vers le bas.

DONNÉES IMPORTANTES

CONFIANCE DES CONSOMMATEURS PAR SECTEUR

- Les réseaux sociaux sont le secteur auquel le moins de confiance est accordée parmi cinq grands secteurs, avec seulement 28 % de personnes déclarant avoir confiance dans la capacité de ces plateformes à protéger leurs informations personnelles, ce qui n'est pas surprenant compte tenu des problèmes en matière de respect de la vie privée ayant eu lieu ces dernières années.

- Moins des deux tiers des personnes ont confiance en la capacité des services financiers à protéger leurs données (63 %), soit légèrement plus que pour les services de santé (61 %).

- L'hôtellerie et le retail se situent au milieu des secteurs mentionnés, avec 38 % des consommateurs faisant confiance à l'hôtellerie et 36 % au retail.

PRÉOCCUPATIONS CROISSANTES EN MATIÈRE DE TECHNOLOGIE

- Parmi trois questions clés, à savoir la sécurité des données, l'exploitation des données en ligne et l'accès aux comptes en ligne, la majorité (57 %) des personnes interrogées a déclaré être plus inquiète pour la sécurité des données en ligne, suivie par (25 %) plus inquiète par le fait que les entreprises exploitent leurs données à des fins promotionnelles ou publicitaires. Ceci, comparé à seulement 12 % surtout inquiètes de ne pas pouvoir accéder rapidement et facilement à leurs comptes, et 5 % qu'aucune de ces questions n'inquiète.

- Les gens s'attendent à ce que les problèmes de confidentialité empirent : 39 % ont placé la confidentialité des données comme inquiétude technologique numéro un pour l'année à venir, au-dessus de la sécurité, de la surveillance, de la désinformation en ligne ou de l'automatisation.

- Les gens sont davantage gênés par les entreprises qui abusent de leurs données que par le fait d'être piratés : 54 % ont déclaré que le fait de partager leurs données sans leur autorisation a plus de risques d'endommager leur perception de cette organisation qu'un piratage (29 %).

Il est intéressant de noter que l'Allemagne se trouve à un niveau plus élevé que les autres pays concernant les préoccupations relatives à la surveillance, tandis que les États-Unis sont plus hauts pour la confidentialité des données. En réalité, les personnes interrogées provenant de pays situés dans l'Union européenne (Royaume-Uni, Allemagne et France) étaient moins inquiètes que celles provenant des États-Unis et de l'Australie concernant la confidentialité des données, ce qui montre probablement l'impact du RGPD.

LA CONFIDENTIALITÉ L'EMPORTE SUR LE CONFORT (ET MÊME SUR LA SÉCURITÉ)

À RETENIR

Les consommateurs s'orientent vers les techniques et pratiques de sécurisation des données qu'ils considèrent être les plus sûres, plutôt que de choisir l'option la plus pratique. Mais la confidentialité est la plus grande priorité, puisque les consommateurs renoncent aux options qu'ils considèrent les plus sécurisées lorsque celles-ci posent des problèmes en termes de confidentialité. Malgré cela, les consommateurs continuent d'être frustrés par leurs expériences de connexion et par le fait d'avoir leur compte en ligne bloqué, et n'hésitent pas à agir lorsqu'ils sont confrontés à une expérience de connexion peu pratique.

