THALES
Building a future we can all trust

#2025TRUSTINDEX

2025

En partenariat avec
kuppingercole
ANALYSTS

DIGITAL TRUST INDEX

Comprendre l'impact des expériences numériques sur la confiance des utilisateurs

Résumé

La relation qui lie un service web à ses utilisateurs repose sur la confiance. Elle se bâtit au prix de nombreux efforts mais peut s'effriter en un instant. L'an dernier, le Digital Trust Index s'intéressait déjà à l'équilibre fragile entre fluidité de l'expérience utilisateur, sécurité et respect de la vie privée, trois piliers essentiels de la confiance accordée à une marque. Les résultats de cette année marquent un tournant : désormais, les utilisateurs semblent porter une grande partie de ce contrat de confiance. Ils doivent déchiffrer des formulaires de consentement toujours plus complexes, veiller à la protection de leurs données personnelles et rester en alerte face aux risques de violation. L'expérience utilisateur est laborieuse et se heurte à de nombreux processus fastidieux. Résultat : la confiance globale envers les services numériques stagne, voire recule, y compris dans les secteurs les plus encadrés. Cette tendance traduit un scepticisme grandissant et appelle les organisations à agir. Elle doivent reprendre l'initiative pour mériter à nouveau la confiance de leurs clients.

Les cybermenaces évoluent sans relâche. Elles deviennent plus nombreuses, plus sophistiquées. Les organisations doivent donc adapter leur sécurité en continu pour garder une longueur d'avance. Les utilisateurs, eux, attendent davantage d'innovation et une meilleure protection des données de la part des entreprises. Ils attendent d'elles qu'elles optent pour des solutions de pointe capables non seulement de sécuriser les informations personnelles, mais aussi de simplifier leur expérience.

La relation de confiance qui soutient le monde numérique ne peut reposer uniquement sur les consommateurs. Les entreprises doivent se montrer proactives : elles doivent limiter les casse-têtes utilisateurs, renforcer la sécurité et communiquer avec transparence sur les mesures mises en place. Ainsi, elles pourront instaurer une relation numérique plus solide et plus durable avec leurs clients.

Sponsorisé par

EXCLUSIVE NETWORKS

« La confiance mondiale accordée aux services numériques recule ou, au mieux, stagne, même dans les secteurs les plus réglementés. »

Sommaire

Principaux résultats

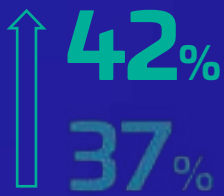
LA CONFIANCE MONDIALE ACCORDÉE AUX SERVICES NUMÉRIQUES EST EN BAISSE

Moins de 50%

La plupart des secteurs ont vu leur niveau de confiance baisser par rapport à l'an passé, aucun n'atteignant le niveau de 50% de confiance des utilisateurs.

LA BANQUE RESTE LE SECTEUR « LE PLUS DIGNE DE CONFIANCE»

...bien que ce chiffre ait chuté de 44 % à seulement 32 % pour les 16-24 ans.



42%

37%

Les organisations gouvernementales constituent le seul secteur où la confiance a progressé par rapport à l'an dernier (42 % contre 37 %).

LES MÉDIAS, CONSIDÉRÉS COMME LE SECTEUR LE MOINS FIABLE

Seulement 3%

Parmi les utilisateurs interrogés, très peu d'entre eux font confiance aux médias d'information pour la gestion de leurs données personnelles, ce qui place ce secteur en dernière position.

LA DEMANDE POUR UNE CONNEXION SANS MOT DE PASSE CONTINUE DE CROÎTRE

75%

Trois consommateurs sur quatre estiment que l'authentification sans mot de passe, via l'utilisation de données biométriques ou d'un code PIN, est devenue essentielle (contre 72 % l'an dernier).

86%, SOIT PLUS DE QUATRE UTILISATEURS SUR CINQ

attendent des entreprises qu'elles accordent de l'importance au respect de leur vie privée

19%

SOIT PRESQUE UNE PERSONNE SUR CINQ

a été informée que ses données personnelles avaient été compromises au cours de l'année écoulée.

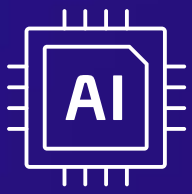
« AUCUNE ALTERNATIVE POSSIBLE »

37% **DES CONSOMMATEURS CONTRAINTS DE PARTAGER LEURS DONNÉES**

Un sentiment d'obligation plutôt qu'une démarche volontaire.

L'ADOPTION DE TECHNOLOGIES INNOVANTES ET AVANCÉES

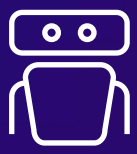
64% des utilisateurs affirment que leur confiance envers les entreprises augmenterait nettement si celles-ci adoptaient des technologies innovantes pour renforcer leur sécurité et leur protection des données.



TROP DE RESPONSABILITÉS INCOMBENT À L'UTILISATEUR

63% des consommateurs estiment que les organisations font peser trop de responsabilité sur eux concernant la protection des données.

LES BOTS PEUVENT TERNIR L'IMAGE DE MARQUE DES ENTREPRISES



Un consommateur sur trois se dit frustré par le commerce en ligne, en raison des bad bots qui perturbent le processus d'achat et détériorent l'expérience client.

33%

Contexte mondial

Quelle que soit leur localisation ou leur secteur d'activité, les organisations doivent impérativement protéger les données de leurs clients tout en garantissant une expérience client de qualité. Il n'y a pas de compromis possible : les deux sont indispensables.

La confiance se mérite et les entreprises ne tiennent pas toujours leurs promesses. Rien que ces douze derniers mois :

19% des consommateurs ont été avertis que leurs données personnelles avaient été compromises

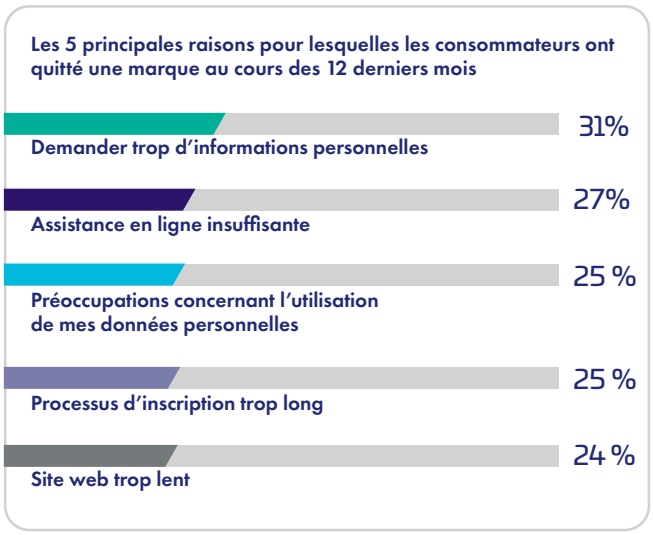
10% Plus d'un utilisateur sur dix s'est fait voler des données bancaires ou de carte de crédit

28% des consommateurs ont constaté des variations de prix sur un produit ou service qu'ils souhaitaient acheter

27% Plus d'un quart des utilisateurs ont rencontré des interruptions ou une navigation lente sur le site d'une organisation ou d'un prestataire

13% des consommateurs ont été éjectés d'une file d'attente en ligne permettant d'accéder à un produit ou un service

Sécurité, confidentialité et expérience sont les piliers de la confiance. Pas étonnant, alors, que la vaste majorité des consommateurs dans le monde (82 %) se soient détournés d'au moins une marque au cours des 12 derniers mois.



