dashlane

Digital indifference in the workplace

Contents

Introduction from

Emmanuel Schalit, CEO Of Dashlane

The business world has transformed tremendously over the past few years. The advent of Big Data, the proliferation of smartphones, tablets and home laptops, flexible working, and ultra-fast broadband connections have resulted in a completely different way of working. Indeed, it is estimated that 90 percent of the world's data has been produced in the last two years. It's undoubtedly an exciting time to be in business as technology has enabled us to research, connect and transact with all corners of the globe.

But with these great opportunities, there are also great threats. **Hackers have never been more sophisticated.** Organizations have implemented security measures, but the transformation of how we work and collaborate means that these precautions may not be enough. We advise that all employees must be **the first line of defense for external threats** through effective password security. However, our concern is that employees in this market suffer from **a state of digital indifference**: they are too lax with their handling of employers' sensitive and confidential information. This is why we commissioned research to examine just how safe employees in the UK, US, and France are with sensitive information, and just how at-risk organizations are. The findings make for very interesting reading.

Executive Summary

As more of our working lives are now spent online, passwords are more central to how we work, whether we're accessing databases, media hubs, or other services specific to our industry or profession. Given this, as well as the issue of online security in terms of the data held by organizations, Dashlane wanted to look at how secure businesses are when it comes to their approach to passwords and password security.

Organizations are the sum of their individual talent, so we decided to speak to 3,000 people across three international markets (US, UK and France) to explore how people are using passwords in their workplace, what policies and practices are common, and how passwords impact on our working lives.

Our survey was designed to explore:

- Current password practices and policies
- Security gaps that potentially exist because of lax password management
- Employee attitudes toward passwords and their impact on efficiency in the workplace

The following section examines the key takeaways from the US survey. This is followed by a detailed analysis of each question, an international comparison of the results from France and the UK, and conclusions and recommendations.

Key Takeaways

Young people are more casual with their approach to password sharing

67% of people between the ages of 16-24 in the US admit to sharing a password with a colleague

One of the key themes of this report — something that is likely to concern employers — is that young people are the most likely to share work accounts and passwords with one another. Those aged 16–24 (and to a lesser extent those aged 25–34) share passwords more often and are not given the tools and guidelines to do so in a safe way. They also more frequently confirm that they could use old passwords to access accounts and services belonging to a former employer.

Too many people can access accounts that belong to former employers

42% of people admitted they could access an account belonging to a previous employer

Nearly half of people admitted they could still access an account or subscription-based service belonging to an old employer. While this could simply be accessing a trade publication or newspaper subscription with an old employer's login details, and therefore likely to be harmless, there are instances where this could be extremely risky.

Employers need password specific policies

61% of people say they don't know their company's password policy or that their employer doesn't have one

Most organizations do not appear to have defined password policies. In many cases, passwords are dealt with as a minor subset of an overarching IT or network policy. **This means that employees have little formal guidance from their employers.** This results in a situation where the path of least resistance becomes conventional practice.

People find ways to manage their passwords, but they still impact work efficiency

41% of US respondents said passwords impacted on their workplace efficiency in some way

Passwords are now pivotal in the modern workplace; we use them every day. In fact, we use them without thinking, and it is easy to take them for granted. However, getting locked out of key services, asking for password reminder emails and searching around for the right code can all impact our efficiency. This is something that many respondents acknowledged, and there is clearly a need for password management standardization within our workplaces.

Password sharing is widespread and needs to be properly managed

53% of people acknowledged they had shared a password with a colleague at some point

Password sharing is extremely common and something that is required more and more often in today's workplace. While the best practice would be for each employee to have their own specific log-ins and passwords, this is not always practical. **Passwords should be shared safely and securely.**

The Research

How are passwords are used?

We want to kick our study off by establishing an overall snapshot of how passwords are used in the modern workplace.

We put four different statements to the sample group on a range of topics related to password security and password management in the work place. Respondents were asked how strongly they agreed or disagreed.

1 If I wanted to, I could still use passwords from a previous employer to access accounts (such as database access or media subscriptions)

The first statement explored the issue of exploiting poor password management practices to access accounts associated with former employers. **42% of those polled in the US agreed they could access old accounts.** Indeed, there have been some extreme and high profile instances of people accessing social media accounts after having left a job in order to cause an former employer reputational damage. The examples of the HMV workers live-tweeting their sackings or chef Jim Knight hijacking his employee's Twitter feed are just two that have made the national news recently.

