Étude 2020 sur les comportements liés à la sécurité des mots de passe et à l'authentification

Les professionnels de l'IT et les utilisateurs français ont-ils la même approche de la sécurité ?

Selon une récente étude du Ponemon Institute, les professionnels de l'IT et les utilisateurs ont des comportements dangereux en matière de sécurité et ce, malgré des risques croissants pour la sécurité et la confidentialité. Toutefois, les attentes ne correspondent pas toujours à la réalité lorsqu'il s'agit de mettre en œuvre des solutions de sécurité d'utilisation aisée et qui correspondent à leurs souhaits.

Particuliers vs professionnels de l'informatique : comportements et connaissances en matière de sécurité

Particuliers		Professionnels de l'informatique
25 %	**S'inquiètent fortement** de la confidentialité et de la sécurité de leurs données personnelles depuis deux ans.	30 %
76 %	Des utilisateurs et des professionnels de l'informatique dont le **compte a été piraté** ont modifié la façon dont ils gèrent leurs mots de passe ou protègent leurs comptes.	58 %
64 %	N'utilisent **pas** l'authentification à deux facteurs pour protéger leurs comptes personnels.	57 %
39 %	**Réutilisent** les mêmes mots de passe dans leurs comptes professionnels.	48 %
51 %	Partagent parfois ou fréquemment leurs **mots de passe** avec des collègues.	56 %

Protection des utilisateurs

57 % des professionnels de l'IT ont déclaré que leur entreprise a subi une **attaque par phishing, 17 %** un vol d'identifiants, et **8 %** une attaque de type MITM (**homme du milieu**).

35 % des professionnels de l'IT ont indiqué que leur entreprise utilise un **gestionnaire de mots de passe,** un outil efficace pour créer, gérer et stocker des mots de passe en toute sécurité.

46 % des professionnels de l'IT déclarent que leur entreprise utilise des **Post-its** pour gérer les mots de passe.

52 % des professionnels de l'IT indiquent que leur entreprise **s'appuie sur la mémoire des utilisateurs** pour gérer les mots de passe.

Gestion des mots de passe et protection contre le piratage des comptes

46 % des professionnels de l'IT **exigent l'utilisation de l'authentification à deux facteurs** pour accéder aux comptes professionnels.

37 % des entreprises qui utilisent l'authentification à deux facteurs pour sécuriser les comptes professionnels ont **recours à des applis mobiles,** et **26 % à l'envoi de codes par SMS.**

23% des utilisateurs estiment que les techniques d'authentification à deux facteurs mobiles ou par SMS ne sont **vraiment pas pratiques.**

54 % des personnes interrogées déplorent que les applications d'authentification à deux facteurs mobiles ou par SMS **perturbent leur productivité.**

47 % des personnes interrogées estiment qu'il est **ennuyeux** de copier-coller un code de sécurité à usage unique.

Sécurité des utilisateurs mobiles

61 % des entreprises **autorisent l'utilisation de terminaux mobiles personnels.**

62 % des entreprises estiment qu'elles ne prennent pas les mesures nécessaires pour **protéger les informations stockées sur les terminaux mobiles.**

56 % des utilisateurs qui recourent à un appareil personnel pour accéder à des documents à usage professionnel **n'ont pas recours à une solution d'authentification à deux facteurs.**

Protection des comptes clients

Pour les professionnels de l'IT, les **informations des clients** et les **informations personnelles identifiables** arrivent en tête de liste des éléments à protéger. Toutefois, **64 %** d'entre eux signalent que les comptes de clients ont été piratés.

61 % d'entre eux estiment que leur nom d'utilisateur et leur mot de passe assurent un niveau de **sécurité suffisant.**

24 % des professionnels de l'IT **n'envisagent pas** de proposer une solution d'authentification à deux facteurs à leurs clients.

51 % d'entre eux estiment que cette solution ne serait **pas pratique** pour les clients.

S'agissant de l'accès aux informations en ligne, les utilisateurs considèrent que la sécurité (56 %), le coût (57 %) et la facilité d'utilisation (35 %) sont des critères très importants.

Vers un avenir plus sûr

56 % des utilisateurs n'adopteront de nouvelles technologies que si elles sont faciles à utiliser et qu'elles améliorent considérablement la sécurité des comptes.

55 % des professionnels de l'IT et des utilisateurs préfèrent une méthode de protection des comptes sans mot de passe.

66 % des professionnels de l'IT estiment que la suppression des mots de passe **améliorerait la sécurité de leur entreprise.**

56 % des professionnels de l'IT sont convaincus que l'élimination des mots de passe **améliorerait le confort des utilisateurs.**

70 % des professionnels de l'IT pensent que **le recours à la biométrie** améliorerait la sécurité de leur entreprise.

53 % des utilisateurs pensent que le recours à **la biométrie améliorerait la sécurité** de leurs comptes.

53 % des professionnels de l'IT considèrent que l'utilisation de **clés de sécurité matérielles** améliorerait la sécurité.

60 % des utilisateurs se déclarent prêts à payer de **50 à 60 €** pour bénéficier du plus haut niveau de sécurité sur tous leurs comptes en ligne.

Pour de plus amples informations à propos de l'étude du Ponemon Institute, lire l'étude intitulée 2020 State of Password and Authentication Security Behaviors Report
Visitez le site https://www.yubico.com/authentication-report-2020/

Visit https://www.yubico.com/authentication-report-2020/

yubico

www.yubico.com

La société Yubico a été fondée en 2007 dans le but de simplifier les connexions sécurisées au bénéfice du plus grand nombre. En étroite collaboration avec les grands noms du Web et les principaux leaders d'opinion, Yubico a contribué à la création des standards ouverts d'authentification FIDO2, WebAuthn et FIDO U2F, qui sont intégrés aux principaux navigateurs et plateformes en ligne. Cette intégration facilite l'utilisation des méthodes d'authentification à deux facteurs ou multifacteurs, ainsi que les connexions sans mot de passe pour rendre Internet plus sûr pour des m illiards de personnes.

© 2020 Yubico