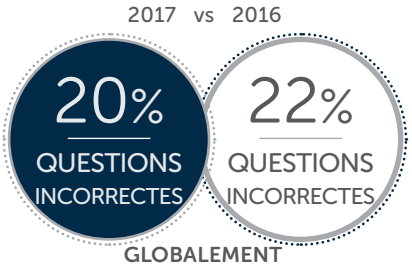
Wombat Security's 2017

BEYOND THE PHISH™

Rapport

wombat® security technologies

#BeyondthePhish



Beyond the Phish

Les professionnels de la sécurité des informations du monde entier le savent très bien : les cybercriminels exploitent les attaques basées sur les e-mails dans leur propre intérêt. En tant que pionnier dans le développement et l'utilisation d'attaques simulées, nous savons que l'apprentissage des techniques anti-hameçonnage est plus important que jamais. Avec le spear phishing, les e-mails commerciaux frauduleux (BEC, pour « business email compromise ») et les ransomware utilisant les e-mails, les équipes en charge de leur prévention et de leur correction sont sur le pied d'alerte. Mais ce ne sont pas les seuls moyens par lesquels les attaquants peuvent pénétrer dans une organisation et compromettre des données sensibles et des systèmes.

Notre deuxième rapport *Beyond the Phish*™ annuel comprend des résultats pour **plus de 70 millions de questions** auxquelles ont répondu les utilisateurs finaux de nos clients sur dix catégories tirées de notre évaluation des connaissances CyberStrength® et de nos modules de formation interactifs. Nous y mettons en avant les forces et les faiblesses directement liées à l'hameçonnage, mais nous allons également **au-delà** pour analyser les meilleures pratiques commerciales, y compris les mesures de protection des données, le partage sécurisé sur les réseaux sociaux, la sécurité des appareils mobiles et la sécurisation des mots de passe.

Bien que nous ayons remarqué une légère amélioration en termes de réponses incorrectes par rapport à 2016 — **20% vs. 22%** — les gains de certains domaines ont été mitigés par les pertes dans d'autres. Le rapport de cette année offre une comparaison **d'une année à l'autre** au niveau des catégories, mais aussi une analyse des **faiblesses par industrie** et des réflexions sur certaines des questions spécifiques que les utilisateurs avaient plus de chances de répondre incorrectement. Nous avons également ajouté des données dans une nouvelle catégorie – Vous protéger contre la fraude – qui se focalise sur la compréhension des utilisateurs finaux des techniques d'ingénierie sociale courante utilisées pour une grande variété de vecteurs d'attaque.

Les points forts de notre *Rapport sur les risques liés aux utilisateurs de 2017*, ont également fait leur apparition cette année. Il rassemble les résultats d'une **enquête internationale tierce auprès de 2 000 adultes actifs – 1 000 aux États-Unis et 1 000 au Royaume-Uni** — et révèle les comportements courants en termes de cybersécurité dans des domaines similaires à ceux évalués dans nos données *Beyond the Phish*.

Bien qu'il ne s'agisse pas d'une étude scientifique, ce rapport permet aux organisations de comparer la compréhension en termes de cybersécurité de leurs utilisateurs finaux par rapport à ces deux populations professionnelles et d'évaluer leurs niveaux de connaissance par rapport à la moyenne de l'industrie. En examinant les chiffres présentés ici, il est important de prendre en considération votre niveau de proactivité sur le front des formations et de la sensibilisation et les implications liées au fait d'assumer que vos employés possèdent les compétences nécessaires pour protéger les données personnelles et corporatives, les appareils et les systèmes.

TIP !

Consultez notre **Rapport sur les risques liés aux utilisateurs** pour connaitre les résultats d'une enquête de sensibilisation internationale sur la cybersécurité.

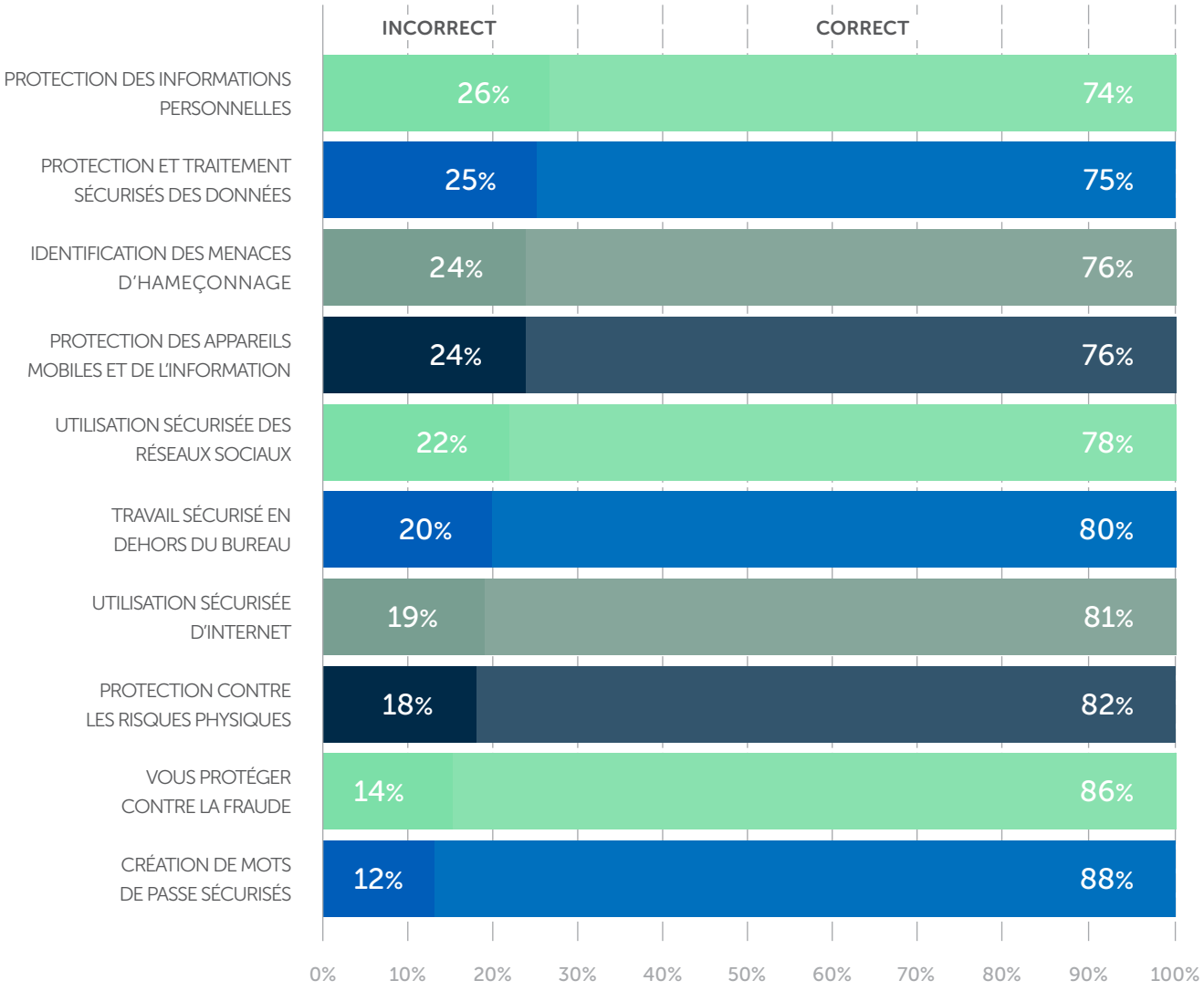
info.wombatsecurity.com/user-risk-report

