Lookout®

RAPPORT

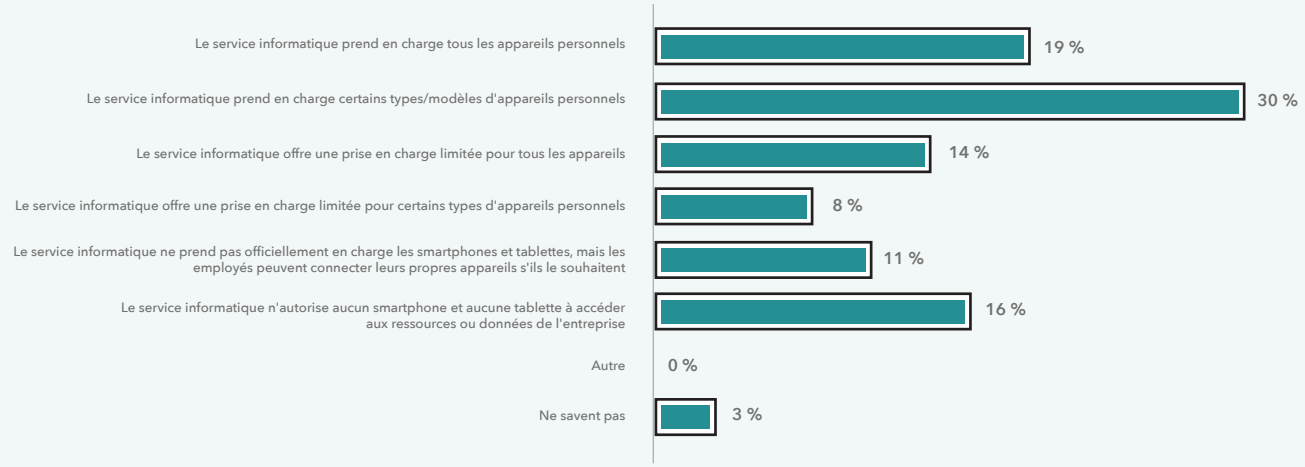
Entreprises européennes :

vous avez un programme BYOD, que vous le vouliez ou non

« Nous n'avons pas de programme BYOD. »

Voilà ce que disent de nombreuses entreprises européennes à propos de l'utilisation des appareils mobiles au travail lorsqu'on leur demande de protéger les données hautement confidentielles et les informations à caractère personnel, et de gérer les autorisations et les accès des employés à ces données. Les entreprises pensent souvent à tort qu'elles sont à l'abri des cybermenaces sur les appareils mobiles simplement parce qu'elles n'autorisent pas les appareils mobiles personnels à accéder à leurs réseaux. Mais, ne leur déplaise, elles ont toutes une politique BYOD et cette attitude met en péril la sécurité des données.

Politique informatique officielle de prise en charge des smartphones et tablettes personnels des employés

