Audit et tableau d'honneur de la confiance en ligne 2018

Reconnaître l'excellence dans les pratiques en matière de sécurité, de protection des consommateurs et de confidentialité

OTA
Online Trust Alliance
an **Internet Society** initiative

TABLE DES MATIÈRES

Présentation et contexte

Cet audit et ce tableau d'honneur de la confiance en ligne 2018, qui présentent un aperçu de l'adoption des meilleures pratiques à la fin de 2018, représente la 10ème édition annuelle de recherches de référence par l'Online Trust Alliance (OTA) afin de promouvoir les meilleures pratiques en matière de sécurité, la gestion responsable des données et les pratiques responsables en matière de confidentialité. Les principaux objectifs de ce travail consistent notamment à élever le niveau de sécurité et de confidentialité des données et à reconnaître les organisations qui ont fait preuve d'excellence en matière de sécurité et de confidentialité. En plus du statut du tableau d'honneur (annexe D), cet audit comprend une liste « Première classe » qui présente les 50 meilleures organisations, en fonction de leur score total (annexe C).

Les récentes révélations concernant la compromission des e-mails d'entreprises (123 millions de dollars extraits de Facebook et de Google), des piratages importants (383 millions d'enregistrements de Marriott), un traitement douteux des données des utilisateurs (série de révélations concernant Facebook), ainsi que le lancement du règlement général sur la protection des données (RGPD) de l'UE, renforcent la nécessité pour les organisations d'adopter les meilleures pratiques dans tous les domaines : la sécurité des e-mails, la sécurité des sites et les pratiques en matière de confidentialité. L'enquête mondiale CIGI-Ipsos de 2018 sur la sécurité et la confiance sur Internet continue de brosser un tableau sombre de l'état de la confiance en ligne. Plus de la moitié des personnes interrogées sont plus préoccupées par la confidentialité que l'année précédente et la majorité d'entre elles ont une grande méfiance à l'égard des plateformes de médias sociaux, des moteurs de recherche et des entreprises de technologie basées sur Internet.[1] [2] [3] [4] [5]

Dans de nombreux domaines, les pratiques des entreprises s'éloignent des attentes des consommateurs. Si rien n'est fait, le manque de confiance dans la confidentialité et la sécurité offertes par les organisations risque d'avoir des effets paralysants. Pour que l'économie de l'Internet prospère, les utilisateurs doivent pouvoir être sûrs que leurs informations personnelles seront sécurisées, leurs préférences respectées et leur confidentialité protégée.

Les recommandations et les meilleures pratiques de l'OTA évaluées dans le cadre de cet audit s'appliquent non seulement aux e-mails, aux sites Web et aux applications mobiles, mais également à l'univers étendu des offres en matière d'objets connectés (IoT). En plus de cet audit, les fabricants d'objets connectés devraient examiner le cadre de confiance en matière d'objets connectés de l'OTA pour des recommandations spécifiques à ces offres.[6] L'audit de 2018 a été amélioré dans plusieurs domaines : des sous-secteurs supplémentaires, un nouveau secteur majeur (santé) et des critères élargis dans chaque catégorie principale, ce qui représente désormais plus de 100 attributs de données (annexe B), offrant ainsi une vue d'ensemble plus complète sur la confiance en ligne au travers d'un plus grand nombre d'organisations concernées. De nouveaux critères ont été ajoutés et la pondération a été mise à jour pour refléter l'évolution du paysage des menaces, de l'environnement réglementaire et des pratiques acceptées à l'échelle mondiale. En outre, les principes de niveau élevé liés au RGPD ont été pris en compte pour créer une base de référence pour les futurs audits. Pour aider les organisations, ce

rapport comprend une liste de contrôle des meilleures pratiques (annexe E), ainsi que des ressources pour l'implémentation (annexe F).

Il est important de noter que l'audit est limité à une période spécifique. Compte tenu de la nature dynamique des configurations des sites Web et des applications, les scores des organisations peuvent avoir évolué depuis la fin de l'audit. Toutes les analyses ont été effectuées sans la contribution active des sites analysés. Les sites ont été sélectionnés en fonction de leur classement dans leurs secteurs individuels ou dans les listes publiques (ou de l'adhésion de leur organisation à l'Internet Society). Dans les cas où une vulnérabilité importante a été identifiée, l'OTA a respecté les pratiques de divulgation coordonnée, et a tenté de contacter l'entité « à risque » pour lui donner une chance de remédier au problème constaté et de se réorganiser avant la publication du présent rapport.

Synthèse et points importants

L'audit et le tableau d'honneur de la confiance en ligne 2018 évaluent près de 1 200 organisations et examinent les pratiques en matière de sécurité, de confidentialité et de protection des consommateurs.[7] Les améliorations apportées à l'audit comprennent l'ajout de nouveaux sous-secteurs dans les secteurs des actualités et médias et de la consommation (informations sportives, diffusion vidéo en continu et services de paiement), ainsi que la création d'un nouveau secteur, la santé. Ce secteur comprend les principales compagnies d'assurance médicale, les pharmacies, les laboratoires de tests médicaux et les chaînes hospitalières. Les secteurs examinés et les organisations afférentes les mieux classées comprennent :

- Top 500 des détaillants en ligne 2018 (IR 100 et IR 500)[8]
- Top 100 des banques fédérales de réserve (Bank 100)[9]
- Top 100 des organisations du gouvernement fédéral américain
  (Federal 100)
- Top 100 des entreprises de services aux consommateurs (Consumer 100)[10]
- Top 100 des organisations liées aux actualités et aux médias (News 100)
- Top 100 des FAI, opérateurs et hébergeurs (ISP/Hosts 100)
- Top 100 des organisations liées à la santé (Health 100)
- Organisations membres de l'OTA de l'Internet Society (OTA)[11]

« Nous sommes ravis de constater qu'au fil du temps, de plus en plus d'organisations satisfont aux critères du tableau d'honneur d'Online Trust Alliance, et évoluent pour répondre à la demande croissante de la société d'un Internet plus sûr ». - Neil Daswani, vice-président principal, responsable de la sécurité des systèmes d'information, Norton LifeLock

Bien que la majorité des segments restent les mêmes, la liste réelle des organisations auditées chaque année évolue en fonction du classement des revenus ou du trafic et de la consolidation du marché. Cette année, avec l'ajout du secteur de la santé et des ajouts ou des changements des organisations figurant sur les listes de classement, environ 30 % des organisations auditées sont nouvelles.

Comme les années précédentes, 100 points de référence peuvent être acquis dans chacune des trois grandes catégories d'évaluation (protection du consommateur, sécurité du site et confidentialité). Des points de bonus sont attribués aux meilleures pratiques émergentes et des points de pénalité aux

violations, aux règlements judiciaires et aux vulnérabilités observées. Un score minimal de 60 est requis dans chacune des trois catégories. Les points de bonus sont limités à 20 % du score de référence. Les sites se qualifient pour le tableau d'honneur lorsqu'elles obtiennent un score global de 80 % ou plus et n'échouent dans aucune des trois catégories principales.

En 2018, des records de réussite ont été enregistrés : 70 % des organisations ont atteint le statut du tableau d'honneur (le précédent record était de 52 % dans l'audit de 2017). Étant donné que la méthodologie a été mise à jour pour « relever la barre » dans les trois catégories de notation, cela est impressionnant. Les scores des anciens membres de l'OTA ne sont pas intégrés aux résultats (à l'exception des meilleurs scores globaux) car ils les fausseraient (98 % ont atteint le statut de tableau d'honneur).

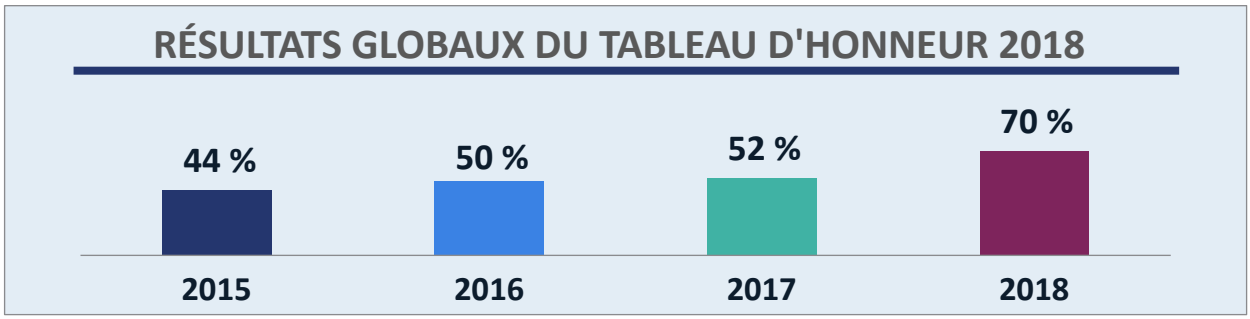


Figure 1 – Résultats globaux du tableau d'honneur par année, 2015 à 2018

Comme le montre la figure 2, les résultats du tableau d'honneur ont progressé dans tous les secteurs malgré des critères plus stricts définis dans l'audit de cette année.[12] Le Federal 100 a obtenu de meilleurs résultats que tous les autres secteurs, avec un taux de réussite de 91 %, dépassant le Consumer 100, qui a été le meilleur secteur pendant six années consécutives. Les entités du gouvernement fédéral américain sont celles qui ont également été les plus améliorées, suivies de près par le Bank 100 et le News 100. Le secteur de la santé, nouvellement ajouté, affiche une réalisation de 57 % au tableau d'honneur, en retard par rapport à tous les autres secteurs.

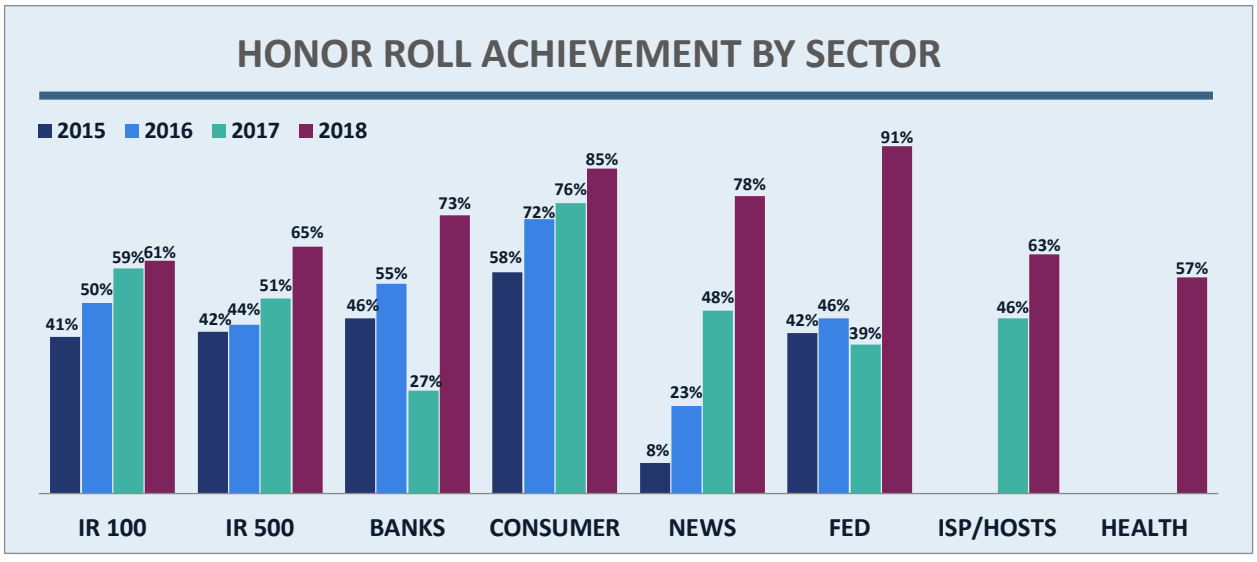


Figure 2 – Pourcentage d'atteinte du statut de tableau d'honneur par secteur, 2015 à 2018

Comme les années précédentes, les résultats ont été quasiment bimodaux, la majorité des sites se qualifiant pour le tableau d'honneur ou échouant dans un ou plusieurs domaines. Comme le montre la figure 3, globalement seuls 3 % n'ont pas échoué, mais ne se sont qualifiés pour le tableau d'honneur, ce résultat allant de 0 % à 7 % pour les secteurs individuels.

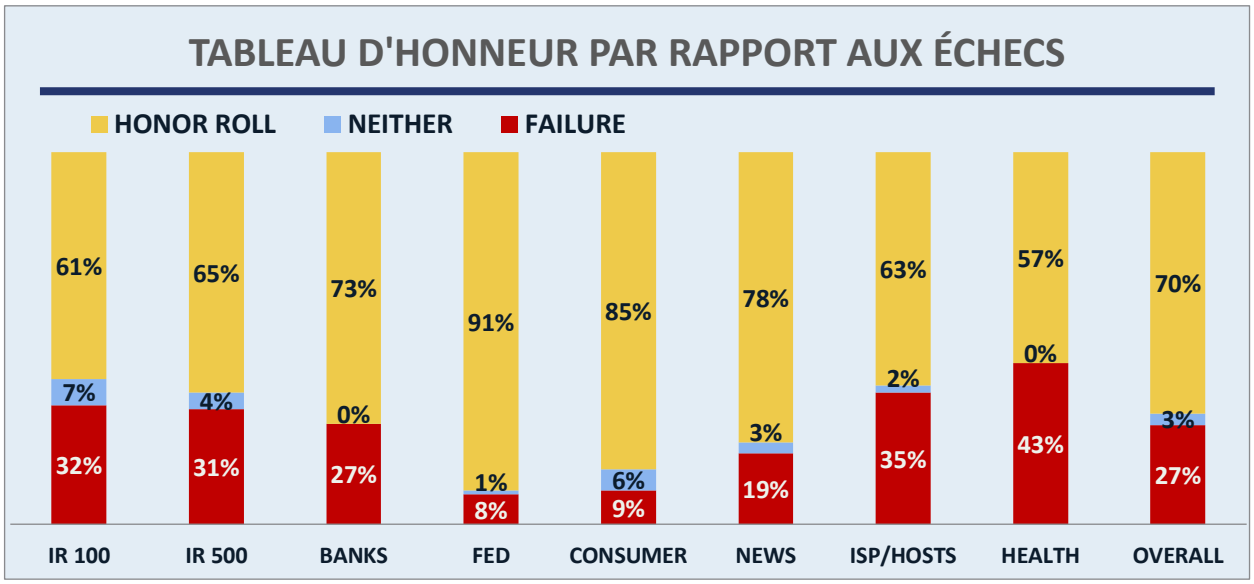


Figure 3 - Répartition du tableau d'honneur et des échecs par secteur

Lors de l'audit de 2017, une catégorie « Première classe » a été créée, représentant les 50 meilleurs scores (Top 50). Cette année, tous les secteurs sont représentés dans le Top 50, comme le montre le tableau ci-dessous (il est à noter que, comme plusieurs organisations appartiennent à différents secteurs, le total dépasse 100 %). Le secteur fédéral a enregistré la plus forte augmentation dans le Top 50, passant de 12 % en 2017 à 26 % cette année. Le secteur bancaire, qui n'était pas présent en 2017, avait trois organisations dans le Top 50 cette année. L'annexe C contient une liste complète des 50 organisations ayant le meilleur score.

TOP 50 DES PERFORMANCES SECTORIELLES

Code	Secteur	% du Top 50
C	Services aux consommateurs	40 %
F	Gouvernement fédéral américain	26 %
R	Détaillants en ligne	14 %
O	Membres de l'OTA (Internet Society)	12 %
B	Banques	6 %
H	Santé	4 %
I	FAI, opérateurs et hébergeurs	4 %
N	Actualités / Médias	4 %

Figure 4 - Top 50 des performances par secteur

Le score global le plus élevé de l'audit a été acquis par Google Actualités, qui avait également le meilleur score dans le secteur des actualités / médias. Les autres secteurs gagnants ont été 23andMe (Santé),

l'agence fédérale des situations d'urgence - FEMA (gouvernement fédéral américain), First National Bank of Omaha (banques), Google Cloud (FAI / Hébergeurs), Google Play (détaillants en ligne), Online Trust Alliance (membres de l'OTA de l'Internet Society) et PayPal (consommateur).

Les résultats globaux des échecs, comme présentés à la figure 5, montrent que la confidentialité était la principale cause d'échec pour tous les secteurs (15 %), suivie de la protection des consommateurs (13 %) et de la sécurité des sites (3 %). Le taux d'échec dans la catégorie Protection des consommateurs a été considérablement amélioré par rapport aux 33 % de 2017, principalement en raison d'une adoption nettement plus élevée du DKIM (DomainKeys Identified Mail). Les taux d'échec ont varié considérablement selon les secteurs (figure 6). Dans l'ensemble, 27 % des sites ont échoué dans un ou plusieurs domaines (contre 47 % en 2017). Les principales causes d'échec étaient l'absence d'authentification des e-mails dans les secteurs de la santé et des FAI / Hébergeurs, suivies de l'inadéquation des déclarations de confidentialité pour les secteurs des détaillants en ligne et des FAI / Hébergeurs. Inversement, le secteur fédéral et celui des actualités n'ont connu aucun échec dans la sécurité des sites, et le secteur fédéral et celui de la consommation ont dominé en matière de confidentialité, avec seulement 2 % d'échec.

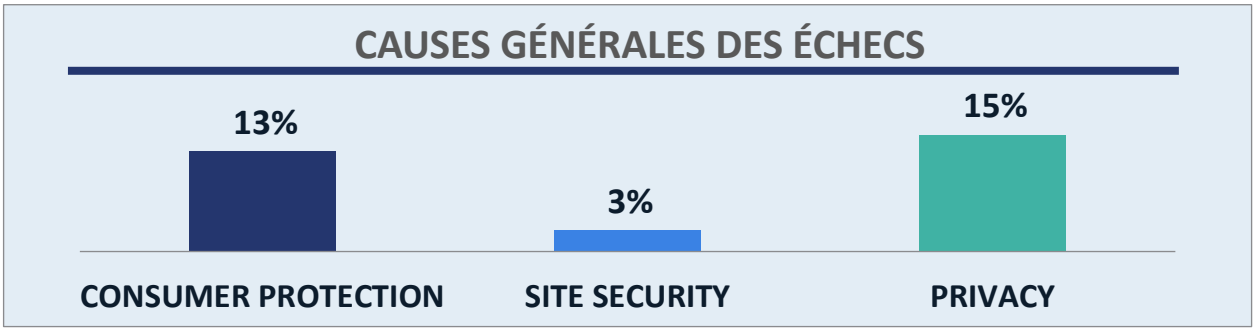


Figure 5 - Causes des échecs par catégorie d'audit

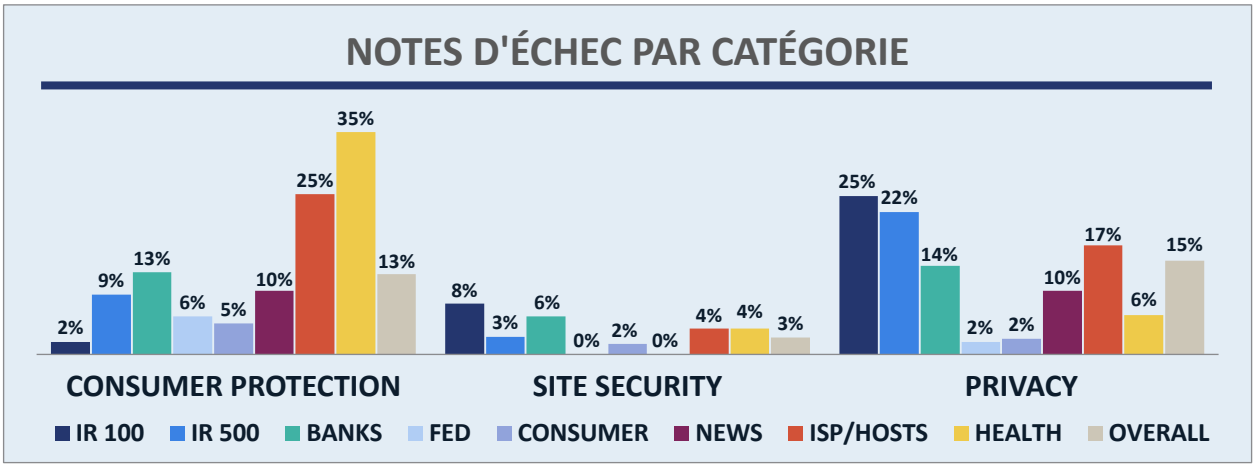


Figure 6 - Pourcentage des entreprises ayant un taux d'échec, par secteur et par catégorie

Une perspective supplémentaire peut être obtenue en normalisant les 300 points de référence sur une échelle de 100 points (appelée « Indice de confiance en ligne ») et en comparant les indices hauts, bas et médians de différents secteurs. Pendant plusieurs années, la médiane dans la plupart des secteurs a oscillé autour du seuil de 80 % pour le tableau d'honneur, ce qui signifie que de nombreuses

organisations étaient très proches d'atteindre le tableau d'honneur. La figure 7 montre que cette année, la médiane pour tous les secteurs est supérieure au seuil de 80 % et qu'elle dépasse 90 % pour plusieurs d'entre eux.