Quel est la position des utilisateurs finaux ?

+ de 70 millions
DE QUESTIONS POSÉES
ET RÉPONDUES

Nous avons examiné les réponses à plus de **70 millions** de questions dans **10 catégories** entre **juin 2016 et mai 2017**. L'amélioration de **22%** à **20%** de réponses incorrectes est une nouvelle positive et les utilisateurs se sont bien débrouillés dans l'ensemble en répondant correctement à plus de 75 % des questions sur la plupart des catégories. Cependant, étant donnée la nature critique de ces sujets, il est clair qu'il existe encore une marge de progression.

POURCENTAGE MOYEN DES RÉPONSES CORRECTES ET INCORRECTES

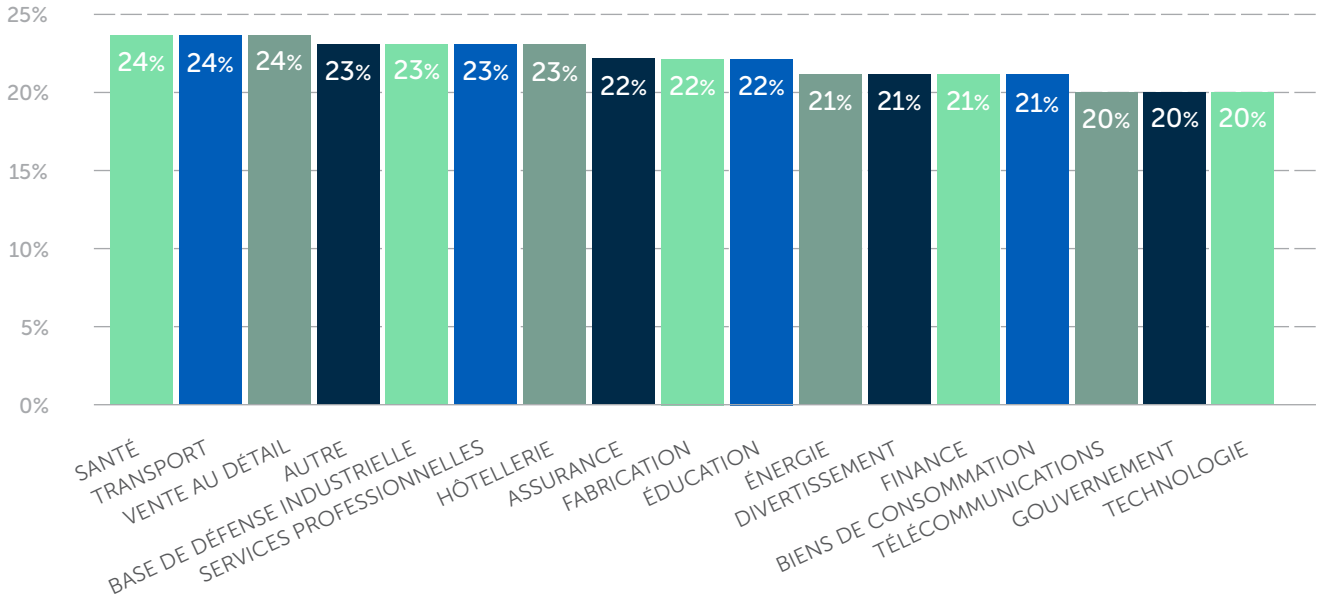


Un plus grand focus sur les données de l'industrie

Dans notre **rapport de 2016**, nous avions inclus un nombre important de données de l'industrie, mais nous voulions étudier ces chiffres plus en profondeur cette année. Comme nous l'avons indiqué dans notre introduction, nous avons remarqué une réduction générale (bien que modeste) du pourcentage de réponses incorrectes d'une année à l'autre. Alors que nous plongeons plus en détails dans chacune de nos catégories de cybersécurité et que nous examinons les améliorations mais aussi les progressions négatives, vous serez certainement intéressé, comme nous l'avons été, par le fait que certaines industries ont du mal à gérer des sujets donnés et vous découvrirez quelles sont les implications pour les activités quotidiennes (pour ne rien dire de la sécurité nationale).

Vous trouverez ci-dessous la répartition par industrie des lacunes de connaissance moyennes sur toutes les catégories. Bien que les produits et les services varient énormément entre ces secteurs, il est intéressant de remarquer que le niveau de connaissance des utilisateurs finaux en termes de cybersécurité est dans l'ensemble similaire. Au cours de notre progression dans ce rapport, nous présenterons des chiffres plus granulaires qui montreront quelles industries ont le plus de difficultés avec chaque sujet.

POURCENTAGE MOYEN DES RÉPONSES INCORRECTES SUR TOUTES LES CATÉGORIES



Protection des informations confidentielles

2017 vs 2016

Tout comme l'année dernière, cette catégorie – qui se concentre sur les meilleures pratiques de cybersécurité des utilisateurs finaux en termes de conformité PCI DSS et HIPAA — a été celle qui a posé le plus de problèmes aux employés.

