2018

Psychology of Passwords:

Neglect is Helping Hackers Win

LastPass ••• |
by LogMeIn

Table of Contents

Global Cyber Threats Skyrocket but Password Behaviors Unchanged

The cyber security threats facing enterprises have never been greater than today. In the time it takes for you to read this sentence, there will be approximately 180 data records stolen, with more than five million records breached daily.[1]

Big-name organizations continue to fall victim, with Target, Equifax, Yahoo!, and Uber showing that no organization is immune. Those who've been breached pay dearly, with the **average total cost of a data breach totaling $3.62 million in 2017**, due in large part that it takes an average of 191 days for organizations to identify a breach and 66 days to contain one.[2]

We were curious, with the increased threat landscape and the world's heightened awareness of cyber threats, have individuals' behaviors related to creating, changing and managing passwords evolved? Are employees more vigilant now about password security than in 2016, when we conducted our first survey on the topic?

The Findings

Password behaviors remain largely unchanged from two years ago — translating to some pretty risky behaviors.

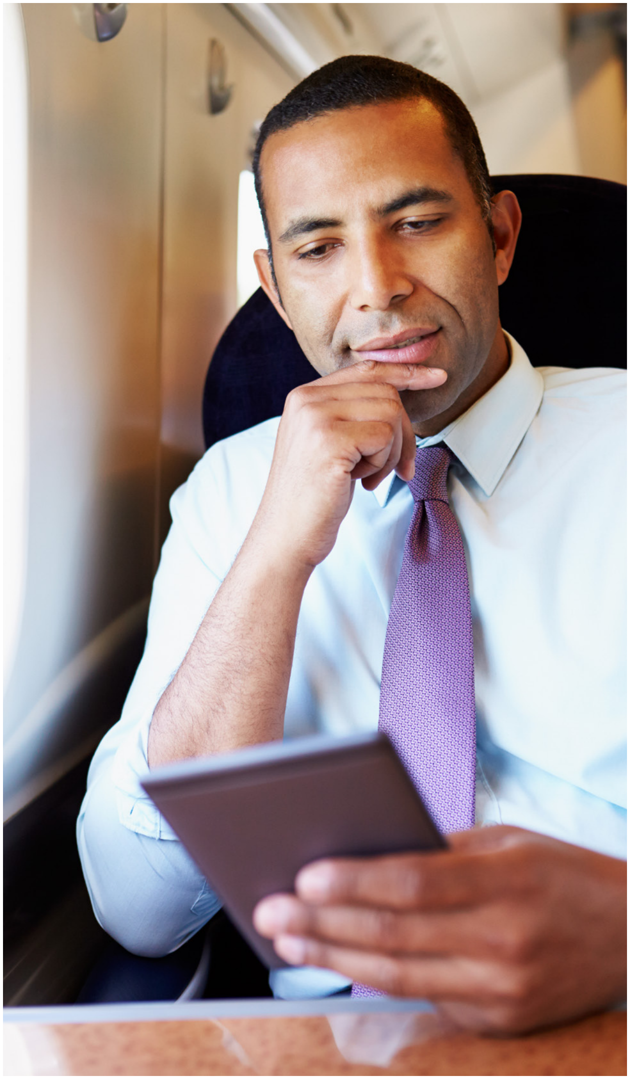
Most individuals still use the **same passwords for multiple accounts**, haven't changed a password in the last year (despite a breach in the news) and indicate there is no difference between passwords created for work and personal accounts.

[1] Breach Level Index, March 16, 2018
[2] Ponemon Institute 2017 Cost of a Data Breach Study, June 2017

In some cases we found that the ongoing news cycle about security breaches has had the opposite effect on password behaviors. For example, only 22% of respondents reported changing passwords when they heard about general industry security issues — down from 25% in 2016. In addition, 57% say a major retailer/ bank breach would make them change a password for an online account to a more secure password— down from 61% in 2016.

But, that's not all. Read our eBook to discover:

- Top factors driving the widespread reuse of passwords
- The reality of workplace password hygiene
- How Type A and B personalities approach password security
- Which online accounts result in more secure password behaviors
- Global differences in password creation and management
- Adoption trends for password management tools



Respondent Demographics

In partnership with Lab42, we conducted a global survey to learn more about how individuals create, change and manage passwords — and what drives the behaviors.