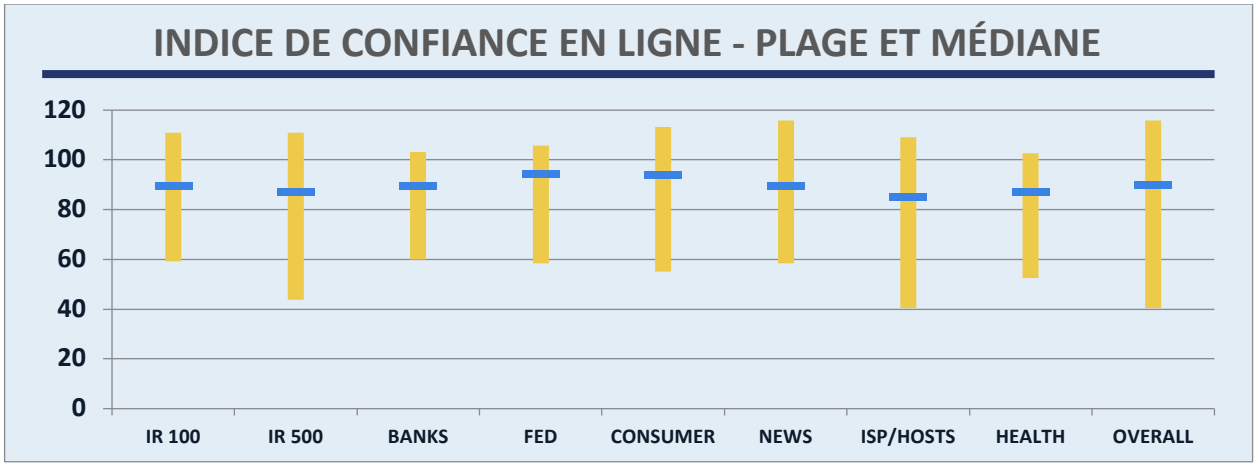


Figure 7 – Plage et médiane des scores de l'indice de confiance en ligne par secteur

Points importants des meilleures pratiques

Ce qui suit est un résumé des meilleures pratiques auditées et préconisées par l'OTA. Des informations supplémentaires sont fournies dans les sections suivantes : 1) Protection du domaine, de la marque et du consommateur, 2) Sécurité du site, du serveur et de l'infrastructure, et 3) Confidentialité, transparence et divulgation.

Protection du consommateur

Authentification des e-mails – La méthodologie a été mise à jour en 2017 pour garantir que les enregistrements SPF et DMARC (Authentification, rapport et conformité de message par domaine) étaient conformes aux spécifications publiées. Les enregistrements non conformes ont, reçu un crédit partiel ou ont été totalement disqualifiés. Parmi toutes les organisations, 3 % avaient un enregistrement SPF invalide et 13 % avaient des erreurs qui ne leur ont permis de recevoir qu'un crédit partiel. De même, 2 % des enregistrements DMARC ont été jugés invalides. Cela souligne la nécessité pour les sites de surveiller en permanence leurs enregistrements afin de maximiser la protection de la marque et du consommateur. S'ils ne sont pas surveillés, les marques peuvent avoir un faux sentiment de sécurité, car certains réseaux et FAI peuvent ne pas tenir compte de ces enregistrements « invalides ».

- Dans l'ensemble, le recours à l'authentification des e-mails a atteint des niveaux record. L'adoption de SPF dans le domaine de premier niveau est passée de 77 % à 89 %, tandis que l'adoption de DKIM dans le domaine de premier niveau a augmenté de manière encore plus spectaculaire, passant de 56 % à 83 %.
- Le recours aux enregistrements DMARC a augmenté de 34 % à 50 %. Le DMARC est utilisé conjointement avec le SPF et le DKIM pour se défendre contre les e-mails frauduleux et falsifiés utilisés pour l'hameçonnage et l'attaque des e-mails d'entreprise.
- L'adoption des enregistrements de rejet ou de mise en quarantaine de DMARC dans le domaine de premier niveau est passée de 15 % à 24 %. Cette politique de « mise en vigueur » demande aux destinataires d'e-mails de mettre en quarantaine ou de bloquer les messages qui échouent à l'authentification, protégeant ainsi les consommateurs des e-mails frauduleux.

TLS opportuniste – Il chiffre les messages entre les serveurs de messagerie. Son adoption continue de progresser, passant de 65 % à 73 %. (Points de bonus)

Extensions de sécurité DNS (DNSSEC) – L'adoption a légèrement diminué, passant de 12 % à 10 %. Ceci peut être entièrement attribué aux modifications apportées aux listes des secteurs. (Points de bonus)

IPv6 – L'adoption a légèrement baissé, passant de 14 % à 12 %, principalement en raison de critères plus stricts (les sites Web devaient être accessibles via IPv6. Les années précédentes, seul le service de nom devait être conforme à IPv6). Même avec cette barre plus haute, certains secteurs ont progressé dans son adoption (banques : de 0 % à 6 %, consommateurs : de 12 % à 15 % et détaillants en ligne : de 5 % à 7 %). (Points de bonus)

Sécurité de site

HSTS (HTTP Strict Transport Security), Toujours en SSL ou HTTPS Partout – Cet élément est devenu une partie de la notation de référence cette année (auparavant, il faisait gagner des points de bonus). Son adoption a de nouveau fortement progressé, passant à 93 %, contre 30 % en 2016 et 52 % en 2017. Cette augmentation est attribuée à l'attention accrue portée au chiffrage en ligne en tant que « norme »

pour la communication sur Internet. Elle est fondée sur les préoccupations de la surveillance des activités sur le Web par des tiers et par le gouvernement. Lors des audits précédents, 99 % des sites prenaient en charge le chiffrage, mais celui-ci s'appliquait souvent uniquement aux pages de connexion ou de transaction financière plutôt qu'à la totalité de la session Web.

Scores globaux de sécurité du site – Les scores globaux ont légèrement diminué, passant de 91 à 89 (sur 100), entièrement en raison de la pondération accrue des scores de réputation de l'IP, des correctifs logiciels et de la sécurité des en-têtes de sites Web. De nombreux sites ne définissent toujours pas de stratégie de sécurité du contenu et ne limitent pas l'exposition aux vulnérabilités introduites par les cookies et autres contenus tiers en configurant des en-têtes de sécurité Web. La part la plus conséquente du score de sécurité du site est toujours liée à la configuration SSL / TLS, et les scores ont en réalité été améliorés de 2 % dans cet aspect, car davantage de sites utilisent des configurations appropriées de protocoles et de méthodes de chiffrement. Les sites présentant des scores en échec présentaient les mêmes problèmes que ceux observés au cours des années précédentes : méthodes de chiffrement faibles ou non sécurisées, utilisation de protocoles non sécurisés et chaînes de certificats incomplètes conduisant à des vulnérabilités et à des menaces telles que l'attaque ROBOT. Les banques avaient le taux d'échec le plus élevé (6 %). L'utilisation de nouveaux protocoles TLS a continué d'évoluer : 29 % des sites ne prennent pas en charge les protocoles plus anciens que TLS1.2 et 7 % prennent déjà en charge TLS1.3, qui a été officiellement publié par l'IETF (Internet Engineering Task Force) en août 2018.[13]

« Il s'agit de l'audit d'OTA le plus complet à ce jour et nous avons enregistré des bonds record dans l'adoption de pratiques clés telles que l'authentification des e-mails et le chiffrage de bout en bout », a déclaré Olaf Kolkman, responsable des technologies Internet à l'Internet Society. « C'est encourageant et nous espérons que cela motivera toutes les organisations à faire de même. Les pratiques que nous auditons renforcent la confiance des consommateurs, non seulement dans l'organisation individuelle, mais également dans l'Internet dans son ensemble ».

Autorisation d'autorité de certification (CAA) – Cela permet aux sites de publier une liste des autorités de certification autorisées à émettre des certificats pour leur domaine, limitant ainsi les abus. Cet élément a été ajouté à l'audit de 2018 car, depuis septembre 2017, le forum des autorités de certification a imposé aux autorités de certification de vérifier la CAA avant d'émettre ou de renouveler des certificats. Malheureusement, seuls 6 % de l'ensemble des sites tirent parti de cette capacité, avec en tête les secteurs Consommateur et FAI / Hébergeurs, respectivement à 20 % et 13 %. L'adoption dans tous les autres secteurs est inférieure à 6 %. (Points de bonus)

Mécanismes / programmes de divulgation de la vulnérabilité – Ceci a été ajouté en 2017 et est reconnu comme une meilleure pratique par la NTIA (National Telecommunications and Information Administration), la NIST (National Institute of Standards and Technology), la FTC (Federal Trade Commission) et l'OTA. L'adoption a augmenté globalement de 6 % à 11 % pour les sites dotés d'un mécanisme de rapport visible sur leur site ou répertoriés avec des fournisseurs de services de recherche de faille par des tiers, appelés « bug bounty ». Le secteur de la consommation a dépassé tous les autres avec une adoption à 43 %, suivi des FAI / hébergeurs avec 25 %, des actualités / médias avec 9 % et des banques avec 6 %. Disposer de tels mécanismes est essentiel pour répondre efficacement aux rapports des chercheurs et des utilisateurs tiers et est relativement simple à mettre en œuvre. (Points de bonus)

Vulnérabilités XSS (scripts intersite) – Après avoir augmenté de 27 % en 2016 à 50 % en 2017, la présence de vulnérabilités XSS a chuté de manière significative à 21 % lors de cet audit. Les sites d'actualités affichaient le taux le plus élevé (43 %) et les banques, le plus faible (5 %). Plusieurs secteurs se situaient aux alentours de la moyenne globale entre 21 % et 23 %.

Tendances en matière de confidentialité

Les scores combinés (déclaration de confidentialité et utilisation de traceurs tiers) ont chuté de 73 à 70 cette année, principalement en raison de la notation plus stricte de certains critères clés de la déclaration de confidentialité.

Déclaration de confidentialité – Le score global des déclarations de confidentialité est passé de 31 en 2017 à 27 en 2018. Des changements importants ont été observés dans le texte sur la conservation des données (baisse de 49 % à 2 % car il nécessite désormais un délai de conservation spécifique comme stipulé dans le RGPD), les déclarations par couches (augmentation de 29 % à 47 %) et l'exigence vis-à-vis des fournisseurs tiers du respect des mêmes pratiques de confidentialité que l'organisation (augmentation de 48 % à 57 %). En outre, le critère de partage des données a été divisé en deux parties - texte sur le partage de base (par exemple, « nous ne partageons pas les données sauf avec des tiers qui fournissent le service » - 67 % ont une telle déclaration, une augmentation modeste par rapport à 63 % en 2017.) et texte « affilié » (par exemple, « nous ne partageons pas avec des affiliés ou d'autres tiers » - seuls 20 % ont une telle restriction). Cela signifie que 80 % partagent ou pourraient partager des données avec des tiers. L'exception concernant le partage avec les affiliés est préoccupante, car elle permet souvent un marketing ciblé et d'autres activités auxquelles l'utilisateur ne s'attend pas.

Pour la première fois, l'affichage des dates de déclaration de confidentialité a été pris en compte lors de l'audit de cette année, car ils étaient jugés présenter un intérêt compte tenu de l'entrée en vigueur du RGPD en mai 2018. Dans l'ensemble, 31 % des sites n'indiquaient pas de date, 11 % une date antérieure à 2017, 11 % une date en 2017 et 47 % indiquaient une date plus récente que le 1er janvier 2018. Le secteur de la consommation avait les déclarations de confidentialité les plus « fraîches » (71 % plus récentes que le 1er janvier 2018), tandis que le secteur de la santé présentait les déclarations les moins récentes (seulement 19 % plus récentes que le 1er janvier 2018).

Harmonisation avec le RGPD – Depuis que le RGPD est entré en vigueur au milieu de 2018, diverses données relatives au RGPD ont été prises en compte pour créer une base de référence, et des points de bonus ont été attribués aux organisations qui incluent des principes clés liés au RGPD dans leur déclaration de confidentialité. Des points de bonus (par rapport à la base de référence) ont été attribués, car la plupart des organisations (et les sites connexes) auditées et évaluées sont basées aux États-Unis. Par conséquent, le RGPD ne s'y applique pas nécessairement. Les analyses ont montré que :

- 32 % des déclarations de confidentialité ont été jugées faciles à lire (ce qui implique un besoin évident d'amélioration pour près de 70 % d'entre elles),
- 95 % des déclarations expliquaient suffisamment quelles données étaient collectées et pour quelle raison,
- Moins de 1 % ont nommé les catégories de tiers avec lesquels ces données sont partagées,
- 70 % ont identifié un moyen de contacter le responsable de la protection des données,
- Seulement 1 % ont indiqué comment les informations personnelles sensibles (données biométriques, origine raciale ou ethnique, opinions politiques, convictions religieuses ou

philosophiques, etc.) recueillies par des tiers sont traitées (cette déclaration n'est nécessaire que si ces données sont traitées), et
- 50 % ont décrit le processus permettant aux utilisateurs d'accéder aux données collectées par l'organisation à leur sujet.

Traceurs tiers – Dans l'ensemble, les scores relatifs aux traceurs problématiques sont restés stables, augmentant légèrement de 42,0 en 2017 à 42,4 en 2018. Ce sont des traceurs connus pour partager des données avec des tiers (ce qui ne prend pas en compte les données prises en compte pour des mesures anonymes ou sous pseudonymes pour le site). Le nombre de traceurs uniques observés sur tous les sites allait de 0 à 40. Le secteur des actualités et médias affichait plus du double de la moyenne globale tous secteurs confondus, ce qui témoigne de sa dépendance à l'égard de la publicité et du ciblage des utilisateurs du site.

Pertes et piratages des données – Les résultats des mesures réalisées entre juin 2017 et décembre 2018 indiquent que 15 % des sites ont subi un ou plusieurs incidents (contre 12 % en 2017). Le secteur de la consommation avait le taux le plus élevé (34 %), suivi du secteur de la santé (30 %). Les banques, qui avaient le taux le plus élevé lors de l'audit de 2017, suivaient avec 20 %. Les organisations dont le nombre de violations dépassait 1 000 enregistrements ont été sanctionnées. Cette année, la pénalité a été rendue proportionnelle à l'étendue du piratage.[14]

Amendes et règlements judiciaires – Dix-huit organisations ont été sanctionnées pour avoir eu des procès ou des règlements cette année (en baisse par rapport à 21 en 2017), le secteur Consommateur en ayant le plus (14). Les données comprennent les actions du bureau de la protection financière des consommateurs (CFPB), des bureaux du procureur général de chaque État, des recours collectifs et des agences internationales ainsi que de la commission fédérale du commerce (FTC) aux États-Unis. Aux fins de l'audit, l'accent est mis sur les mesures de protection du consommateur en matière de sécurité et de confidentialité et n'inclut pas les règlements relatifs aux fusions et acquisitions ou les questions relatives au droit du travail.

Protection du domaine, de la marque et du consommateur

En utilisant l'authentification des e-mails (SPF et DKIM), les organisations peuvent protéger leurs marques et empêcher les consommateurs de recevoir des e-mails frauduleux et falsifiés. L'authentification des e-mails permet aux expéditeurs de spécifier qui est autorisé à envoyer un e-mail en leur nom. S'appuyant sur les protocoles d'authentification des e-mails, le DMARC ajoute un argument à cette politique, indiquant aux destinataires comment gérer les messages qui dont l'authentification échoue. Le TLS opportuniste fournit un moyen de chiffrer les messages entre les serveurs de messagerie, protégeant à la fois la marque et le consommateur. Le verrouillage de domaine garantit que la propriété du domaine ne peut pas être transférée sans l'autorisation du propriétaire. Les extensions de sécurité DNS (DNSSEC) renforcent la sécurité et l'intégrité du DNS, en aidant à prévenir les attaques de « l'homme du milieu » (MitM), l'empoisonnement de cache et les attaques associées au DNS. IPv6 augmente le nombre d'adresses IP uniques, prenant ainsi en charge la croissance d'Internet, y compris la demande de nouvelles adresses IP générées par les objets connectés.[15] [16]

Les meilleures pratiques incluent :

- L'implémentation à la fois de SPF et de DKIM pour les domaines de premier niveau, les domaines « parqués » (non utilisés pour l'e-mail) et tous les sous-domaines principaux vus sur les sites Web ou utilisés pour l'e-mail.
- L'optimisation des enregistrements SPF avec un maximum de 10 requêtes DNS.
- L'implémentation du DMARC, initialement en mode « surveillance » pour obtenir les commentaires du destinataire et vérifier l'exactitude de l'authentification des e-mails, et éventuellement passer à la « mise en application » (signaler une stratégie de « rejet » ou de « mise en quarantaine » aux destinataires).
- L'obligation de l'utilisation des fonctionnalités de génération de rapports de DMARC avec les rapports RUA et RUF
- La mise en place des contrôles d'authentification des e-mails entrants et du DMARC sur tous les réseaux pour vous protéger contre les e-mails malveillants et l'hameçonnage prétendant provenir d'expéditeurs légitimes.
- L'implémentation du TLS opportuniste pour protéger les e-mails en transit entre les serveurs de messagerie.
- L'assurance du verrouillage des domaines pour empêcher leurs prises de contrôle.
- L'implémentation de DNSSEC pour protéger l'infrastructure DNS d'un site.
- Le déploiement d'IPv6.
- La mise en place des technologies et des processus d'atténuation des attaques DDoS (déni de service distribué).
- La mise en place d'une authentification multifacteur.

Authentification des e-mails

Les technologies d'authentification, à savoir SPF et DKIM, aident à lutter contre l'hameçonnage et l'envoi de courriers indésirables. OTA recommande l'utilisation de l'authentification des e-mails dans le domaine de premier niveau (ou « corporatif »), ainsi que dans tout autre domaine utilisé pour l'envoi

d'e-mail ou susceptible d'être utilisé pour tromper les consommateurs. Une télémétrie supplémentaire a été ajoutée lors de l'audit de 2017 afin d'évaluer la validité des enregistrements SPF et DMARC. L'authentification par le domaine de premier niveau a reçu une pondération accrue pour la troisième année consécutive.

La figure 8 illustre l'adoption de SPF et de DKIM dans le domaine corporatif de premier niveau et l'utilisation combinée de SPF et de DKIM à tous les niveaux, y compris pour les sous-domaines. En règle générale, l'adoption de SPF est supérieure à celle de DKIM, bien que l'écart se resserre. D'après nous, ceci est principalement dû à sa facilité d'implémentation. L'utilisation à la fois de SPF et de DKIM permet aux destinataires de détecter et de bloquer les e-mails malveillants tout en réduisant le risque de faux positifs.

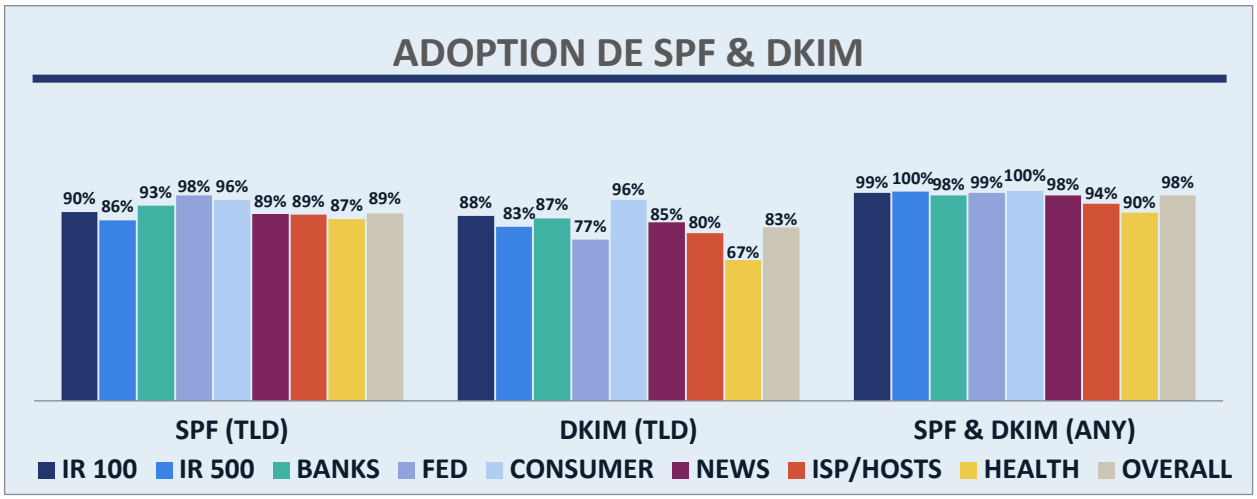


Figure 8 - Authentification des e-mails et adoption du DMARC par secteur

Comme le montre la figure 9, tous les secteurs ont enregistré une croissance et nombre d'entre eux approchent de l'adoption à 100 %. Des bonds significatifs ont été observés dans le secteur fédéral (de 46 % à 94 %, principalement grâce à la directive DHS 18-01) et dans le secteur bancaire (60 % à 87 %).[17] Les secteurs de la santé et des FAI / Hébergeurs sont en retard avec respectivement 65 % et 75 %. Bien que les écarts se réduisent, dans certains secteurs, la prise en charge de l'authentification des e-mails au niveau du domaine de premier niveau fait encore défaut (notez l'écart entre « DKIM TLD » et « SPF et DKIM » dans la figure 8 ci-dessus). Cela souligne que des efforts supplémentaires sont nécessaires pour stimuler l'implémentation de DKIM afin de protéger les domaines corporatifs de premier niveau et d'entreprise des abus.