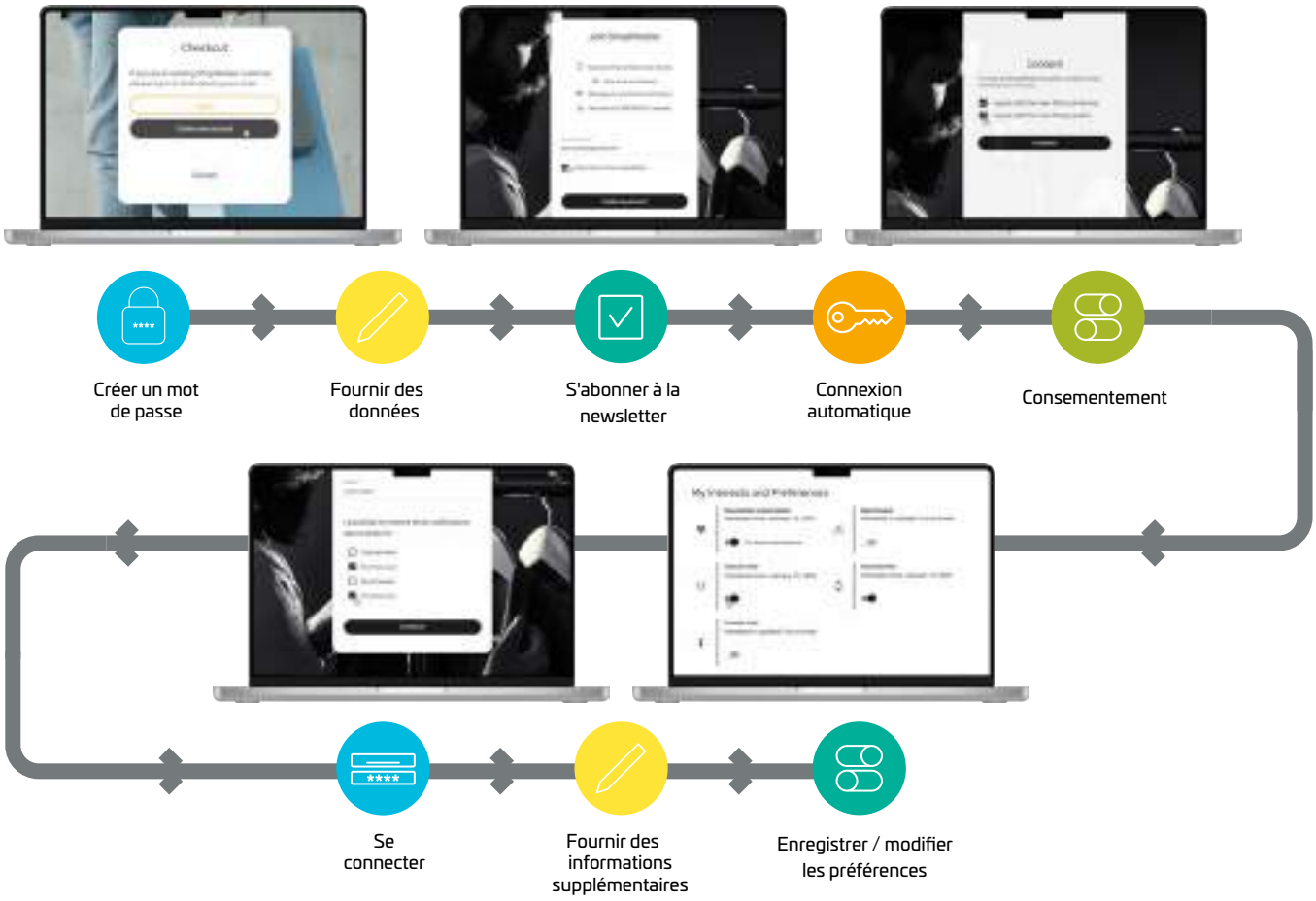
L'Indice de Confiance Mondial

Demander trop d'informations personnelles reste la principale raison qui a poussé les consommateurs à se détourner d'une entreprise ces 12 derniers mois : 31 % d'entre eux citent ce motif comme la cause numéro un de rupture avec une marque donnée.

La présente étude a également demandé aux clients dans quels secteurs ils se sentaient le plus à l'aise pour partager leurs données personnelles.

Profilage progressif

Pour répondre à ce besoin, certaines entreprises privilégient le profilage progressif : une approche qui consiste à recueillir les données de façon transparente et par étapes, afin de ne pas submerger l'utilisateur. De courts formulaires ou sondages sont proposés lors de plusieurs interactions pour enrichir le profil utilisateur au fil du temps.



Classement de l'Indice de confiance 2025

Quels secteurs vous inspirent confiance pour partager vos données personnelles ?

1	Banque	44%
2	Services publics	41%
3	Santé	40%
4	Assurance	24%
5	Éducation	17%
6	Hôtellerie	7%
7	Transports (compagnies aériennes, trains, etc.)	6%
8	Commerce	5%
8	Divertissement	5%
9	Réseaux sociaux	4 %
9	Automobile	4 %
9	Logistique	4 %
10	Organisations médiatiques	3 %

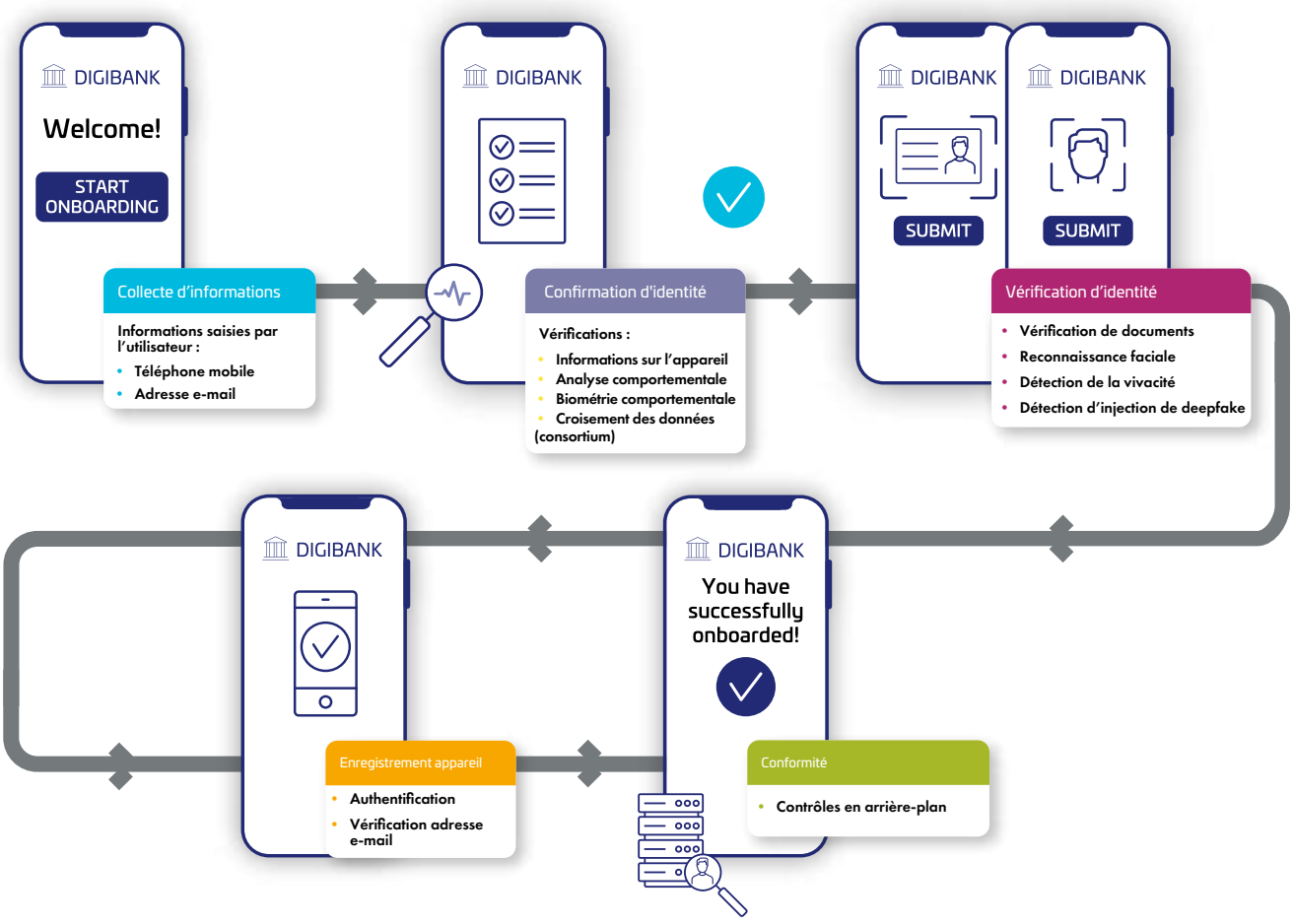
La confiance mondiale envers les services numériques s'effrite

Dans l'ensemble, les résultats révèlent une baisse généralisée de la confiance envers les services numériques, la plupart des secteurs affichant un recul par rapport à l'an dernier ou, au mieux, une stagnation.

En matière de protection des données personnelles, les utilisateurs accordent davantage leur confiance au secteur bancaire, aux services publics et à la santé. Ce niveau de confiance plus élevé dans les secteurs réglementés confirme la tendance observée l'année passée. Pourtant, même dans ces domaines réputés les plus sûrs, la confiance demeure relative : aucun secteur n'obtient plus de 50% de confiance, ce qui souligne l'ampleur du travail qu'il reste à accomplir.

Le saviez-vous ?

Aujourd'hui, près de huit clients sur dix estiment que toute inscription doit pouvoir être faite en ligne, ce qui est très compréhensible. Prenons l'exemple du nouveau client d'une banque : dans un parcours traditionnel, il devrait encore se déplacer en agence, patienter au guichet et attendre que les procédures administratives suivent leur cours. À l'inverse, l'intégration numérique offre une expérience beaucoup plus fluide : les opérations de vérification et de traitement existent toujours, mais elles se déroulent en arrière-plan. Pour le client, tout semble simple et instantané : quelques clics suffisent pour ouvrir son compte et commencer à l'utiliser.