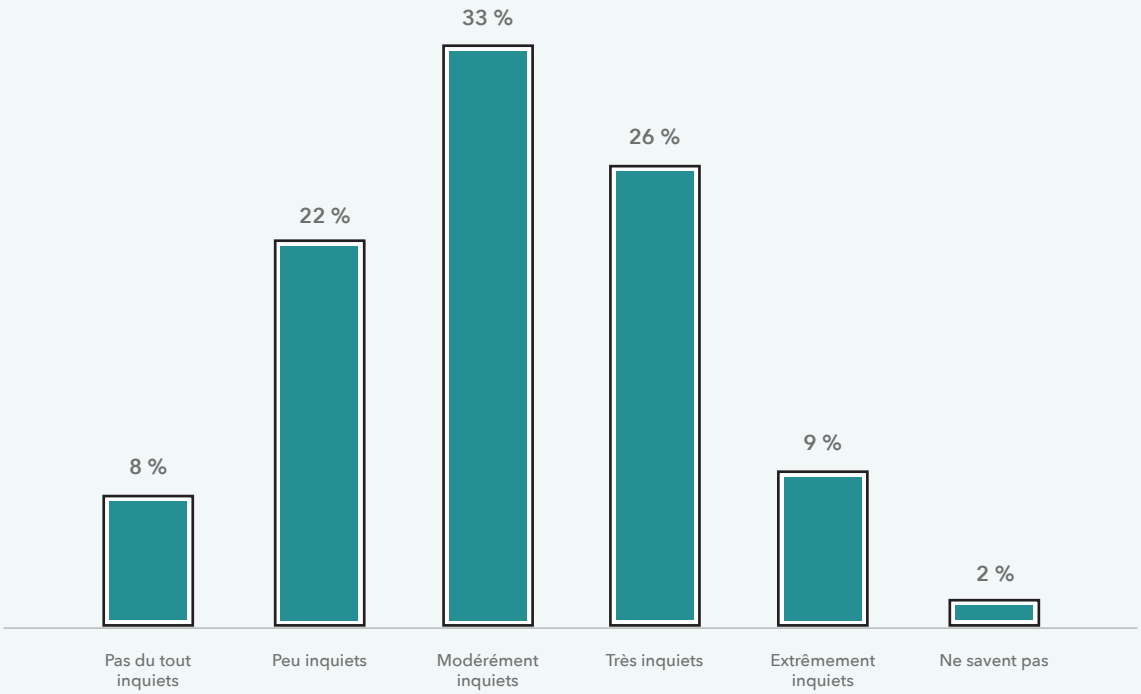


Base : N=37 décideurs en matière de sécurité des clients (Amériques ; gouvernement, éducation ou santé)
Source : Forrester's Global Business Technographics Security Survey, 2016

Lookout a analysé les comportements des employés du gouvernement américain, une institution pour laquelle la protection des données est extrêmement importante, et a fait de cette analyse une étude de cas pour les entreprises européennes. Conclusion : les employés connectent leurs appareils mobiles à des systèmes contrôlés sans que vous soyez forcément au courant.

Les résultats de cette analyse pourront être utiles à toute entreprise qui doit sécuriser ses données, se protéger de l'espionnage ou de toute autre activité criminelle, et protéger les données de ses employés et clients.

Inquiétudes relatives aux risques auxquels sont exposés les informations et à leur impact potentiel sur l'entreprise :
utilisation de technologie personnelle et cloud par les employés



Base : N=171 décideurs en matière de sécurité des clients (Amériques ; gouvernement, éducation ou santé)
Source : Forrester's Global Business Technographics Security Survey, 2016

Le « BYOD parallèle » est le vrai problème

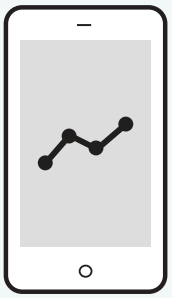
En analysant 20 agences américaines et plus de 1 000 employés du gouvernement américain, Lookout a découvert que 14 622 appareils utilisant Lookout étaient associés à des réseaux gouvernementaux. Cela signifie que les employés connectent leurs appareils personnels à des systèmes gouvernementaux. De plus, la fréquence des menaces mobiles graves rencontrées chaque année sur ces appareils s'élevait à 11 %, un chiffre particulièrement élevé.

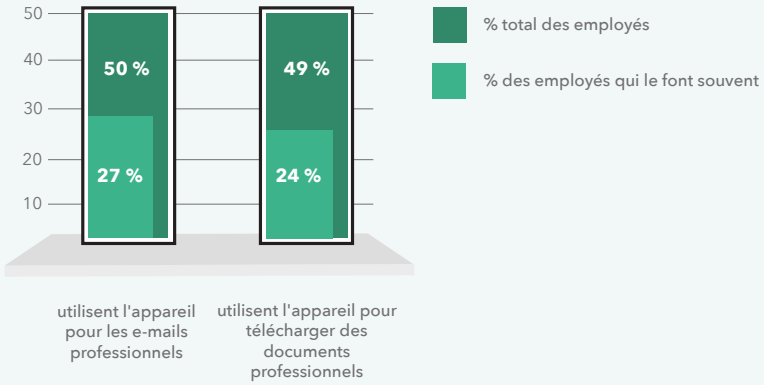
Le problème vient en fait du « BYOD parallèle », un terme qui renvoie aux appareils mobiles non gérés ou inconnus qui accèdent à un réseau. Similaire à l'informatique parallèle, le BYOD parallèle expose les données sensibles à des risques de fuite en raison du manque de visibilité et de contrôle sur les appareils qui peuvent accéder à telles ou telles données.