2 My company has a policy to change passwords every time an employee that had access to them leaves

This statement sought to establish whether or not respondents' employers have policies to change passwords every time someone who had access to them leaves the business. The results were more encouraging, with over **68% of respondents agreeing that their employer did change passwords if somebody left the business**. Only 20% of respondents disagreed, which suggests that many employers are getting savvier at understanding the need to change passwords when key members of staff leave.

3 Managing passwords and log-in issues have reduced my efficiency at work

41% agreed that passwords have impacted their workplace efficiency. This shows that bad password management practices can hamper the workday efficiency for larger numbers of employees.

4 Passwords are shared around the office

The final statement explored how prevalent password sharing is within the office. **Half of people (50%) admitted that some passwords are shared within their office.** This is not necessarily a bad thing, as long as passwords are shared securely.

44% of respondents, however, responded that passwords are not shared in the workplace. This is surprising, as there are often good practical reasons to share accounts with colleagues (for example: so that multiple employees can manage a social media account). As stated above, the issue is ensuring that password sharing is done securely and not in a haphazard or casual way.

Gender & Age analysis

One of the more interesting aspects to emerge, is that there was very little gender difference in terms of the responses. In fact, the male/female split never varied by more than a single percentage point. However, the same cannot be said of the splits according to age.

Young people are:

- More likely to admit to being able to access on old employers accounts
- Less likely to be aware of a company policy to change passwords after employees leave the company
- Much more likely to share password with colleagues
- More likely to indicate that passwords affected their efficiency negatively

A nation of password hoarders?

Next, we examined the most popular tools and techniques for sharing and storing passwords in the American workplace. Aside from password managers, respondents noted using spreadsheets, paper-based systems (some casually strewn across desks on pieces of scrap paper), sharing passwords via email and text, and even simply retaining them in their heads.

A **staggering two thirds (62%) rely on their own memory to save passwords.** While seemingly harmless, this approach is vulnerable to issues if the user forgets their password. In a business setting, using your head to remember passwords is unhelpful for colleagues who also need to access shared services — particularly if you leave the business.

Alarmingly 30% of people also confessed they still write passwords down on a piece of paper in the office. This is an approach is dangerous on a number of levels. Even if users have the world's best passwords, they will still be in danger if they are stored offline on paper that can be easily lost or stolen.

13% of respondents noted filing their passwords in a formal spreadsheet, or similar document. This is an option that is convenient as all of the information is stored in an orderly fashion in a location that can be accessed by colleagues. But this approach leaves users seriously vulnerable to unwanted access from third parties and hackers, who can easily collect a host of passwords in one fell swoop.

20% of respondents noted using a password manager. Only 8% admitted using a single password for all of their accounts, which demonstrates that progress has been made in making workers aware of the serious risks of this approach.

Gender & Age Analysis

45–54 age group has the strongest adoption of password managers as 26% use a password manager, compared to 13% of 16–24. Paper-based systems were more common among younger respondents — 43% of users aged 16–24 used this method, compared to 26% of 55+.

62% memory

30% written down

20% password manager

13% shared spreadsheet

8% one password for all systems

7% email, text or instant message

The new CSR: Corporate Security Responsibility

We sought to evaluate organizational approaches to password sharing; whether they employed a stringent policy (and if so, how familiar employees were with this) and if not, if employees thought that the company should have one.

Only 39% stated that their business has a clear password policy that they follow. With more education at both individual and management levels, this number could easily be much higher. More than one in four (26%) respondents stated their company did not have a password policy because management considered it to be unnecessary. This suggests that there is much work to be done in educating businesses on the importance of having a password policy to protect the company and employees against breaches.

Furthermore, 17% admitted they weren't even sure if their company had a password policy. This lack of clarity shows that many businesses must take a much firmer approach to adopting clear password policy processes, communicating what these are to their employees, as well as why it's important that they are understood and followed.

18% of respondents revealed they didn't have a policy, but, somewhat encouragingly, believed their employers should. This shows that some progress has been made in raising awareness of the importance of password management at an individual level, but that more needs to be done in order to encourage both employees and employers to take that next step.