À LA FOIS SPF ET DKIM

	2015	2016	2017	2018
Top 100 des détaillants en ligne	90 %	92 %	92 %	98 %
Top 500 des détaillants en ligne	78 %	85 %	83 %	95 %
Bank 100	63 %	69 %	60 %	87 %
Federal 100	48 %	58 %	46 %	94 %
Consumer 100	76 %	86 %	88 %	95 %

News 100	56 %	75 %	77 %	94 %
ISP/Hosts 100	-	-	55 %	75 %
Health 100	-	-	-	65 %

Figure 9 - Adoption à la fois du SPF et du DKIM par secteur

Dès 2017, les enregistrements de SPF ont été analysés plus en détail et n'ont reçu qu'un crédit partiel ou ont été considérés comme invalides s'ils contenaient des erreurs qui les rendaient inutilisables ou inefficaces. Cela a eu un impact sur 16 % de l'ensemble des organisations et particulièrement chez les détaillants (20 %). Le secteur fédéral présente le taux d'erreur le plus faible (4 %). Les principales raisons de ne recevoir qu'un crédit partiel étaient les résolutions DNS excessives et les références à des enregistrements SPF non existants ou non valides d'autres domaines.[18] Les principales raisons pour considérer les enregistrements comme invalides étaient l'utilisation de plusieurs enregistrements SPF et des erreurs de syntaxe rendant l'enregistrement inutilisable. En outre, l'utilisation d'une instruction « +all » ou « ?all » a été observée, qui indique de fait aux destinataires (des FAI et des réseaux corporatifs) d'autoriser une adresse IP à envoyer un e-mail ou d'ignorer l'enregistrement. Ces enregistrements ont également été jugés invalides. Beaucoup de ces organisations peuvent avoir un faux sentiment de sécurité, ne sachant pas que leurs enregistrements de SPF ne protègent pas efficacement leur domaine.

En dehors du domaine ou de la capacité de cet audit, toutes les organisations doivent déployer des contrôles d'authentification des données entrantes et appliquer les stratégies de DMARC. En tant que pratique recommandée pour la réduction des risques, les principaux fournisseurs, partenaires commerciaux et prestataires de services devraient être tenus de déployer une authentification de bout en bout, notamment SPF, DKIM et DMARC.

Authentification, rapport et conformité de message par domaine (DMARC)

Le DMARC s'appuie sur les résultats de SPF et de DKIM, fournit un moyen de générer des rapports de rétroaction et ajoute une visibilité aux destinataires sur la manière de traiter les messages dont l'authentification échoue. En plus de la notation de référence de 2013, un poids supplémentaire a été attribué à l'utilisation des politiques de rejet et de mise en quarantaine par DMARC en 2016, avec le nombre maximal de points attribués aux politiques de rejet. La pondération a été augmentée pour l'utilisation de la politique de rejet cette année.

Comme le montrent les figures 10 et 11, l'adoption du DMARC a progressé dans la plupart des secteurs, notamment dans le secteur fédéral (20 % à 93 %, principalement en raison de la directive 18-01), le secteur bancaire (39 % à 70 %) et le secteur des actualités (29 % à 50 %). Des enregistrements de DMARC invalides ont été observés dans près de 2 % des organisations, mais surtout dans le secteur des FAI / Hébergeurs (5 %). Les principales raisons pour invalider un enregistrement étaient un enregistrement « nu » (p=none et pas de rapport RUA ou RUF) et des rapports pointant vers des domaines incapables de les accepter.

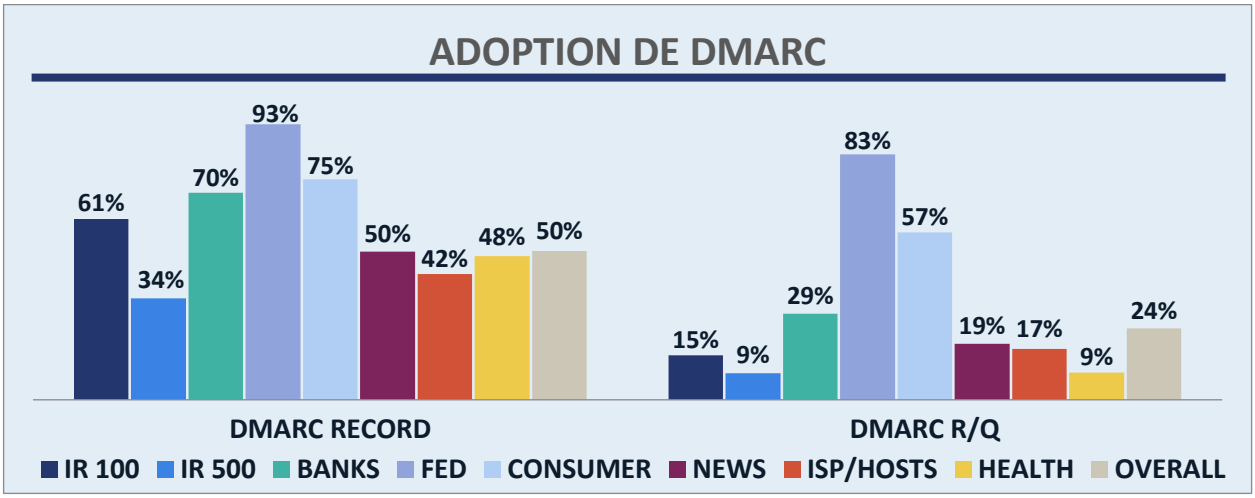


Figure 10 - Adoption et politiques de DMARC

ADOPTION DE DMARC

	2015	2016	2017	2018		
	Enregistrement	Enregistrement	Enregistrement	Tous les enregistrements	Enregistrement valide	R ou Q *
Top 100 des détaillants en ligne	20 %	30 %	50 %	61 %	61 %	15 %
Top 500 des détaillants en ligne	8 %	21 %	33 %	34 %	33 %	9 %
Bank 100	24 %	33 %	39 %	70 %	70 %	29 %
Federal 100	14 %	20 %	20 %	93 %	93 %	83 %
Consumer 100	48 %	64 %	62 %	75 %	74 %	57 %
News 100	10 %	21 %	29 %	50 %	48 %	19 %
ISP/Hosts 100	-	-	25 %	42 %	37 %	17 %
Health 100	-	-	-	48 %	47 %	9 %

Figure 11 - Adoption de DMARC par secteur. * R ou Q = Politique de Rejet ou politique de mise en Quarantaine

Sécurité de la couche de transport (TLS) opportuniste pour l'e-mail

Le traçage du TLS opportuniste pour l'e-mail a été ajouté lors de l'audit de 2015 afin de répondre aux préoccupations croissantes en matière de confidentialité concernant la surveillance des e-mails en transit. Le TLS chiffre les messages en transit d'un serveur à un autre et les déchiffre facilement avant leur livraison à l'utilisateur. L'adoption de TLS est en croissance constante, passant de 65 % en 2017 à 73 % cette année. Le secteur fédéral continue à accuser un retard avec 51 %, tandis que les secteurs de la consommation et des actualités arrivent en tête avec une adoption de 83 %. La croissance est attribuée à un appel global au chiffrement lancé par des dizaines d'organisations, notamment Internet Society, ainsi que Google et Twitter, qui fournissent des données sur l'utilisation de TLS opportuniste. Depuis début 2016, Gmail a également mis en évidence les messages sans TLS avec un cadenas rouge déverrouillé.[19]

Verrouillage de domaine

Le verrouillage de domaine est devenu un élément de notation en 2013 en raison de son importance dans la prévention des prises de contrôle de domaine (une pénalité est attribuée si le domaine n'est pas verrouillé). Plus de 95 % des organisations, dans tous les secteurs, verrouillent leurs domaines. Le secteur fédéral arrive en tête avec une adoption à 100 %, suivi de près par le secteur de la consommation (98 %) et celui de la santé (97 %). Les secteurs des détaillants, des banques, des actualités et des FAI / Hébergeurs se situent tous entre 93 % et 94 %.

Extensions de sécurité DNS (DNSSEC)

DNSSEC renforce la sécurité d'une requête DNS. Il est conçu pour aider à lutter contre les attaques de « l'homme du milieu » (MitM) et l'empoisonnement de cache en authentifiant l'origine des données DNS et en vérifiant leur intégrité lors de leurs déplacements sur Internet. DNSSEC est maintenant déployé pour .com, .gov, .org, .net et plus de 135 autres domaines de premier niveau, prenant potentiellement en charge plus de 90 millions d'enregistrements de noms de domaine dans le monde, uniquement pour le domaine .com.[20] L'adoption de DNSSEC a chuté de 12 % en 2017 à 10 % cette année en raison de changements dans la liste des organisations auditées. Le secteur fédéral arrive en tête des adoptions (87 %) principalement en raison d'une obligation de 2008, suivi du secteur bancaire (10 %) et du secteur des FAI / Hébergeurs (8 %).[21] L'implémentation plus large de DNSSEC continue d'être entravée par les systèmes en place et le manque d'infrastructures écosystémiques.

Protocole Internet Version 6 (IPv6)

IPv6 est la version la plus récente du protocole Internet (IP), protocole de communication qui fournit un système d'identification et de localisation des ordinateurs sur Internet et qui augmente considérablement le nombre d'adresses disponibles. L'OTA soutient un déploiement plus large, attribuant des points de bonus à son adoption. L'adoption dans le monde entier est en croissance, le Top 1000 des sites Web du classement Alexa étant accessible à plus de 26 % sur IPv6, soit 2 % de plus qu'en 2017.[22] L'adoption globale lors de l'audit d'OTA est passée de 14 % en 2017 à 12 % cette année en raison d'exigences plus strictes : les sites Web devaient être accessibles via IPv6, alors que les années précédentes, seul le service de nom devait être conforme à IPv6. Le secteur fédéral arrive en tête avec une adoption de 46 %, suivi du secteur des FAI / Hébergeurs à 20 % et du secteur organisations de consommateurs à 15 %.

Authentification multifacteur (AMF)

L'ajout d'une autre couche d'authentification, en plus du nom d'utilisateur et du mot de passe simples, est une étape efficace pour lutter contre les accès non autorisés aux comptes, les prises de contrôle de comptes et les réinitialisations de mots de passe. L'authentification multifacteur (AMF) nécessite des informations d'identification supplémentaires autres que le nom d'utilisateur et le mot de passe pour accéder à une application, un site ou des données. Dans une authentification typique à deux facteurs, un mot de passe à usage unique ou un code est généré par un jeton logiciel ou matériel (quelque chose que l'utilisateur possède) pour vérifier l'autorisation d'accès au compte. Compte tenu en particulier de la vague d'attaques sur les informations d'identification en 2018 et de l'énorme base de données de noms d'utilisateur / mots de passe piratée, le recours à l'authentification multifacteur est une pratique fortement recommandée.[23] [24] Les données d'authentification multifacteur ont été collectées lors de l'audit de 2017, mais couvraient moins du quart des organisations auditées. En raison de données incomplètes, l'AMF n'a pas été évaluée dans le présent audit, bien que l'intention soit de l'intégrer à la méthodologie de l'audit lorsque suffisamment de données seront disponibles.

Sécurité de site, de serveur et d'infrastructure

La fiabilité d'un site dépend en grande partie de la sécurité de l'infrastructure et des pratiques de confidentialité associées. Les utilisateurs ont besoin d'avoir la garantie que le site et leurs données sont sécurisés. L'implémentation appropriée des meilleures pratiques dans cette catégorie protège également le site lui-même contre les attaques. L'audit 2018 a été étendu à une évaluation plus approfondie de la santé du DNS, de la notoriété de l'IP, de la sécurité des applications et de la cadence des correctifs. En outre, la barre de notation sur la sécurité des serveurs a été relevée cette année en combinant les résultats de High-Tech Bridge (devenue ImmuniWeb), Qualys SSL Labs, Mozilla Observatory et SiteCheck. Les meilleures pratiques incluent :

- Optimiser l'implémentation SSL / TLS à l'aide d'informations tirées d'outils publics, en mettant l'accent sur les vulnérabilités notées « F » ou en échec (60 points ou moins) dans l'un des principaux sous-composants de la notation (qui conduit normalement à une note globale de « C »).[25] [26] Cela inclut d'éliminer l'utilisation de chiffrements et d'anciens protocoles non sécurisés, ainsi que des vulnérabilités potentiellement exploitables par POODLE et ROBOT.[27]
- Implémenter la politique de sécurité des données et des en-têtes associés, pour le contenu tiers utilisé sur le site. Cela peut empêcher les vulnérabilités introduites par des données externes.[28] [29] [30]
- Examiner les capacités des autorités de certification pour vous assurer qu'elles répondent à vos exigences en matière de support. Utiliser les certificats SSL EV pour les catégories de sites fréquemment usurpées et pour lesquelles les utilisateurs doivent être assurés qu'ils visitent et consultent un site légitime.
- Mettre en œuvre l'autorisation d'autorité de certification (CAA) pour empêcher la délivrance de certificats non autorisés.[31]
- Implémenter le HSTS (HTTP Strict Transport Security), également appelé AOSSL (Always on SSL) ou HTTPS partout, sur toutes les pages, pour optimiser la sécurité des données et la confidentialité en ligne. HSTS permet de garantir que toutes les données échangées entre un site et un dispositif sont cryptées.
- Implémenter un pare-feu pour applications Web pour surveiller les conversations HTTP et bloquer les attaques courantes telles que les scripts intersite (XSS) et les injections SQL.
- Analyser de manière proactive les sites pour rechercher des liens malveillants, des exploitations d'iFrame, des malwares et du malvertising.[32]

« Les consommateurs méritent de connaître les pratiques mises en place par les entreprises pour que leurs données restent privées et en sécurité. L'audit annuel de la confiance en ligne fournit cette transparence chaque année. Cet audit indépendant aide les entreprises de toutes tailles à comprendre quelles sont les meilleures pratiques de confidentialité et de sécurité à adopter pour protéger leurs clients et leur activité ». – Ashutosh Agrawal, directeur principal, Sécurité, Confidentialité et Conformité, 23andMe

- Implémenter la détection et l'atténuation des robots pour aider à prévenir les attaques par force brute, l'extraction de contenu Web, le piratage de compte, les analyses de vulnérabilité non autorisées, les courriers indésirables et les attaques sur un intermédiaire.
- Fournir aux visiteurs du site et aux tiers un mécanisme de rapport de vulnérabilité, identifiable et accessible, afin qu'ils puissent signaler ces vulnérabilités.

Comme le montre la figure 12, les scores récapitulatifs concernant la sécurité se situent dans une plage relativement étroite, tandis que le taux d'adoption des principales améliorations clés varie considérablement :

- Les scores concernant la sécurité des sites, qui représentent l'essentiel du score de référence dans cette catégorie, sont fortement concentrés autour de la moyenne globale de 89 (contre 92 en 2017), le secteur fédéral étant en tête à 94, suivi par les secteurs de la consommation et des actualités à 91. La baisse des scores est entièrement due à l'importance accrue attribuée aux autres éléments de la sécurité du site : implémentation d'en-têtes de sécurité et de contenus tiers, cadence des correctifs et réputation de l'IP.
- L'adoption globale de « Always On SSL » (qui fait maintenant partie du score de référence) a nettement progressé, pour parvenir à 93 % (à partir de 30 % en 2016 et 52 % en 2017). L'écart dans l'adoption entre les secteurs s'est quant à lui réduit, allant de 82 % pour le secteur de la santé à 100 % dans le secteur fédéral (contre 26 % à 91 % en 2017). Les sites d'actualités ont affiché la plus forte croissance, augmentant de 26 % à 93 %.
- L'adoption du SSL EV est en moyenne de 25 %, mais varie considérablement d'un secteur à l'autre - il est le plus élevé pour le secteur bancaire (71%, dépassant tous les autres secteurs de plus du double) et plus bas pour les secteurs des actualités et fédéral (8 %), suivi de près par le secteur de la santé (9 %).
- Le traçage de CAA récemment ajouté a montré que seuls 6 % de la totalité des sites ont tiré parti de cette fonctionnalité, qui permet aux propriétaires de domaine de publier la liste des autorités de certification autorisées à émettre des certificats en leur nom, limitant ainsi les abus. L'adoption était la plus forte dans les secteurs de la consommation (20 %) et des actualités (13 %) et la plus faible chez les détaillants en ligne (2 %).

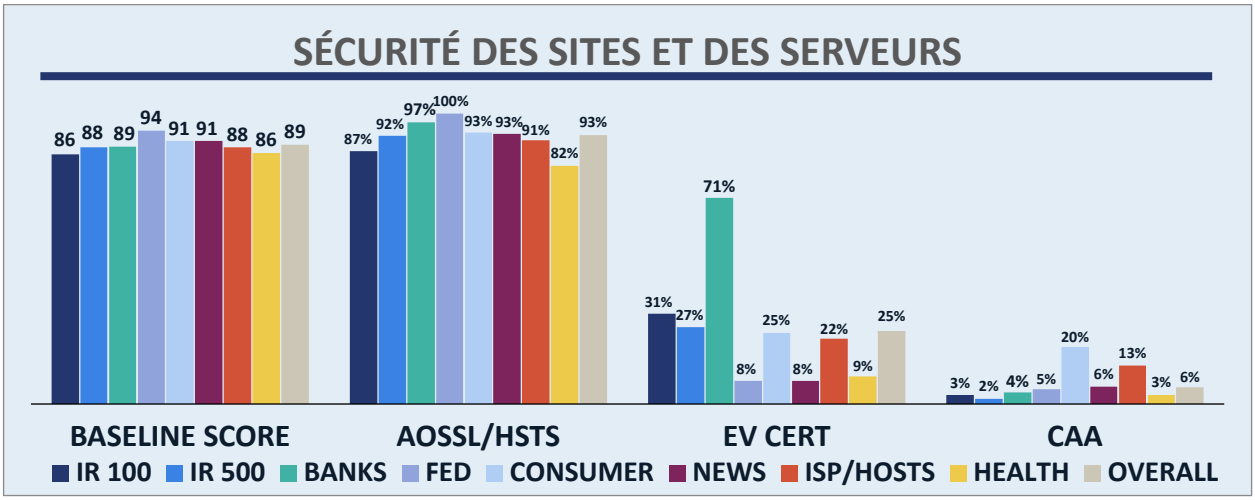


Figure 12 - Scores / adoption de la sécurité des sites et des serveurs par secteur

Implémentation de serveur et analyse de vulnérabilité

La surveillance permanente de la configuration SSL / TLS et l'utilisation des configurations de sécurité associées sont une condition fondamentale pour optimiser la sécurité et contrecarrer les vulnérabilités. L'audit de 2018 a élargi l'analyse en ajoutant de nouveaux outils, notamment ceux fournis par ImmuniWeb, Internet.nl, Mozilla, Sucuri, Symantec et SSL Labs. Les données ont été collectivement utilisées pour évaluer l'implémentation de SSL / TLS sur les sites, l'adoption de SSL EV, de CAA et d'AOSSL, la configuration de données de tiers, l'utilisation de pare-feux pour applications Web et la vulnérabilité aux scripts intersite (XSS), aux exploitations d'iFrame, aux malwares et aux liens malveillants.

En référence à l'état général de la sécurité SSL / TLS, le rapport mensuel SSL Pulse du 2 mars 2019 indiquait que 66 % des 139 822 sites testés étaient considérés comme sécurisés, une augmentation continue par rapport à 58 % en juin 2017 et à 43 % en juin 2016.[33] À titre de comparaison, 83 % des sites de l'audit d'OTA sont considérés comme sécurisés, ce qui indique que l'échantillon de l'audit réalise des performances significativement supérieures à la moyenne de l'ensemble des sites Web. Lors du processus d'analyse des scores de sécurité du site, plusieurs tendances ont été observées :

- L'utilisation de paramètres d'échange de clés, de chiffrements et de protocoles vulnérables a diminué, mais de nombreux sites prennent toujours en charge des implémentations plus anciennes. Les problèmes généralement signalés étaient des paramètres Diffie-Hellman faibles, des chiffrements RC4 et l'utilisation de protocoles SSL3 ou TLS1.0 (TLS1.0 était obsolète dans le cadre de la norme PCI à partir de juin 2018).[34]
- 29 % des sites ne prennent en charge que TLS1.2 ou ultérieur, ce qui est la recommandation de meilleure pratique. Il existe toujours problèmes de compatibilité avec les anciens navigateurs empêchant les organisations de supprimer complètement TLS 1.0 et 1.1, mais un changement important a été opéré pour supprimer les protocoles antérieurs à TLS1.2. Sept pour cent des sites prennent en charge TLS1.3, qui a été officiellement publié en août 2018. Les secteurs des FAI / Hébergeurs et de la Santé sont en tête avec 11 %.

- La plupart des sites ne définissent pas de politique de sécurité des données et ne profitent pas des en-têtes susceptibles de limiter les vulnérabilités liées aux données de tiers, telles que les cookies. Des résultats spécifiques peuvent être observés à l'aide du test de sécurité de site Web d'ImmuniWeb et de Mozilla Observatory.