DONNÉES IMPORTANTES

LA SÉCURITÉ, LA CONFIDENTIALITÉ ET LA COMMODITÉ : CLASSEMENT

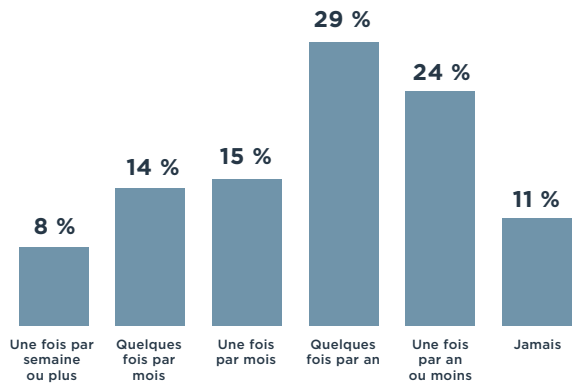
- Parmi les préoccupations relatives à la sécurité, les gens choisissent la sécurité à la commodité, et priorisent la confidentialité par-dessus tout.
- L'authentification multifacteur a été classée comme méthode de connexion la plus sécurisée par les personnes interrogées, et elle figure également parmi les méthodes les plus largement diffusées.
- L'utilisation d'un mot de passe fort et unique pour chaque compte a été classé comme troisième option la plus sécurisée, et elle se place au même niveau que l'authentification multi-facteurs parmi les méthodes les plus utilisées. Le manque de commodité a cependant été cité comme inhibiteur fréquent : 38 % de ceux qui n'utilisent pas un mot de passe fort et unique ont déclaré que cela n'était pas pratique, et 30 % de ceux qui n'utilisent pas l'authentification multi-facteur ont déclaré que cela n'était pas pratique.
- Lorsqu'il s'agit de choisir une méthode de connexion, les consommateurs font passer les questions de confidentialité avant la sécurité. La biométrie, par exemple, a été classée comme deuxième méthode de connexion la plus sécurisée et comme la deuxième méthode en termes de commodité. Toutefois, 49 % des personnes interrogées indiquent que la reconnaissance faciale les inquiète en termes de confidentialité, alors qu'il s'agit d'une forme courante de technologie, et la biométrie n'est utilisée que par 31 % des personnes interrogées.

    > Parmi les personnes que la reconnaissance faciale inquiète en termes de confidentialité, les principales inquiétudes sont liées au fait que l'appli partagera leurs informations avec d'autres et au fait que le gouvernement les utilise à des fins de surveillance.

PROBLÈMES RELATIFS À LA CONNEXION

- Alors que la commodité n'est plus une priorité pour les consommateurs, une majorité d'entre eux (65 %) sont toujours frustrés par les expériences de connexion.
- 65 % des personnes interrogées indiquent qu'elles ont dû changer leur mot de passe après le blocage de leur compte au moins quelques fois par an ou plus, ceci arrivant à 22 % au moins une fois par mois.
- Un tiers (33 %) des personnes interrogées ont cessé d'utiliser un terminal, une application ou un service ou ont laissé un mauvais commentaire à la suite d'une expérience de connexion peu pratique.

À quelle fréquence changez-vous votre mot de passe à la suite du blocage d'un compte (par ex. Suite à l'oubli de votre mot de passe ?)



LES CONSOMMATEURS CONTINUENT D'ADOPTER DES PRATIQUES DE SÉCURITÉ RISQUÉES

À RETENIR

Malgré de fortes préoccupations en termes de sécurité et de confidentialité, les consommateurs continuent à faire des choix risqués concernant leur sécurité. En général, les plus jeunes générations prennent plus de risques avec leur sécurité. Étant donné que les entreprises sont souvent accusées de fraude et de fuites de données, y compris si celles-ci résultent de choix potentiellement peu sûrs des consommateurs, les entreprises doivent aller plus loin encore pour protéger les données de leurs clients.

DONNÉES IMPORTANTES

PRINCIPALES ERREURS EN MATIÈRE DE SÉCURITÉ

- 43 % des personnes interrogées ne conservent pas un mot de passe fort et unique pour chaque compte.
- Près de la moitié (47 %) des personnes interrogées ont déjà laissé quelqu'un d'autre utiliser leur mot de passe pour accéder à un service de divertissement ou de e-commerce, et 18 % le font souvent. Près d'un quart (24 %) de ceux qui ont déjà partagé un mot de passe sont susceptibles d'utiliser ce même mot de passe pour se connecter à un service permettant d'accéder à des informations plus personnelles, telles qu'une messagerie électronique ou un compte en banque.
- Un quart (26 %) des gens ne changent pas leurs mots de passe pour un service en ligne immédiatement après le piratage d'un fournisseur de services.