Exception - La confiance envers l'administration publique progresse

Par rapport à l'an dernier, le seul secteur à enregistrer une hausse globale de confiance est celui des services publics, avec une augmentation de 5 % en 2024. Il dépasse ainsi le domaine de la santé dans le classement mondial.

Les citoyens souhaitent de plus en plus accéder à des services numériques. Pour les gouvernements, cette transition permet de gagner en efficacité, de réduire les coûts et de rendre les services plus accessibles à tous. Un bel exemple de cette évolution est la mise en place du permis de conduire dématérialisé (DDL) dans l'État du Queensland, en Australie.

Le saviez-vous ?

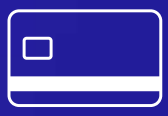
Lancée à la fin de l'année 2023 par le Department of Transport and Main Roads du Queensland, la nouvelle application Digital Licence a déjà séduit plus de 500 000 utilisateurs. Conçue par Thales en partenariat avec les entreprises locales Code Heroes et Aliva, elle marque une étape importante dans la modernisation des services publics australiens. Dès sa conception, la priorité a été donnée à la sécurité et à la protection de la vie privée. La plateforme d'identité numérique de Thales, au cœur du dispositif, assure un hébergement cybersécurisé des données personnelles et garantit que chaque interaction reste sous le contrôle de l'utilisateur. L'application QLD Digital Licence se distingue par sa simplicité d'usage et son haut niveau de fiabilité. Elle intègre un système d'authentification multifactorielle, une connexion directe au service Queensland Digital Identity (QDI), ainsi qu'un mécanisme de vérification intégré pour des échanges d'informations sécurisés entre utilisateurs. Son fonctionnement fondé sur le consentement offre à chacun une pleine maîtrise de ses données : il est possible de ne partager que ce qui est strictement nécessaire, selon le contexte. Par exemple, pour prouver sa majorité, l'application affiche simplement la mention « plus de 18 ans », sans révéler ni la date de naissance, ni l'adresse, ni les informations du permis de conduire, une option très appréciée des usagers.

Les réglementations du secteur bancaire

Bien qu'il reste encore du chemin à parcourir, le secteur bancaire retrouve sa place en tête de l'indice de confiance, en partie grâce au renforcement des réglementations visant à améliorer l'expérience utilisateur et à sécuriser les données.

Règlement sur la résilience opérationnelle numérique (DORA) :

Ce règlement de l'Union européenne (UE), applicable depuis janvier 2025, vise à renforcer la sécurité informatique et la résilience des institutions financières, telles que les banques et les compagnies d'assurance. DORA veille à ce que ces entités puissent résister à de graves perturbations opérationnelles en harmonisant les règles de gestion des risques.



Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS 4.0)

À compter du 31 mars 2025, PCI DSS 4.0 devient la nouvelle norme mondiale en matière de protection des données des titulaires de cartes. Cette version intègre 12 exigences principales telles que l'installation de contrôles de sécurité réseau, la sécurisation des données enregistrées et la surveillance régulière des réseaux. Conçue pour répondre aux nouvelles menaces et aux évolutions technologiques, la norme PCI DSS 4.0 met notamment l'accent sur le renforcement de l'authentification multifactorielle (MFA) pour garantir la sécurité de ces données.

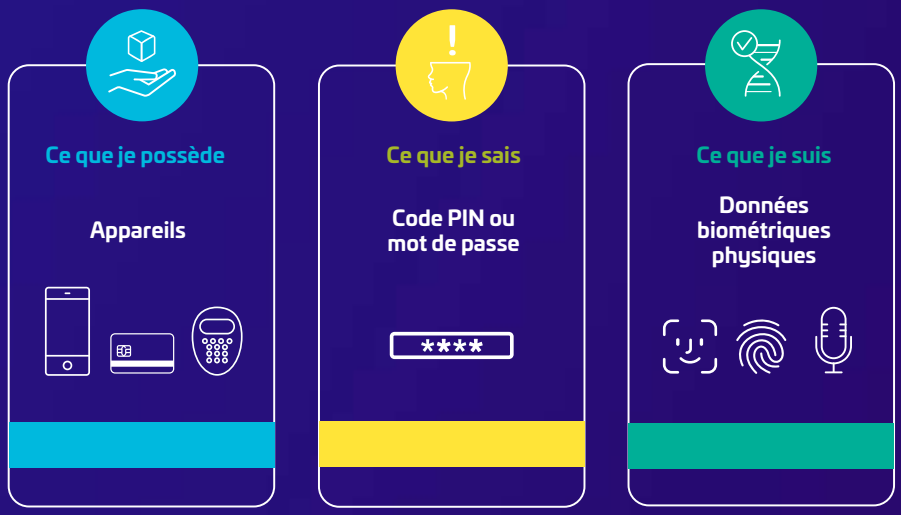
Troisième directive sur les services de paiement (PSD3) :

En vigueur depuis juin 2023, la PSD3 modernise le cadre des paiements électroniques au sein de l'UE. Elle vise à stimuler la concurrence et l'innovation tout en renforçant la protection des consommateurs.

Parmi les points essentiels : une authentification renforcée pour les clients, une prévention accrue contre la fraude, et un accès facilité aux systèmes de paiement pour les prestataires non bancaires.

Le saviez-vous ?

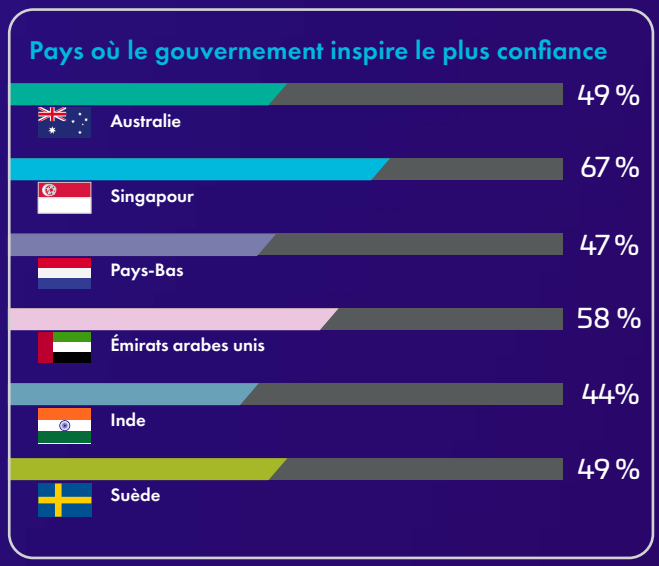
Dans la plupart des pays, les établissements financiers sont tenus d'utiliser l'authentification forte (SCA). La SCA exige au moins deux des éléments suivants (ou « facteurs ») pour être conforme.

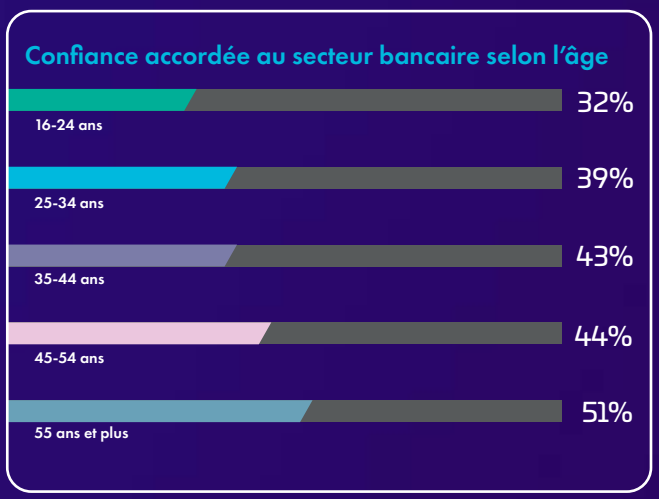


Le secteur bancaire reste le plus digne de confiance

Bien que la banque arrive globalement en tête, on observe quelques différences selon les profils démographiques :

- Les personnes interrogées de 55 ans et plus sont celles qui font le plus confiance au secteur bancaire concernant leurs données personnelles, contrairement aux 16-24 ans qui accordent le moins leur confiance à ce secteur (**51 % contre 32%**).
- À l'inverse, les 16-24 ans interrogés font davantage confiance aux services publics(**35%**) et au secteur de la santé (**35%**).
- Aux États-Unis, la santé inspire davantage de confiance avec **41%**. La confiance accordée aux services publics en matière de données personnelles y est bien inférieure à la moyenne, avec **29%**.
- En Australie, à Singapour, aux Pays-Bas, aux Émirats arabes unis, en Suède et en Inde, ce sont les services publics qui inspirent le plus confiance.