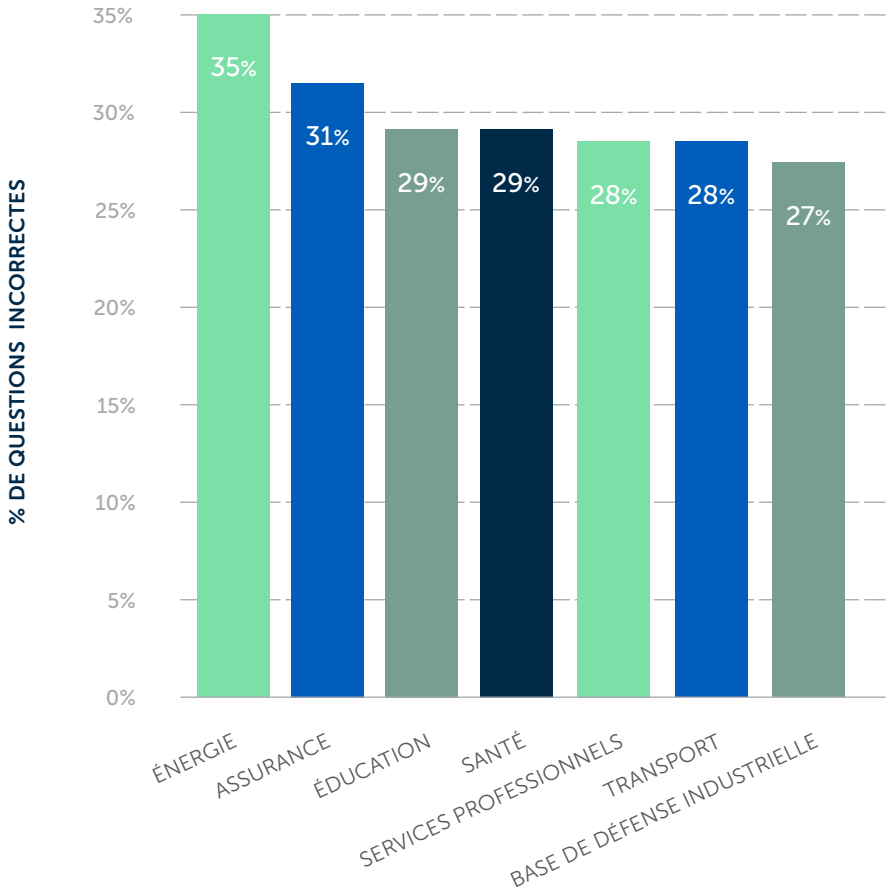
Les légères améliorations d'une année à une autre dans les industries comme la santé (le secteur ayant les moins bonnes performances en 2016), divertissement et fabrication ont été contrebalancées par un mouvement inverse chez les utilisateurs finaux des secteurs de l'énergie, de l'assurance et de l'éducation. À vrai dire, les moins bonnes performances cette année furent obtenues par les industries qui avaient également des difficultés en **2016**.

FAIT !

L'une des questions qui a pose le plus de problems concernait l'utilisation d'idientifiants de connexion partagés.

Pour minimiser cette pratique, les employés doivent être au courant des implications personnelles liées à l'éccès de leurs collègues à des systems de santé et commerciaux sensibles à l'aide de leurs identifiants de connexion.

INDUSTRIES AVEC LE PLUS DE DIFFICULTÉS



2017 vs 2016

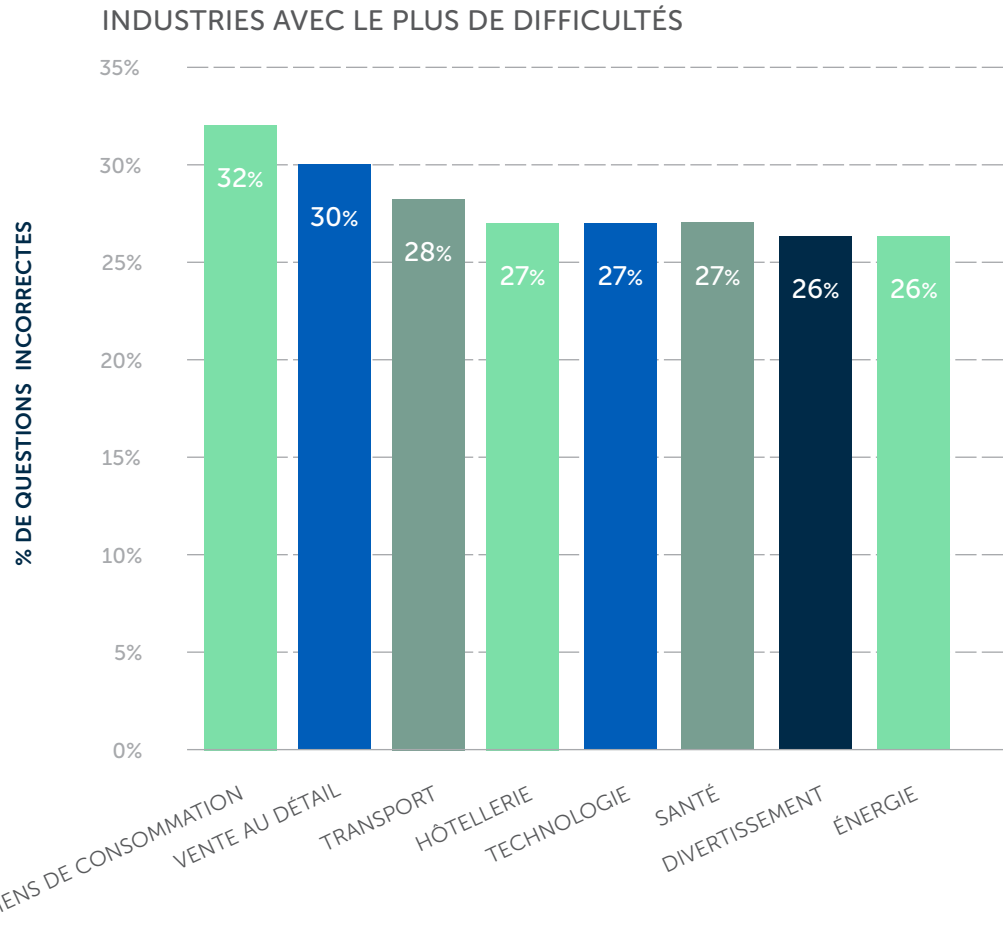
25% QUESTIONS INCORRECTES

30% QUESTIONS INCORRECTES

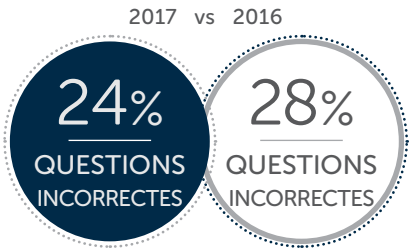
Protection et traitement sécurisés des données

Cette catégorie inclut une évaluation et des questions de formation se focalisant sur le cycle de vie des données, de leur création à leur destruction, mais aussi sur les techniques de traitement des données personnelles en général. Les sujets abordaient entre autre la destruction des documents électroniques et physiques, l'utilisation d'appareils USB et la classification des données sensibles.