LES MAUVAISES HABITUDES VARIENT EN FONCTION DE L'ÂGE

Les baby boomers sont les moins susceptibles de partager leurs mots de passe (seulement 20 %), tandis que 71 % de la génération Z et 58 % de la génération Y le font.

Parmi ceux qui réutilisent leurs mots de passe, les plus grands contrevenants sont la génération Z (34 %) et la génération Y (31 %).

LA DÉCONNEXION : LES PENSÉES ET LES ACTES DES CONSOMMATEURS NE COÏNCIDENT PAS TOUJOURS

- Les gens sous-estiment la difficulté de conserver un mot de passe unique et fort pour chaque compte (ou surestiment leur capacité à bien le faire).
  - > 46 % placent cela en deuxième position en termes de commodité, avant la biométrie, le gestionnaire de mot de passe et les options de single sign-on, qui, en pratique, sont plus faciles à utiliser et à gérer.
  - > Cela malgré le fait que 65 % des personnes interrogées indiquent avoir dû changer leur mot de passe au moins quelques fois par an après le blocage de leur compte, ce qui signifie qu'elles sont peut-être trop sûres de leur capacité à se souvenir de mots de passe uniques pour chaque compte.

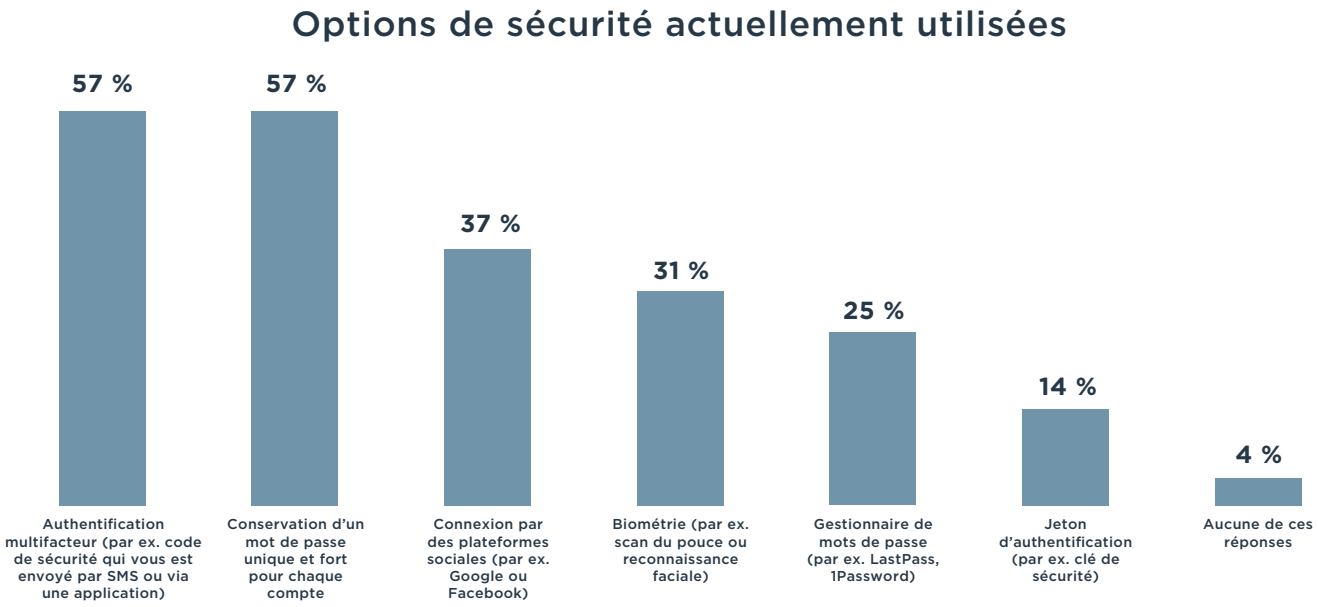
POURQUOI CE MANQUE DE CONNAISSANCES SUR LA SÉCURITÉ ?