We had 2,000 respondents across five countries and compared the data to a similar survey conducted in 2016, where relevant.

Respondents

2000

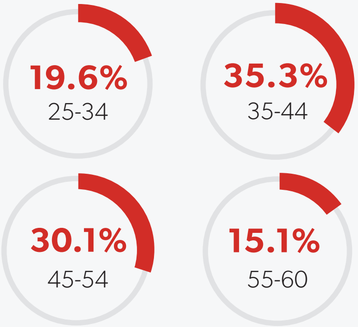
Gender

MALE
50.4%

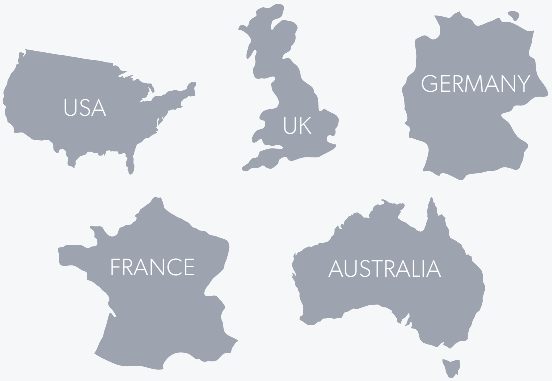
FEMALE
46.7%

Ages

25-60



Regions covered



Findings at-a-glance

Password beliefs don't mirror actions

91%

know that using the same passwords for multiple accounts is a security risk, yet 59% mostly or always use the same password

91%

Work and personal lines are blurred

47%

say there is no difference in passwords created for work and personal accounts

47%

News headlines don't spur password changes

53%

have not changed a password in the last 12 months after a breach in the news

53%

Not even a breach to their own account drives password movement

If their account was hacked, only

55%

would update the password for that account

55%

Many think they are immune or not a target

51%

believe there is no way a hacker could guess one of their passwords from information shared on social media

51%

There's denial about password risks

21%

do not believe that using the same or similar passwords causes an increased security risk to their accounts or information

21%

The number one reason for not changing passwords is…

61%

are afraid of forgetting login information

61%

This leads to passwords being stored on phone or paper

2 in 5

(42%) keep passwords in a file (on mobile device, handwritten note, Word, Excel, etc.)

42%

Germany is most proactive about regularly changing passwords

42%

change passwords regularly, on their own accord, because it makes them feel safer

42%

And, Type A personalities like to maintain password control

80%

of Type As need to know all of their passwords in order to feel secure

80%

Fear is Driving Password Reuse

When respondents were asked how often they use the same or a variation of the same password, the majority replied, "always" or "mostly." The fear of forgetfulness was the number one reason for reuse, followed by wanting to know and be in control of all of their passwords.

59% mostly or **always use the same password** or a variation of the same password

Why do you reuse passwords over creating a unique, more secure password?

- I'm afraid of forgetting my login information – 61%
- I want to be in control and know all of my passwords – 50%
- I don't think a hacker would target me – 18%
- I don't trust password management services or browsers with my login credentials – 18%

38%

reset passwords every few months because they couldn't remember them

Let's hope individuals don't forget where their password are stored.

- 42% keep passwords in a file (on a mobile device, handwritten note, Word doc, Excel spreadsheet, etc.)

Password Security Worries Don't Spur Action

The large majority of respondents are quite concerned about password security and accounts being compromised, particularly when they hear about a password breach in the news.

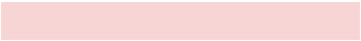
- **92%** feel that **password security is a serious matter**

- **88%** feel that **password hacking is a serious global threat**

- **83%** say that having a **strong password makes them feel like they are protecting themselves and their family**

- **79%** say that having **passwords compromised is something they are concerned about**

- **69%** are **fearful when they hear news of password hacking**



Yet, despite these concerns, many believe securing passwords only gets them so far.

- 90% believe that no matter how good a password, accounts are always at risk
- 87% feel other things outside of a weak password could compromise their online security

And, still others aren't buying the hype.