Gender & Age analysis

Considering a password policy to be unnecessary was particularly common among older respondents, with 34% of those aged 55+ agreeing with this claim, compared to just 21% of 16–24 year olds. And organizations that have clearly defined a password policy have a younger employee base, with 47% of 16–25 year olds stating that they use of such a policy, versus just 32% of those aged 55+. These facts appear to validate the perception that much of the responsibility for poor corporate password policies lies at the senior management level in businesses.

61% of people aren't even aware if their company has a password sharing policy

Mi casa, Su casa

The headline news, here, is: a staggering % of US respondents admitted to sharing passwords with colleagues. Interestingly, men were more likely to share their passwords with colleagues.

Perhaps surprisingly, only a very small proportion of people said that sharing their passwords with colleagues made them uncomfortable.

Young people between the ages of 16–24 are much more likely to 'frequently' share passwords with their colleagues, with 13% saying that this is something they do. This drops to 6% for 45–54 year olds and 3% for 55+ year olds.

To further emphasize this difference between the generations, we can examine the responses from people who said that they 'never' share their passwords.

16–24	25–34	35–44	45–54	55+
33.3%	41.4%	48.4%	54.1%	52.4%

It is clear that older people are more likely to NOT to share passwords within the workplace.

The main conclusion that can be drawn from this question, is that password sharing is incredibly common, and rather than trying to prevent the practice, the most sensible approach would be to try and manage it properly, ensuring passwords are shared efficiently and securely.

International Comparison

Our research included respondents in the USA, UK and France. We found several interesting trends and comparisons across the three regions:

Tools used to store and share passwords

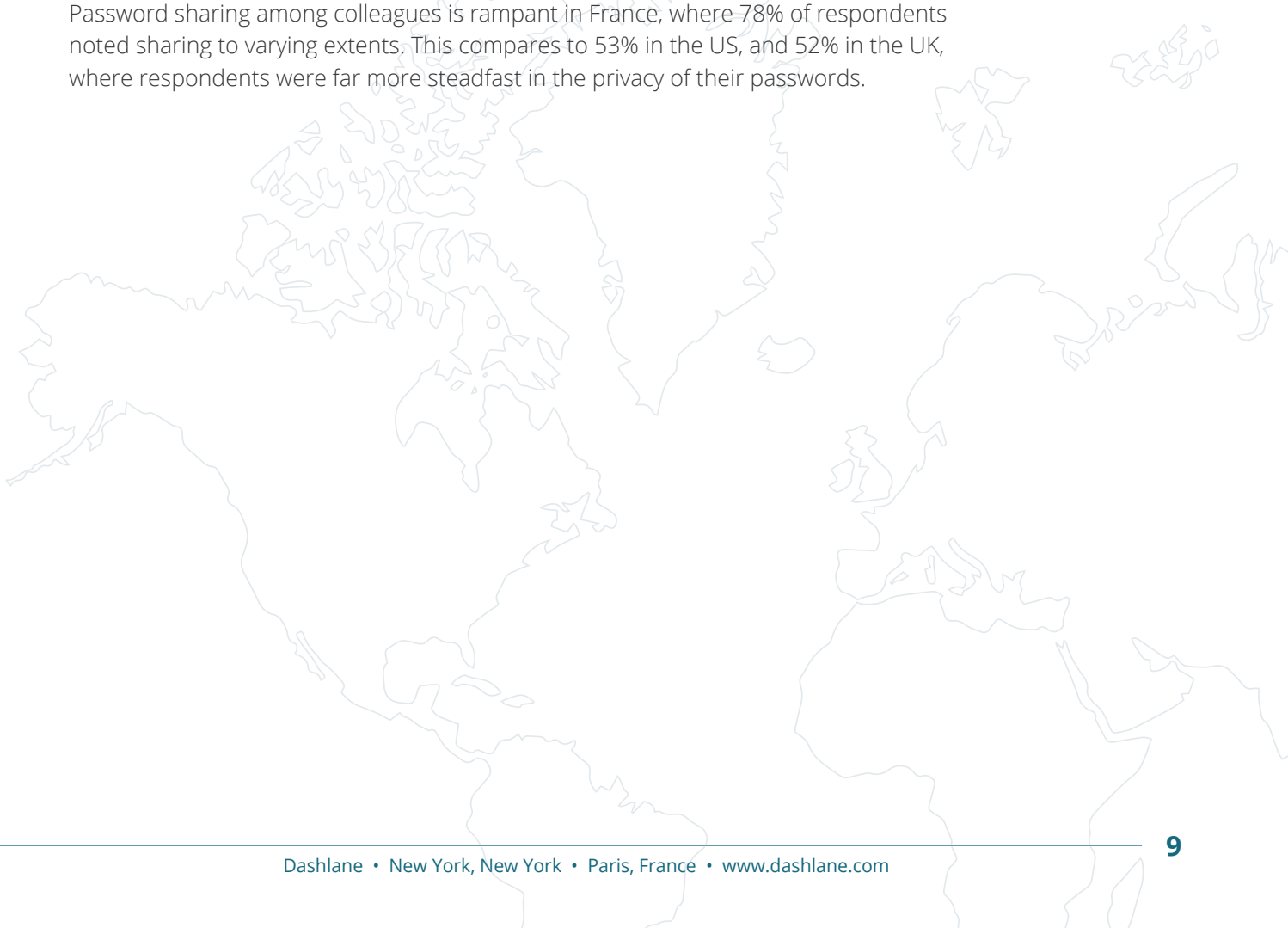
Workers in US and France generally demonstrated a more laid-back approach to security, with 30% in the US and 31% in France suggesting that they write passwords down on pieces of paper. In the UK, this was lower at 20%.

