dashlane

L’insouciance numérique met les entreprises françaises en danger

Table des Matières

Emmanuel Schalit, CEO de Dashlane

Le monde du travail s'est radicalement transformé ces dernières années. Le Big Data, l'utilisation des smartphones, des tablettes et des ordinateurs portables, le télétravail via le haut débit, sont autant de tendances qui bousculent nos quotidiens et changent radicalement notre manière de travailler. Ce n'est pas un hasard si on estime que 90% des données stockées en ligne ont été générées au cours des deux dernières années. Il est bien sûr fascinant de pouvoir aussi facilement échanger de l'information, communiquer, réaliser des transactions, quel que soit l'endroit où l'on se trouve dans le monde. Mais ce nouveau paradigme apporte aussi son lot de menaces. Les compétences des pirates évoluent aussi vite que les technologies. Les organisations répondent à ces menaces par des mesures de sécurité, mais sont-elles suffisantes au regard des profonds changements que connait notre manière de travailler ? Chez Dashlane, nous pensons que les employés doivent constituer **la première ligne de défense des entreprises** contre les menaces externes. Il semblerait que ça n'est pourtant pas le cas dans toutes les entreprises où les données sensibles et confidentielles sont souvent gérées **avec une forme d'insouciance**. Nous avons réalisé cette étude pour en savoir plus sur cette « Insouciance numérique ».

Présentation

Les mots de passe occupent une place centrale dans notre vie numérique et notre vie professionnelle. Nous les utilisons en effet quotidiennement pour accéder à des bases de données en ligne, des medias en ligne et des logiciels spécifiques à notre profession.

Compte-tenu de l'importance des enjeux de sécurité en ligne pour les entreprises, nous avons voulu étudier la manière dont les mots de passe étaient gérés dans les entreprises.

Les organisations sont constituées d'individus et nous avons décidé d'interroger 3 000 personnes (1 000 dans chaque pays) situées en France, au Royaume-Uni et aux Etats-Unis. Nos questions ont porté sur la manière dont les mots de passe sont gérés sur leur lieu de travail et les politiques mises en place pour assurer la sécurité de l'entreprise.

Nous nous sommes intéressés à :

- La manière dont les mots de passe sont gérés au quotidien, et les politiques mises en place par les entreprises
- Les trous de sécurité potentiels liés à la mauvaise gestion des mots de passe
- L'attitude des employés concernant les mots de passe et son éventuel impact sur leur productivité

Points à Retenir

Les jeunes sont plus insouciants concernant la sécurité des mots de passe

84% des moins de 24 ans partagent des mots de passe avec leurs collègues et 33% d'entre eux les partagent sur papier.

C'est l'un des constats phares de ce rapport. Les jeunes ont une approche plus insouciante de la gestion des mots de passe. C'est très prégnant pour les moins de 24 ans et dans une moindre mesure pour les 25–34 ans, qui admettent partager des mots de passe, rarement de manière sécurisée. Les jeunes sont aussi plus nombreux à reconnaître qu'ils ont encore la possibilité d'utiliser des mots de passe de leur précédent employeur.

Trop de gens peuvent encore utiliser des mots de passe de leur précèdent employeur

69% des personnes interrogées reconnaissent qu'ils pourraient, s'ils le souhaitaient, accéder aux outils en ligne de leur précédent employeur.

Pour une majorité des employés, quitter une entreprise ne rime ainsi pas avec une perte totale des accès aux sites utilisés. Si dans certains cas (base de données, abonnement à des journaux), cela ne prête pas à des conséquences graves, cela peut aussi parfois concerner des données très sensibles.

Les entreprises ont besoin d'une politique de gestion des mots de passe

55% des employés n'ont pas connaissance de l'existence d'une politique de partage des mots de passe dans leur entreprise.

La plupart des organisations ne semblent pas avoir mis en place de vraie politique de gestion des mots de passe. Quelques conseils sont parfois glissés dans les consignes générales concernant les outils informatiques mais les employés manquent d'indications concrètes pour gérer les problèmes quotidiens de gestion de mots de passe. C'est souvent donc la politique du moindre effort qui s'impose comme nous avons pu le constater en analysant les méthodes de partage de mots de passe.

Les employés ont trouvé des méthodes pour gérer leurs mots de passe, mais elles nuisent à leur productivité

58% des gens considèrent que la gestion des mots de passe réduit leur productivité.

Les mots de passe sont partout. Nous les utilisons sans même y penser. Mais ils se rappellent aussi souvent à nous lorsque nous les oublions, que nous n'arrivons pas à nous connecter à un site, pile au moment où nous en avons besoin, et cela perturbe notre travail. La plupart des personnes interrogées font ce constat et manifestent le besoin de méthodes et d'outils standardisés pour la gestion de leurs mots de passe.