- 51% believe there is no way a hacker could guess one of their passwords from information shared on social
- 38% believe their accounts aren't valuable enough to make them worth a hacker's time

Attention IT: Password Behaviors Same at Work and Home

The vast majority of respondents (79%) report having between one and 20 online accounts for work and personal use, such as email, banking, social media and retail. And, when it comes to password creation, nearly half treat these accounts the same — regardless of whether they are used for work or personal matters.

- Number of online accounts for work and personal: 1-10 (47%); 11-20 (32%); 21-30 (11%); more than 30 (11%)
- 47% say there is no difference in passwords created for work and personal accounts
- Only 19% create more secure passwords for work
- 38% never reuse the same password between work and personal accounts – which means that 62% do

Germany (50%) **creates more secure passwords for work accounts** than other countries

Ages 18-24 most likely (45%) to **create stronger, more complex passwords** for work accounts

Which account would you create a stronger password for?

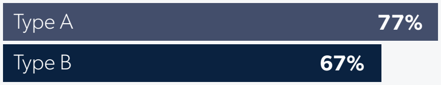
- Financial – 70%
- Email accounts – 53%
- Medical records/healthcare-related – 42%
- Work – 41%
- Retail/shopping – 39%

Type A Personalities Live up to the Stereotype

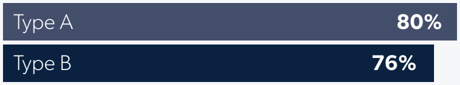
For the most part, Type A respondents were in line with temperament characteristics, showing a need for control when it comes to password creation and management.

Type A personalities pride themselves on being educated about password best practices and worrying about password hacking when discussed in the news.

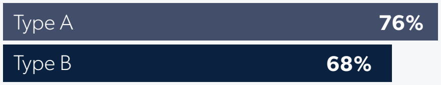
I put a lot of thought into my passwords



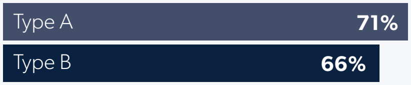
I need to know all of my passwords in order to feel secure



I consider myself informed on password best practices

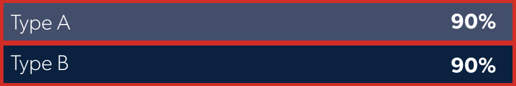


I am fearful when I hear news of password hacking



No personality difference for:

No matter how secure my password is, my accounts are always at risk



Tech-savvy Millennials Most Likely to Reuse Passwords

We typically think of millennials as pretty comfortable with and well versed on technology. Yet, our survey revealed surprising password behaviors and a lack of concern about being a target of a breach.

The youngest demographic is most worried about memory.

- 63% reuse passwords because of fear of forgetting
- 67% use a variation of 1-2 passwords they can remember

But, 33% say they can guess their significant others' passwords

And, feel somewhat invincible.

- 72% consider passwords sufficient protection for online information
- 34% do not believe they are a target and therefore don't feel the need to put much thought into passwords
- 56% believe that there is no way a hacker could guess one of their passwords from information posted on social media
- 44% think their account isn't valuable enough to make them worth a hacker's time

Password Security Keeps Baby Boomers Up at Night

62%

have **proactively changed a password** in the last month

Among the three age demographics, individuals ages 55+ recognize the severity of the current threat landscape and are most concerned about having passwords breached.

- 95% feel that password security is a serious matter
- 89% feel that password hacking is a serious global threat
- 81% are concerned about having passwords compromised
- 72% are fearful when they hear news of password hacking

They don't just worry; they act.

- 52% know it's a best practice to create a unique password for each online account

Top Five Contradictions: Security-conscious Thinking Doesn't Translate to Action

We all know that flossing is good for us, but yet many don't do it — despite telling the dental hygienist the opposite.

A survey found that **in reality only 30% of people actually floss every day** (and 32% never at all – gasp!)[3]

Our research uncovered similar contradictions, with respondents saying one thing and in turn, doing another.