Des malwares ont été observés sur 2 % de l'ensemble des sites et étaient plus répandus parmi les banques (10 %). Des vulnérabilités XSS / iframe ont été observées sur 21 % des sites, soit une baisse de plus de la moitié par rapport aux 50 % observés en 2017. Une pénalité XSS a été imposée aux sites qui avaient une occurrence en 2018 ou qui n'avaient pas corrigé une vulnérabilité XSS signalée avant 2018.[35] Les banques présentaient la plus faible présence de vulnérabilités XSS / iframe (5 %), mais 43 % des sites d'actualités et plus d'un cinquième des sites de consommateurs, des sites fédéraux et des sites d'actualités étaient vulnérables. Bien que les résultats représentent une amélioration depuis 2017, la présence globale de vulnérabilités reste préoccupante et renforce la nécessité pour les organisations de surveiller en permanence leurs sites et leurs systèmes de gestion des données.

SCORES DE SÉCURITÉ DE SITE				
	2015	2016	2017	2018
Top 100 des détaillants en ligne	85,7	89,6	91,1	86,0
Top 500 des détaillants en ligne	85,3	88,3	90,6	88,4
Bank 100	83,0	88,3	87,7	88,6
Federal 100	83,6	91,6	95,2	94,2
Consumer 100	86,1	89,9	93,1	81,2
News 100	83,0	85,0	88,8	90,6
ISP/Hosts 100	-	-	92,9	88,4
Health 100	-	-	-	86,3

Figure 13 – Score de sécurité de site, Moyenne par secteur, 2015 à 2018

Comme le montre la figure 13, les scores de sécurité ont chuté année après année dans la plupart des secteurs (les secteurs bancaires et d'actualités étant les exceptions). Cette baisse des scores est entièrement due au poids accru attribué aux facteurs de non-configuration de SSL / TLS et principalement en raison des faibles scores constatés lors des tests de sécurité de site Web d'ImmuniWeb et de Mozilla Observatory. Le secteur fédéral arrive en tête pour la troisième année consécutive avec une note de 94,2. Comme avec les XSS et les malwares, la configuration et l'implémentation de SSL / TLS et des éléments de sécurité de site connexes nécessitent une surveillance continue, car de nouvelles vulnérabilités apparaissent fréquemment. L'expérience d'OTA montre que les changements peuvent être apportés rapidement et à moindre coût une fois que les décideurs sont engagés.

Types de certificat SSL / TLS

Reconnaissant l'importance des certificats de confiance et les préoccupations croissantes concernant l'acquisition de certificats pour des sites frauduleux se faisant passer pour des destinations populaires pour les consommateurs, l'OTA a commencé le traçage des types de certificats en 2015. Il existe trois principaux types de certificats : la validation de domaine (DV), la validation d'organisation (OV) et la validation étendue (EV). Ils disposent de méthodes très différentes pour valider l'identité de l'entité

recevant le certificat. Le nom et la localisation officiels des entités achetant des certificats OV et EV sont vérifiés et confirmés directement auprès de l'entité par les autorités de certification et inclus dans le certificat. En revanche, les certificats DV sont généralement vérifiés par un processus automatisé, les rendant plus efficaces et moins coûteux à acquérir. Cela a pour conséquence une augmentation importante de l'utilisation de TLS. Suivant cette tendance, les cybercriminels les ont également utilisés pour l'hameçonnage et pour créer des domaines et contenus paraissant réels.[36] [37] [38]

Les certificats SSL EV fournissent un niveau de vérification supérieur, nécessitant un processus d'audit complet. Le SSL EV permet la différenciation en affichant le nom de l'entité et un indicateur de confiance visuel vert dans la barre d'adresse ou dans l'affichage du navigateur, bien que cette différenciation se soit amenuisée ces dernières années et ne soit pas implémentée dans de nombreux navigateurs pour appareils mobiles. Les certificats SSL EV sont obligatoires dans certains secteurs (par exemple, les fournisseurs de fichiers électroniques gratuits de l'IRS).[39]

Récemment, l'industrie a eu un débat important sur la valeur des différents types de certificats, certains soutenant que rien, au-delà du niveau DV, n'ajoutait la moindre valeur.[40] D'autres soutiennent que les certificats EV et OV méritent leur coût supplémentaire en raison de la différenciation dans le navigateur (EV) ou de la prise en charge supplémentaire de la gestion de lots importants de certificats ou de la révocation de certificats compromis.

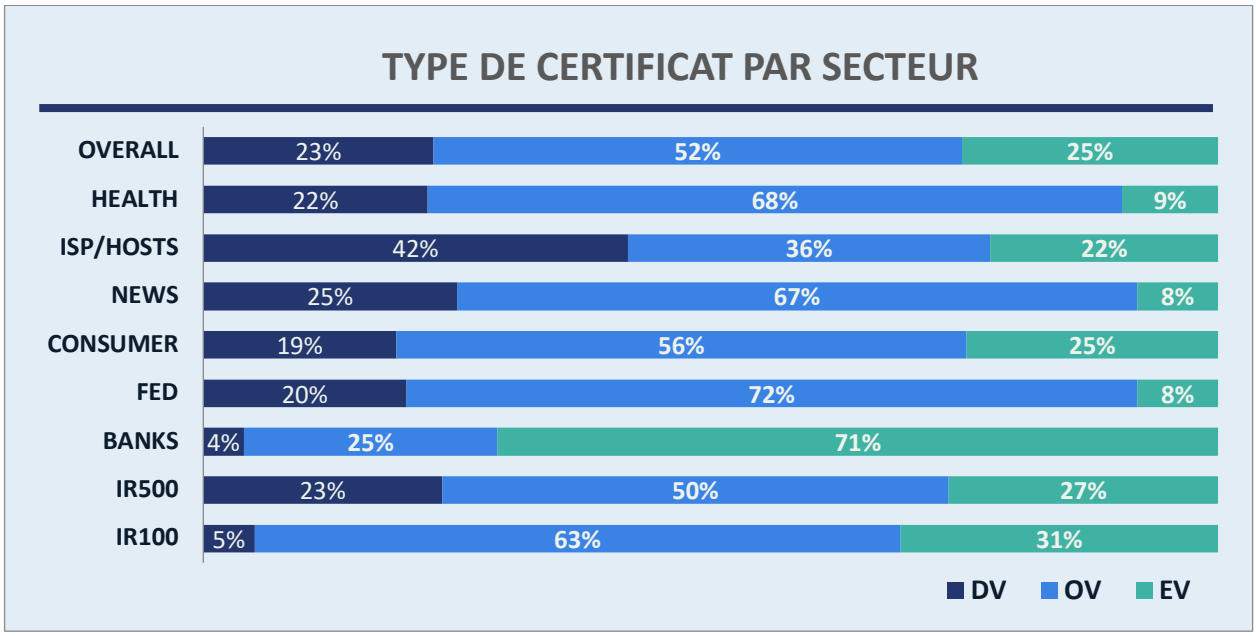


Figure 14 - Type de certificat SSL / TLS par secteur, 2018

La figure 14 présente les taux d'adoption pour chaque type de certificat par secteur. Les taux varient considérablement d'un secteur à l'autre, les banques privilégiant fortement les certificats EV (71 %), les sites fédéraux, de santé et d'actualités préférant les certificats OV (67 % à 72 %) et les sites des FAI / Hébergeurs se tournant vers les certificats DV (42 %). La figure 15 illustre l'évolution globale dans le temps et montre une diminution modeste des certificats EV en faveur des certificats DV, les certificats OV restant inchangés.[41] Lors du choix des autorités de certification et du type de certificat à utiliser, les propriétaires de domaine doivent avoir une vision globale de la situation et envisager un support et des

services en plus de l'émission de base des certificats.

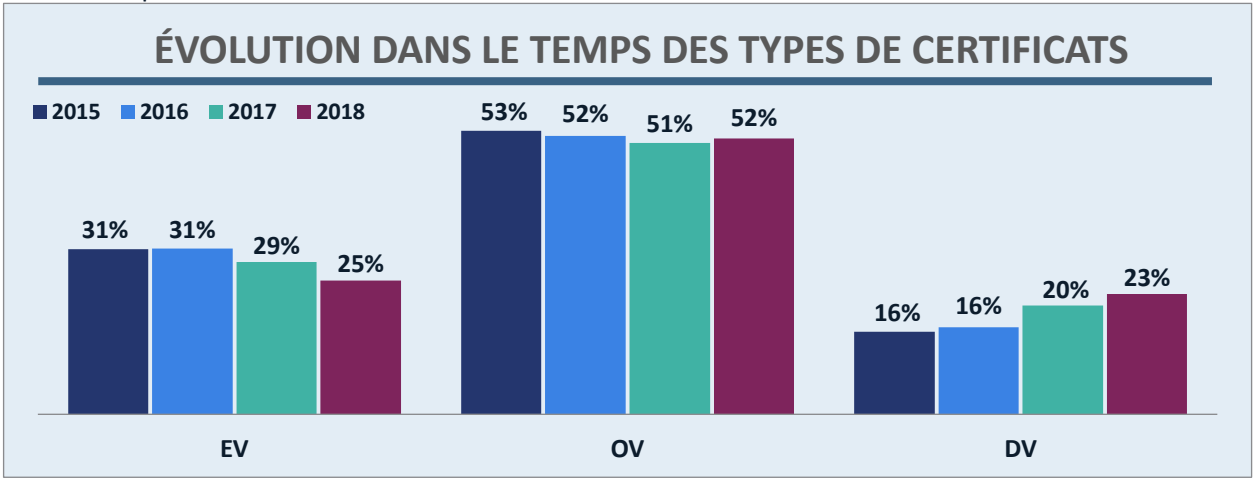


Figure 15 - Type de certificat SSL / TLS, 2015 à 2018

Atténuation des attaques DDoS

En dehors du cadre de la méthodologie de l'audit de cette année, les entreprises doivent implémenter des mesures permettant de détecter et d'atténuer les effets d'une attaque DDoS. Selon Kaspersky Labs, l'activité de DDoS a baissé de 13 % en 2018 par rapport à 2017, mais la durée moyenne des attaques est passée de 95 minutes au premier trimestre de 2018 à 218 minutes au quatrième trimestre.[42] À l'échelle mondiale, ces attaques restent imprévisibles et chroniques, et varient considérablement en termes de volume, de vitesse et de complexité. Pour lutter contre ces incidents, il est de plus en plus important de surveiller en permanence les menaces afin d'optimiser la stratégie d'atténuation. OTA recommande des pare-feux sur site et des dispositifs dédiés aux attaques DDoS (ou des services cloud équivalents) pour aider à bloquer le trafic malveillant. Lorsque ces systèmes sont configurés correctement, le trafic malveillant associé peut être efficacement bloqué et supprimé avant d'atteindre les serveurs qu'il vise.

Mécanismes de rapports de vulnérabilité

Cela a été ajouté à la méthodologie en 2017. Des points bonus ont été attribués aux organisations disposant d'un mécanisme leur permettant de soumettre des rapports de vulnérabilité soit directement sur leur site, soit via des programmes de « bug bounty » par des tiers. Cela a notamment été ajouté car il s'agit d'une pratique reconnue comme exemplaire par NTIA, NIST et la FTC. Le recours à cette pratique a presque doublé, passant de 6 % à 11 % depuis sa première évaluation en 2017, mais reste néanmoins assez faible. Le secteur de la consommation était en tête avec une adoption de 43 %, suivi des FAI / hébergeurs avec 25 %, des actualités / médias avec 9 % et des banques avec 6 %. Disposer de tels mécanismes est reconnu comme essentiel pour répondre efficacement aux rapports des chercheurs et des utilisateurs tiers et est relativement simple à mettre en œuvre. OTA plaide pour que les sites disposent d'un mécanisme de signalement des vulnérabilités, hébergé sur leur site (tel que le formulaire en ligne conçu par OTA) ou par l'un des principaux programmes de « bug bounty » par des tiers.[43]

Malvertising

Des cybercriminels ont identifié la vulnérabilité inhérente à l'univers de la publicité et ont utilisé sa complexité pour diffuser des publicités ou des messages trompeurs contenant du code malveillant afin de compromettre les dispositifs des utilisateurs et les systèmes d'entreprises. Connue sous le nom de publicité malveillante ou « malvertising », cette pratique représente une menace croissante pour tous

ceux qui accèdent à des données et services financés par la publicité en ligne. Au cours de la dernière année, de nouvelles techniques ont été utilisées pour dissimuler les publicités malveillantes. Un cabinet a estimé que le malvertising coûte au secteur de la publicité en ligne plus d'un milliard de dollars par an.[44] À la fin de 2018, Amazon a intenté une action en justice contre les exploitants d'un site utilisant le malvertising pour rediriger les utilisateurs vers leur site frauduleux.[45] Bien que les incidents concernant le malvertising n'aient pas été tracés dans l'audit, les organisations doivent comprendre l'univers publicitaire de leurs sites et les protections existantes pour bloquer les publicités malveillantes.

Confidentialité, transparence et divulgations

Remarque : dans les audits précédents, le terme « politique de confidentialité » était utilisé pour faire référence à la représentation des pratiques de confidentialité d'un site. Pour s'harmoniser avec la nomenclature mondiale, le terme a été remplacé par « déclaration de confidentialité ». Il convient également de noter que l'audit évalue les assertions formulées dans la déclaration de confidentialité, mais pas les pratiques réelles de l'organisation, qui peuvent être très différentes des politiques énoncées, car l'audit n'est qu'une vision externe.

L'audit de 2018 a révélé une légère augmentation de la transparence et de la lisibilité des déclarations de confidentialité publiées, avec des possibilités d'amélioration considérables. De plus en plus de déclarations sont agencées par couches, les divulgations sont plus complètes et le langage est en train de passer à une formulation plus agréable pour le consommateur, plutôt qu'à un contrat rédigé à destination de juristes. Cela est peut-être dû en partie à une sensibilisation accrue au règlement général sur la protection des données (RGPD) de l'UE et à son respect.

Avec l'avènement du RGPD, il est plus important que jamais que les organisations adoptent une gestion responsable des données. En outre, les organisations doivent être conscientes des autres règles régionales transfrontalières telles que le système de règles de confidentialité pour les communications transfrontalières de l'APEC. Celles-ci constituent un ensemble de normes de confidentialité facultatives mais contraignantes permettant aux données de circuler dans la région Asie-Pacifique.[46] En 2020, la California Consumer Privacy Act (CCPA), largement inspirée des principes du RGPD, entrera en vigueur, obligeant les organisations basées aux États-Unis à implémenter des protections supplémentaires en matière de confidentialité si elles souhaitent s'engager sur le plus grand marché des États-Unis.[47] OTA plaide depuis 2009 pour une transparence et une accessibilité accrues des déclarations de confidentialité, notamment en recommandant la divulgation des pratiques de collecte, d'utilisation, de partage et de conservation des données. Les meilleures pratiques incluent :

Éléments basiques d'avis / de divulgation

- S'assurer que la déclaration de confidentialité dispose d'un lien et est facilement accessible à partir de la page d'accueil.
- Inscrire la date de révision de la déclaration en haut de la page.
- Fournir un accès aux versions archivées de la déclaration, permettant aux utilisateurs de voir ce qui a changé.
- Utiliser un avis simple par couches ou un avis bref pour aider les consommateurs à comprendre la déclaration.

- Utiliser des icônes pour aider les consommateurs à se repérer dans les déclarations de confidentialité en conjonction avec les avis courts ou par couches.
- Rédiger des déclarations adaptées au public et aux segments démographiques cibles du site. Envisager de fournir des versions multilingues pour prendre en charge les visiteurs non anglophones du site.

Énoncer clairement les principales politiques de conformité

- Conformité à la loi sur la protection de la vie privée en ligne des enfants (COPPA) ou aux réglementations connexes.[48]
- Indiquer si le site respecte les paramètres « Ne pas tracer » (Do Not Track - DNT) des navigateurs et, de préférence, les paramètres DNT du navigateur utilisé par les utilisateurs.
- Fournir un résumé de la politique de conservation des données, y compris une période spécifique et la raison pour laquelle les données sont conservées.

Protéger la vie privée et définir le partage protégé

- Ne pas partager de données personnelles avec des tiers, sauf pour fournir un service à l'utilisateur. Fournir une déclaration claire incluant des détails à savoir si des données sont partagées, lesquelles et à quelles fins.
- Exiger un contrat de conformité de la part des fournisseurs et informer les consommateurs qu'il est interdit aux fournisseurs de services d'utiliser ou de partager leurs données à d'autres fins que la fourniture de services pour le compte du site.
- Fournir la divulgation du traçage inter-dispositifs.
- Utiliser des systèmes de gestion des balises ou des solutions de confidentialité pour gérer les traceurs tiers.
- Indiquer si les données seront partagées en conformité avec les obligations légales et s’efforcer d’avertir les consommateurs si leurs données sont requises par des tiers en raison d’exigences légales.

En 2017, les 100 points de référence ont été réaffectés, de 50 % pour les éléments de déclaration de confidentialité et 50 % pour l'utilisation du traçage à 55 % pour la déclaration de confidentialité et 45 % pour l'utilisation du traçage. Les scores de confidentialité ont été en moyenne de 70 cette année, en baisse par rapport à 73 en 2017, principalement en raison de la notation plus stricte. Les scores allaient de 67 pour les détaillants en ligne à 76 pour les sites de consommateurs. Alors que la plupart des scores des secteurs étaient en baisse, les banques sont passées de 65 à 69 et les actualités de 70 à 71.

Dans l'ensemble, un peu moins d'organisations ont reçu un score d'échec pour la confidentialité (baisse de 16 % à 15 %), bien que les résultats varient considérablement d'un secteur à l'autre (les échecs dans la confidentialité ont augmenté de 16 % à 23 % pour les détaillants en ligne et baissé de 34 % à 14 % pour les banques et de 19 % à 10 % pour les actualités). Comme le montre la figure 16, les scores pour l'élément Déclaration de confidentialité (valant 55 points) se situaient dans une fourchette assez étroite, de 25 à 33. Fait décevant, la moyenne globale de 27 signifie que la plupart des organisations ne gagnent que la moitié des points disponibles pour la déclaration de confidentialité. Les scores du traçage étaient

beaucoup plus encourageants puisque tous les secteurs ont gagné plus de 87 % des 45 points disponibles.

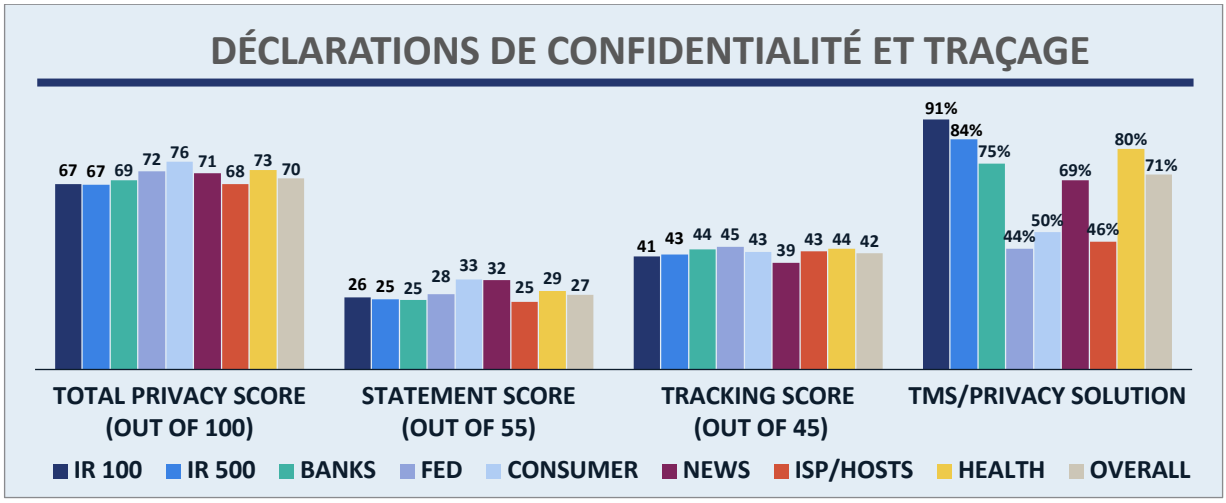


Figure 16 - Scores des déclarations de confidentialité et traçage, par secteur

Les sites qui dépendent de la publicité et des analyses de tiers sont confrontés au défi de la gestion du traçage par des tiers. Un défi croissant pour les propriétaires de sites consiste à connaître les pratiques de partage des données respectives des partenaires et l'effet domino pouvant survenir lors de la divulgation de données personnelles. Les systèmes de gestion de balises et les solutions de confidentialité aident à surveiller la collecte et le partage de données par des tiers en temps réel. Des points de bonus ont été attribués s'ils existaient.[49] L'adoption globale a augmenté de 69 % en 2017 à 71 %, et cet élément est actuellement considéré pour la notation de référence dans les futurs audits. Les détaillants en ligne ont été en tête dans l'adoption (84 %). Le secteur fédéral a enregistré le taux d'adoption le plus faible (44 %). Cela s'explique par le faible nombre de balises utilisées et par le fait que ce secteur ne dépend pas de la publicité ou du partage de données.