Le partage des mots de passe est sensible. Il doit être sécurisé.

78% des gens reconnaissent avoir déjà partagé un mot de passe avec un collègue.

Le partage de mots de passe est devenu extrêmement fréquent. Bien qu'il soit parfois préférable d'avoir des identifiants pour chacun, cela n'est parfois pas possible. Partager un mot de passe ne pose pas de problème si cela est fait de manière sécurisée mais trop de gens utilisent encore des post-it, l'email ou des fichiers partagés non sécurisés pour le faire.

L'Etude Dashlane

Comment les mots de passe sont-ils utilisés aujourd'hui ?

Dans un premier temps, nous avons souhaité avoir un aperçu de la manière dont les mots de passe sont utilisés et gérés dans les entreprises.

Nous avons proposés les quatre phrases ci-dessous aux personnes interrogées en leur demandant à quel point elles étaient en accord ou en désaccord.

1 Si je le souhaitais, je pourrais encore accéder via un mot de passe aux outils en ligne (base de données, abonnements...) que j'utilisais dans mon précédent travail

L'objectif de cette question était de savoir si l'absence de gestion des mots de passe rendait l'accès à des abonnement ou logiciels possibles par d'anciens employés. **69 % des personnes interrogées reconnaissent pouvoir accéder aux systèmes de leur ancien employeur**, s'ils le souhaitent. C'est surprenant, voire effrayant, surtout lorsqu'on sait ce à quoi cela peut conduire. Les exemples d'employés licenciés qui se vengent en "piratant" les réseaux sociaux de leur ancien employeur sont légions. On se souvient par exemple d'un chef anglais qui avait dénoncé son licenciement sur le compte Twitter de son employeur.

2 Mon entreprise change les mots de passe utilisés par un employé lorsque celui-ci quitte l'entreprise

Nous avons voulu savoir si le laxisme des entreprises était à mettre en cause. **Les résultats sont plutôt surprenants puisque, pour 80% des employés, les entreprises changent les mots de passe lorsqu'un employé quitte l'entreprise.** Cette réponse semble en contradiction avec le constat précédent. Plusieurs hypothèses peuvent expliquer ce décalage. Un écart entre le discours et les faits : certaines entreprises ont des règles mais qui ne sont pas appliquées dans les faits ? Une focalisation sur les mots de passe principaux comme celui permettant d'accéder à son ordinateur ou sa boîte mail mais une négligence sur tous les autres sites utilisés comme les réseaux sociaux, dont l'équipe IT n'a parfois même pas connaissance ?

3 La gestion des mots de passe et des problèmes de connexion à des sites/logiciels a réduit ma productivité au travail

Quelles conséquences a la gestion des mots de passe sur la productivité des employés? **Pour 58% des employés, elles sont négatives.** Cela confirme le constat que nous faisons tous : gérer les dizaines de comptes qu'on utilise est une gageure sans les bonnes méthodes et les bons outils.

4 Certains mots de passe sont partagés entre collègues

64% des employés reconnaissent que des mots de passe sont partagés au travail. Encore une fois, cela confirme un constat que nombre d'entre nous font dans leur quotidien. Cela n'est pas nécessairement une mauvaise chose ! L'un des intérêts du mot de passe comme mode d'authentification est justement qu'il peut être partagé. Mais cela doit être fait de manière sécurisée.

Analyses concernant le genre et l'âge

Sur l'ensemble de ces questions, on dénote assez peu de différences entre les réponses des femmes et des hommes. Elles laissent toutefois apparaître un vrai clivage générationnel.

Les jeunes sont en effet:

- Plus nombreux à reconnaître qu'ils pourraient accéder à des comptes de leur ancien employeur
- Plus nombreux à constater le partage de mots de passe sur leur lieu de travail
- Plus nombreux à reconnaître que leur productivité a baissé à cause des mots de passe

Les entreprises cherchent encore la bonne méthode pour le stockage et le partage

Quels outils sont utilisés en entreprise pour stocker et partager les mots de passe ? Si les gestionnaires de mots de passe comme Dashlane sont de plus en plus utilisés, il semblerait que beaucoup de personnes utilisent encore des méthodes plus « archaïques » comme le post-it ou l'email. Nous avons interrogé notre échantillon sur ce sujet.

55% des employés français interrogés reconnaissent utiliser leur mémoire pour stocker les mots de passe. Si cela peut paraître naturel lorsqu'on a que quelques mots de passe à retenir, cela devient très compliqué lorsqu'on doit en mémoriser des dizaines et en partager certains avec des collègues. Cela conduit nécessairement à utiliser des mots de passe faibles, à utiliser les mêmes pour plusieurs sites, et à s'y perdre de temps en temps, quand on en vient pas à multiplier les aide-mémoires qui sont autant de failles de sécurité potentielles.