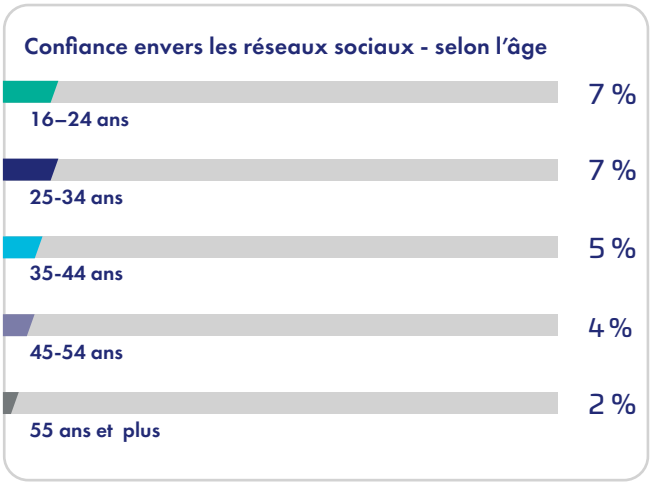
Méfiance envers les médias

Les médias se situent tout en bas de l'indice de confiance lorsqu'il s'agit du partage de données personnelles. Seuls 3% des utilisateurs déclarent faire confiance aux organisations médiatiques pour la protection de leurs données personnelles un score inférieur à celui de tous les autres secteurs.

Cette méfiance s'explique en grande partie par la prolifération de la désinformation et par la montée en puissance des technologies de falsification numérique, comme les deepfakes, qui brouillent la frontière entre vrai et faux. Les utilisateurs deviennent de plus en plus sceptiques quant à l'authenticité des contenus qu'ils consultent et, par ricochet, se méfient des plateformes qui les diffusent.

Les réseaux sociaux souffrent du même phénomène : leur niveau de confiance a chuté de 33 % en un an. Ils obtiennent un score légèrement supérieur à celui des médias traditionnels — 4 % — : la confiance y est donc marginale et ne se maintient que chez les publics les plus jeunes.

Quel que soit le secteur, les entreprises sont tenues de respecter les réglementations internationales sur la protection des données. Cependant, les acteurs les moins bien classés sont souvent soumis à un cadre réglementaire moins strict en matière de sécurité et de confidentialité. Ces secteurs gagneraient à s'inspirer des pratiques exemplaires mises en place dans les domaines plus réglementés et mieux notés. Renforcer la confiance est en effet une condition essentielle pour encourager les utilisateurs à partager leurs données, ce qui, à terme, permet d'améliorer la qualité et la personnalisation de leur expérience.



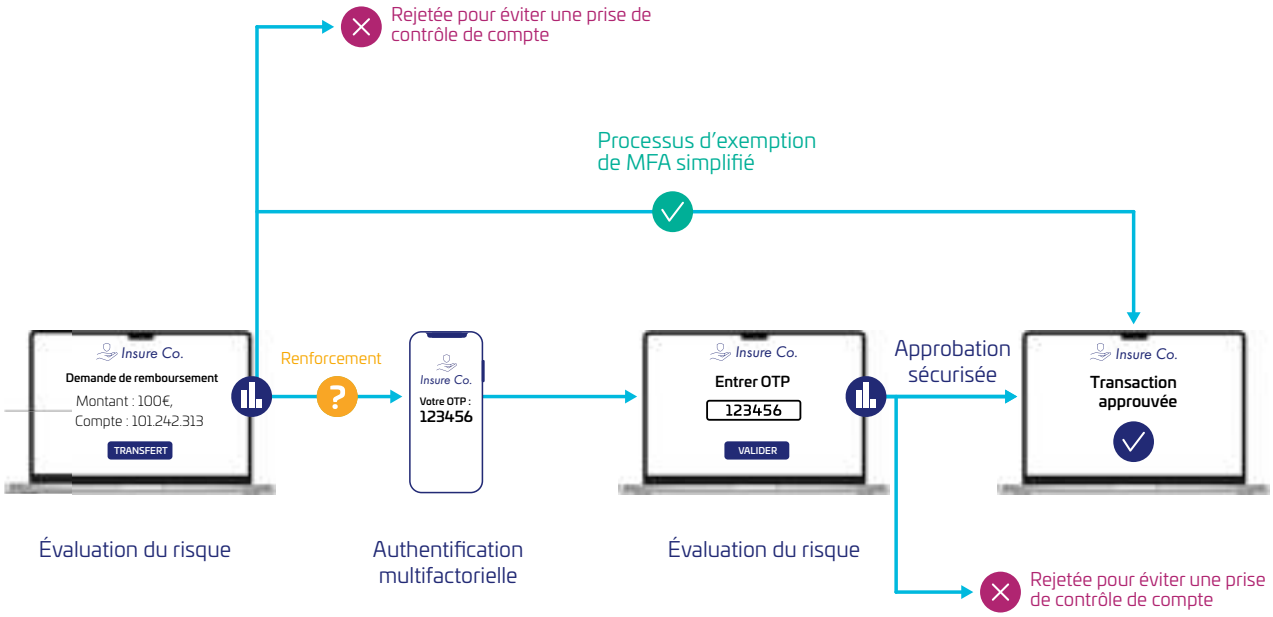
Le saviez-vous ?

Meta, la maison mère de Facebook et d'Instagram, a décidé de se passer des services de vérification indépendants. L'entreprise mise désormais sur un système communautaire baptisé Community Notes, où les utilisateurs eux-mêmes signalent les informations fausses ou trompeuses. Cette décision suscite de nombreuses inquiétudes : sans contrôle externe, le risque de propagation de fausses informations s'accroît, au point de fragiliser encore davantage la confiance déjà ébranlée envers ces plateformes.

Le saviez-vous ?

Authentication basée sur le risque *(Risk-Based Authentication - RBA)*

L'authentification adaptative fondée sur le risque (Risk-Based Authentication, ou RBA) repose sur une approche dynamique : le niveau de vérification s'ajuste en fonction du profil et du comportement de chaque utilisateur. Le système évalue automatiquement le niveau de risque associé à une connexion ou à une transaction, en tenant compte de plusieurs éléments : adresse IP, localisation géographique, type d'appareil, historique de navigation ou encore habitudes d'utilisation. Chaque action fait ainsi l'objet d'une évaluation individualisée, contrairement aux systèmes d'authentification classiques qui appliquent les mêmes contrôles à tous les utilisateurs. Pour l'utilisateur, cette approche offre un haut niveau de sécurité tout en préservant la fluidité de l'expérience : les contrôles s'intensifient uniquement lorsque le contexte l'exige, ce qui limite les interruptions inutiles et renforce la confiance dans l'usage quotidien des services numériques.



Cet exemple simple de RBA illustre comment il est possible de rendre la vérification d'identité à la fois plus fluide et plus sûre. Le système agit discrètement en arrière-plan : il évalue en continu le niveau de risque associé à chaque connexion et décide, le cas échéant, de renforcer l'authentification par une méthode plus sécurisée.

Exigences des utilisateurs en matière de confidentialité

Les internautes sont de plus en plus réticents à l'idée de livrer une quantité excessive d'informations personnelles. Cette méfiance est même l'une des principales raisons qui les poussent à mettre fin à une relation commerciale. Cela ne veut pas dire pour autant qu'ils refusent de partager leurs données : la plupart acceptent de le faire, à condition que ce soit dans un cadre transparent.

Près de neuf clients sur dix (89 %) se disent prêts à communiquer leurs données à une organisation, mais sous certaines conditions. Et plus de quatre sur cinq (86 %) attendent des entreprises qu'elles respectent leur vie privée en ligne, un résultat concordant avec l'étude de l'année passée.

Ils expriment deux grandes attentes : être informés lorsque leurs données personnelles sont collectées (52 %) et pouvoir demander leur suppression à tout moment (53 %). Par ailleurs :

37% souhaitent pouvoir rectifier leurs données personnelles.

31% souhaitent obtenir une copie de leurs données personnelles.

25% souhaitent pouvoir transférer leurs données d'une plateforme à une autre.

Y compris lorsque la relation commerciale s'arrête, les utilisateurs ont certaines attentes en matière de gestion des données. Près de la moitié des consommateurs interrogés (49 %) n'apprécient pas l'idée qu'une entreprise conserve l'accès à leurs données une fois qu'ils ont cessé d'utiliser un produit ou un service. À l'inverse, seuls 19 % déclarent ne pas y voir d'inconvénient, étant convaincus que leurs données seront utilisées à des fins légitimes.