Transparence

Fournir à la fois un avis clair présentant les révisions des déclarations de confidentialité avec une date en haut de page et un lien vers les versions archivées des précédentes déclarations de confidentialité permet d'optimiser la transparence. Ces deux éléments font partie de la notation de référence de l'audit de 2018. Dans l'ensemble, 47 % des organisations avaient une date en haut de page (en légère hausse par rapport à 46 % en 2017), mais l'adoption variait considérablement - de 2 % seulement dans le secteur fédéral à 74 % dans le secteur des actualités. Pour la première fois, les dates des déclarations de confidentialité ont été prises en compte : 31 % des déclarations ne portaient pas de date, 11 % avaient une date antérieure à 2017, 11 % étaient datées de 2017 et 47 % avaient une date postérieure au 1er janvier 2018. Les déclarations de confidentialité du secteur de la consommation sont les plus récentes (71 % sont de 2018 ou plus tard), alors que le secteur de la santé a les déclarations les moins récentes (seulement 19 % sont de 2018 ou plus tard). L'utilisation du traçage des versions pour la comparaison historique des déclarations de confidentialité est passée de 6 % en 2017 à 3 % cette année, principalement en raison de modifications dans la liste des organisations auditées. En tête du classement se trouvent les secteurs de la consommation (12 %) et des FAI / Hébergeurs (10 %).

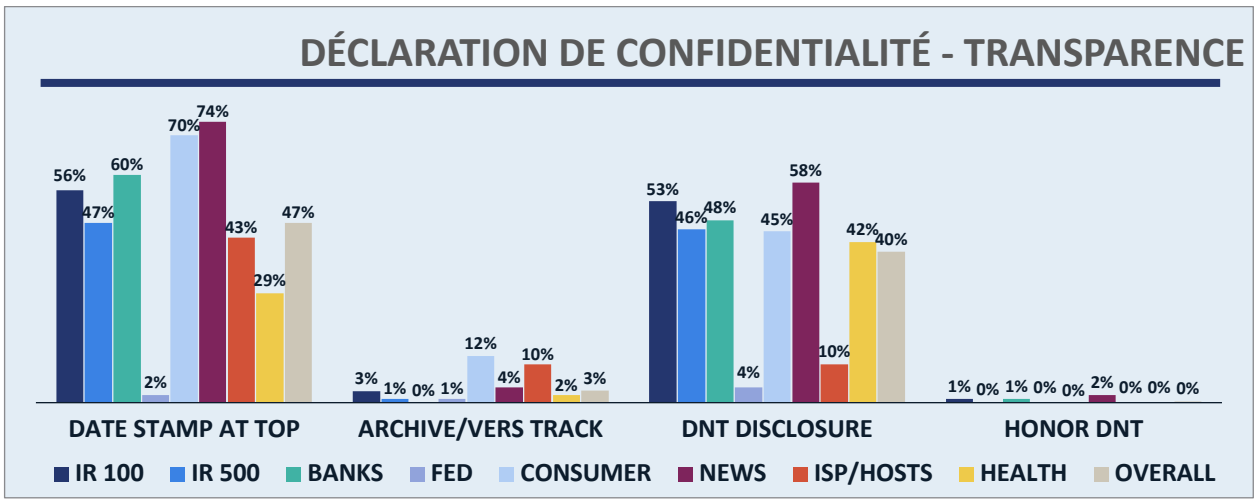


Figure 17 – Transparence de la déclaration de confidentialité par secteur

Étant donné que la divulgation de la politique DNT (Ne pas tracer) d'un site est actuellement une obligation légale dans de nombreuses juridictions, il est important que les sites indiquent leur politique DNT et, dans l'idéal, respectent les paramètres DNT du navigateur lorsque les utilisateurs visitent le site. Comme le montre la figure 17, la divulgation globale de la politique DNT continue d'augmenter, atteignant 40 % contre 37 % en 2017 et 13 % il y a quatre ans. Cependant, le respect des paramètres DNT a diminué encore davantage, passant de 2 % en 2017 à moins de 0,5 % cette année. Dans l'ensemble, le DNT semble toucher à sa fin. La plupart des navigateurs intègrent désormais d'autres mécanismes permettant soit de bloquer automatiquement les traçages en ligne (par exemple via des fonctionnalités, des extensions ou des plug-ins natifs), soit de donner aux utilisateurs un contrôle direct sur des listes à bloquer. Récemment, la prise en charge de DNT a été supprimée dans la version 12.1 du navigateur Safari d'Apple, le projet a été déclaré final par le W3C et la nouvelle California Consumer Privacy Act (CCPA), qui entre en vigueur le 1er janvier 2020, ne l'exige plus.[50] [51] Compte tenu de cette tendance, il est probable que DNT soit supprimé en tant qu'élément de score lors des futurs audits, bien qu'une partie importante du score de confidentialité soit toujours liée aux traceurs sur les sites.

Lisibilité et divulgations

Concevoir une déclaration de confidentialité d'un site pour des lecteurs à qui elle est destinée et non pour un public de juristes est depuis longtemps reconnu par les professionnels de la confidentialité comme un changement nécessaire. Non seulement le texte doit être écrit à un niveau de lecture approprié, mais sa structure doit optimiser sa lisibilité. La figure 18 présente les résultats pour trois éléments de notation : avis courts par couches (référence), icônes ergonomiques (bonus) et affichage de la déclaration de confidentialité en plusieurs langues (bonus). L'utilisation des avis par couches a considérablement augmenté, passant de 29 % en 2017 à 47 %, le secteur des actualités arrivant en tête avec 71 %. L'utilisation d'icônes a doublé, passant de 1 % à 2 %, le secteur de la consommation arrivant en tête avec 7 %. La prise en charge des déclarations de confidentialité multilingues a en réalité chuté, passant de 7 % à 4 %, ce qui peut être principalement attribué aux modifications apportées à la liste des organisations auditées. OTA considère que la disponibilité de la déclaration de confidentialité en plusieurs langues contribue à améliorer la transparence et la lisibilité. Il a été observé que, dans certains cas, la langue utilisée pour la déclaration de confidentialité était activée par les paramètres du navigateur ou la localisation de l'adresse IP, de sorte que toutes les offres multilingues n'ont peut-être pas été prises en compte dans l'audit.

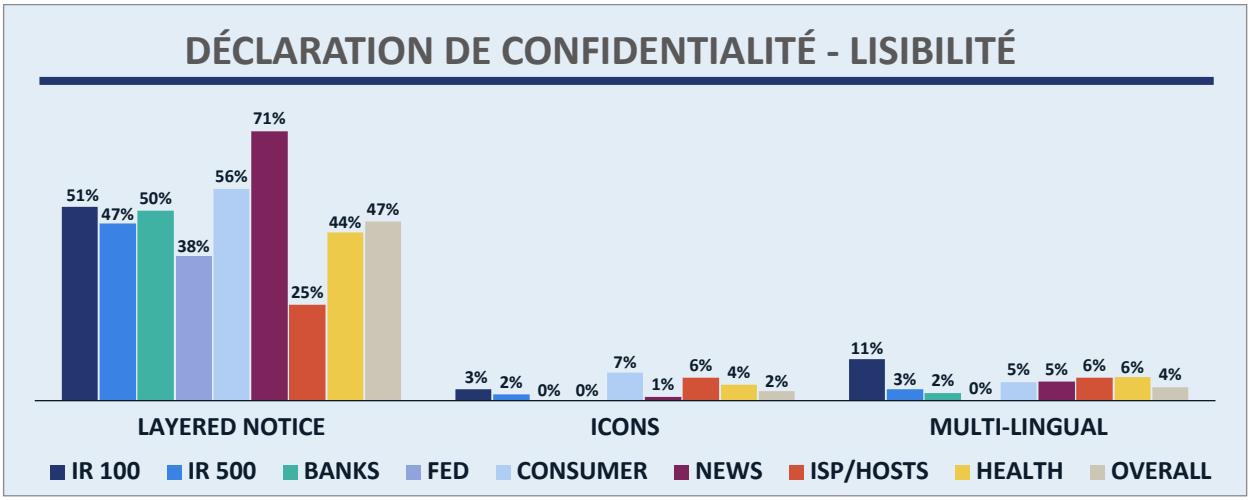


Figure 18 – Lisibilité de la déclaration de confidentialité par secteur

Traitement des données

La gestion et la divulgation des pratiques de partage et de conservation des données constituent un élément essentiel de la déclaration de confidentialité. Lors de l'audit de 2018, l'élément de partage des données était divisé en deux parties : une pour le concept fondamental selon lequel les données ne sont pas partagées, sauf éventuellement avec des tiers qui aident à fournir le service, et une autre pour le texte traitant du partage de données avec des affiliés ou d'autres tiers externes. La figure 19 présente les résultats.

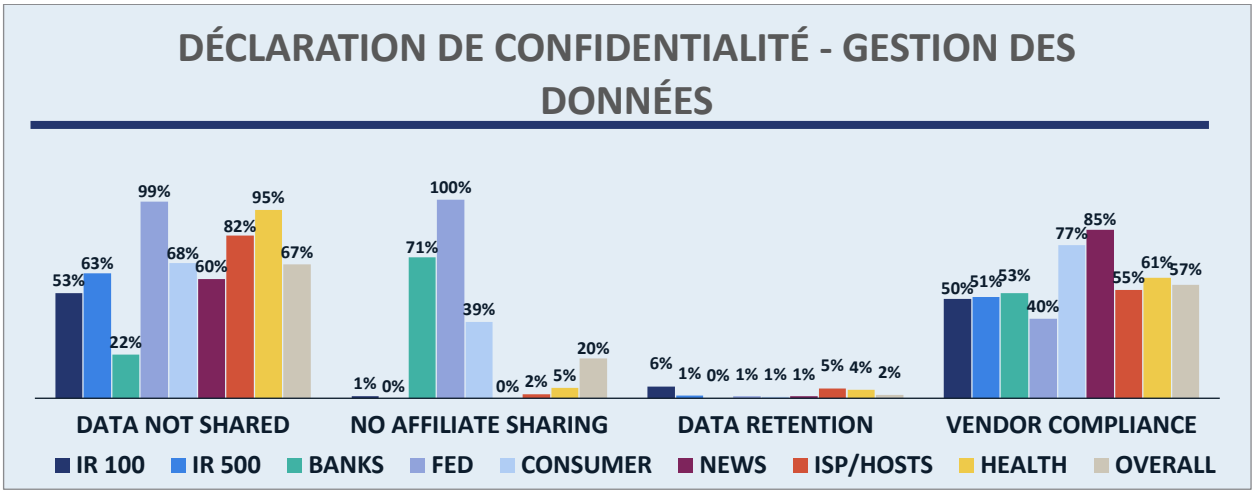


Figure 19 – Traitement des données de la déclaration de confidentialité par secteur

Le texte adopté pour le partage des données (par exemple, « nous ne vendons, ne louons, ni ne partageons de données qu'aux tiers qui aident à fournir le service ») est utilisé par 67 % des organisations (contre 63 % en 2017), mais varie considérablement. Le texte sur le partage des données avec les affiliés varie encore plus, les secteurs des détaillants en ligne et des actualités étant à 0 % (ce qui signifie qu'ils ont tous un texte indiquant qu'ils partagent des données avec les affiliés) et le secteur fédéral à 100 %. Le texte sur la conservation des données a été noté beaucoup plus strictement cette année afin de se conformer aux principes du RGPD. En 2017, l'adoption était de 49 % et un crédit a été attribué à presque toutes les références à la conservation des données. Cette année, le texte devait être

plus spécifique, avec un calendrier spécifique indiqué dans la mesure du possible. L'utilisation du texte sur la conformité des fournisseurs (les tiers doivent se conformer à la déclaration de confidentialité de l'organisation) est passée de 48 % en 2017 à 57 % cette année, le secteur des actualités arrivant en tête avec 85 %. L'adoption de cet élément a nettement progressé dans deux secteurs : le secteur des banques est passé de 18 % à 53 % et celui des actualités de 51 % à 85 %.

Conformité au RGPD

Pour la première fois cette année, l'audit a inclus six variables destinées à prendre en compte les aspects clés de la conformité au RGPD. Il est important de noter que la plupart des entreprises de l'audit sont basées aux États-Unis et n'ont peut-être pas besoin de se conformer directement au RGPD. Cependant, l'OTA a estimé qu'étant donné la portée du RGPD et son impact sur les lois relatives à la confidentialité dans le monde entier, il était important de commencer à mesurer la manière dont les organisations se conformaient à ses principes clés.

Premièrement, 32 % des déclarations de confidentialité ont été jugées faciles à lire. L'objectif de cette exigence du RGPD est que les déclarations de confidentialité soient faciles à comprendre par la plupart des utilisateurs, notamment en ce qui concerne les données utilisateur collectées et partagées. Les banques affichaient le pourcentage le plus élevé de déclarations faciles à lire (47 %), tandis que le secteur des actualités avait le niveau le plus faible, à seulement 8 %. Il est clair que davantage de travail est nécessaire ici, car plus des deux tiers des déclarations de confidentialité n'atteignent pas cet objectif.

Le RGPD ne spécifie pas exactement comment une organisation doit communiquer quelles données sont collectées et pour quelles raisons, mais simplement que l'entreprise doit transmettre ces informations aux utilisateurs. Dans cet esprit, la plupart des organisations (95 %) ont suffisamment défini les données collectées et les raisons pour lesquelles elles l'ont été. Les banques étaient en tête avec 99 %, tandis que les secteurs fédéral et des FAI / Hébergeurs étaient les plus bas avec 90 %.

D'autres aspects du RGPD ont des exigences plus spécifiques. Par exemple, 70 % des organisations de l'audit ont identifié un moyen de contacter le responsable de la protection des données, le secteur de la consommation arrivant en tête avec 81 %. Le secteur fédéral, avec 38 %, était en retard dans cette catégorie. Une autre exigence du RGPD est que les organisations définissent le processus par lequel les utilisateurs peuvent demander leurs données, ainsi que les types de données qu'ils peuvent demander. Dans l'ensemble, seules 50 % des organisations ont satisfait à cette exigence, les détaillants en ligne arrivant en tête avec 71 %.

Enfin, il existait deux exigences du RGPD avec des taux d'adoption très faibles. La première expose la nécessité pour les organisations de révéler si elles ont reçu des types spécifiques de données « sensibles » de la part de tiers (par exemple données biométriques, origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, etc.). Comme cette exigence ne s'applique que dans des cas limités, une faible adoption ne pose pas nécessairement problème. Seulement 1 % des organisations ont spécifiquement abordé cette question dans leur déclaration de confidentialité, le secteur de la santé arrivant en tête avec 4 %. La seconde exige que les organisations identifient les catégories de tiers avec lesquelles elles partagent des données, et devrait donc s'appliquer à toute organisation partageant des données. Moins de 1 % des organisations remplissent cette condition.

Suivi inter-appareils

Depuis l'audit de 2017, en réponse au rapport 2017 sur le traçage multi-dispositifs de la FTC, la divulgation du traçage de divers dispositifs (par exemple, ordinateur, téléphone, tablette, etc.) a été prise en compte et reçoit des points bonus. Cette année, 48 % des sites disposaient d'une telle divulgation, en augmentation par rapport à 44 % en 2017. Il convient de noter que le traçage inter-dispositifs peut présenter des avantages, notamment une amélioration de l'expérience utilisateur lors du passage d'un dispositif à l'autre, ainsi que des avantages en termes de sécurité pour les utilisateurs se connectant à partir d'autres dispositifs ou adresses IP, mais que cela pose également des problèmes de confidentialité. Le secteur des actualités a enregistré l'adoption le plus élevée (91 %), suivi du secteur de la consommation (80 %), tandis que le secteur fédéral affichait la plus faible adoption (12 %).

Enregistrements WHOIS

Lorsqu'une entreprise enregistre un nom de domaine, l'ICANN (Internet Corporation for Assigned Names and Numbers) lui demande de fournir ses coordonnées. Ces informations sont publiées dans la base de données WHOIS, qui est accessible à tous, à condition que l'enregistrement ne soit pas privé. L'avènement du RGPD a compliqué les listes WHOIS car les informations de contact personnelles ont été supprimées de nombreux enregistrements pour des raisons de confidentialité. De nombreuses organisations sont allées plus loin et ont expurgé toutes leurs informations (même au niveau organisationnel), ce qui rend difficile la détermination du détenteur du domaine.

En conséquence, les enregistrements privés (définis par la capacité de déterminer quelle entité est propriétaire du domaine) ont augmenté cette année. Globalement, 78 % des inscriptions étaient publiques (contre 87 % en 2017). Une analyse plus approfondie révèle que 7 % des enregistrements « privés » étaient directement liés aux purges en rapport avec le RGPD, ce qui donne un taux d'enregistrement public réel de 85 %. Les secteurs où les enregistrements WHOIS privés sont les plus utilisés sont les FAI / Hébergeurs (32 %), les banques (29 %) et la santé (28 %). Les enregistrements privés limitent la capacité des consommateurs à découvrir qui est le propriétaire d'un site, entravent la transparence et peuvent réduire la confiance des consommateurs, sans parler de la possibilité pour un tiers de contacter le propriétaire du site au sujet d'une vulnérabilité constatée. À l'inverse, les inscriptions privées sont une pratique valide et légitime pour l'enregistrement en « mode furtif » d'un domaine pour une entreprise, un produit ou un effort marketing futurs, même si ceux-ci devraient être rendus publics après le lancement.

Incidents de perte de données et règlements juridiques

Les violations de données et les règlements juridiques peuvent indiquer un mauvais niveau de sécurité et de confidentialité, ainsi que de médiocres pratiques des entreprises. En tant que tels, ils peuvent avoir un impact majeur sur la réputation d'une entreprise et le niveau de confiance qui en résulte, tout en mettant en péril la confidentialité et l'identité des utilisateurs. Dans le même temps, il est important de reconnaître qu'il n'existe pas de sécurité parfaite et qu'un ennemi déterminé disposant de suffisamment de temps et de ressources peut compromettre la plupart des organisations. Comme indiqué dans le Rapport 2018 sur les tendances en matière d'incidents cybernétiques et d'infractions de l'OTA, plus de 159 700 incidents concernant la perte de données ont été répertoriés dans le monde en 2017.[52]

L'audit de cette année comprenait des données supplémentaires provenant de diverses sources, offrant un aperçu plus complet de ces incidents. L'analyse de l'OTA a révélé que 15 % des entreprises auditées avaient été touchées par un ou plusieurs incidents, en hausse par rapport à 13 % en 2017 et 5 % en 2016. Le nombre d'enregistrements perdus variait d'un seul enregistrement à plus de 150 millions.

Considérant que tous les incidents ne sont pas égaux, les organisations ayant subi une perte cumulée de 1000 enregistrements ou moins au cours de la période d'audit n'ont pas été pénalisées, tandis que la pénalité attribuée aux violations de plus de 1000 enregistrements a été pondérée proportionnellement à l'ampleur de la violation. Compte tenu de cet ajustement, seules 12 % des organisations ont été sanctionnées pour un piratage des données. Le secteur de la consommation affichait le niveau le plus élevé de violations (34 %), suivi du secteur de la santé (30 %).

En matière réglementaire, 2 % des organisations auditées ont reçu une pénalité cette année au titre de poursuites ou de règlements liés à la protection des consommateurs (stable par rapport à 2017), le secteur de la consommation arrivait en tête avec 12 %. L'évaluation comprenait les règlements de la FTC, de la FCC, du CFPB, des États et des agences internationales. L'accent a été mis sur les règlements liés aux actions de protection du consommateur en matière de sécurité et de confidentialité et n'incluait pas les règlements relatifs aux fusions et acquisitions ou au droit du travail.

Conclusion

Comme dans les années précédentes, l'audit et le tableau d'honneur de la confiance en ligne visent trois objectifs principaux :

- Promouvoir les meilleures pratiques pour améliorer les pratiques en matière de sécurité des sites, de protection des données et de confidentialité.
- Reconnaître l'excellence en matière de pratiques de protection des consommateurs, de sécurité et de confidentialité responsable
- Fournir aux consommateurs une transparence accrue en ce qui concerne les pratiques de sécurité et de confidentialité des sites qu'ils visitent

L'audit de 2018 a enregistré des niveaux record dans de nombreux domaines : la plus forte progression d'une année sur l'autre pour l'inscription au tableau d'honneur (de 52 % à 70 %), les taux d'adoption de l'authentification des e-mails les plus élevés (76 % de prise en charge de SPF et DKIM au niveau du domaine de premier niveau) et les niveaux les plus élevés du chiffrage Internet (73 % utilisent le TLS opportuniste pour les e-mails et 93 % chiffrent toutes les sessions sur leur site Web). Ceci malgré des critères méthodologiques plus stricts, une notation plus rigoureuse et un poids accru attribué aux meilleures pratiques clés en matière de protection des consommateurs, de sécurité des sites et de confidentialité.

Certains secteurs ont brillé cette année : les agences du gouvernement fédéral ont récupéré après une mauvaise performance lors de l'audit de 2017 et arrivent en tête devant tous les autres secteurs avec 91 % de succès au tableau d'honneur. Les organisations du secteur des actualités / médias ont poursuivi leur croissance quasi géométrique dans leur succès au tableau d'honneur, repassant dans le groupe de tête avec 78 %. Le secteur de la santé, nouvellement ajouté, est arrivé dernier avec 57 % (ce qui aurait été une bonne performance les années précédentes), principalement en raison de l'absence d'authentification des e-mails.