Nous avons pu voir une amélioration générale dans cette catégorie cette année. Deux industries, la télécommunication et la fabrication, ont même connu une évolution à double chiffres entre **2016** et **2017**. Cependant, les utilisateurs finaux de toutes les industries ont répondu incorrectement à un quart des questions de cette catégorie. Et les données de l'industrie restent décevantes dans l'ensemble. Bien que le classement ait connu des changements, les industries ayant rencontré le plus de difficultés en **2017** étaient classées parmi les pires de **2016**.



Identification des menaces d'hameçonnage



Cette catégorie, qui se penche sur les différents indicateurs et ramifications des attaques, fournit les résultats les plus réguliers cette année. Le taux de réponses incorrectes varie de 21 % à 27 %, toutes les industries obtenant de meilleurs chiffres que la moyenne de 28 % l'année dernière.

Bien qu'il soit logique que les organisations se concentrent sur les attaques simulées pour évaluer la propension de leurs utilisateurs finaux aux hameçonnages, l'évaluation des connaissances basée sur des questions offre un indicateur plus précis de la compréhension des employés en ce qui concerne les menaces d'hameçonnage. Évidemment, nous encourageons nos clients à effectuer des tests d'hameçonnage ; à vrai dire, les recherches innovantes de nos fondateurs ont entrainé l'utilisation de ce type d'évaluations. Mais même à cette époque, nous reconnaissions que les exercices de clic/pas de clic n'étaient qu'un composant d'un programme de sensibilisation à la sécurité efficace.

Lorsque nous regardons ces deux types d'évaluation côte à côte – attaques simulées par rapport à des évaluations à base de questions – les résultats montrent l'intérêt d'avoir une vue plus complète :

SANTÉ

18%
TAUX DE CLIC
SUR LES ATTAQUES*
D'HAMEÇONNAGE SIMULÉES

VS

26%
DE QUESTIONS INCORRECTES
DANS L'ÉVALUATION DES
CONNAISSANCES

GOUVERNEMENT

14%
TAUX DE CLIC
SUR LES ATTAQUES*
D'HAMEÇONNAGE SIMULÉES

VS

24%
DE QUESTIONS INCORRECTES
DANS L'ÉVALUATION
DES CONNAISSANCES

*Les données du taux de clic sont tirées de notre rapport *State of the Phish de 2017.*

FAIT !

Ce sujet est le plus populaire auprès de nos clients. Plus de la moitié des questions **d'évaluation et de formation** posées aux utilisateurs finaux pendant la période étudiée était liée aux menaces d'hameçonnage et un plus grand accent était porté sur ce sujet comparé à l'année dernière.

TIP !

Consultez notre rapport **State of the Phish™ Report** pour obtenir plus de données sur les attaques d'hameçonnage.

info.wombatsecurity.com/state-of-the-phish

2017 vs 2016

24% QUESTIONS INCORRECTES

15% QUESTIONS INCORRECTES

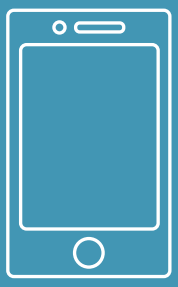
Protection des appareils mobiles et de l'information

Cette catégorie a vu la plus importante dégradation des performances d'une année à l'autre, avec seulement une industrie (télécommunications avec **14 %** de réponses incorrectes) dépassant la moyenne définie en **2016**. Comme vous le verrez ci-dessous, l'augmentation du nombre de questions répondues incorrectement par les utilisateurs a augmenté de manière significative, deux industries montrant une **hausse** équivalant au **double des chiffres** moyens de **2016**.

SELON PEW RESEARCH, EN JANVIER 2017

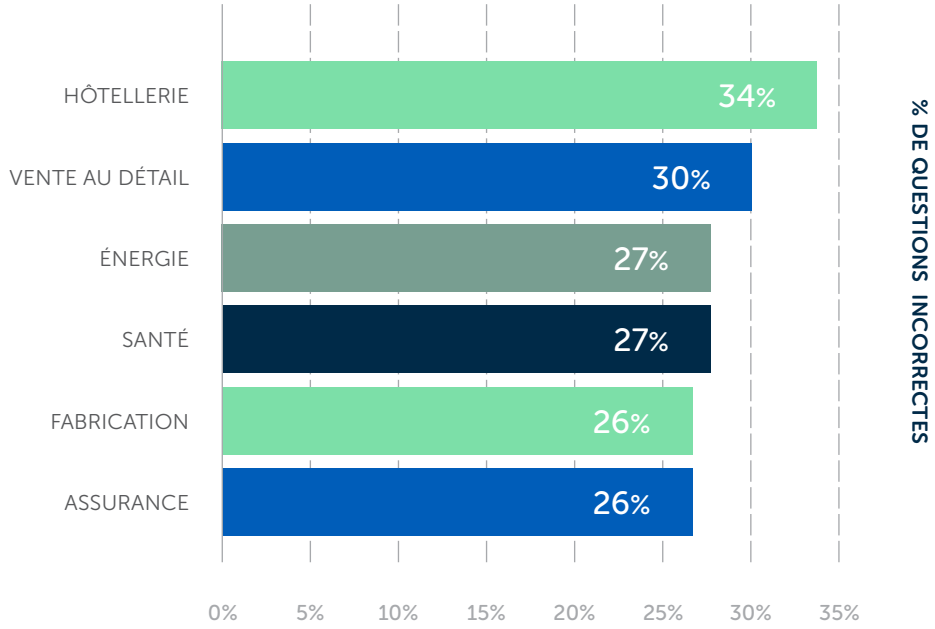
92% DES AMÉRICAINS ÂGÉS DE 18 À 29 ANS POSSÈDENT UN SMARTPHONE

88% DES AMÉRICAINS ÂGÉS DE 30 À 49 ANS POSSÈDENT UN SMARTPHONE



Nos données démontrent que les utilisateurs ont du mal à comprendre les implications et les ramifications des applications mobiles non sécurisées et des autorisations invasives.