Plus alarmant, plus de 30% des personnes interrogés confessent partager les mots de passe sur un papier, post-it ou cahier. Il s'agit là clairement d'une mauvaise pratique qui met en péril la sécurité des systèmes concernés. On se souvient de TV5 Monde qui, quelque jour après avoir été victime d'un piratage, avait laissé traîner devant des caméras de télévision un post-it indiquant leur mot de passe Youtube…

Pour 22% des personnes interrogées, c'est le fichier partagé qui s'impose. Si cela peut paraître une bonne idée, cela pose souvent des réels problèmes de sécurité (ils ne sont pas toujours bien chiffrés) et des problèmes pratiques car les mots de passe ne sont souvent pas mis à jour lorsqu'ils sont modifiés.

Dans la catégorie des mauvaises pratiques, on retrouve aussi le partage par mail ou chat (7% des réponses) ou l'utilisation du même mot de passe partout (6%).

Les mots de passe sont de précieux sésames nous permettant d'accéder à des données sensibles qui ont généralement une forte valeur pour l'entreprise. La meilleure manière de les stocker consiste à utiliser un gestionnaire de mot de passe, un outil qui permet de les chiffrer localement à l'aide d'une clé de chiffrement qui ne sera jamais connue de personne d'autre que l'utilisateur. 19% des personnes interrogées ont recours à un gestionnaire de mot de passe. Il y a ainsi une réelle adoption des outils adaptés mais un réel travail d'éduction reste à faire pour que plus d'entreprises aient connaissance de ces outils.

Analyses concernant l'âge

Les jeunes de moins de 34 ans sont 33% à partager les mots de passe sur un Post-it alors que cela ne concerne que 23% des 45–54 ans et 16% des plus de 55 ans. L'insouciance des jeunes les conduit ainsi à prendre plus de risques avec les mots de passe de leurs employeurs. On retrouve la même tendance concernant l'utilisation d'un fichier partagé alors que les plus de 45 ans semblent plus faire confiance à leur mémoire.

56% mémoire

31% papier

22% fichier informatique

19% gestionnaire de mots de passe

7% email, chat, SMS

6% mot de passe unique

Les entreprises doivent affronter le sujet

Si l'insouciance des employés, en particulier les jeunes, conduit à de réelles failles de sécurité dans la manière dont les mots de passe sont gérés, que font les entreprises pour pallier ce problème ?

55% des employés français considèrent que leur entreprise n'a pas de politique concernant le partage des mots de passe ou qu'ils ne sont pas au courant. Cela souligne l'importance de sensibiliser les entreprises au problème de la gestion des mots de passe. Leurs employés partagent, souvent sans sécurité, des accès à des sites critiques, et la plupart de font rien pour réguler cela !

Un signe encourageant toutefois, 21% des personnes interrogés ont pris conscience du problème et pensent que leur entreprise devrait avoir une politique claire à ce sujet.

55% **des gens ignorent si leur entreprise a une politique de partage de mots de passe**

Les jeunes sont en pointe sur la tendance du partage

Le constat est frappant: 78% des employés français admettent avoir déjà partagé un mot de passe avec un collègue.

C'est une pratique courante et totalement admise, puisque à peine 6% des personnes interrogées indiquent être mal à l'aise en partageant des mots de passe. C'est sans doute parce qu'il s'agit de mots de passe professionnels et non personnels.

Il est très clair que cette tendance est poussée par les jeunes. 37% des moins de 24 ans indiquent partager des mots de passe fréquemment contre seulement 16% des 35–44 ans et 12% des 45–54 ans.

A l'inverse, plus les gens sont âgés, plus ils considèrent cette pratique avec défiance. Il est ainsi intéressant d'analyser par tranche d'âge le nombre de gens qui indiquent qu'ils ne partageront jamais de mots de passe.

16–24	25–34	35–44	45–54	55+
15.5%	16%	22.8%	35.1%	43.2%

Il est clair que les gens plus âgés sont moins enclins à partager leurs mots de passe. Bien sûr cela peut traduire en partie le fait qu'ils occupent des positions plus élevées dans l'entreprise et manipulent des données plus sensibles. Mais les contrastes observées dans les résultats semblent toute de même indiquer un clivage générationnel important sur la manière dont les informations sont partagés et sécurisées dans l'entreprise.