State of password sharing policies

French organizations appear to be further ahead in terms of implementing and communicating password policies, with 45% of respondents noting that their employers used this practice, compared to 39% and 36% in the US and in the UK respectively.

Sharing of passwords amongst colleagues

Password sharing among colleagues is rampant in France, where 78% of respondents noted sharing to varying extents. This compares to 53% in the US, and 52% in the UK, where respondents were far more steadfast in the privacy of their passwords.



The Dashlane View:

Work To Be Done

When we commissioned this report, we had our suspicions that workplace security was lax. After our analysis of the results we continue to believe that much work remains to be done.

First, we should admit that there are encouraging signs. High profile breaches of both corporate and personal information have thrust the issue into the limelight. There is clearly increased awareness surrounding password and security policies than in years past. However, if you were to ask if we think company data and information is mostly safe and free from external threats, the answer is a resounding "no".

The greatest challenge to organizations that want to protect their data and business is properly enabling the influx of Millennials entering the workplace to use and share company accounts and tools in a secure way. This generation that has grown up with the likes of Facebook, Twitter and Instagram — a society where everything is shared. Research reveals that this age group is more relaxed when it comes to their security and passwords. This is undoubtedly affecting the business world, where personal approaches to sharing and security are seeping into corporate practices. Don't forget, these employees grew up with smartphones, tablets and personal computers at home, school and work. The age of Bring Your Own Device, only causes greater risks for IT departments and SME owners.

As a result, business leaders, of organizations of all sizes, need to educate their employees about the importance of password security. They need to instill the thinking that all workers, no matter where they are on the corporate ladder, are on the front line of defense from potential hacks.

Password sharing doesn't have to be a bad thing. It can make a company much more efficient, but it needs to be done the right way. The sooner companies are able to implement effective password management the sooner we can rid businesses of digital indifference. Implementing effective password management (an unbelievably simple process) will foster more innovation, prosperity, and profitability.

Methodology & Credits

The Passwords in the Workplace Report was compiled in September 2015 using an online survey of 3,000 employees, who use a computer in their daily tasks, in the US, UK and France. The research was carried out by Opinion Matters.

About Dashlane

Dashlane makes identity and payments simple with its password manager and secure digital wallet app. Dashlane allows its users to securely manage passwords, credit cards, IDs, and other important information via advanced encryption and local storage. Dashlane has helped over 3 million users manage and secure their digital identity, and has enabled over $2.6 billion in e-commerce transactions. The app is available on PC, Mac, Android and iOS, and has won critical acclaim by top publications including **The Wall Street Journal**, **The New York Times,** and **USA Today**. . Dashlane is free to use on one device, and Dashlane Premium costs $39.99/year to sync between an unlimited number of devices.

Dashlane was founded by Bernard Liautaud and co-founders Alexis Fogel, Guillaume Maron and Jean Guillou. The company has offices in New York City and Paris, and has received $30 million in funding from Rho Ventures, FirstMark Capital and Bessemer Venture Partners. Learn more at Dashlane.com.