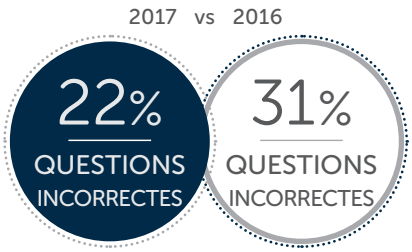
INDUSTRIES AVEC LE PLUS DE DIFFICULTÉS



Bien que nous ayons constaté une légère hausse des clients ayant tendance à s'évaluer et se former sur ce sujet en 2017, leur réticence antérieure à aborder la sécurité des appareils mobiles semblent avoir placé les utilisateurs en difficulté à propos de leur connaissance. Dans l'enquête effectuée pour notre **rapport de 2016**, seulement 52 % des organisations déclaraient évaluer les connaissances de leurs utilisateurs finaux sur ce sujet.

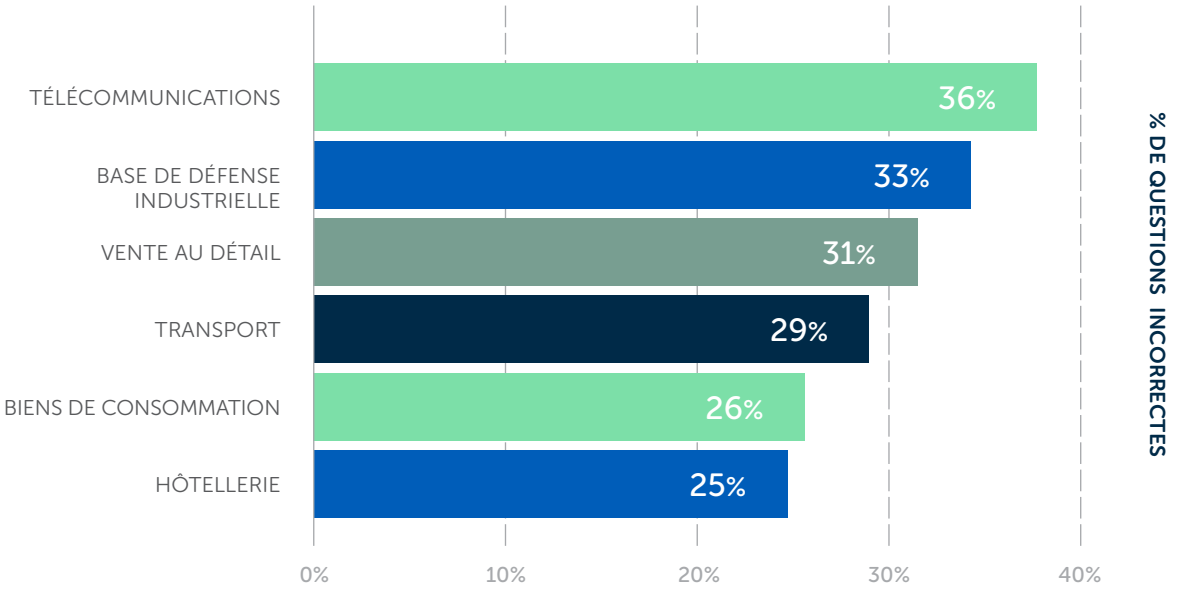
Comme le montrent les chiffres de Pew Research, nous approchons rapidement un taux **d'adoption des smartphones de 100 %** chez les **adultes de 18 à 49 ans**. Ces appareils deviennent de plus en plus compliqués et interconnectés et, comme vous le découvrirez dans la page suivante de notre rapport, la démarcation entre informatique personnel et corporatif est floue pour de nombreux utilisateurs. Un manque de conscience continu et de connaissances chez les utilisateurs mobiles impactera la sécurité des données commerciales et des systèmes de manière négative.

Utilisation sécurisée des réseaux sociaux



C'est dans cette catégorie que s'est produite la meilleure amélioration d'une année à l'autre – une tendance positive compte tenu de la hausse continue de l'utilisation des réseaux sociaux dans le monde entier. Au cours de l'année, plusieurs initiatives publiques de premier plan pour améliorer la sécurité et réduire les comptes d'imposteurs ont probablement aidé à contribuer aux efforts continus de nos clients pour informer les utilisateurs finaux et leur faire comprendre les meilleures pratiques. Et même parmi les industries ayant rencontré des difficultés sur ce sujet, seules deux ont obtenu de moins bonnes performances que les moyennes de l'année passée.

INDUSTRIES AVEC LE PLUS DE DIFFICULTÉS



Ceci est un point de vue peu clairvoyant quand on voit que notre **rapport de 2016** a révélé que **75 %** des organisations autorisent l'accès aux sites et aux applications de réseaux sociaux sur les appareils professionnels. Et même celles qui verrouillent l'accès au sein des systèmes corporatifs sont vulnérables en dehors des heures de bureau. Il est important de reconnaitre (et d'essayer de mitiger) les risques associés avec les mauvaises habitudes sur les réseaux sociaux, ce qui peut être fait en sensibilisant et en éduquant les utilisateurs finaux.

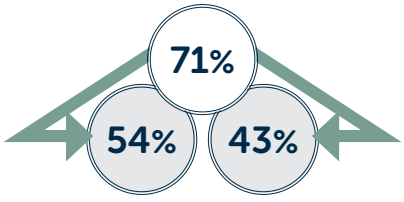
Gardez ces risques liés aux utilisateurs finaux à l'esprit

Notre *Rapport sur les risques liés aux utilisateurs de 2017* a révélé les points d'inquiétude suivants en ce qui concerne les meilleures pratiques des réseaux sociaux chez les participants américains à l'enquête :

71% utilisent régulièrement les appareils professionnels en dehors du bureau

54% consulte ou postent sur les réseaux sociaux à l'aide de ces appareils

43% permettent à leurs amis ou à leur famille de voir ou de poster sur les réseaux sociaux à l'aide de ces appareils



2017 vs 2016

Travail sécurisé en dehors du bureau

Nous avons remarqué une amélioration significative d'une année à l'autre dans cette catégorie – ce qui est bon signe compte tenu du fait que de plus en plus d'employés travaillent en dehors du bureau, que ce soit par le télétravail, en voyage ou autre. Comme vous pourrez le voir dans le classement des meilleures aux pires performances, toutes les industries ont obtenu de meilleurs résultats que le pourcentage moyen atteint en 2016, bien qu'il existe une grosse marge entre les meilleures et les moins bonnes notes.

SELON GALLUP

43%

DES EMPLOYÉS TRAVAILLENT À DISTANCE AU MOINS UNE PARTIE DU TEMPS

FAIT !