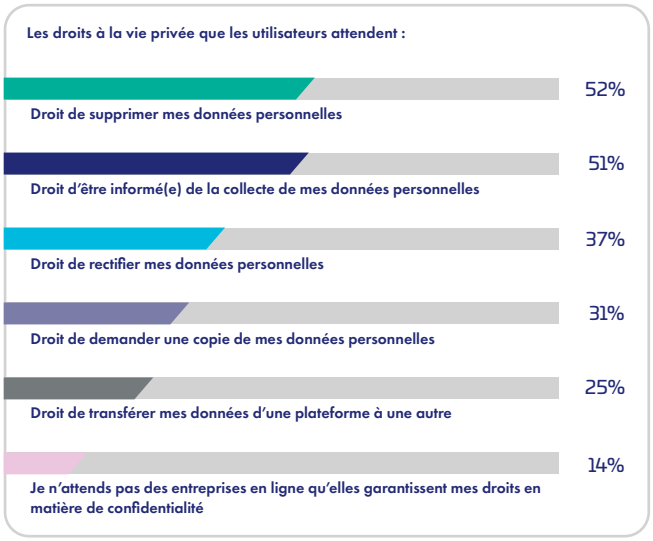
Le saviez-vous ?

Destinée à remplacer la loi actuelle sur la protection des renseignements personnels et les documents électroniques (LPRPDE, ou PIPEDA en anglais), la CPPA vise à moderniser le cadre canadien de protection des données. Elle introduit des exigences de consentement plus strictes ainsi que de nouveaux droits renforcés pour les citoyens : elle leur permet notamment d'accéder à leurs données personnelles et d'en garder un meilleur contrôle.

Les demandes d'accès aux données personnelles

Une Data Subject Request (DSAR) est une demande qu'une personne peut faire à une entreprise ou une organisation pour savoir quelles informations personnelles sont collectées sur elle, et comment elles sont utilisées. Elle peut aussi en demander la mise à jour ou la suppression. Ce droit, aussi appelé SRR, SAR ou DSR, permet à chacun de mieux contrôler ses données personnelles. Il est garanti par plusieurs cadres réglementaires, notamment le RGPD (Union européenne), la LPRPDE au Canada (PIPEDA en anglais) et le CCPA en Californie.

La protection de la vie privée doit être intégrée dès la conception du parcours utilisateur. Pour pouvoir répondre efficacement aux demandes d'accès ou de gestion des données personnelles, les entreprises doivent conserver certaines métadonnées relatives à ces informations sensibles.



Le saviez-vous ?

Inspirée du RGPD européen, la loi générale sur la protection des données au Brésil (LGPD) confère aux citoyens brésiliens un ensemble complet de droits en matière de protection des données. Elle prévoit notamment la possibilité d'accéder à ses données personnelles, d'en demander la rectification ou la suppression. Ces dernières années, cette loi a donné lieu à un renforcement des mesures de contrôle et des actions de conformité.

« Le RGPD demeure la référence mondiale en matière de protection des données. Il accorde à chaque individu le droit d'accéder à ses informations personnelles, d'en demander la rectification ou la suppression. »

Le saviez-vous ?

Entrée en vigueur en août 2023, la loi indienne sur la protection des données personnelles numériques (DPDP) vise à protéger les données personnelles des citoyens indiens. Elle encadre les activités de traitement des données et garantit aux individus le droit d'y accéder, de les corriger ou d'en demander la suppression. Cette loi prévoit également des dispositions spécifiques concernant la gestion des risques, les prestataires tiers et la notification des incidents. Ces mesures visent à renforcer la sécurité des données et la résilience des organisations opérant en Inde.

Qu'est-ce qu'un bot ?

Un bot est un programme automatisé qui réalise des tâches sur internet. Certains bots sont utiles, comme ceux des moteurs de recherche qui indexent des contenus. D'autres sont nuisibles et utilisés à des fins malveillantes.

Qu'est-ce qu'un bad bot ?

Les bots malveillants sont des programmes automatisés conçus pour mener des actions nuisibles, comme l'extraction de données, l'envoi de spams ou les attaques par déni de service. Ils peuvent imiter les comportements humains, ce qui les rend difficiles à repérer et à bloquer.

« Au cours de l'année écoulée, 67 % des utilisateurs ont été confrontés à des perturbations de leur expérience de navigation »

La montée en puissance des bad bots : un problème grandissant

La protection de la vie privée n'est qu'une seule pièce du puzzle de la confiance des consommateurs. L'expérience en ligne joue, elle aussi, un rôle déterminant dans la perception et la crédibilité d'une entreprise. Au cours des douze derniers mois, la mauvaise qualité des services client en ligne a été identifiée comme la deuxième cause la plus fréquente d'abandon des relations commerciales.

Aujourd'hui, près de la moitié du trafic internet est générée par des robots (bots), dont un tiers provient de programmes malveillants. Ces « bad bots » prennent de nombreuses formes et contribuent directement à la perte de confiance numérique.

Bots de prise de contrôle de comptes
Ces attaques consistent à s'emparer illégalement des comptes utilisateurs. Elles reposent sur des méthodes automatisées telles que le credential stuffing (tests massifs d'identifiants volés pour en vérifier la validité) ou le credential cracking (tentatives répétées pour deviner des combinaisons identifiant/mot de passe).

Bots de revente (« scalping »)
Le scalping consiste à acquérir des produits ou services rares ou à forte demande par des moyens déloyaux, afin de les revendre plus cher. Ces bots faussent la concurrence et nuisent à l'expérience légitime des consommateurs.

Bots de fraude à la carte bancaire
Ces programmes sont utilisés pour tester des numéros de carte volés en effectuant de petites transactions (carding), ou pour deviner des informations manquantes comme la date d'expiration ou le code de sécurité (card cracking). Ils font baisser les scores de fiabilité des entreprises et entraînent une hausse des coûts liés aux remboursements de transactions frauduleuses.

Bots de spams et de désinformation
Ces bots diffusent de fausses informations, manipulent les avis en ligne ou publient de fausses critiques pour nuire à des concurrents. Certains dissimulent aussi des logiciels espions ou des virus derrière des liens attrayants ou des publicités mensongères.

Les bots, sources de problèmes pour les entreprises

Les bots malveillants constituent plusieurs grands défis :

Risques pour la sécurité

Les bots malveillants peuvent mettre en danger la sécurité des sites web et des applications via des violations de données et d'autres menaces informatiques.

Coûts opérationnels

La gestion des bots indésirables peut faire grimper les coûts opérationnels car elle requiert des mesures de sécurité supplémentaires et davantage de ressources pour contrôler le trafic.

Expérience client

La présence de bots malveillants peut considérablement détériorer l'expérience utilisateur, suscitant frustration et perte de confiance chez les clients.

Si la prolifération des bots malveillants peut avoir de lourdes conséquences sur la sécurité et la vie privée, elle peut aussi fortement nuire à l'expérience des internautes. Nous avons leur demandé ce qui leur a fait perdre patience au cours des douze derniers mois :

28% ont perdu patience en ligne à cause des tests CAPTCHA imposés pour prouver qu'ils ne sont pas des robots.

27% ont été frustrés par l'attente dans de longues files d'attente virtuelles.

14% ont été agacés par la tarification dynamique.

Les organisations ont besoin de stratégies de protection contre les bots

En mettant en place des stratégies de protection contre les bots, les entreprises peuvent préserver l'expérience en ligne et renforcer la confiance des internautes. Une protection efficace contre les bots permet de :

Renforcer la sécurité

Prévenir les fuites de données et les menaces numériques en détectant et bloquant le trafic malveillant des bots.

Optimiser l'expérience utilisateur

Diminuer le recours aux tests CAPTCHA et aux files d'attente en ligne, pour un parcours client plus fluide et agréable.

Réduire les coûts

Réduire les coûts opérationnels en limitant l'impact des bots malveillants sur la performance et la sécurité du site web.

« Les organisations doivent investir dans des stratégies robustes de protection contre les bots afin de conserver la confiance des utilisateurs. »

Accès refusé : les mots de passe restent un problème

La grande majorité des utilisateurs (87 %) ont perdu patience en ligne au cours des douze derniers mois.