Dans de nombreux domaines, l'adoption des meilleures pratiques est presque complète, à 90 % ou plus. Même s'il convient de le saluer, il incombe toujours aux organisations qui n'ont pas encore adopté ces pratiques de base largement reconnues de donner la priorité à leur implémentation.

Dans d'autres domaines, il existe des tendances inquiétantes. En dépit de la prise de conscience et de la sensibilité accrues sur les questions de confidentialité suscitées par le RGPD, la California Consumer Privacy Act et la forte médiatisation des échecs de grandes entreprises en matière de protection de la confidentialité, les déclarations de confidentialité ne se sont que très peu améliorées et la plupart des entreprises obtiennent un score de moins de 50 % sur cette partie de l'audit. Le partage de données avec des affiliées tiers, qui reste largement flou, est particulièrement préoccupant. Le référentiel initial des exigences liées au RGPD a révélé un large éventail d'adoptions - de 1 % à 95 %, en fonction des critères - et il faudra y remédier, car l'environnement réglementaire, que ce soit au niveau national ou mondial, continue d'évoluer.

Pour l'avenir, les entreprises ont de nombreuses occasions de limiter l'impact des piratages massifs de données et de mettre un terme aux pratiques douteuses de collecte et de traçage de données. De nombreux propriétaires de sites empêchent désormais les utilisateurs d'utiliser uniquement la paire nom d'utilisateur / mot de passe et implémentent une authentification multifacteur pour limiter

l'impact des mots de passe piratés. Des fonctionnalités similaires sont également en train d'être intégrées aux navigateurs. En outre, comme de nombreux propriétaires de sites Web ne s'efforcent pas de limiter la collecte et le traçage des données, d'autres ont comblé ce vide. La plupart des navigateurs intègrent désormais un certain niveau de blocage de la publicité et du traçage.

L'amélioration de la sécurité et de la confidentialité est une responsabilité collective de tous les acteurs, et nous devons tous remplir notre part pour maintenir la confiance dans l'Internet. OTA collabore avec tous les acteurs des secteurs public et privé pour travailler à l'amélioration et au renforcement de la santé de l'Internet, en fournissant une plateforme fiable pour l'innovation. Pour en savoir plus, visitez le site https://otalliance.org/TrustAudit.

Résultats de l'audit et tableau d'honneur de la confiance en ligne 2018

L'Online Trust Alliance de l'Internet Society réalise chaque année un audit et un tableau d'honneur de la confiance en ligne : l'étalon manifeste pour reconnaître l'excellence en termes de protection des consommateurs en ligne, de sécurité des données, et de responsabilité des pratiques en matière de confidentialité.

Record absolu, résultant en grande partie des améliorations en termes de chiffrement et d'authentification par e-mail.

TABLEAU D'HONNEUR PAR SECTEUR

GOUVERNEMENT FÉDÉRAL DES ÉTATS-UNIS	91 %	(meilleure progression, par rapport à 39 % en 2017)
SERVICES AUX CONSOMMATEURS	85 %	
INFORMATIONS ET MÉDIAS	78 %	(augmentation rapide et continue au fil des années : 4 %, 8 %, 23 %, 48 %, 78 %)
BANQUES	73 %	(presque triplé par rapport à 27 % en 2017)
DÉTAILLANTS EN LIGNE	65 %	
FAI, OPÉRATEURS, HÉBERGEURS ET FOURNISSEURS DE MESSAGERIE	63 %	
SANTÉ	57 %	(nouveau cette année)

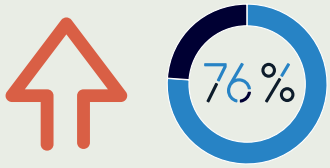
OTA
Online Trust Alliance
an Internet Society initiative

https://otalliance.org/2018HonorRoll

Points clés 2018 par catégorie

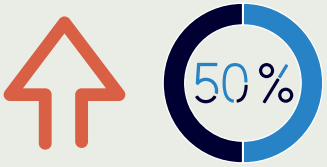
PROTECTION DES DOMAINES (TLD), DES MARQUES ET DES CONSOMMATEURS

Niveaux records d'authentifications par e-mail



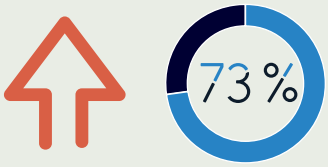
76 % utilisent à la fois les protocoles SPF et DKIM pour les domaines de premier niveau

Les protocoles SPF et DKIM empêchent les e-mails frauduleux et usurpés.



50 % disposent d'un enregistrement DMARC

Le DMARC fournit des indications sur la façon de traiter les messages lorsque l'authentification échoue.



73 % utilisent le protocole TLS opportuniste

Le protocole TLS chiffre les messages entre les serveurs de messagerie.

SÉCURITÉ DES SITES, DES SERVEURS ET DES INFRASTRUCTURES

Sessions Web chiffrées

52 % → 93 %

Augmentation considérable par rapport à un taux de 52 % en 2017
93 % utilisent toujours HSTS/Always-On SSL/HTTPS Everywhere

6 % Seulement 6 % utilisent la spécification Certification Authority Authorization (CAA)

La CAA limite les fraudes de certification.

11 % Seulement 11 % utilisent des méthodes de divulgation des vulnérabilités

Permet de signaler les bugs et les problèmes de sécurité.

CONFIDENTIALITÉ, TRANSPARENCE ET DIVULGATIONS

70

Le score total a chuté à 70 (73 l'an dernier) en raison d'une notation plus rigoureuse compte tenu du RGPD, de la CCPA (loi californienne sur la protection de la confidentialité des consommateurs) et d'autres mesures législatives.

77 %

utilisent des traqueurs Web qui partagent des informations avec des tiers.

15 %

15 % ont reporté au moins un incident de perte ou de violation de données.

https://otalliance.org/2018HonorRoll

Points clés 2018 par secteur

SERVICES AUX CONSOMMATEURS

Ajout de services de paiement et de services de streaming vidéo cette année.

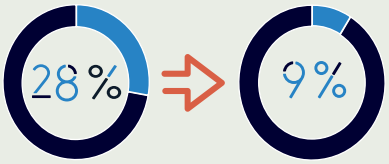
96 %
Meilleure adoption de l'authentification par e-mail (96 %).

76
Meilleur score global en termes de confidentialité (76).

43 %
Meilleure utilisation du signalement des vulnérabilités (43 %, le 2e meilleur score étant de 25 %).

34 %
Taux de violation le plus élevé (34 %).

DÉTAILLANTS EN LIGNE



Nette amélioration de l'authentification par e-mail (les défaillances ont chuté de 28 % à 9 %) malgré une adoption du DMARC plus faible (34 %).

50 %
Les atteintes à la vie privée ont augmenté de près de 50 % (pour atteindre 23 %) en raison du partage avec des tiers.

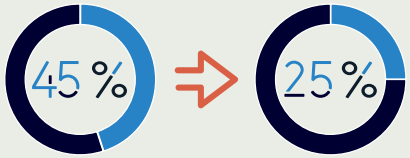
INFORMATIONS ET MÉDIAS

Ajout de sites sportifs cette année.

Une amélioration nette et continue dans tous les secteurs, qui se traduit par une hausse des performances au tableau d'honneur (pour atteindre 78 %).

x4
Utilisation presque 4 fois supérieure des sessions toujours chiffrées (passage de 26 % à 93 %).

FAI, OPÉRATEURS, HÉBERGEURS ET FOURNISSEURS DE MESSAGERIE



Nette amélioration en termes d'authentification par e-mail (les défaillances ont chuté de 45 % à 25 %).

1er 11 %
Adoption la plus élevée du protocole TLS 1.3

2e 20 %
2e en termes de prise en charge du protocole IPv6

GOUVERNEMENT FÉDÉRAL DES ÉTATS-UNIS

Meilleure performance globale du tableau d'honneur (91 %) : revirement important par rapport au dernier rapport alors qu'il avait chuté de 46 % à 39 %.

94
Meilleur score en termes de sécurité (94).

1er 93 %
Adoption du DMARC et application de la politique DMARC les plus élevées (93 % et 83 %, respectivement).

46 %
Adoption la plus élevée du protocole IPv6 (46 %).

BANQUES

45 % → 13 %
Nette amélioration en termes d'authentification par e-mail (les défaillances ont chuté de 45 % à 13 %).

2e 84 %
2e en termes d'utilisation des protocoles SPF et DKIM pour les domaines de premier niveau (84 %, par rapport à seulement 30 % lors du dernier audit).

1er 71 %
Meilleure utilisation des Certificats à Validation Étendue pour les sites Web (71 % : plus du double du secteur arrivant en 2e place).

SANTÉ

NEW

Nouveau cette année, comprend un ensemble de grandes pharmacies, de laboratoires d'analyses, de compagnies d'assurance maladie et de chaînes d'hôpitaux.

57 %
Performance globale du tableau d'honneur la plus faible (57 %), en raison principalement du manque d'authentification par e-mail (35 % de défaillances dans cette catégorie).

2e 73
2e score de confidentialité le plus élevé (73). Adoption la plus faible de sessions toujours chiffrées (82 %).

https://otalliance.org/2018HonorRoll

Annexe B - Méthodologie et notation

Les critères et la méthodologie de l'audit évoluent chaque année, en fonction de l'évolution des normes de sécurité, des normes de confidentialité et du déploiement concret. Chaque année, l'OTA sollicite activement l'internet dans son ensemble par le biais d'une consultation publique de 60 jours généralement lancée au début de septembre.[53] En outre, plusieurs agences gouvernementales américaines et organismes de normalisation du secteur sont consultés. Après examen, le comité de planification de l'audit de confiance d'OTA intègre certaines des directives essentielles en matière de sécurité et de confidentialité, notamment les principes de pratique équitable du traitement de l'information (FIPP), les normes NIST et celles prises en charge par le programme Deploy360 de l'Internet Society.[54] En tenant compte de ces données combinées, la pondération et les scores sont réexaminés chaque année, puis réaffectés pour tenir compte de l'évolution du paysage des menaces, de l'environnement réglementaire et de la facilité de déploiement. Le résultat final se concentre sur les meilleures pratiques admises qui reflètent le déploiement concret, comblant le fossé entre les normes et les communautés d'affaires. La méthodologie finale de l'audit de cette année a été publiée en août 2018 et fait l'objet d'une large promotion afin de permettre aux organisations de réévaluer leurs pratiques et d'optimiser leurs scores.[55]

L'audit de confiance en ligne comprend une analyse composite axée sur trois grandes catégories :

- Protection du consommateur (protection du DNS, du domaine et de la marque)
- Sécurité de site, de serveur, d'application et d'infrastructure
- Confidentialité, transparence et divulgations

Les sites pour recevoir jusqu'à 300 points de base (jusqu'à 100 points dans chaque catégorie) et jusqu'à 60 points de bonus (20 % du score de base) pour l'implémentation des meilleures pratiques émergentes. En outre, les entreprises pouvaient perdre des points en raison de règlements juridiques, de piratages de données, de vulnérabilités observées et d'autres lacunes importantes.

Pour se qualifier pour le tableau d'honneur, les sites devaient recevoir un score composite d'au moins 80 % des points de référence *et* **un score d'au moins 60** dans chacune des trois catégories principales. Le seuil d'échec a été élevé à 60 en 2017, afin de reconnaître que « la sécurité est seulement aussi forte que son maillon le plus faible » et que les sites sont construits sur une « chaîne de confiance ».

L'audit de 2018 a été alimenté par des analyses techniques et des données fournies par plus d'une douzaine d'organisations. Sans leur aide et leur soutien, cet audit et cette télémétrie n'auraient pas été possibles. L'échantillonnage des données s'est déroulé entre le 10 décembre 2018 et le 31 janvier 2019. Les organisations qui ont fourni des données sont notamment Agari, Disconnect, dmarcian, ImmuniWeb, Infoblox, Internet.nl, Microsoft, Mozilla, SSL Labs, Sucuri, Symantec, Valimail et Verisign. Des données supplémentaires ont été obtenues auprès de sources de données publiques, notamment BugCrowd, Google, HackerOne, Open Bug Bounty, Twitter et d'autres. Il est important de noter que la configuration ou les pratiques d'un site peuvent avoir changé depuis l'échantillonnage et que les données ne reflètent que les constatations effectuées au cours de cette période précise.

Protection du consommateur (protection du DNS, du domaine et de la marque)

L'e-mail continue d'être le principal vecteur d'attaque, générant la compromission de l'e-mail en entreprise (BEC), le vol des identifiants et des identités, les prises de contrôle de comptes bancaires et la

diffusion de malwares.[56] Le FBI a signalé que la fraude liée aux BEC avait généré des pertes financières de 12,5 milliards de dollars depuis 2013, dont la plupart auraient pu être évitées.[57] Au cours des dix dernières années, OTA a plaidé pour une authentification des e-mails de bout en bout afin de détecter et de bloquer les e-mails malveillants et usurpés de tous les domaines et sous-domaines gérés par une organisation. L'adoption aide à protéger les consommateurs et les destinataires d'e-mails contre la diffusion de malwares, les Keyloggers et les menaces connexes, notamment les ransomwares, le cryptomining et les prises de contrôle de compte, tout en protégeant la réputation de la marque ciblée.

- Authentification des e-mails (SPF, Sender Policy Framework et DKIM, DomainKeys Identified Mail) dans les domaines de premier niveau (« corporatifs ») et les sous-domaines d'e-mail. L'audit de 2018 accroît le poids de l'authentification des domaines de premier niveau (les plus reconnaissables par l'utilisateur et les plus souvent usurpés), avec un nombre de points réduit pour des sous-domaines délégués distincts. De plus, les sites avec des enregistrements SPF non valides n'ont reçu qu'un crédit partiel ou aucun crédit - *partie du score de base* [58]
- Authentification, rapport et conformité de message par domaine (DMARC). Les enregistrements DMARC avec p=none et sans rapport (RUA ou RUF) ne reçoivent aucun crédit. Appelés « enregistrements DMARC nus », ils ne fournissent aucune valeur en matière de protection du consommateur ou de la marque, car les réseaux de réception ne se conforment pas à la politique et les marques ne reçoivent pas de rapport d'authentification et d'abus. Le poids a été augmenté pour l'utilisation de la politique de « rejet » – *partie du score de base* [59]
- Implémentation du TLS « opportuniste » pour le courrier électronique. L'importance a été augmentée en 2018 - *points de bonus* [60]
- Verrouillage de domaine – *pénalité si le domaine n'est pas verrouillé*
- Extensions de sécurité DNS (DNSSEC) – *points de bonus* [61]
- Implémentation du protocole Internet version 6 (IPv6) pour l'accès au serveur Web – *points de bonus* [62]
- Authentification multifacteur - Bien que l'authentification multifacteur ait été récompensée lors de l'audit de 2017, cela ne s'est pas répété dans cet audit en raison de sources de données insuffisantes dans tous les secteurs.

Sécurité de site, de serveur et d'infrastructure

Meilleures pratiques pour sécuriser les données en transit et collectées par les sites Web, et empêcher l'exploitation malveillante des dispositifs des clients. Les sites étaient éligibles pour obtenir jusqu'à 100 points de base, à condition qu'aucun des critères SSL / TLS essentiels (chiffrements, échange de clé ou prise en charge du protocole) n'ait obtenu un score inférieur à 60. Les sites ont été testés avec plusieurs outils pour rechercher les vulnérabilités connues, la configuration HSTS et les certificats incompatibles. [63, 64] En 2017, la sécurité des serveurs a été étendue pour inclure la sécurité des applications, la cadence des correctifs et la réputation de l'IP. Elle a été de nouveau étendue en 2018 pour inclure de rigoureuses évaluations de la politique de sécurité des données et des mesures de prévention relatives aux données de tiers sur les sites. La prise en charge de Always On SSL a été intégrée à la notation de référence en 2018.[65]

Points de bonus / de pénalité

- Certificats SSL à validation étendue (SSL EV) – *points de bonus* [66]

- Autorisation de l'autorité de certification (CAA) – nouveau en 2018 – *points de bonus*
- Pare-feu pour applications Web – *points de bonus*
- Tests pour XSS, exploitations d'iFrame, malwares, liens malveillants – *pénalité si ces menaces existent*
- Mécanisme de signalements des vulnérabilités et des bogues (institué en 2017). Les sites gagnent des points de bonus pour les mécanismes de signalements, notamment les formulaires en ligne ou l'utilisation de signalements par des bug bounty tiers. Les données ont été analysées par des recherches en ligne à l'aide de mots-clés, ainsi que par la recherche de programmes de bug bounty tiers tels que HackerOne et Bugcrowd[67, 68] – *points de bonus*

Confidentialité, transparence et divulgations

Les meilleures pratiques pour toutes les organisations consistent à offrir aux utilisateurs des avis clairs, une transparence et un contrôle des données collectées, tracées et partagées avec des tiers. Le score de confidentialité peut atteindre jusqu'à 100 points et couvre : l'inclusion des divulgations appropriées, la structure de la déclaration de confidentialité (y compris l'adoption des principes de pratique équitable du traitement de l'information (FIPP) généralement reconnues), le traçage et la collecte de données tiers.[69] Les déclarations de confidentialité ont été lues et notées par les analystes d'OTA / de l'Internet Society.

Déclaration de confidentialité – Possibilité d'obtenir 55 points. Les sites peuvent recevoir des scores maximums en respectant les directives suivantes :

- Lien / accessibilité depuis la page d'accueil
- Date de la déclaration de confidentialité en haut de la page
- Divulgation concernant la gestion du paramètre DNT (Ne pas tracer) du navigateur
- Déclaration de politique de conservation des données avec une référence au délai spécifique de conservation (le délai a été nouvellement inclus en 2018)
- Données personnelles non partagées, sauf avec des tiers qui fournissent le service
- Données personnelles non partagées avec les affiliés ou les partenaires (directive séparée du partage de données de base de 2018)
- Conformité des fournisseurs : divulgation du fait que les fournisseurs de services doivent se conformer à la déclaration de confidentialité de l'organisation et qu'il est interdit d'utiliser ou de partager des données à des fins autres que la fourniture de services pour le compte de l'organisation
- Traçage des versions (ou accès aux versions précédentes), y compris l'affichage des annotations de révision (points de bonus avant 2018)
- Conception comme un avis court ou par couches
- Conformité à la loi sur la protection de la vie privée en ligne des enfants ou aux réglementations connexes[70]

Traçage de tiers sur site – 45 points possibles pour les sites dépourvus de traceurs de tiers (à l'exception des analyses anonymes). L'observation de traceurs connus pour partager des données avec des tiers entraîne une réduction du nombre de points.[71]

Points de bonus

- Utilisation d'icônes ergonomiques pour aider à la navigation
- Déclaration localisée ou multilingue, où l'anglais peut être une « seconde langue »
- Respect du paramètre DNT (Ne pas tracer) du navigateur de l'utilisateur
- Divulgations sur le traçage inter-dispositifs (ajouté en 2017)[72]
- Mise en place de systèmes de gestion des balises ou de solutions de confidentialité pour gérer les balises tierces

Points de pénalité

- Piratages des données - pour les violations de plus de 1000 enregistrements. Pour l'audit de 2018, la pénalité a été réduite proportionnellement à l'étendue du piratage des données – *pénalité en cas d'incident notable entre le 1er juin 2017 et le 31 décembre 2018*
- Règlements juridiques avec la Commission fédérale du commerce (FTC), la Commission fédérale de la communication (FCC), le Bureau de la protection financière du consommateur (CFPB)[73], niveau national ou mondial – *pénalité si le règlement a eu lieu entre le 1er juin 2017 et le 31 décembre 2018.*
- Enregistrement WHOIS public / privé – *pénalité si privé*

Annexe C – Top 50 du Tableau d'honneur 2018

Secteur	Organisation	Secteur	Organisation
C	1040.com	C, **R**	**Google Play**
H	**23 and Me**	O	Internet Society
C	Airbnb	C	Lyft
C	Amazon Payments	G	Agence américaine d'observation océanique et atmosphérique (NOAA)
R	Apple Inc.	C	Netflix
C	Blogger	C, O	Norton LifeLock
R	Casper	G	Office of Personnel Management (OPM)
H	Costco Pharmacy	**O**	**Online Trust Alliance**
G	Département de l'agriculture (Service de la sécurité et de l'inspection des aliments)	**C**	**PayPal**
G	Ministère de la Santé et des Services sociaux (Medicare)	R	Petco Animal Supplies Inc.
G	Ministère de la Santé et des Services sociaux (Healthcare.gov)	C, N	Reddit
G	Département du Trésor	G	Securities and Exchange Commission (SEC)
C	DocuSign	C	Snapchat
G	Commission fédérale des communications (FCC)	G	Administration de la sécurité sociale (SSA)
G	**Agence fédérale des situations d'urgence (FEMA)**	C	Square Cash
G	Federal Trade Commission (FTC)	I	Sucuri
B	**First National Bank of Omaha**	B	TD Bank, National Association
R	Fitbit Inc.	B	The Huntington National Bank
C	Flickr	C	Tinder
R, O	Gap Inc.	O	TrustSphere
G	Administration des services généraux (GSA)	C, O	Twitter
I	**Google Cloud**	C	UpWork
C	Google Drive	G	Forces armées des Etats-Unis - Garde-côte
N	**Google News** ◆	R	Walmart Inc.
C	Google Pay	C	YouTube

Codes des secteurs : C - Services aux consommateurs, B - Banques, G - Gouvernement fédéral américain, H - Santé, I - FAI / Hébergeurs, N - Actualités / Médias, O - Membre d'OTA ou de l'Internet Society, R - Détaillants en ligne. Comme indiqué, les organisations peuvent appartenir à plusieurs segments.