SOURCE: *STATE OF THE AMERICAN WORKPLACE REPORT*

PIRES PERFORMANCES

- **25%** SERVICES PROFESSIONNELS
- **25%** TÉLÉCOMMUNICATIONS

MEILLEURES PERFORMANCES

- **14%** HÔTELLERIE
- **15%** ASSURANCE

Ces organisations qui n'évaluent pas et ne forment pas les utilisateurs finaux sur les meilleures pratiques à employer en dehors du confin des lieux et des réseaux professionnels devraient repenser leur approche.

Notre *Rapport sur les risques liés aux utilisateurs de 2017* a révélé que l'employé moyen n'est pas bien au courant de l'utilisation des moyens de protection les plus simples :

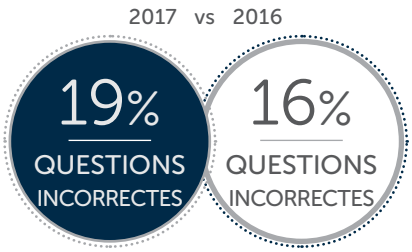
54%
des travailleurs américains pensent qu'ils peuvent faire confiance au réseaux Wifi ouverts dans les lieux de confiance.

Près de **40%**
des travailleurs anglais ayant installé un VPN déclare qu'ils l'utilisent rarement ou jamais.
.

14%
des travailleurs anglais ne disposent d'aucun mécanisme de verrouillage sur leur appareil mobile.

Plus de **50%**
des travailleurs anglais et américains seraient prêts à laisser un ordinateur corporatif dans leur voiture plutôt que de le prendre avec eux au restaurant.

Utilisation sécurisée d'internet



Cette catégorie a malheureusement connu de nombreux reculs comparée à **2016**. À vrai dire, une seule industrie – la base de défense industrielle, dont les utilisateurs ont mal répondu à **14 %** des questions – a obtenu de meilleures résultats que l'année dernière.

PIRES PERFORMANCES

- 23% TÉLÉCOMMUNICATIONS
- 22% BIENS DE CONSOMMATION
- 22% DIVERISSEMENT
- 21% ÉDUCATION

MEILLEURES PERFORMANCES

- 18% TECHNOLOGIE
- 17% GOUVERNEMENT
- 14% BASE DE DÉFENSE INDUSTRIELLE

Il est difficile d'expliquer cette chute dans ce domaine, surtout que l'étude de l'année dernière a démontré que ceci est inclus dans la grande majorité des programmes de formation sur la cybersécurité. Il est possible que les organisations aient fait un pas en arrière suite aux **chiffres positifs de 2016**, s'éloignant de la sécurité sur internet pour se concentrer sur des sujets tels que la prévention de l'hameçonnage et des ransomware.

Peu importe la raison, il est clair que les organisations ne peuvent pas se baser sur des suppositions sur les niveaux de risque d'une année à la suivante. Les sujets clés – comme les meilleures pratiques pour naviguer sur le web et examiner les URL inconnues et potentiellement dangereuses – doivent être couverts régulièrement afin de développer une culture de sécurité au sein de l'organisation.

QUESTIONS LES MOINS BIEN RÉPONDUES

Voici certains les sujets avec lesquels les utilisateurs ont eu le plus de difficultés :

- Les risques associés aux URL courtes
- Identification des sites sécurisés par rapport aux sites risqués
- Les implications de l'utilisation des identifiants de connexion aux réseaux sociaux en dehors des réseaux sociaux

2017 vs 2016

18% QUESTIONS INCORRECTES

15% QUESTIONS INCORRECTES

Protection contre les risques physiques

En **2016**, il s'agissait d'un des sujets les mieux compris par les utilisateurs finaux, bien que nous ayons constaté une légère baisse cette année. Nos données montrent une raison possible : les organisations mettent moins l'accent sur ce sujet cette année par rapport à l'année dernière.

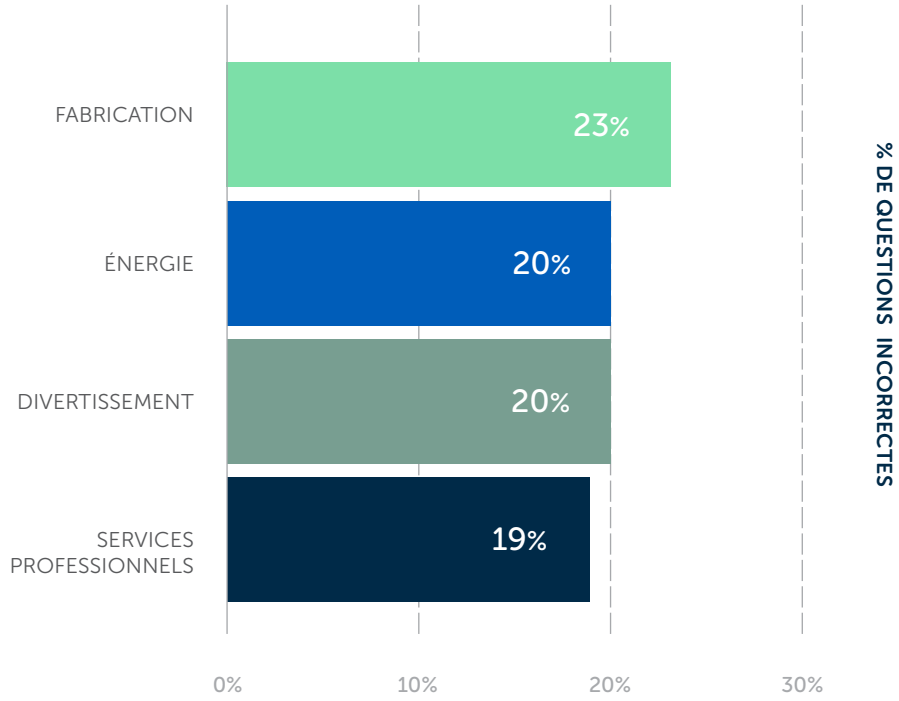
Parmi les secteurs ayant rencontré le plus de problèmes (notés ci-dessous) ; nous avons de nouveau vu des représentants d'industries clés. Ceci est particulièrement inquiétant car une violation physique de ces types d'organisation pourrait avoir d'énormes répercutions qui affecteraient la sécurité publique et même la sécurité nationale.

TIP !

Nos données indiquent que les utilisateurs finaux ont souvent du mal à voir l'important de protéger physiquement certains objets comme les badges d'identification, les annuaires téléphoniques imprimés et les fichiers donnant des détails sur des prestataires de services (comme les techniciens HVAC et les cabinets juridiques).