Raisons pour lesquelles les utilisateurs perdent patience

1	Pop-ups publicitaires	38%
2	Réinitialisation de mot de passe	31%
3	Devoir ressaisir ses identifiants après avoir déjà utilisé un service	28%
4	Devoir réaliser une CAPTCHA (prouver ne pas être un robot)	28%
5	Longues files d'attente en ligne	27%
6	Chatbots	24%
7	Options compliquées de cookies	23%
8	Entrer des données de paiement	18%
9	Vérification bancaire	17%
10	Tarification dynamique	14%
11	Services utilisés précédemment et qui oublient les préférences utilisateur	14%

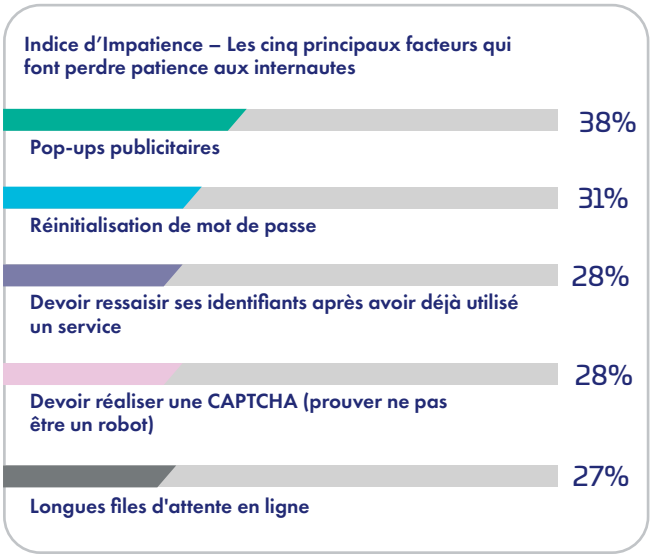
Les problèmes liés aux identifications et vérifications continuent d'être sources de frustration : les réinitialisations des mots de passe, les saisies répétées d'identifiants ou encore les oublis des préférences en ligne tendent à exaspérer les internautes.

Les mots de passe ont la vie dure, malgré les appels à leur suppression. Ils demeurent la méthode d'authentification la plus courante, au grand désarroi des utilisateurs agacés, qui parfois abandonnent leur tentative de connexion.

- **Frustration liée aux mots de passe :** de plus en plus d'internautes se détournent de certains services à cause de mots de passe oubliés. Au cours des douze derniers mois, 17 % des utilisateurs ont cessé d'utiliser un service après avoir oublié leur mot de passe (contre 16 % l'an dernier). Par ailleurs, 16 % mentionnent la nécessité de créer des mots de passe longs et complexes comme principale raison de leur désengagement.
- **Impact sur la loyauté de l'utilisateur :** les difficultés liées aux mots de passe figurent parmi les causes les plus fréquentes de désengagement. 18 % des utilisateurs estiment que l'obligation de créer des mots de passe longs, uniques et difficiles à mémoriser constitue un frein majeur à leur fidélité.

Ces résultats montrent que la gestion des mots de passe demeure une source majeure de difficulté pour les utilisateurs, avec un impact tangible sur l'engagement. Pour améliorer l'expérience client, les organisations doivent désormais s'attaquer à cet écueil trop souvent négligé.

« 91 % des 16-25 ans ont perdu patience sur internet, contre 82 % des plus de 55 ans »



Appel à l'authentification sans mot de passe et à l'authentification multifactorielle :

- **Authentification sans mot de passe :** la demande d'expériences de connexion sans mot de passe a nettement augmenté cette année. Trois quarts des internautes (75 %) estiment que l'authentification sans mot de passe, par exemple via des données biométriques ou un code PIN, est importante (contre 72 % l'an passé). Plus d'un tiers (35 %) considèrent même cette option comme essentielle.

- **Passkeys :** les passkeys s'imposent comme une alternative à la fois sécurisée et pratique aux mots de passe traditionnels. Elles reposent sur des clés cryptographiques stockées sur l'appareil de l'utilisateur, garantissant une connexion fluide sans devoir mémoriser de mots de passe complexes. 48 % des internautes interrogés affirment qu'ils feraient davantage confiance à un site web proposant les passkeys.

- **Authentification multi-facteurs (MFA) :** près de 9 utilisateurs sur 10 (86 %) soulignent l'importance de la MFA pour renforcer la sécurité des comptes en ligne, contre 81 % l'an dernier. La moitié des sondés (50 %) jugent cette fonctionnalité très importante.

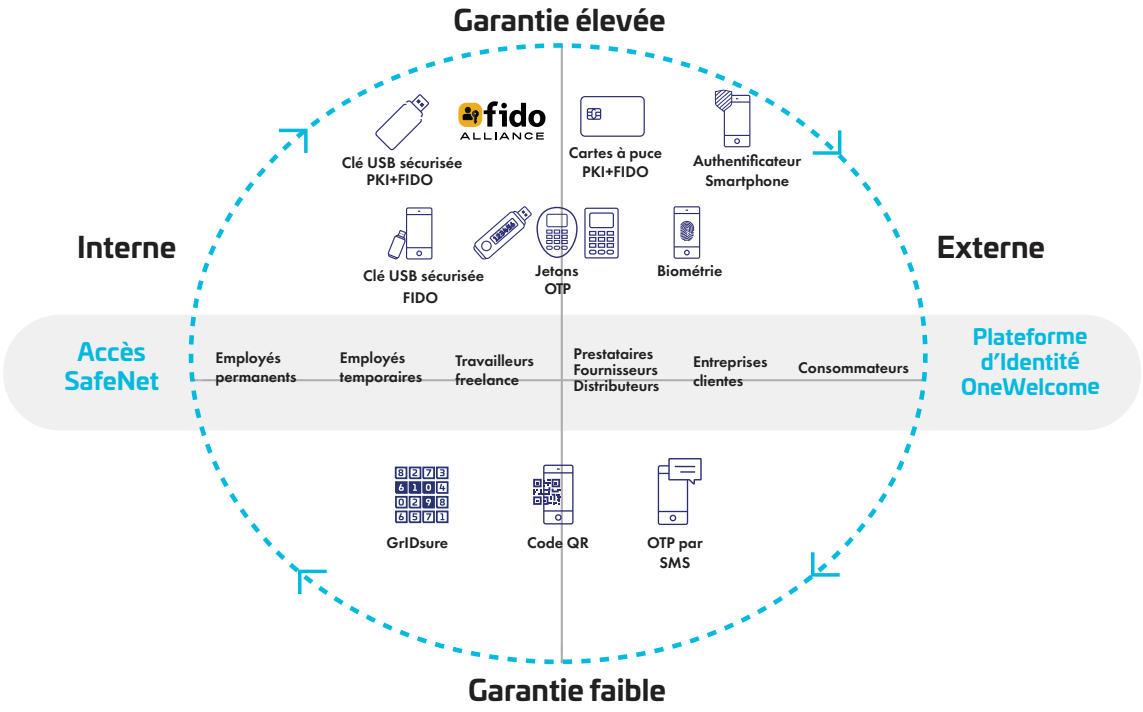
Ces résultats révèlent une préférence croissante des internautes pour des méthodes d'authentification à la fois plus sûres et plus simples à utiliser. Mettre en place l'authentification sans mot de passe, les passkeys ou la MFA peut améliorer significativement la satisfaction et limiter le désengagement.

Il est possible de concilier sécurité et fluidité. Les entreprises peuvent trouver le juste équilibre grâce à des technologies de gestion des risques qui fonctionnent discrètement en arrière-plan. Ces solutions permettent de mettre en place une authentification adaptative (Risk-Based Authentication ou RBA, parfois appelée authentification multifactorielle dynamique). Ainsi, le niveau de vérification supplémentaire n'est demandé que lorsque le risque est élevé, ce qui limite les vérifications inutiles et les interruptions pour l'utilisateur.

Le saviez-vous ?

Thales Passwordless 360° est une solution complète permettant une authentification sans mot de passe, pour différents profils utilisateurs et niveaux de confiance.

- **Couverture étendue :** prise en charge de différents profils utilisateurs, notamment les employés, clients, partenaires commerciaux et fournisseurs.
- **Technologies de pointe :** cette solution combine les innovations les plus récentes comme les passkeys FIDO, la reconnaissance biométrique ou les clés de sécurité matérielles tout en capitalisant sur les infrastructures déjà en place pour favoriser une expérience sans mot de passe.
- **Sécurité renforcée :** en supprimant les mots de passe traditionnels, les risques liés au vol ou au phishing sont considérablement réduits.
- **Expérience utilisateur :** une connexion fluide et sans tracas, pour améliorer la satisfaction des utilisateurs et limiter la réinitialisation des mots de passe.
- **Authentification basée sur le risque :** Thales Passwordless 360° intègre l'authentification adaptative (RBA) et l'authentification multifactorielle adaptative (MFA). Cette solution n'exige de vérifications supplémentaires qu'en cas de risque élevé.

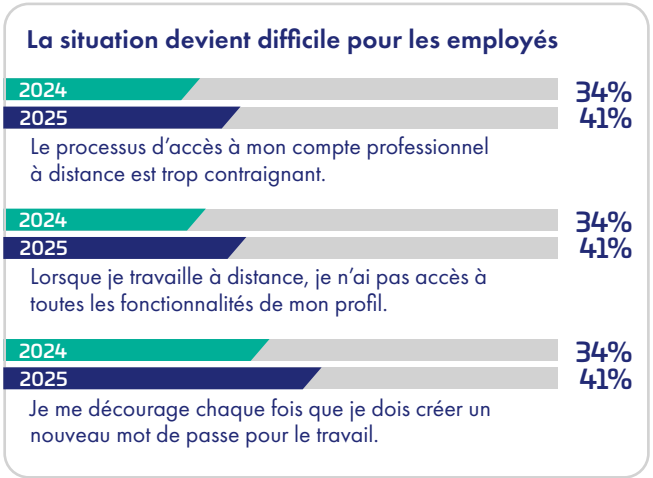


L'expérience des employés

Offrir aux salariés un environnement numérique à la fois fluide et sûr est devenu une condition essentielle pour préserver la productivité et le bien-être au travail. À une heure où le travail hybride se généralise, les entreprises doivent veiller à optimiser les conditions de travail de leurs employés travaillant à distance.