Les meilleurs scores de chaque secteur sont en gras. Le score global le plus élevé est marqué d'un ◆.

Annexe D – Lauréats du tableau d'honneur 2018

Top 500 des détaillants en ligne 2018 - Tableau d'honneur

65 % de tableau d'honneur - 31 % d'échec - 14% de « Première classe »

- ❷ 1-800 Contacts Inc.
- 1-800-Flowers.com Inc.
- 1Sale
- ❷ Abercrombie & Fitch Co.
- ❷ AC Lens
- adidas AG
- Adorama Camera Inc.
- ❷ Adore Me Inc.
- Aéropostale Inc.
- AJ Madison Inc.
- ❷ Albertsons Inc.
- Aleph Objects Inc.
- ❸ Alex and Ani LLC
- ❼ Alibris Inc.
- Allied Electronics
- ❼ Amazon.com Inc.
- ❼ American Greetings Corp.
- American Standard Brands
- AmeriMark Direct LLC
- ❹ APMEX Inc.
- ❸ **Apple Inc.**
- Aquasana Inc.
- Art.com Inc.
- Ascena Retail Group
- ❷ Ashley Stewart Inc.
- ASOS Plc Holdings
- ❷ AutoZone Inc.
- ❷ B&H Foto & Electronics Corp.
- ❷ Backcountry.com
- Balsam Brands
- Barcodes Inc.
- Bare Necessities
- ❷ Barnes & Noble Booksellers Inc.
- Barneys New York Inc.
- ❼ Bass Pro Shops
- ❷ BaubleBar Inc.
- BeachCamera.com
- bebe stores Inc.
- Belk Inc.
- ❻ Best Buy Co. Inc.
- ❷ Better World Books
- Big 5 Corp.
- Birchbox Inc.
- Bissell
- ❹ BJ's Wholesale Club
- Black & Decker Inc.
- Black Diamond Equipment Ltd.
- Blain Supply Inc.
- ❷ Blue Nile Inc.
- ❸ Bluefly Inc.
- Bob's Discount Furniture LLC
- Boohoo.com plc
- ❸ Bookbyte
- Boot Barn Inc.
- ❷ Boscov's Department Store LLC
- Boston Proper LLC
- ❸ Boxed Wholesale
- Brilliant Earth LLC
- Brooklinen
- Brooks Brothers
- ❻ BuildASign.com
- ❹ BuildDirect Technologies Inc.
- ❹ Burberry Ltd.
- CafePress Inc.
- Camping World Inc.
- ❷ Carter's Inc.
- ❷ **Casper**
- Chanel S.A.
- ❸ Chico's FAS Inc.
- ❷ Christopher & Banks Corp.
- Classic Firearms
- ❸ Code42 Software Inc.
- Columbia Sportswear Co.
- Concept2 Inc.
- Cool Stuff Inc.
- ❹ Costco Wholesale Corp.
- Crocs Inc.
- Crucial Technology
- ❹ Crutchfield Corp.
- ❷ CustomInk
- Cutlery and More LLC
- ❷ CVS Caremark Corp.
- ❸ Cymax Stores Inc.
- Databazaar.com
- dbrand
- Deckers Brands
- ❷ DeepDiscount.com
- ❷ Dell Inc.
- Destination XL Group Inc.
- Dick Blick Holdings Inc.
- ❷ Diesel
- Digi-Key Electronics
- ❹ Dollar Shave Club
- Dollar Tree Inc.
- ❷ Dolls Kill
- ❷ Dover Saddlery Inc.
- DrJays.com
- Duluth Trading Company
- Dyson Ltd.
- eCampus.com
- ❹ Eddie Bauer LLC
- ❹ Entertainment Earth Inc.
- ❻ Etsy Inc.
- Everlane Inc.
- Evine Live Inc.
- ❷ Fanatics Inc.
- Fashion Nova
- ❸ **Fitbit Inc.**
- Flight Club
- Floor & Décor Outlets of America Inc.
- Focus Camera Inc.
- ❸ Follett Higher Education
- ❷ Foot Locker Inc.
- ❹ Forever 21
- ❹ Fossil Inc.
- FragranceNet.com Inc.
- FreshDirect LLC

Gras – Top 50 global ◆ – Meilleur score dans le secteur ❷ ❸ ❹ ❺ ❻ ❼ – Années consécutives en tant que récipiendaire du tableau d'honneur

Top 500 des détaillants en ligne 2018 – Tableau d'honneur, suite

Full Compass Systems Ltd.
Furniture.com Inc.
6 GameFly Inc.
Gander Mountain
4 Gap Inc.
Gardeners Supply Company
Gear Patrol LLC
GlassesUSA LLC
Global Equipment Company Inc.
Glossier Inc.
GNC Holdings Inc.
2 Godiva Chocolatier Inc.
3 Google Play ◆
3 GoPro Inc.
GrabAGun.com
Grizzly Industrial Inc.
Groupon Goods
Guess Inc.
Hallmark Cards Inc.
HanesBrands Inc.
Hanover Company Store LLC
3 Harry's Inc.
Helix Sleep
Herman Miller Inc.
3 hhgregg Appliances Inc.
Hobbico
2 Home Chef
2 Hot Topic Inc.
HP Home & Home Office Store
4 iHerb Inc.
4 IKEA
2 Indigo Books & Music Inc.
Inditex Group
J. Crew Group Inc.
J. Jill
2 J.C. Penney Co. Inc.
2 J.Hilburn Inc.
Jabra
6 JackThreads Inc.
JEGS High Performance Inc.
JetPens.com
JM Bullion Inc.
4 Joann.com
KEH Inc.
2 Keurig Green Mountain Inc.
Klipsch Group Inc.
2 Lakeshore Learning
3 Lands' End
LD Products Inc.
2 Leesa Sleep LLC
2 Lenovo Group Ltd.
Leslies Poolmart Inc.
Levi Strauss & Co.
4 LifeWay Christian Resources
2 LightIntheBox Ltd.
2 Living Spaces
6 LivingSocial Inc.
Loot Crate Inc.
3 Lowe's Cos. Inc.
LuckyGunner LLC
LuLuLemon Athletica Inc.
2 LuLu's Fashion Lounge Inc.
Lumber Liquidators Inc.
LVMH
M. Gemi
2 Macy's Inc.
Mattel
2 Mattress Firm Inc.
Meijer Inc.
2 Michael Kors Holdings Ltd.
Micro Electronics Inc.
2 MidwayUSA Inc.
MLB Advanced Media
Moda Operandi Inc.
4 Monoprice Inc.
Monrovia
2 MotoSport LLC
Mouser Electronics Inc.
MSC Industrial Supply Co. Inc.
2 MVMT Watches
NakedWines.com Inc.
4 National Hockey League
3 NatureBox Inc.
2 Nebraska Furniture Mart
4 New Avon LLC
2 New Balance Athletics Inc.
New York & Co. Inc.
5 Newegg Inc.
5 Nike Inc.
2 Nine West Holdings Inc.
5 Nordstrom Inc.
2 Office Depot Inc.
4 OmahaSteaks.com Inc.
OMEGA Engineering Inc.
OpticsPlanet Inc.
3 O'Reilly Auto Parts
2 Otto Group
OvernightPrints.com
7 Overstock.com Inc.
Painful Pleasures Inc.
Palmetto State Armory
2 Panasonic Corp.
2 Patagonia
7 Payless ShoeSource Inc.
PC Connection Inc.
Performance Bicycle
4 Petco Animal Supplies Inc.
3 PetFlow
2 PetSmart Inc.
4 Pier 1 Imports Inc.
3 Power Equipment Direct Inc.
Primary Arms LLC
Pro:Direct
3 PropertyRoom.com Inc.
Provo Craft & Novelty Inc.
2 Purple
2 Qurate
4 REI
2 Reitmans (Canada) Ltd.
Rent the Runway Inc.
2 Replacements Ltd.
3 Restoration Hardware
RevZilla Motorsports LLC
2 Richline Group
RobotShop Inc.
6 RockAuto LLC
Rockler Companies Inc.
Rooms To Go Inc.
2 rue21 Inc.

Gras – Top 50 global ◆ – Meilleur score dans le secteur 2 3 4 5 6 7 – Années consécutives en tant que récipiendaire du tableau d'honneur

Top 500 des détaillants en ligne 2018 – Tableau d'honneur, suite

Rural King
❸ Saatva Inc.
Samsonite International S.A
Scholastic Inc.
School Specialty Inc.
❷ Sears Holdings Corp.
Sears Hometown/Outlets
Sennheiser Electronic GMBH & Co.
❹ Shindigz
Shoe Carnival Inc.
Shoes of Prey Inc.
ShoppersChoice.com LLC
Shutterfly Inc.
Signet Jewelers Ltd.
Silver Star Brands
Skinit Acquisition LLC
Sonos Inc.
❻ Spiraledge
ssense.com
❷ Staples Inc.
SteelSeries ApS
Stitch Fix
❸ Summit Racing Equipment
Sun Basket
❷ Sur La Table Inc.
❺ Sweetwater
Tackle Warehouse LLC
Tapestry
❷ Target Corp.
Tarte Inc.
Teespring Inc.
❷ Tennis Warehouse
❹ The Clymb
The Container Store Inc.
The Estee Lauder Cos. Inc.
The Finish Line Inc.
❷ The Great Courses
❸ The Home Depot Inc.
❹ The Honest Company Inc.
❷ The Kroger Co.
❷ The Lakeside Collection
The Men's Wearhouse Inc.
❹ The Nature's Bounty Co.
❹ The Orvis Co. Inc.
❸ The RealReal Inc.
The Walt Disney Company Ltd.
❷ ThriftBooks Global LLC
❷ Thrive Market
❷ Tiffany & Co.
❹ Tilly's Inc.
❹ TJX Cos. Inc.
❹ TOMS Shoes LLC
Tory Burch LLC
Traeger Grills
Trans World Entertainment
TSC
❷ Tuft & Needle
Uniqlo
United States Mint
Value City Furniture
Vera Bradley Retail Stores LLC
VIPOutlet
Vitamin Shoppe Industries Inc.
Vizio Inc.
W.W. Grainger Inc.
❷ **Walmart Inc.**
❹ Warby Parker
❻ Wayfair Inc.
Weber Grills
Whirlpool
❷ Wolverine Worldwide Inc.
Xerox Corp.
YDesign Group LLC
❹ Zazzle Inc.
Zenni Optical Inc.
❹ Zumiez Inc.

Gras – Top 50 global ◆ – Meilleur score dans le secteur ❷ ❸ ❹ ❺ ❻ ❼ – Années consécutives en tant que récipiendaire du tableau d'honneur

Top 100 des banques 2018 – Tableau d'honneur

73 % de tableau d'honneur – 27 % d'échec – 6 % de « Première classe »

American Express National Bank
5 Arvest Bank
Associated Bank, National Association
BancorpSouth Bank
7 Bank of America, National Association
3 Bank of Hawaii
Bank of Hope
3 Bank of the West
Bank OZK
Barclays Bank Delaware
5 Branch Banking and Trust Company
4 Capital One, National Association
Cathay Bank
Centennial Bank
Charles Schwab Bank
2 Chemical Bank
CIBC Bank USA
5 Citibank, National Association
2 Citizens Bank, National Association
5 City National Bank
3 Comerica Bank
3 Commerce Bank
3 Compass Bank
3 Deutsche Bank Trust Co, Americas
4 Discover Bank
E*TRADE Bank
4 Fifth Third Bank
First Hawaiian Bank
First Midwest Bank
2 First Nat'l Bank of Omaha ◆
4 First Republic Bank
7 Frost Bank
Goldman Sachs Bank USA
3 Hancock Whitney Bank
HSBC Bank USA, National Association
4 Iberiabank
Investors Bank
3 JPMorgan Chase Bank, National Assoc
3 KeyBank National Association
Manufacturers & Traders Trust Co.
MB Financial Bank, National Assoc.
MidFirst Bank
6 Morgan Stanley Bank, National Assoc.
4 MUFG Union Bank, National Assoc.
New York Community Bank
Old National Bank
Pacific Western Bank
Pinnacle Bank
PNC Bank, National Association
Prosperity Bank
5 Regions Bank
Sallie Mae Bank
2 Signature Bank
2 Silicon Valley Bank
South State Bank
Stifel Bank and Trust
3 SunTrust Bank
2 Synovus Bank
3 TCF National Bank
3 TD Bank, National Association
2 The Bank of New York Mellon
4 The Huntington National Bank
The Northern Trust Company
TIAA, FSB
7 U.S. Bank National Association
UBS Bank USA
UMB Bank, National Association
3 Umpqua Bank
United Bank
USAA Federal Savings Bank
Washington Federal, National Assoc.
Western Alliance Bank
Zions Bancorporation, N.A.

Gras – Top 50 global ◆ – Meilleur score dans le secteur ❷ ❸ ❹ ❺ ❻ ❼ – Années consécutives en tant que récipiendaire du tableau d'honneur

Top 100 du gouvernement fédéral américain – Tableau d'honneur

91 % de tableau d'honneur – 8 % d'échec – 26 % de « Première classe »

Bureau administratif des tribunaux des États-Unis (Judiciaire)

Bureau of Labor Statistics (BLS)

4 Census Bureau

Centres pour le contrôle et la prévention des maladies (CDC)

Bureau américain de protection des consommateurs

2 Département de l'Agriculture

Département de l'Agriculture (ChooseMyPlate.gov)

Département de l'Agriculture (Service de sécurité et d'inspection des aliments)

Département du Commerce

Département du Commerce - National Weather Service/NOAA

Département du Commerce (Exports)

2 Département du Commerce (NIST)

2 Département du Commerce (NTIA)

Département du Commerce (Brevets & Marques)

Département du Commerce (Privacy Shield)

Département de la Défense

4 Département de l'Éducation

2 Département de l'Éducation (Bourses et aides)

Département de l'Éducation (Centre national de la statistique de l'éducation)

Département de l'Éducation (Prêts étudiants)

4 Département de l'Énergie

2 Département de l'Énergie (Energy Star)

Ministère de la Santé et des Services sociaux (Medicare)

Ministère de la Santé et des Services sociaux (Medicare/Medicaid)

Ministère de la Santé et des Services sociaux (Santé des femmes)

3 **Ministère de la Santé et des Services sociaux (Healthcare.gov)**

2 Ministère de la Santé et des Services sociaux (HHS)

Département de la Sécurité intérieure (Douanes et services d'immigration)

Département de la Sécurité intérieure (Douanes et protection des frontières)

2 Département de la Sécurité intérieure (DHS)

Département de la Sécurité intérieure (DHS)

Département de la Sécurité intérieure (ICE)

Département de la Sécurité intérieure (Douanes et dossiers d'immigration)

Département du Logement et du Développement urbain (HUD)

4 Département de l'Intérieur

Département de l'Intérieur (Institut d'études géologiques)

2 Département de l'Intérieur (Institut d'études géologiques)

Département de la Justice (Bureau des prisons)

3 Département de la Justice (DOJ)

2 Département du Travail

Département du Travail (OSHA)

Département d'État

Département d'État (Bureau des historiens)

Département d'État (Demandes de visa en ligne)

Département d'État (Voyage)

Département des Transports

Département du Trésor

Département du Trésor (TreasuryDirect)

Agence de Protection de l'Environnement

Federal Aviation Administration (FAA)

4 Bureau fédéral d'investigation (FBI)

2 **Commission fédérale des communications (FCC)**

2 Federal Deposit Insurance Corporation (FDIC)

2 **Agence fédérale des situations d'urgence (FEMA)** ◆

Réserve fédérale

2 Federal Trade Commission (Info consommateur)

2 Federal Trade Commission (Do Not Call)

4 **Federal Trade Commission (FTC)**

4 First Gov (USA.gov)

Food and Drug Administration (FDA)

Administration des services généraux (GSA)

2 Internal Revenue Service (IRS)

4 National Aeronautics and Space Admin (NASA)

National Highway Traffic Safety Administration

National Institutes of Health (Cancer.gov)

National Institutes of Health (MedlinePlus)

4 National Institutes of Health (NIH)

2 **Agence américaine d'observation océanique et atmosphérique (NOAA)**

4 National Park Service (NPS)

2 National Science Foundation (NSF)

Office of Personnel Management (OPM)

Office of the Federal Register

Peace Corps

Securities and Exchange Commission (SEC)

2 Small Business Administration

4 Administration de la sécurité sociale (SSA)

Forces armées des Etats-Unis - Garde-côte

Forces armées des Etats-Unis (Armée de l'air)

Gras – Top 50 global ◆ – Meilleur score dans le secteur ❷ ❸ ❹ ❺ ❻ ❼ – Années consécutives en tant que récipiendaire du tableau d'honneur

Top 100 du secteur de la consommation 2018 – Tableau d'honneur

85 % de tableau d'honneur – 9 % d'échec – 40 % de « Première classe »

- ❸ **1040.com**
- ❸ 1040NOW
- Addicting Games
- ❸ **Airbnb**
- **Amazon Payments**
- ❸ Ancestry
- Answers.com
- AOL
- Ask.fm
- ❼ Badoo.com
- BigFishGames
- Bing
- **Blogger**
- ❸ Booking.com
- ❺ Box
- ❸ CareerBuilder
- ❷ Classmates
- Craigslist
- Dailymotion
- DeviantArt
- ❸ **DocuSign**
- ❺ Dropbox
- eBay
- eHow
- ❹ eSmart (Liberty Tax)
- ❸ Expedia
- ❹ ezTaxReturn.com
- ❸ FileYourTaxes
- ❻ Fiverr
- ❹ **Flickr**
- ❸ Free Tax Return.com
- ❹ FreeTaxUSA
- ❸ Glassdoor
- ❹ **Google Drive**
- **Google Pay**
- **Google Play**
- ❸ H&R Block
- HBO Now
- Hotels.com
- Hotwire
- Hulu
- ❺ iCloud
- ID Watchdog
- ❸ Identity Guard
- IdentityForce
- IMDb
- ❸ Imgur
- ❸ Indeed
- ❻ Instagram
- JobDiagnosis.com
- ❸ KAYAK
- ❼ LinkedIn
- ❸ **Lyft**
- ❹ Match.com
- ❸ MediaFire
- ❸ Meetup
- ❸ Miniclip
- ❸ Monster
- MSN
- MySpace
- **Netflix**
- ❹ **Norton LifeLock**
- ❸ OkCupid
- OLT Online Taxes
- OneDrive
- ❸ Orbitz
- ❸ Pandora
- **PayPal** ◆
- ❻ Pinterest
- Pogo
- ❸ Priceline
- ❼ Publishers Clearing House
- ❸ **Reddit**
- Shutterfly
- Simply Hired
- ❸ **Snapchat**
- ❸ SoundCloud
- ❸ Spotify
- **Square Cash**
- ❹ TaxACT
- ❹ TaxSlayer
- **Tinder**
- Travelocity
- TripAdvisor
- ❼ Tumblr
- ❸ TurboTax
- ❼ **Twitter**
- **UpWork**
- Venmo
- Vimeo
- VRBO
- Western Union
- Wikia
- wikiHow
- Wikipedia
- ❻ Wordpress
- Xoom
- Y8
- ❺ Yahoo!
- Yelp
- ❻ **YouTube**
- Zelle
- ❸ Zoosk
- ❼ Zynga

Gras – Top 50 global ◆ – Meilleur score dans le secteur ❷ ❸ ❹ ❺ ❻ ❼ – Années consécutives en tant que récipiendaire du tableau d'honneur

Top 100 du secteur des Actualités / Médias 2018 – Tableau d'honneur

78 % de tableau d'honneur – 19 % d'échec – 2 % de « Première classe »

- ❸ American City Business Journals
- ❷ AOL News
- AP
- Axios
- Bankrate
- BBC.com
- Bleacher Report
- Bloomberg News
- ❷ Boston.com
- Breitbart
- ❸ Business Insider
- ❸ BuzzFeed
- Cars.com
- CBS News
- CBS Sports
- Chicago Tribune
- Chron
- CNBC
- ❷ CNET
- CNN
- Consumer Reports
- Daily Caller
- Deadspin
- Digital Trends
- ❸ Engadget
- ESPN
- ❷ Everyday Health
- ❷ Fox News
- Fox Sports
- ❸ Gizmodo
- ❺ **Google News** ◆
- ❷ Huffington Post
- ❷ Independent
- ❷ Kotaku
- Lifewire
- Live Science
- Los Angeles Times
- ❷ Mashable
- ❸ MSN News
- ❷ National Geographic
- NBC Sports
- New York Magazine
- ❺ New York Times
- Newsweek
- NJ.com
- ❷ NPR
- NY Daily News
- Patch
- PBS
- ❷ Politico
- Polygon
- ❸ **Reddit**
- Reuters
- SB Nation
- SFGate
- ❷ Slate
- ❷ TechCrunch
- ❸ The Atlantic
- ❷ The Daily Beast
- ❸ The Guardian
- The Motley Fool
- The National Weather Service
- The New York Post
- The Sun
- The Telegraph
- ❷ TMZ
- US News
- USA Today
- ❸ Vice
- ❷ Vox
- Wall Street Journal
- Washington Post
- Washington Times
- Weather Channel
- Weather Underground
- ❸ WebMD
- ❷ Wired
- ❸ Yahoo News