Il faudrait rappeler aux employés que la sécurité physique et la cybersécurité sont liées. Les individus, les biens et les zones doivent aussi bien être protégées hors ligne qu'en ligne.

INDUSTRIES AVEC LE PLUS DE DIFFICULTÉS



L'essence de la sécurité physique se trouve dans la vigilance continue. Bien qu'il puisse être tentant de considéré ce type de protection comme faisant partie du « bon sens », les organisations ne devraient pas rejeter l'idée de la sensibilisation et de la formation de leurs employés sur l'importance des meilleures pratiques liées à la sécurité physique. Un bureau propre et bien rangé et des actions relativement simples, comme fermer les portes à clé et vérifier les identifiants, offrent des possibilités à faible cout d'améliorer la posture sécuritaire dans son ensemble.

Vous protéger contre la fraude

2017

14%
QUESTIONS INCORRECTES

Nous avons inclus cette catégorie dans nos **données de 2017** afin de mieux examiner la compréhension des utilisateurs finaux sur le principe fondamental de l'ingénierie sociale. Bien qu'elles soient souvent associées aux e-mails d'hameçonnage, les cybercriminels et les escrocs utilisent des techniques d'ingénierie sociale sur un large éventail de vecteurs d'attaque, y compris les appels d'hameçonnage vocal (vishing), les SMS d'hameçonnage (smishing), les faux-semblants sur les réseaux sociaux et les rencontres en personne.

Il est encourageant de voir que les utilisateurs finaux ont obtenu de bons résultats en moyenne (seule la catégorie Création de mots de passe sécurisés a généré de meilleurs scores). Seules deux industries se retrouvent en-dessous de la moyenne et trois industries ont surpassé les autres, et de loin :

FAIT !

L'extraction de données pour des attaques en lieu a souvent lieu dans des espaces en dehors du cyberspace.

PIRES PERFORMANCES

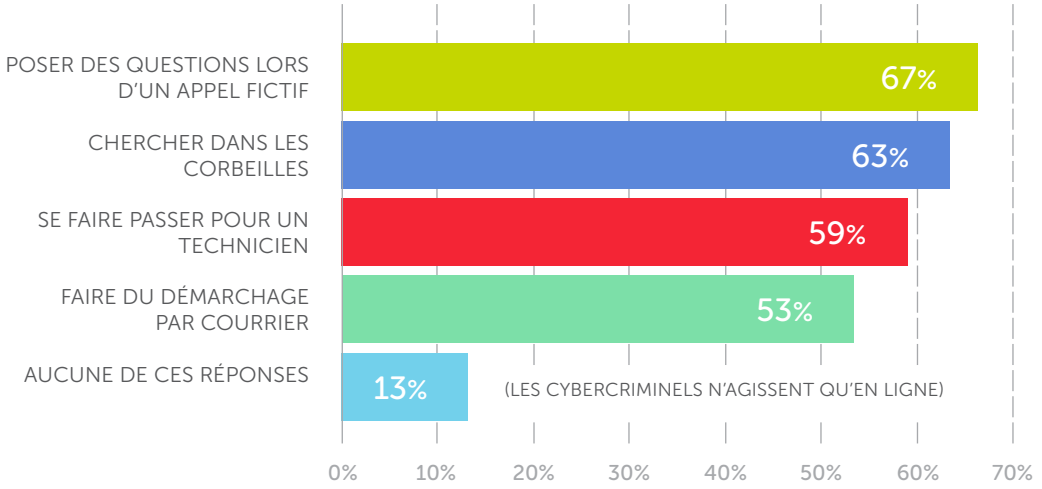
- 22% TRANSPORT
- 19% VENTE AU DÉTAIL

MEILLEURES PERFORMANCES

- 10% ÉDUCATION
- 11% TÉLÉCOMMUNICATIONS
- 11% BASE DE DÉFENSE INDUSTRIELLE

Nous recommandons cependant aux organisations de ne pas se reposer sur leurs lauriers en ce qui concerne la sensibilisation aux menaces d'ingénierie sociale. De nombreux utilisateurs finaux ne considèrent pas que le cybercrime dépasse les activités en ligne, comme l'indique les réponses de l'enquête de notre *Rapport sur les risques liés aux utilisateurs de 2017* (voir ci-dessous). Il est important de former les employés sur les différentes techniques utilisées par les ingénieurs sociaux pour recueillir des informations et gagner un accès.

COMMENT LES CYBERCRIMINELS OBTIENNENT-ILS LES INFORMATIONS ? (PLUSIEURS RÉPONSES AUTORISÉES)



2017 vs 2016

Création de mots de passe sécurisés

Tout comme l'année dernière, les utilisateurs finaux ont obtenu les meilleurs scores en répondant aux questions concernant la sécurité des mots de passe. Les mots de passe étant des moyens de protection utilisés depuis longtemps et les organisations ayant établi des politiques à ce sujet, il est raisonnable de penser les employés sont conscients du besoin d'appliquer ces protections aux comptes et systèmes sensibles.

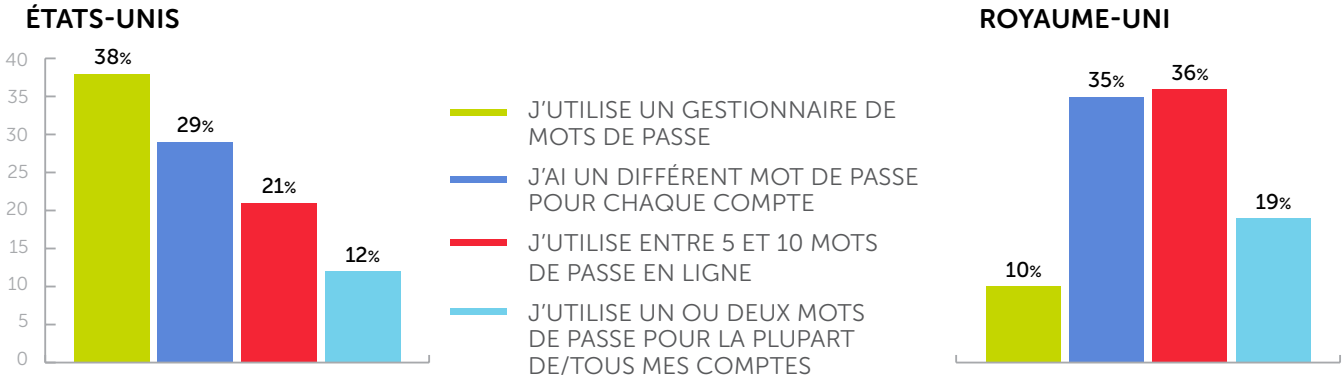
Il reste cependant du travail à faire. Comme indiqué ci-dessous, les utilisateurs finaux de plusieurs industries ont du mal avec les meilleures pratiques liées à la création et à l'application de mots de passe, certains secteurs connaissant des performances bien moins bonnes que la moyenne :