À RETENIR

Les incompréhensions et le manque de connaissances signifient que les consommateurs continuent d'avoir des pratiques risquées en termes de sécurité, bien que celle-ci les inquiète beaucoup. Les gens ne connaissent pas plusieurs options de connexion sécurisées, ou ne savent pas comment on les utilise.

ANGLES MORTS DE LA SÉCURITÉ

- L'authentification multifacteur est classée comme option de connexion la plus sécurisée ou seconde option la plus sécurisée par 56 % des personnes interrogées. Pourtant, 43 % d'entre elles ne l'utilisent pas actuellement. Parmi celles qui ne l'utilisent pas, 16 % ne savent pas comment l'utiliser, 19 % pensent qu'ils n'y ont pas accès et 11 % n'en ont jamais entendu parler.
- Seulement 25 % des personnes interrogées utilisent actuellement un gestionnaire de mots de passe. Parmi celles qui n'en utilisent pas, 22 % ne savent pas utiliser cette méthode de connexion, tandis que 17 % n'en ont jamais entendu parler.
- Les jetons d'utilisation sont les moins utilisés et ceux qu'on comprend le moins. Seulement 14 % des personnes interrogées indiquent utiliser cette option, et parmi celles qui ne l'utilisent pas, 20 % n'ont jamais entendu parler de jetons d'authentification et 24 % ne savent pas comment les utiliser.



Les gens font davantage confiance aux mots de passe qu'aux autres mesures de sécurité qui sont en réalité moins susceptibles d'être contournées ou corrompues. Par exemple, les personnes interrogées ont placé le fait d'avoir un mot de passe unique et fort pour chaque compte comme plus sécurisé que l'utilisation d'un jeton d'authentification ou d'un gestionnaire de mots de passe. En réalité, les pratiques de mots de passe risquées constituent le fondement des raisons pour lesquelles les failles peuvent créer autant de dommages. Non seulement les pratiques des consommateurs sont laxistes, mais les mots de passe sont faciles à déchiffrer en utilisant des outils automatisés. La réutilisation de mots de passe permet aux malfaiteurs de pénétrer facilement sur d'autres site web et d'autres comptes utilisateurs.

CONCLUSION

Les consommateurs, où qu'ils soient, attendent toujours plus des entreprises dès qu'il s'agit de confidentialité et de sécurité des données. En même temps, la confiance que les consommateurs ont dans la capacité des entreprises à protéger leurs données et leur vie privée est faible, et leurs propres pratiques et comportements en termes de sécurité sont loin d'être parfaits. Pour ce qui est des entreprises qui adoptent les nouvelles réalités du paysage numérique actuel post-failles, il n'y a jamais eu de meilleures occasion de gagner la confiance et la fidélité des clients, et cela commence par le fait de trouver le juste milieu entre confidentialité, sécurité et commodité.

Pour en savoir plus sur la manière dont la gestion de l'identité et des accès peut vous aider à protéger les données de vos clients sans sacrifier la commodité, rendez-vous sur pingidentity.com.

MÉTHODOLOGIE

Ping Identity a mandaté Market Cube pour réaliser une enquête sur 4 017 consommateurs aux États-Unis, au Royaume-uni, en Australie, en France et en Allemagne, âgés de plus de 18 ans et utilisant au moins l'un des sites ou services en ligne : shopping en ligne, banque en ligne, services cinéma/TV en ligne, services musicaux, services gouvernementaux, sites de voyage ou sites de transports. De plus, les personnes interrogées devaient avoir saisi au moins l'un des éléments suivants sur un site web ou une appli au cours des 12 derniers mois : adresse, date de naissance, numéro de téléphone, numéro de carte bancaire, informations bancaires, numéro de sécurité sociale ou numéro de permis de conduire. La répartition géographique des personnes interrogées est la suivante : États-Unis : 1 004, Royaume-Uni : 753, Australie : 755, France : 751, Allemagne : 754. Cette enquête a été réalisée en ligne entre le 31 juillet et le 6 août 2019. La marge d'erreur est plus ou moins de 1,6 points de pourcentage.

#3464 | 10.08.19 | v003