1 **72% say they feel informed on password best practices**
Yet, of those, 64% say having a password that's easy to remember is most important

2 **91% recognize that using the same or similar passwords for multiple logins is a security risk**
Yet, 58% mostly or always using the same password or variation of the same password

3 **51% of Type As know it's a best practice to create a unique password for each account and follow this**
Yet, 45% have a personal "system" for creating passwords (e.g., use the name of the account plus numbers that have meaning)

4 **69% are fearful when hear news of password hacking**
Yet, only 55% would change their password if their account was hacked

5 **Nearly half of respondents (47%) cite having between 1-10 online accounts**
Yet, our Password Expose showed that the average employee (using LastPass) has to keep track of 191 passwords — revealing that people often underestimate the number of accounts they truly have

[3] National Health and Nutrition Examination Survey, June 2016

Global Snapshot: Prevailing Behaviors by Region

U.S. and Australia most likely to take action in face of breach

- 60% update all personal passwords if an account is hacked
- 43% add two-factor authentication to all accounts if an account is hacked

Germany leads the way with proactive security measures

- 72% prefer secure over easy to remember passwords
- 84% put a lot of thought into passwords they create
- 60% create secure passwords for personal and work accounts because security is important to them

France most concerned about password security risks

- 90% believe password hacking is serious threat
- 90% believe that other things outside of a weak password could compromise online security

Yet, 34% (more than any other country) **feel the talk about password protection is overrated**

UK in security denial

- 73% consider their passwords sufficient protection for online information
- 58% believe there is no way a hacker could guess one of their passwords from information shared on social media
- And, most likely (28%) to reset passwords at least once a month because they couldn't remember them

Even Breaches Don't Spur Password Changes

Not only do most respondents (59%) use the same password for multiple accounts, but many continue to use that password as long as humanly possible — until required by IT to update or if impacted by a security incident.

- 39% say if it's not required, they never change their password

What would drive respondents to proactively change passwords?

- One of their online accounts was hacked – 69%
- Identity theft (personal) – 65%
- Major retailer/bank breach – 59%
- Identity theft of someone close to them (family, friend, etc.) – 50%

48% have not changed password in last 12 months after a breach in the news

Changing passwords is more of a drag than laundry.

- 15% would rather do household chores than change their password
- 11% would rather sit in traffic
- 9% would rather wait on hold with a customer service agent

Adoption of Password Management Tools up from 2016

Ages 35-54 **most likely to choose a password manager** because of mistrust of the security of browsers (46%)

One of the positive trends in this year's survey is the increased use of password management tools. More individuals are embracing more secure password storage and automated password resets (to eliminate the fear of forgetting) to making going online easier and safer.

- **16% use password management tools** – up from 11% in 2016

LastPass remains at the top spot, used by more than a quarter of respondents. Here are the top five solutions in play:

- LastPass (27.3%)
- Keeper (20.9%)
- 1Password (18.4%)
- KeePass (18.7%)
- Dashlane (12.9%)

The Smart Fix for Chronic Password Neglect

The cyber threats facing organizations and consumers are real, with 81% of data breaches in 2017 involving weak, reused or stolen credentials — up from 63% in 2016. Yet, there remains a huge disconnect: individuals do not recognize the critical role that passwords have in protecting personal and work information and continue to reuse the same passwords again and again. Plus, they falsely believe they are not a target for hackers. And, even if breached, that would not necessarily be a tipping point for a proactive password change.

Will there be a tipping point?
If the alarming rise of cyber-attacks has not resulted in meaningful password behavior shifts, organizations and consumers can take the burden of responsibility off of the individual and make password creation and management an automated and simplified experience.

Password management tools give individuals the desired balance of security and convenience — and make the worry of forgetting passwords a thing of the past. Automated password creation, centralized storage and the same high level of password security applied to all accounts — work, financial, social media and others. Individuals can ditch the password spreadsheets and enterprises can rest assured that employees' passwords for sensitive work accounts aren't also being used on Instagram or Facebook.

LastPass is the number one most preferred password manager — trusted by 13 million people and 33,000 businesses. We believe that security starts with strong passwords. Learn more about LastPass for individuals, families and business teams of all sizes at www.lastpass.com.

LastPass •••|
by LogMeIn