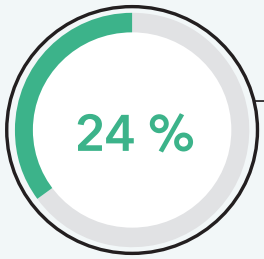
Les employés du gouvernement américain ramènent leur travail chez eux, ce qui peut aller à l'encontre des règles de l'agence. Ils sont même 50 % à accéder à leurs e-mails professionnels sur leur appareil personnel et 49 % à l'utiliser pour télécharger des documents professionnels. Et il ne s'agit là que d'un exemple du volume considérable de mouvements de données entre les comptes personnels et professionnels. Il est essentiel que chaque entreprise, qu'elle œuvre pour le gouvernement ou non, s'efforce de gagner en visibilité sur les mouvements de données pour mieux les contrôler.

Utilisation des appareils personnels

Savez-vous combien d'employés utilisent leur appareil mobile personnel pour le travail dans votre entreprise ?

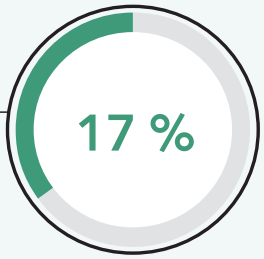






envoient des documents professionnels vers des comptes de messagerie personnels

stockent des documents professionnels dans des applications de partage de fichiers personnelles



Enquête Lookout menée auprès de 1 002 employés du gouvernement fédéral américain en juin 2015

Il n'est pas si difficile de débrider le système d'exploitation d'un appareil mobile

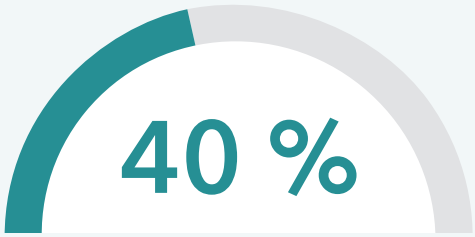
De nombreux employés du gouvernement accèdent à leurs documents et communications professionnels sur des appareils personnels, et certains tentent même de jailbreaker ou de rooter leur appareil. Des manipulations qui leur permettent de télécharger des applications sur des App Stores non officiels ou, plus simplement, de modifier leur écran d'accueil.

Environ 7 % des employés du gouvernement américain déclarent avoir rooté ou jailbreaké un appareil qu'ils apportent ou utilisent au travail. Un pourcentage relativement élevé qui révèle que le jailbreak et le rootage ne sont pas réservés aux geeks.

Le problème est que ces méthodes de débridage peuvent exposer les systèmes d'exploitation à des vulnérabilités non corrigées et encourager les utilisateurs à télécharger des applications sur des App Stores non officiels qui distribuent des applications malveillantes. Sur le long terme, ces problèmes peuvent exposer les données à des risques bien plus grands.

Non-respect des règles

Les politiques mobiles restrictives qui interdisent l'utilisation d'appareils mobiles personnels ne fonctionnent pas