Le lien entre télétravail et performance se confirme : 56% des employés estiment que le travail à distance renforce leur efficacité, contre 47% l'année précédente. Ce résultat rappelle combien il est important de proposer des solutions d'accès simples et fiables pour soutenir cette dynamique.

Pourtant, les employés estiment qu'il devient plus difficile pour eux d'accéder à leurs outils lorsqu'ils sont à distance. Aujourd'hui, 41% des employés jugent les démarches d'accès à leur compte professionnel trop contraignantes, contre 36% l'an passé. Les dispositifs de sécurité et les procédures de connexion, souvent trop complexes ou trop longues, freinent l'expérience du télétravail.



Des processus trop complexes et un manque d'efficacité

Plus de la moitié des salariés (56%) rapportent de la frustration chaque fois qu'ils doivent créer un nouveau mot de passe pour leur compte professionnel, une hausse notable par rapport aux 48% enregistrés l'an dernier.

Impact sur le travail au quotidien

Près de la moitié (42%) affirment ne pas pouvoir accéder à l'ensemble des fonctionnalités de leur profil professionnel lorsqu'ils travaillent à distance, ce qui nuit à leur efficacité. Ils n'étaient que 37% à faire ce constat en 2024.

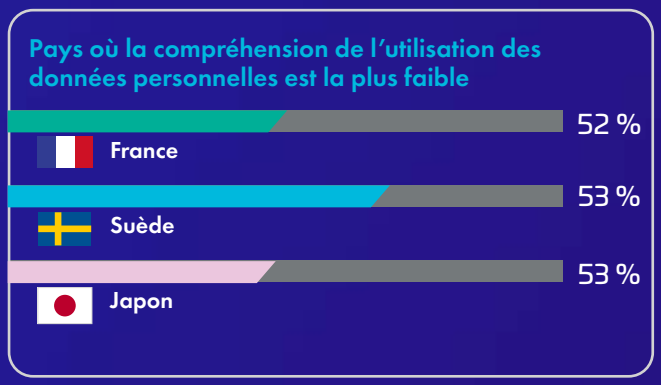
Fait encourageant, 57% des employés estiment que leur employeur accorde de l'importance à la qualité de leur expérience numérique. 9% partagent le constat inverse, un chiffre qui atteint 13% en Allemagne. Ces résultats montrent que, malgré les efforts des entreprises pour améliorer les outils et parcours numériques, une part non négligeable des salariés considère encore que leurs besoins ne sont pas pleinement pris en compte.

Un lourd poids, qui pèse sur les utilisateurs

À l'ère du numérique, échanger ses données personnelles contre des services est devenu monnaie courante. Pourtant, cette pratique transactionnelle soulève de nombreux défis, notamment en matière de transparence et de bénéfices perçus. Beaucoup d'internautes se sentent obligés de partager leurs informations sans vraiment savoir comment elles seront utilisées, ce qui nourrit une méfiance croissante. En effet, 45 % des utilisateurs ne font pas confiance aux entreprises sur cette question, un chiffre qui grimpe à 57 % en France.

Manque de bénéfices perçus

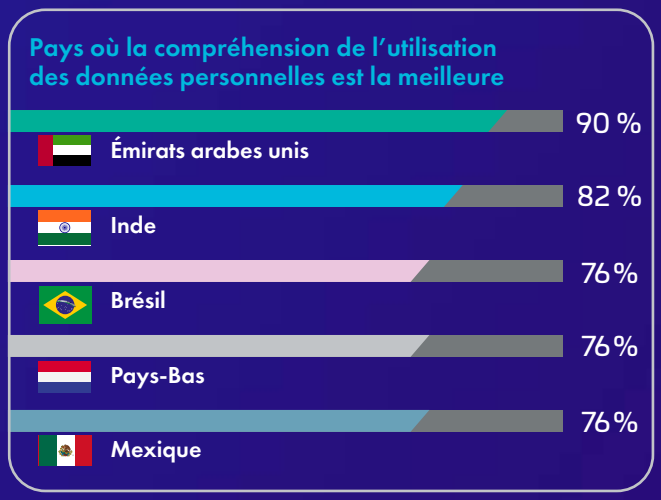
Les chiffres révèlent une réelle lacune dans la communication entre les entreprises et leur clientèle. Par exemple, 37 % des internautes ne partagent leurs données que parce qu'ils n'ont pas d'autre choix, ce qui met en lumière un sentiment de contrainte plutôt qu'un acte volontaire. Cette tendance est accentuée par le fait que 33 % des utilisateurs dans le monde ne comprennent pas la gestion de leurs données, ce qui appelle à davantage de transparence.



Trop de responsabilités pour le consommateur

Une part importante des utilisateurs estime que les entreprises leur font porter une responsabilité excessive en matière de protection des données personnelles. Les résultats indiquent que :

- 63 % d'entre eux estiment que les entreprises font porter trop de responsabilité sur les clients en matière de protection des données.
- Cette opinion est encore plus marquée dans certaines régions, avec 75 % au Brésil et en Inde, et 78 % aux Émirats arabes unis.



Conséquences

La tendance croissante à exiger un échange de données pour accéder à des services, combinée au manque de transparence et au poids que cela fait porter aux utilisateurs, fragilise la confiance. Les entreprises doivent comprendre que les clients sont de plus en plus sensibles à la protection de leurs données personnelles et souhaitent avoir une meilleure compréhension et plus de contrôle sur la manière dont celles-ci sont utilisées.

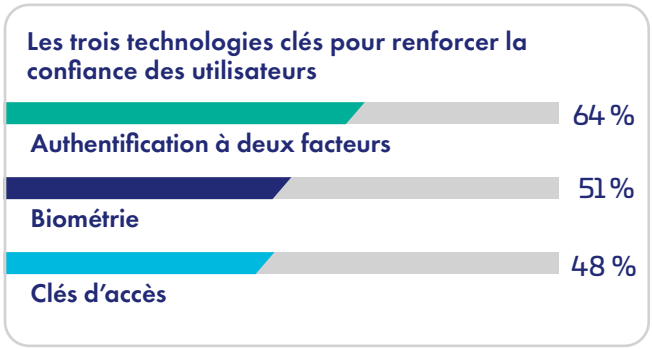
Pour restaurer la confiance, les entreprises doivent :

- **Renforcer la transparence : expliquez clairement comment les données des utilisateurs sont recueillies, utilisées et protégées.**
- **Mettre en place des mesures de protection des données faciles à utiliser, qui ne reposent pas excessivement sur la responsabilité de l'utilisateur.**
- **Afficher un engagement fort envers la confidentialité et la sécurité des données, à travers des stratégies de protection efficaces et des pratiques transparentes.**

Ainsi, les entreprises peuvent établir une relation de confiance avec leurs clients, synonyme d'une meilleure expérience utilisateur et d'un meilleur engagement.

Renforcer la confiance grâce à la technologie

L'adoption des technologies de pointe joue un rôle essentiel dans le renforcement de la confiance des internautes.



Authentification multifactorielle (MFA)

64% des sondés disent accorder davantage de confiance à un service utilisant la MFA. Cette technologie renforce la sécurité en ajoutant une protection supplémentaire, pour que même en cas de compromission des mots de passe, l'accès non autorisé reste bloqué. Les entreprises qui adoptent la MFA se distinguent en démontrant leur engagement pour la sécurité des données des utilisateurs, un enjeu essentiel à l'ère des violations fréquentes de données.

Biométrie :

Plus de la moitié (51 %) des personnes interrogées déclarent accorder davantage leur confiance aux services qui utilisent l'authentification biométrique. Les solutions biométriques, comme la reconnaissance d'empreintes digitales ou la reconnaissance faciale, offrent un moyen simple et sécurisé de vérifier son identité, tout en limitant les risques de fraude.

Les entreprises qui adoptent cette technologie améliorent à la fois l'expérience utilisateur et la sécurité, ce qui renforce la confiance des clients.

Clés d'accès :

48% des utilisateurs disent accorder davantage leur confiance à un service utilisant des clés d'accès. Ces clés remplacent les mots de passe classiques, souvent vulnérables, par des clés cryptographiques spécifiques à chaque utilisateur, ce qui renforce la sécurité.

La transition vers les clés d'accès d'accès vient répondre aux attentes des internautes en matière de sécurité. En adoptant cette technologie, les entreprises limitent les risques liés aux mots de passe et se positionnent comme pionnières du point de vue de la sécurité.