Le partage des mots de passe est en train de rentrer totalement dans les mœurs, par nécessité, et sous l'influence d'une Génération Y ultra connectée et insouciante. Rien ne sert de lutter contre cette tendance. Il faut l'accompagner en proposant les bons outils pour éviter qu'elle ne mette en péril la sécurité des entreprises.

Comparaison Internationale

L'étude Dashlane a été menée sur des échantillons d'employés français, américains et anglais. Il est intéressant de comparer certains résultats:

Outils utilisés pour le partage des mots de passe

Sur ce sujet, la France partage le bonnet d'âne avec les Etats-Unis. 31% des français et 30% des américains partagent des mots de passe sur papier alors que cela concerne moins de 20% des britanniques !

Politiques de partage des mots de passe

Les entreprises françaises sont plus avancées sur la mise en place de politique de partage de mots de passe puisque 45% des personnes interrogées en France indiquent que leur employeur en a une, contre respectivement 36% et 39% des personnes interrogées au Royaume-Uni et aux Etats-Unis !

Partage des mots de passe entre collègues

La France semble être championne du monde de partage de mots de passe. 78% des employés français indiquent avoir déjà partagé un mot de passe avec un collègue contre 53% des américains et 52% des anglais !

L'opinion de Dashlane.

Il y a encore du travail!

Nous avons mené cette étude car nous avions l'intuition que les mots de passe étaient gérés de manière un peu laxiste dans les entreprises. Cette étude confirme notre intuition tout en mettant également en lumière quelques signes encourageants. Le monde de l'entreprise est sensible à la nécessité de gérer les mots de passe, sans doute bien plus qu'il y a quelques années, mais cela ne se traduit pas encore dans les faits. Les usages de partage de mots de passe indiquent clairement que nombre d'entreprises sont susceptibles de se faire prendre à défaut à ce niveau-là.

Il est plus qu'urgent d'agir. Managers, employés, tous doivent prendre conscience de la valeur des informations stockées aujourd'hui en ligne et des conséquences potentiellement néfastes d'une faille de sécurité. Dans les entreprises, les équipes qui partagent des mots de passe sur des papiers ou réutilisent x fois le même mot de passe semble se dire « Personne ne sera intéressé par ces informations ». Aucune entreprise n'est à l'abri des hackers crapuleux ou d'anciens employés qui souhaitent se venger. C'est d'autant plus regrettable que l'utilisation d'un gestionnaire de mots de passe gratuit et une politique de partage de mots de passe résumée sur une page, peuvent souvent suffire à améliorer considérablement la sécurité.

L'arrivée de la Génération Y dans le monde du travail a changé la donne. Les Digital Natives ont grandi avec les réseaux sociaux, où ils partagent beaucoup de détails de leur vie privée. Ils n'ont pas la même perception de ce qui doit être confidentiel ou pas. Ils sont aussi les plus en pointe sur l'utilisation de smartphones et de tablettes, nouveaux lieux de création, de stockage et de partage de données. Ils ont l'insouciance de la jeunesse. Les entreprises ne pourront pas les changer. Elles doivent apprendre à gérer leur insouciance.

Les entreprises doivent bien faire comprendre à leurs employés qu'ils sont la première ligne de défense contre des attaques informatiques et leur fournir les outils et méthodes pour gagner en sécurité sans perdre en productivité. Partager des mots de passe est très utile, mais cela doit être fait de manière sécurisée. Plus vite les entreprises s'adapteront à cette nouvelle réalité, plus vite elles pourront se concentrer sur leur cœur de métier sans craindre en permanence une intrusion informatique.

Méthodologie et Crédits

L'Etude Dashlane a été conduite en septembre 2015 via un questionnaire en ligne, auprès de 3000 employés utilisant un ordinateur quotidiennement dans leur travail aux Etats-Unis, au Royaume-Uni et en France. Le sondage a été mené par Opinion Matters.

A propos de Dashlane

Dashlane simplifie et sécurise la gestion des identités et des paiements pour les particuliers et les entreprises. C'est la solution idéale pour faire face au problème rencontré par des centaines de millions d'utilisateurs dans le monde entier : la gestion des inscriptions, des identifications et des paiements quels que soient le site Web ou le terminal. Plus de 3M de personnes utilisent Dashlane afin de gérer leurs mots de passe, de s'identifier automatiquement, de générer des mots de passe sécurisés, ou encore d'effectuer des paiements sur n'importe quel site Web. La solution a été plébiscitée par de grandes publications, notamment le **Wall Street Journal**, le **New York Times** et **USA Today**. Créée en 2009 à l'initiative de Bernard Liautaud, fondateur de Business Objects, la société a levé 24M€, notamment auprès de Bessemer Ventures, les investisseurs qui ont financé Linkedin, Skype ou encore Criteo à leur démarrage.

Site web : dashlane.com