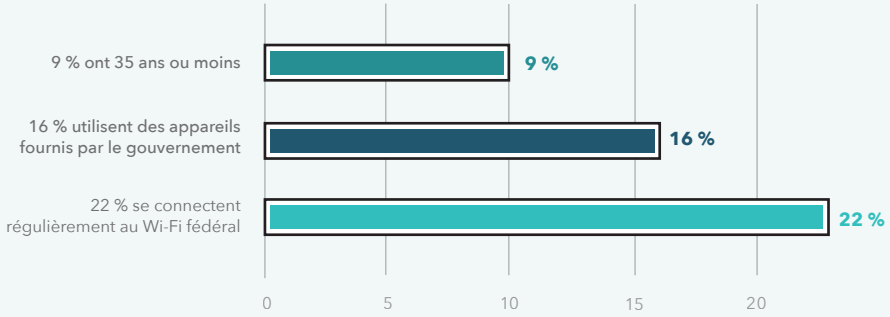


des employés travaillant dans des agences qui interdisent l'utilisation des smartphones personnels au travail déclarent que les règles ont un impact limité voire nul sur leur comportement

ILS COMPROMETTENT MÊME LEURS APPAREILS

7 % des employés ont rooté ou jailbreaké un appareil qu'ils apportent ou utilisent au travail.

Parmi ces employés,



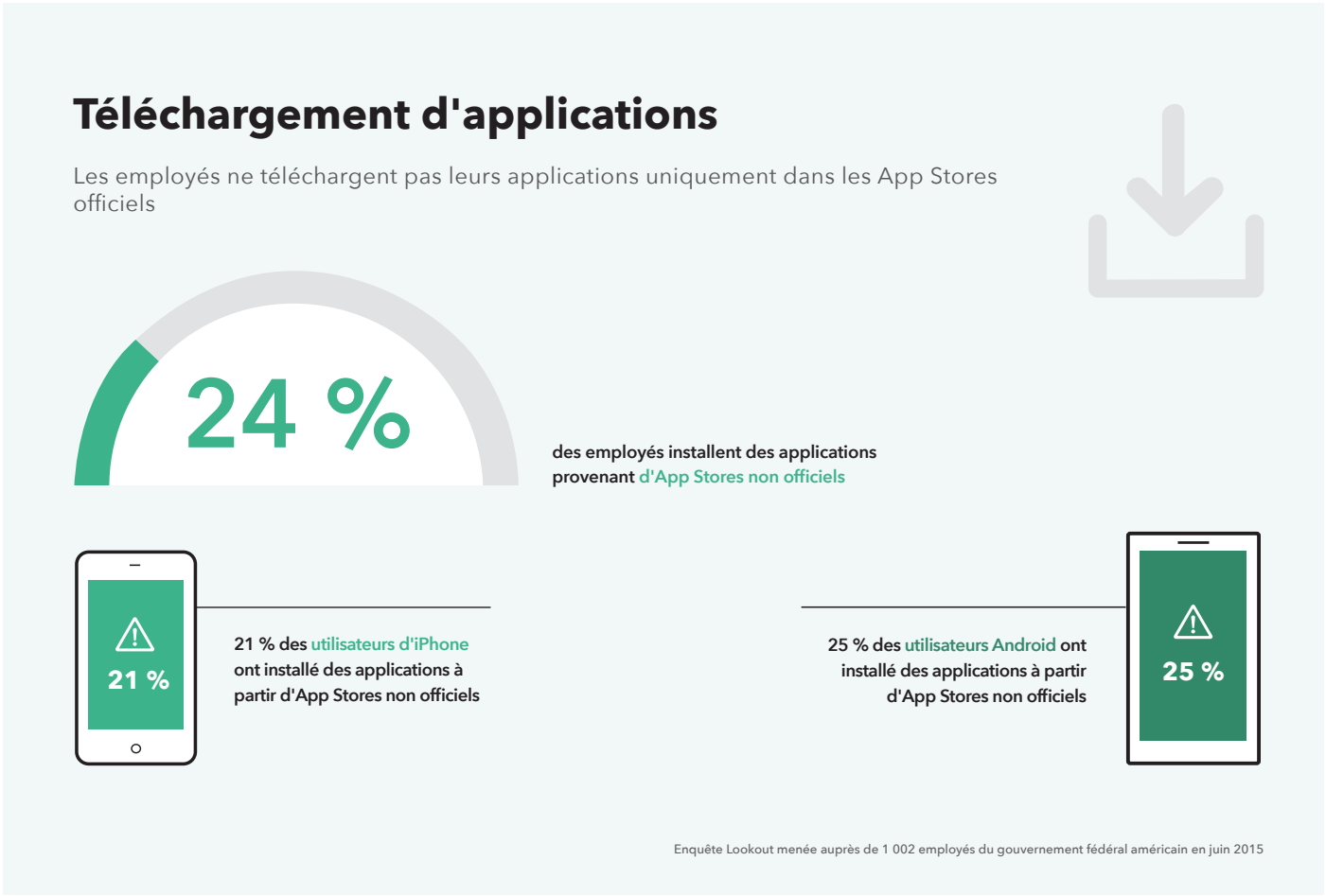
65 % accèdent à la messagerie d'entreprise sur cet appareil