Gras – Top 50 global ◆ – Meilleur score dans le secteur ❷ ❸ ❹ ❺ ❻ ❼ – Années consécutives en tant que récipiendaire du tableau d'honneur

Top 100 des FAI, opérateurs et hébergeurs 2018 – Tableau d'honneur

63 % de tableau d'honneur – 35 % d'échec – 4 % de « Première classe »

- ❷ 1&1
- A2 Hosting
- Akamai Technologies
- Amazon Web Services (AWS)
- ❷ AOL Mail
- AT&T
- AT&T Wireless
- ❷ Automattic
- ❷ BlueHost
- ❷ C Spire Wireless
- Cable ONE
- Comcast
- Consolidated Communications
- ❷ Cox Communications
- Cricket Wireless
- CyrusOne
- ❷ Digital Ocean
- e-vergent
- Etheric Networks
- Everywhere Wireless
- ❷ Frontier Communications
- GoDaddy
- ❷ **Google Cloud** ◆
- ❷ Google Gmail
- ❷ HostGator
- HostMonster
- ❷ iCloud Mail
- ❷ Incapsula Inc
- iPage
- KnownHost
- ❷ Linode
- ❷ LiquidWeb
- ❷ Mail.com
- ❷ MetroPCS
- ❷ Microsoft Azure
- ❷ Microsoft Outlook.com
- ❷ New Dream Network, LLC
- Optimum by Altice
- Peer 1 Network (USA) Inc
- ❷ ProtonMail
- Psychz Networks
- Rackspace
- RCN
- Rise Broadband
- Shopify
- ❷ SingleHop
- ❷ SoftLayer
- ❷ Squarespace
- **Sucuri**
- Suddenlink Communications
- TDS Telecom
- TierPoint
- Tutanota
- ❷ Verizon
- ❷ Verizon Wireless
- WATCH Communications
- ❷ Weebly
- Winters Broadband
- WOW!
- ❷ Yahoo Mail
- Yandex Mail
- ❷ Zoho Mail

Gras – Top 50 global ◆ – Meilleur score dans le secteur ❷ ❸ ❹ ❺ ❻ ❼ – Années consécutives en tant que récipiendaire du tableau d'honneur

Top 100 du secteur de la santé 2018 – Tableau d'honneur

57 % de tableau d'honneur – 43 % d'échec – 4 % de « Première classe »

23andMe ◆
Adventist Health System
Aetna Group
Ahoid Delhaize (Food Lion Pharmacy)
Albertsons Pharmacy
Alere, Inc.
Anthem
Any Lab Test Now
Ascension Health
Baylor Scott & White Health
BCBS of MN
BCBS of NJ GRP
CA Physician's Service (d/b/a BS of CA)
Cambria Health Solutions
Carefirst Inc. Group
Caresource Group
Cigna Health Group
Cigna Pharmacy
Costco Pharmacy
Counsyl
CVS Pharmacy
DaVita Healthcare Partners, Inc.
Dignity Health
Diplomat Pharmacy
Express Scripts
Florida Blue
Gene by Gene
HCSC Group
Health Net of California, Inc.
Highmark Group
Hospital Corporation of America (HCA)
Independence Health Group Inc. Group
Kroger Pharmacy
Laboratory Corporation of America
Mercy Health
Myriad Genetics, Inc.
Northwell Health
Pathway Genomics
PharMerica
Prime Healthcare Services
Providence Health and Services
Publix Pharmacy
Quest Diagnostics, Inc.
Rite Aid Pharmacy
SSM Health Care
Tenet Healthcare
United Health
UnitedHealth (Optum Rx)
Univera Healthcare Advantage
Universal Health Services
Unum Group
UPMC (Hôpitaux)
UPMC Health System Group (Assurance)
Walgreens Boots Pharmacy
Walmart Pharmacy

Membres d'OTA* de l'Internet Society 2018 – Tableau d'honneur

98 % de tableau d'honneur – 2 % d'échec – 12 % de « Première classe »

❻ ACT | The App Association
❹ ADT
❼ Agari
❷ Classmates
❼ Constant Contact
❼ DigiCert
❺ Distil Networks
❸ Dmarcian Inc.
❼ Ensighten
❹ **Gap Inc.**
❼ GetResponse
❷ Global Cyber Alliance
❷ Guardian Life
❼ High-Tech Bridge (devenue ImmuniWeb)
❼ Iconix
❼ Identity Guard
❸ Infoblox
❷ Intelius
❷ **Internet Society**
❼ Intersections
❹ Kromtech Alliance Corp.
❺ LashBack
❹ MacKeeper
❹ Malwarebytes
❼ Marketo
❼ Microsoft
❸ National Association of REALTORS
❹ **Norton LifeLock**
❼ **Online Trust Alliance** ◆
❺ OPTIZMO
❷ PeopleConnect
❹ PhishLabs (auparavant Brand Protect)
❷ Security Scorecard
❹ Simpli.Fi
❼ Symantec
❺ The Media Trust
❼ **TrustSphere**
❼ **Twitter**
❹ UnsubCentral
❸ Valimail
❻ Verisign
❸ Yes Marketing
❸ Zeta Interactive

* Organisations membres de l'Internet Society qui étaient auparavant membres de l'OTA

Gras – Top 50 global ◆ **–** Meilleur score dans le secteur ❷ ❸ ❹ ❺ ❻ ❼ – Années consécutives en tant que récipiendaire du tableau d'honneur

Annexe E - Liste de contrôle des meilleures pratiques

Protection du DNS, du domaine, de la marque et du consommateur		
❑	Enregistrements SPF et DKIM valides au niveau du domaine corporatif et des sous-domaines	Score de base
❑	Enregistrements DMARC avec politique de rejet ou de mise en quarantaine	Score de base
❑	Enregistrements DMARC nus (p=none et pas de RUA ou de RUF)	Invalide
❑	TLS opportuniste pour les e-mails	Points de bonus
❑	DNSSEC implémenté	Points de bonus
❑	Adoption de l'IPV6	Points de bonus
❑	Authentification multifacteur	Points de bonus
❑	Domaine verrouillé	Pénalité pour non verrouillage
❑	Authentification des e-mails entrants et vérification DMARC	Non noté ; recommandé
Sécurité de site, de serveur et d'infrastructure		
❑	Sécurité et configuration du serveur	Score de base - plusieurs tests cumulés
❑	Certificat SSL / TLS, protocole, échange de clé, chiffrements	Score de base - plusieurs tests cumulés
❑	Always on SSL (https par défaut)	Score de base
❑	Cadence des correctifs de serveur	Score de base
❑	Autorisation d'autorité de certification (CAA)	Points de bonus
❑	Type de certificat (SSL EV)	Points de bonus
❑	Pare-feu pour applications Web	Points de bonus
❑	Malwares, liens malveillants	Pénalité
❑	Vulnérabilité XSS / iFrame	Pénalité
❑	Mécanismes de signalement des vulnérabilités / bogues	Points de bonus
❑	Protection contre les robots	Non noté ; recommandé
❑	Mécanismes d'atténuation des attaques DDoS	Non noté ; recommandé
Déclaration de confidentialité, traçage, transparence et divulgation		
❑	Lien vers la déclaration de confidentialité sur la page d'accueil	Score de base
❑	Date de la déclaration de confidentialité en haut de la page	Score de base
❑	Conception d'avis courts par couches (liens / élargissement des sections)	Score de base
❑	Loi sur la protection de la vie privée en ligne des enfants (COPPA) ou réglementations connexes.	Score de base
❑	Divulgation de la politique DNT (Ne pas tracer)	Score de base
❑	Déclaration de conservation de données	Score de base
❑	Données personnelles non partagées, sauf à des tiers pour le service	Score de base
❑	Données personnelles non partagées avec les affiliés / partenaires	Score de base
❑	Fournisseurs contractuellement liés à la déclaration de confidentialité	Score de base
❑	Version archivée / antérieure de la déclaration de confidentialité disponible	Score de base
❑	Icônes utilisées pour identifier clairement les sections	Points de bonus
❑	Lien bien visible vers la version multilingue de la déclaration	Points de bonus
❑	Respect du DNT dans les paramètres du navigateur	Points de bonus
❑	Divulgation sur le traçage inter-dispositifs	Points de bonus
❑	Divulgation sur le partage d'informations à des fins légales	Points de bonus
❑	Notifier l'utilisateur si ses données personnelles sont demandées par un tiers	Points de bonus
❑	Existence d'un système de gestion des balises (TMS)	Points de bonus
❑	Présence de traceurs tiers qui partagent des données	Pénalité, nombre de traceurs
❑	Piratage des données signalé	Pénalité, nombre d'incidents, ampleur du piratage
❑	Action coercitive par FTC/FCC/CFPB/Nationale/Internationale	Sanction, nombre de règlements
❑	Votre enregistrement WHOIS est-il privé ?	Pénalité
❑	Conformité aux réglementations dans les juridictions appropriées (par exemple, RGPD)	Recommandé

Annexe F - Ressources pour l'implémentation

Audit de la confiance en ligne 2018 https://otalliance.org/2018HonorRoll

Méthodologie de l'audit 2018 https://otalliance.org/2018-online-trust-audit-methodology

Meilleures pratiques

Always on SSL https://otalliance.org/AOSSL

Autorisation d'autorité de certification (CAA) https://cabforum.org/

DMARC https://otalliance.org/DMARC

DNSSEC https://www.internetsociety.org/deploy360/dnssec/

Outil de test DNSSEC https://dnssec-debugger.verisignlabs.com/

Meilleures pratiques en matière de certificat SSL https://otalliance.org/SSL

Authentification des e-mails https://otalliance.org/Eauth

Avantages pour la marque des certificats SSL à validations étendues https://otalliance.org/EVSSL

Analyse des normes Internet https://internet.nl/

IPv6 https://www.internetsociety.org/deploy360/ipv6/

Malvertising https://otalliance.org/Malvertising

Vérificateur d'enregistrement SPF / DMARC https://otalliance.org/EauthTool

Outil de test de serveur SSL https://ota.ssllabs.com/

Outils de test de serveur SSL / TLS https://www.immuniweb.com/ssl/

Test de sécurité de serveur Web https://www.immuniweb.com/websec/

Analyse de Malware / Sécurité de site Web https://sitecheck.sucuri.net/

Analyse de sécurité de site Web https://observatory.mozilla.org/

TLS (Transport Layer Security) pour e-mails https://otalliance.org/TLS

Formulaire de signalement de vulnérabilité / bogue https://otalliance.org/VulnerabilityReports

Ressources connexes

Guide de préparation à l'intervention en cas d'incident et de violation cybernétiques https://otalliance.org/Incident

Cadre de confiance concernant les objets connectés https://www.internetsociety.org/iot/trust-framework

Ressources Smart Home https://otalliance.org/SmartHome

Pratique de désabonnement du marketing par e-mail https://otalliance.org/unsub

Audit de transparence de la publicité native https://otalliance.org/Native

Livres blancs sur la vision de la confiance https://otalliance.org/vision-trust

Internet Society – Programme Deploy360 https://www.internetsociety.org/deploy360/

Internet Society – Rapport sur l'Internet mondial http://www.internetsociety.org/globalinternetreport/

Remerciements

Les données et les analyses ont été fournies en partie par Agari, Disconnect, Dmarcian, Google, High-Tech Bridge (devenue ImmuniWeb), Infoblox, Internet.nl, Microsoft, Mozilla, Open Bug Bounty, SSL Labs, Sucuri, Symantec, Twitter, Valimail et Verisign.

À propos d'Online Trust Alliance (OTA) de l'Internet Society

Online Trust Alliance (OTA) de l'Internet Society identifie et promeut les meilleures pratiques en matière de sécurité et de confidentialité qui renforcent la confiance des consommateurs dans Internet. Les principales organisations publiques et privées, fournisseurs, chercheurs et décideurs contribuent aux directives de l'OTA et les respectent, pour aider à rendre les transactions en ligne plus sûres et à mieux protéger les données des utilisateurs. L'Internet Society est une organisation mondiale à but non lucratif dédiée à assurer un Internet ouvert, connecté et sécurisé pour tous.

1604-2

Financé en partie par

Notes de fin

[1] Un escroc plaide coupable d'avoir volé 123 millions de dollars à Google et Facebook dans des escroqueries par BEC https://www.scmagazine.com/home/security-news/cybercrime/google-facebook-fraudster-pleads-guilty-to-stealing-123-million-in-bec-scams/

[2] Marriott affirme que moins de clients ont été touchés par un piratage massif des données https://www.usatoday.com/story/travel/news/2019/01/04/marriott-says-fewer-customers-affected-massive-data-hacking/2481601002/

[3] Problèmes de confidentialité de Facebook : un tour d'horizon https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup

[4] Règlement général sur la protection des données (RGPD) de l'UE https://eugdpr.org/

[5] Enquête mondiale CIGI-Ipsos 2018 sur la sécurité et la confiance sur Internet https://www.cigionline.org/internet-survey-2018

[6] Cadre de confiance concernant les objets connectés de l'OTA https://www.internetsociety.org/iot/trust-framework/

[7] Audit et tableau d'honneur de la confiance en ligne https://otalliance.org/HonorRoll

[8] Liste source d'Internet Retailer® https://www.digitalcommerce360.com/product/top-500-database/. Dans certains graphiques et tableaux, par souci de brièveté, les Top 100 et Top 500 des détaillants en ligne sont respectivement abrégés en « IR 100 » et « IR 500 ».

[9] Banques les mieux classées en fonction de leurs actifs, classement de la FDIC (Federal Deposit Insurance Corporation) https://www.fdic.gov/bank/statistical/

[10] Les sites de consommation ou les fournisseurs de contenus les mieux classés en fonction du trafic sur les sites, pour lesquels le fournisseur demande à l'utilisateur de s'abonner ou de créer un compte afin de pouvoir utiliser le service et qui ne sont ne sont pas axés sur les services financiers ou le commerce électronique.

[11] Les organisations membres de l'Internet Society qui étaient membres de l'OTA avant son intégration dans l'Internet Society.

[12] Les données n'incluent pas les résultats du secteur des membres de l'OTA en raison de leur niveau élevé de réalisation et fausseraient l'axe des graphiques.

[13] Le protocole TLS (Transport Layer Security) version 1.3 https://tools.ietf.org/html/rfc8446

[14] Inclut les incidents de perte de données électroniques et physiques

[15] Pourquoi avez-vous besoin d'IPv6 ? https://www.infoblox.com/solutions/ipv6-readiness

[16] Sécurité IPv6 https://www.internetsociety.org/deploy360/ipv6/security/

[17] Directive opérationnelle contraignante DHS 18-01 https://cyber.dhs.gov/bod/18-01/

[18] IETF RFC 4408 https://www.ietf.org/rfc/rfc4408.txt

[19] Gmail TLS pour l'avertissement par e-mail https://arstechnica.com/information-technology/2016/02/gmail-to-warn-you-if-your-friends-arent-using-secure-email/

[20] Rapport DNSSEC de l'ICANN http://stats.research.icann.org/dns/tld_report/

[21] M-08-23, Sécurisation de l'infrastructure DNS du gouvernement fédéral, août 2008 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/m08-23.pdf

[22] Adoption de l'IPv6 http://www.worldipv6launch.org/measurements/

[23] Qu'est-ce que le Credential Stuffing ? https://www.wired.com/story/what-is-credential-stuffing/

[24] Les pirates informatiques font circuler une énorme fuite d'environ 2,2 milliards d'enregistrements https://www.wired.com/story/collection-leak-usernames-passwords-billions/

[25] Test SSL d'ImmuniWeb https://www.immuniweb.com/ssl/

[26] Qualys SSL Labs https://www.ssllabs.com/projects/documentation/

[27] DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) https://drownattack.com/

[28] Test de sécurité de site Web d'ImmuniWeb https://www.immuniweb.com/websec/

[29] Observatory de Mozilla https://observatory.mozilla.org/

[30] Sucuri SiteCheck https://sitecheck.sucuri.net/

[31] Présentation de la CAA https://blog.qualys.com/ssllabs/2017/03/13/caa-mandated-by-cabrowser-forum

[32] Publicité et intégrité des données de l'OTA https://otalliance.org/resources/advertising-integrity-fraud

[33] Qualys SSL Labs SSL Pulse Report https://www.ssllabs.com/ssl-pulse/

[34] Obsolescence précoce de TLS https://www.ssl.com/article/deprecating-early-tls/

[35] Open Bug Bounty https://www.openbugbounty.org/report/

[36] Let's Encrypt https://letsencrypt.org/

[37] Prédiction du conseil de sécurité de CA pour 2019 http://vmblog.com/archive/2019/01/10/ca-security-council-2019-predictions-the-good-the-bad-and-the-ugly.aspx

[38] La moitié de tous les sites de phishing ont maintenant le cadenas https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/

[39] Sécurité IRS des fichiers électroniques et Mandat relatif aux normes de confidentialité ; publication du 1er janvier 2010 https://www.irs.gov/uac/irs-e-file-security-privacy-and-business-standards-mandated-as-of-january-1-2010

[40] Les certificats à validation étendue sont morts https://www.troyhunt.com/extended-validation-certificates-are-dead/

[41] Notez qu'environ 30 % des sites en 2018 sont nouveaux dans l'audit, ce qui rend difficile une comparaison précise d'une année à l'autre.

[42] Attaques DDoS de Kaspersky Labs, T4 2018, https://securelist.com/ddos-attacks-in-q4-2018/89565/

[43] Formulaire de rapport de vulnérabilité d'OTA https://otalliance.org/VulnerabilityReports

[44] Le code malveillant caché dans les images publicitaires coûte 1,13 milliard de dollars aux réseaux publicitaires https://www.zdnet.com/article/malicious-code-hidden-in-advert-images-cost-ad-networks-1-13bn-last-year/

[45] Amazon poursuit en justice les publicités malveillantes https://www.geekwire.com/2018/amazon-files-suit-malvertising-campaign-alleging-sophisticated-widespread-scheme-deceive-consumers/

[46] Règles de l'APEC sur la confidentialité transfrontalière http://www.cbprs.org/

[47] California Consumer Privacy Act https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

[48] COPPA https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

[49] Notez que, bien que la présence de telles solutions ait été vérifiée, il est possible que des sites n'utilisent pas les solutions ou les données.

[50] Apple supprime « Ne pas tracer » de Safari https://gizmodo.com/apple-is-removing-do-not-track-from-safari-1832400768

[51] Tracking Preference Extension (DNT) https://www.w3.org/TR/tracking-dnt/

[52] Rapport 2018 d'OTA sur les tendances en matière d'incidents et d'infractions cybernétiques https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

[53] Communiqué de presse d'appel à commentaires https://otalliance.org/news-events/press-releases/ota-requests-public-comments-2018-online-trust-audit-methodology

[54] Programme Deploy360 de l'Internet Society https://www.internetsociety.org/deploy360/

[55] Communiqué de presse sur la méthodologie du 23 août 2018 https://otalliance.org/news-events/press-releases/internet-society%E2%80%99s-online-trust-alliance-announces-methodology-tenth

[56] Rapport d'enquêtes sur le piratage des données de Verizon, page 11 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[57] Compromission de la messagerie d'entreprise, une escroquerie à 12 milliards de dollars https://www.ic3.gov/media/2018/180712.aspx

[58] Présentation, ressources et outils pour l'authentification des e-mails d'OTA https://otalliance.org/eauth

[59] Présentation de la DMARC et des ressources d'OTAhttps://otalliance.org/DMARC

[60] Meilleures pratiques de sécurité et de déploiement SSL / TLS https://otalliance.org/resources/ssl-best-practices

[61] Les bases du DNSSEC https://www.internetsociety.org/deploy360/dnssec/basics/

[62] IPv6 https://www.internetsociety.org/deploy360/ipv6/

[63] Qualys SSL Labshttps://ota.ssllabs.com/

[64] ImmuniWeb https://www.immuniweb.com/ssl/

[65] AOSSL https://otalliance.org/AOSSL

[66] SSL EV https://otalliance.org/resources/extended-validation-certificates-evssl

[67] Directives et pratiques en matière de rapports de vulnérabilité de la NTIA https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[68] Formulaire de signalement de vulnérabilité d'OTA https://otalliance.org/VulnerabilityReports

[69] FIPPS https://cryptome.org/2014/11/nstic-fipps.pdf

[70] COPPA https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy

[71] Données des traceurs tiers - La source primaire inclut les données de https://disconnect.me/trackerprotection/blocked résultant en https://disconnect.me/trackerprotection/unblocked

[72] Recommandations en matière de traçage de dispositifs de la FTC https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

[73] CFPB https://www.consumerfinance.gov/