Souveraineté numérique :

37% des utilisateurs font davantage confiance aux entreprises qui mettent en place des mesures de souveraineté numérique. Ces mesures veillent à ce que les données sont stockées et traitées dans des juridictions précises, respectant ainsi les réglementations locales sur la protection des données.

La souveraineté numérique répond à des préoccupations croissantes liées à la confidentialité des données et au respect des réglementations. Les services qui mettent cet aspect en avant peuvent séduire des internautes de plus en plus attentifs à la gestion et à la localisation de leurs données.

Intelligence artificielle :

Environ 32 à 33 % des utilisateurs déclarent faire davantage confiance à une entreprise utilisant l'intelligence artificielle générative ou simplement l'IA. Ces technologies permettent d'améliorer la personnalisation et la sécurité, ce qui rend les échanges plus fluides et plus sûrs.

L'utilisation de l'IA transforme l'expérience client et la personnalisation en offrant un parcours sur mesure. Les entreprises exploitant le plein potentiel de l'IA renforcent leur lien avec leurs clients en répondant mieux à leurs attentes.

L'adoption de technologies innovantes et avancées, synonyme de confiance

Sur la question de la protection de leur données, les utilisateurs sont sensibles à l'adoption de technologies innovantes par les entreprises. 64 % des utilisateurs expliquent qu'ils auraient davantage confiance en une entreprise s'ils savaient qu'elle utilise ces solutions. Cela met en lumière l'importance cruciale de la transparence et d'une adoption proactive de mesures de sécurité innovantes.

En communiquant clairement leur engagement sur ces questions, les entreprises peuvent instaurer un climat de confiance, pour créer une relation plus sûre et fiable avec les clients.

La baisse mondiale de la confiance numérique est mesurable, mais aussi évitable

Conclusion de John Tolbert, directeur de la recherche en cybersécurité chez KuppingerCole Analysts

Cette étude révèle des indicateurs préoccupants pour les entreprises actives en ligne. La baisse mondiale de la confiance numérique est désormais manifeste… mais elle n'a rien d'inéluctable. Parmi les secteurs étudiés, le monde bancaire conserve une longueur d'avance : il n'échappe pas à la défiance générale mais reste perçu comme le plus sûr sur le plan numérique. Les banques ont, depuis longtemps, intégré la sécurité comme pilier central de leur activité : d'abord sous sa forme physique (coffres, alarmes, systèmes de surveillance), puis sous sa forme numérique. L'identité même des établissements bancaires repose sur la réputation de sérieux et la protection des avoirs. Les autres acteurs financiers (prestataires de services de paiement et institutions non bancaires) auraient tout intérêt à s'inspirer de ce modèle. Leur crédibilité et leur capacité à fidéliser dépendront largement de leur aptitude à garantir le même niveau de protection et de transparence que les établissements bancaires. Dans d'autres secteurs, le retard reste considérable : beaucoup d'entreprises cherchent encore à renforcer leurs pratiques de cybersécurité et à instaurer des standards comparables.

Le secteur de la santé conserve, pour l'instant, un niveau de confiance numérique relativement élevé, un paradoxe si l'on considère la multiplication des attaques par ransomware qui ont touché hôpitaux, cliniques et assureurs ces dernières années. Dans d'autres secteurs, de tels incidents auraient provoqué une chute immédiate de la confiance. Les patients continuent à utiliser les services de santé, mais souvent par nécessité plutôt que par conviction : le médical reste un service essentiel, auquel il est impossible de renoncer. Cette situation ne saurait toutefois perdurer sans un renforcement significatif de la cybersécurité. Les acteurs du secteur doivent investir davantage dans la protection des données, la prévention des attaques et la sécurisation des outils numériques destinés aux patients.

Les secteurs du voyage, de l'hôtellerie, du commerce de détail et du divertissement souffrent eux aussi de faibles niveaux de confiance numérique. Les entreprises concernées gagneraient à mener de véritables études d'ergonomie et de parcours utilisateur afin de mieux comprendre les attentes réelles de leurs clients. Écouter les utilisateurs, observer leurs interactions, identifier ce qui crée ou détruit la confiance numérique : autant d'étapes indispensables pour améliorer la relation en ligne. Plusieurs approches contribueraient fortement à restaurer la confiance : par exemple, l'authentification sans mot de passe, une collecte de données personnelles adaptée, davantage de transparence sur l'usage et le partage des données, ou encore la possibilité pour l'utilisateur de les modifier ou de les supprimer.

> « La détection et la gestion des bots n'ont rien d'optionnel. Les bad bots perturbent le trafic des utilisateurs, ce qui entraîne une baisse de l'engagement et des revenus »

Les réseaux sociaux, de leur côté, reposent sur la monétisation des données personnelles, un modèle qui rend la confiance d'autant plus fragile. Faire peser sur les utilisateurs la responsabilité de leur propre vérification d'identité n'est pas une solution viable à long terme. Les médias, quant à eux, enregistrent les niveaux de confiance les plus faibles de l'ensemble des secteurs étudiés. Une situation regrettable, mais liée à plusieurs facteurs : dépendance accrue aux revenus publicitaires, baisse des abonnements et polarisation politique de certains organes de presse. Pour inverser cette tendance, les médias et réseaux sociaux doivent investir à la fois dans le renforcement de la sécurité des utilisateurs et dans des pratiques de vérification rigoureuse des faits. Ils doivent affirmer leur intégrité et leur transparence pour regagner la confiance du public.

Comme le souligne cet index de confiance, les approches combinant authentification multifactorielle, authentification sans mot de passe et authentification adaptative fondée sur le risque (RBA) peuvent, lorsqu'elles sont correctement mises en œuvre, renforcer significativement la sécurité tout en améliorant l'expérience client. Les mots de passe, eux, sont à la fois impopulaires et peu sûrs ; tout le monde le sait. Mais les codes à usage unique envoyés par SMS ne font guère mieux : ils ne sont pas plus sécurisés et dégradent encore davantage l'expérience utilisateur. Les clés d'accès FIDO offrent des modes de connexion plus sûrs, impossibles à usurper, et mieux acceptés par les utilisateurs. L'authentification adaptative ajoute quant à elle une couche de protection presque invisible, que les utilisateurs avertis apprécient particulièrement. Ces modèles d'authentification sont aujourd'hui largement disponibles dans les solutions de gestion des identités et des accès clients (CIAM). Ces solutions combinent souvent différents facteurs d'authentification, pour permettre aux entreprises de choisir la configuration la mieux adaptée. Si votre organisation n'exploite pas encore pleinement les possibilités de l'authentification sans mot de passe, de la MFA et de la RBA, alors elle doit en faire une priorité sans attendre, dès cette année.

La détection et la gestion des bots n'ont plus rien d'optionnel. Les bots malveillants perturbent le trafic sur les sites insuffisamment protégés, ce qui entraîne une baisse de l'engagement et des revenus. Les plateformes de réduction des fraudes (Fraud Reduction Intelligence Platforms – FRIP) intègrent désormais des systèmes avancés de détection et de contrôle des bots, souvent basés sur des biométriques comportementales invisibles pour l'utilisateur. Ces solutions permettent de bloquer les bad bots tout en supervisant l'activité des bots non nuisibles. Complémentaires des systèmes CIAM, ces FRIP jouent aujourd'hui un rôle essentiel : elles améliorent à la fois l'expérience client et la maîtrise des coûts associés aux fraudes.

L'intelligence artificielle générative (GenAI) est une technologie récente, mais déjà bien identifiée par les consommateurs, notamment dans les domaines du marketing et de la relation client. Employée avec discernement, elle peut représenter un véritable atout. Encore faut-il qu'elle facilite réellement l'usage des services numériques sans entraver leur usage. Les chatbots alimentés par l'IA peuvent se révéler utiles dans certaines situations, mais aussi agaçants, voire dissuasifs lorsqu'ils compliquent inutilement l'interaction.

En définitive, les organisations doivent miser sur des solutions adaptées aux besoins d'aujourd'hui. En adoptant une approche intégrée, elles peuvent améliorer à la fois leurs performances et optimiser l'expérience des utilisateurs.

À propos de cette étude

Cette étude a été menée auprès de 14 009 personnes interrogées en Australie, au Brésil, au Canada, en France, en Allemagne, en Inde, au Mexique, au Japon, aux Pays-Bas, à Singapour, en Suède, aux Émirats arabes unis (EAU), au Royaume-Uni et aux États-Unis.

Censuswide, qui a réalisé cette recherche, respecte les normes de la Market Research Society fondées sur les principes ESOMAR, et est également membre du British Polling Council.

THALES
Building a future we can all trust

Contactez-nous

Pour nous contacter, rendez-vous sur
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/digital-trust-index