57 % accèdent à des documents professionnels sur cet appareil

Enquête Lookout menée auprès de 1 002 employés du gouvernement fédéral américain en juin 2015

Des applications potentiellement non vérifiées et non sécurisées se connectent à votre réseau

Un pourcentage étonnamment élevé d'employés du gouvernement américain, 24 %, téléchargent des applications en dehors des App Stores officiels comme le Play Store de Google et l'App Store d'Apple. Ces applications peuvent présenter un risque pour le smartphone, car elles n'ont pas forcément été vérifiées avec autant de rigueur que les applications publiées par Google et Apple. De quoi mettre à mal l'idée selon laquelle il faut obligatoirement passer par un App Store officiel pour télécharger des applications sur iPhone. En réalité, il est très facile de télécharger une application sur un appareil iOS via un site Web ou un lien.



Les menaces sont bien réelles

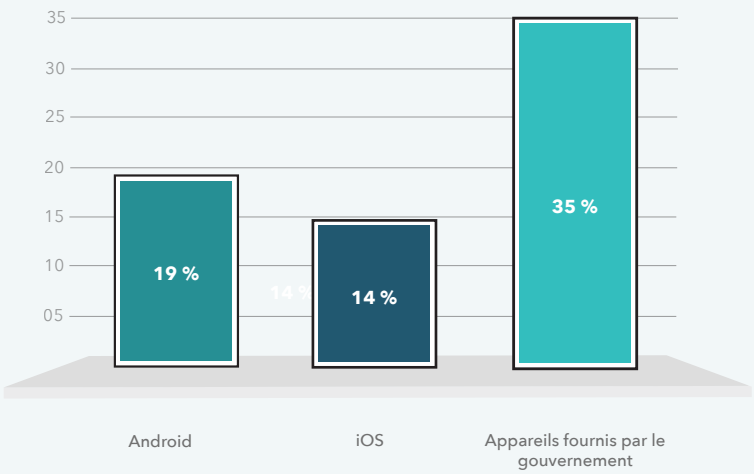
18 % des employés du gouvernement américain disent avoir été confrontés à un logiciel malveillant sur leurs appareils mobiles, tant sur leurs appareils personnels que sur les appareils fournis par le gouvernement. 19 % d'entre eux étaient des utilisateurs Android et 14 % des utilisateurs d'iPhone. Ces pourcentages sont bien plus élevés que les 7 % de logiciels malveillants sur Android annoncés par Lookout en 2014. Ceci étant, il ne faut pas oublier que les personnes qui ont répondu à l'enquête ont déclaré elles-mêmes les incidents et qu'elles ont peut-être cru avoir affaire à un logiciel malveillant alors que ce n'était pas le cas. Malgré ce taux élevé, 49 % des employés du gouvernement américain n'ont toujours pas installé d'application ou de solution de sécurité sur les appareils mobiles qu'ils utilisent ou emmènent au travail.

Logiciels malveillants mobiles

Un nombre surprenant d'employés du gouvernement fédéral a été confronté à un logiciel malveillant mobile

18 % **des employés du gouvernement fédéral utilisant des smartphones (personnels ou fournis par le gouvernement) disent avoir été confrontés à un logiciel malveillant**

QUEL TYPE D'APPAREIL UTILISAIENT-ILS ?