PIRES PERFORMANCES

- **22%** TRANSPORT
- **20%** BASE DE DÉFENSE INDUSTRIELLE
- **18%** HÔTELLERIE
- **17%** VENTE AU DÉTAIL
- **16%** SERVICES PROFESSIONNELS
- **15%** TÉLÉCOMMUNICATIONS

À nouveau, notre *Rapport sur les risques liés aux utilisateurs de 2017* met les organisations en garde afin qu'elles ne fassent pas de suppositions sur les connaissances des utilisateurs finaux quant à la création de mots de passe uniques et sécurisés. Notre enquête a entre autre révélé que les employés réutilisent les mots de passe sur différents sites et systèmes, ce qui est un risque croissant compte tenu du fait que les cybercriminels ont à leur disposition des listes d'identifiants compromis Il est crucial de former vos employés pour qu'ils gèrent efficacement leurs identifiants et leur fournir les outils dont ils ont besoin pour améliorer la sécurité de leurs comptes personnels et professionnels.

COMMENT GÉREZ-VOUS LES MOTS DE PASSE DE VOS COMPTE EN LIGNE ?



La continuité est la clé du succès

Comme l'ont prouvé les cybercriminels ces dernières années, le paysage des menaces est à la fois capables de rester consistent ou de changer. Les attaques d'hameçonnage sont sur notre radar collectif depuis des années, mais certaines des premières ruses – telles que le prince nigérien et sa joyeuse bande d'imitateurs – ont atteint leur objectif. En parallèle, les méthodes se sont transformées : les protections techniques progressant avec le temps, les niveaux de sophistication des attaqueurs ont également dû évoluer. Et la lutte contre l'hameçonnage n'est qu'un des éléments de la gestion du risque couru par les utilisateurs finaux. Avec la prolifération des communications électroniques, des réseaux sociaux et des appareils et des systèmes connectés - pour ne rien dire de l'immense quantité de données produites, qu'IBM a récemment estimé à environ **2,5 quintillions d'octets par jour** – les vies personnelles et professionnelles de l'employé moyen sont très différentes de ce qu'elles étaient il y a quelques années.

Chaque jour, il faut prendre en considération de nombreux aspects du point de vue de la cybersécurité. Et les choses évoluent tous les ans. L'illustration ci-dessous, qui met en avant les données du graphisme d'information de 2017 *Data Never Sleeps* 5.0 (Les données ne dorment jamais 5.0) de Domo, indique clairement pourquoi les utilisateurs comme les organisations doivent rester sur le pied d'alerte pour gérer et protéger les données et les appareils.

Comme l'atteste les comparaisons d'une année à l'autre que nous avons présentées dans ce rapport, **les organisations ne peuvent pas compter sur la sensibilisation et les connaissances pour conserver les mêmes niveaux.** Et même avec des programmes réussis de formation et de sensibilisation à la sécurité – ceux qui s'axe sur le développement d'une culture de sécurité, dans laquelle les employées sont valorisés et responsabilisés pour faire partie de la solution plutôt qu'être relégués au rang de problème constant et immuable – il existe des hauts et des bas. Mais les organisations qui ne mettent pas l'accent sur le rôle des utilisateurs finaux au sein d'une politique de cybersécurité et qui ne l'abordent qu'occasionnellement (ou pire encore, qui abandonnent l'idée dans son ensemble) sont destinées à prendre encore plus de retard par rapport aux autres.

DONNÉES DE 2017 À LA MINUTE

Source: Domo.com

103.4M
Pourriels envoyés

3.6M
Recherches Google

Partage social

4.1M
Vidéos vues sur YouTube

528K
Photos partagées sur Snapchat

456K
Tweets sur Twitter

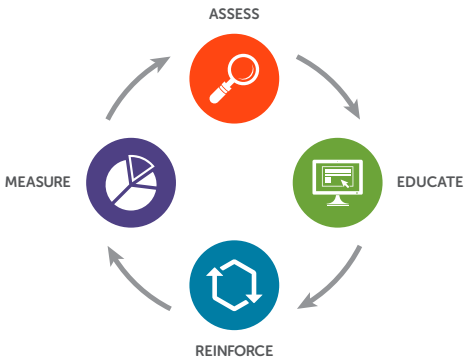
47K
Photos postées sur Instagram

2017	vs	2016
Ventes Amazon		
259 000 $		222 000 $
Demandes de prévision reçues par The Weather Channel		
694 000		569 000
SMS envoyés		
15.2 M		3.6 M

A propos de Wombat Security

Wombat Security Technologies, basées à Pittsburgh, PA, aide à la sensibilisation sur la sécurité et fournit un logiciel de formation pour aider les organisations à enseigner à leurs salariés des comportements sécurisés. Notre Plate-forme d'Enseignement de la Sécurité inclut des évaluations de connaissance intégrées, des attaques simulées et les bibliothèques de modules de formation interactifs et des outils de renforcement.

Wombat est né de recherches menées à l'université de Carnegie Mellon, qui est mondialement reconnue, et ses cofondateurs sont des membres du corps professoral à l'École de la Science Informatique CMU. En 2008 ils ont mené le plus grand projet de recherche national sur comment combattre les attaques d'hameçonnage, avec pour but d'adresser l'élément humain de cyber sécurité et développer des solutions d'anti-hameçonnages nouvelles et plus efficaces. Ces techniques et recherches ont fourni la base pour la Plate-forme d'Enseignement de Sécurité de Wombat et sa Méthodologie de Formation Continue unique. La méthodologie, comprise d'un cycle continu d'évaluation, d'enseignement, de renforcement et de mesure, a permis une réduction de 90 % des attaques d'hameçonnage et de logiciels malveillants.



wombat security technologies

Change Behavior. Reduce Risk.

#BeyondthePhish

Traduit par BSI Group France - www.bsigroup.fr

wombatsecurity.com
info@wombatsecurity.com | 412.621.1484
UK +44 (20) 3807 3472