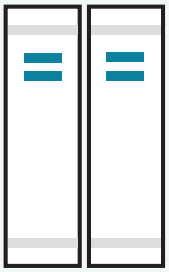
Enquête Lookout menée auprès de 1 002 employés du gouvernement fédéral américain en juin 2015

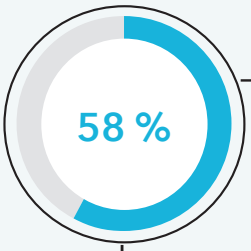
La sensibilisation des employés ne suffit pas

Il s'avère que les employés sont prêts à sacrifier la sécurité gouvernementale pour utiliser un appareil mobile personnel au travail, bien qu'ils aient conscience des problèmes de cybersécurité. 58 % des participants à l'enquête ont indiqué avoir conscience des conséquences de l'utilisation de leurs smartphones personnels au travail du point de vue de la sécurité, mais 85 % d'entre eux sont quand même prêts à les utiliser pour des activités potentiellement risquées. Chacun est très attaché à son confort et choisit généralement la solution de facilité pour atteindre ses objectifs, au détriment des risques. Il est important de sensibiliser les employés, mais les entreprises doivent également s'appuyer sur les technologies existantes lorsque cette sensibilisation ne suffit pas.

La sensibilisation des employés ne suffit pas

37 % des employés sont prêts à sacrifier la sécurité gouvernementale pour utiliser un appareil mobile personnel au travail, tout en étant conscients des problèmes de cybersécurité



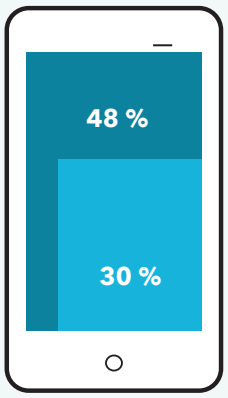


ont conscience des problèmes de cybersécurité et des conséquences que peut avoir l'utilisation de leur smartphone personnel au travail

pourtant, **85 %** admettent utiliser leurs appareils personnels pour des activités potentiellement risquées

48 % des employés déclarent ne pas être autorisés à stocker des informations ou des fichiers professionnels sur leur appareil personnel

pourtant, **30 %** le font quand même



Enquête Lookout menée auprès de 1 002 employés du gouvernement fédéral américain en juin 2015

Conclusion

Les appareils mobiles s'invitent de plus en plus dans tous les aspects de la vie des employés et nombreuses sont les entreprises qui ont du mal à trouver le bon équilibre entre cette nouvelle tendance et la nécessité de sécuriser les données sensibles.

De nombreuses entreprises et entités gouvernementales dans le monde n'ont pas de programme de sécurité mobile officiel, mais cette enquête indique clairement que l'absence d'un tel programme, comprenant une stratégie de gestion du BYOD, expose les données sensibles à des risques, car les employés contournent les règles et utilisent quand même leurs appareils.

Les entreprises qui misent sur le progrès sont de plus en plus nombreuses à adopter l'utilisation des appareils personnels sur le lieu de travail et exploitent les solutions de sécurité et de gestion des appareils actuellement disponibles. Elles considèrent en outre que la sécurité doit faire l'objet d'un effort global et que les appareils mobiles constituent un élément clé de cet effort étant donné le volume important de données auxquelles ils accèdent.

Le BYOD parallèle est une menace qui doit être prise au sérieux par toutes les entreprises. Ne pas inclure les appareils mobiles dans les stratégies de sécurisation des données revient à mettre en péril la sécurité de ces données. Les entreprises européennes doivent faire attention aux appareils qui accèdent à leurs réseaux, car ils accèdent à des informations sensibles, qu'elles le veuillent ou non.

Méthodologie : *Cette enquête a été menée par Market Cube pour le compte de Lookout entre le 19 et le 26 juin 2015 auprès de 1 002 employés du gouvernement fédéral américain. La marge d'erreur est de 3,1 %.*