

PSYCHOLOGY OF PASSWORDS:

**THE ONLINE
BEHAVIOR THAT'S
PUTTING YOU AT RISK**



COGNITIVE DISSONANCE PREVAILS – WILL 2020 BE THE TIPPING POINT FOR BEHAVIOR CHANGES?

Our Psychology of Passwords report examines online security behaviors of 3,250 global respondents, and it shows that people aren't protecting themselves from cyber security risks even though they know they should. Cognitive dissonance prevails.



53%

haven't changed their password in the last 12 months even after hearing about a breach in the news.



42%

say that having a password that's easy to remember is more important than one that is very secure.

As more and more people work and socialize online, protecting your digital identity is more important than ever. Unfortunately, we've seen a spike in hacking attempts – including malware from unvetted software downloads and an increasing number of phishing attacks.

Will this finally be the tipping point that causes people to show more concern for their online data?

This survey data serves as a benchmark to show the current state of online user behavior and will explore the good, the bad and the ugly. Read on to learn more from your peers and ensure you don't make the same mistakes.

PEOPLE KNOW WHAT'S RIGHT, BUT THEY DO THE OPPOSITE

Our survey shows that most people believe they are knowledgeable about the risks of poor password security; however, they are not using that knowledge to protect themselves from cyber threats.

What people say

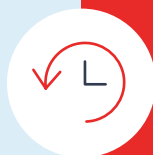
91%

91% say they know using the same or a variation of the same password is a risk ...



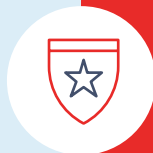
80%

80% agree that having their passwords compromised is something they're concerned about ...



77%

77% say they are informed of password protection best practices ...



What people do

66%

... however, when creating passwords, 66% of respondents always or mostly use the same password or a variation – this is up 8% from our findings in 2018.

48%

... and yet 48% said if it's not required, they never change their password - which is up from 40% in 2018.

54%

... however 54% keep track of passwords by memorizing them

DON'T UNDERESTIMATE YOUR RISK

While the contradictions from our survey are concerning, they do show us that people are thinking about password security and consider themselves well informed. So why aren't they using that knowledge to protect themselves?

Part of the problem is they are underestimating their risk.

Many people don't realize how much of their lives are online. When asked how many online accounts they had, **71% of respondents said 1-20**. However, according to anonymized LastPass user data, **the average LastPass personal user has approximately 38 online accounts** - almost double what the survey respondents think they have.

Why does this matter?

Each online account is a vulnerability point that can be breached, and people don't realize how many points of entry hackers have to their lives. This number of online accounts will only rise as socializing and working online becomes the new norm.

**How many online accounts
people think they have**

1-20



**How many online accounts
people have on average**

≈ 38

Everyone is a target

People also underestimate how valuable their information is.

42% of respondents think their accounts aren't valuable enough to be worth a hacker's time.

Hackers breach large consumer sites to steal the entire database of customer information.

While your credit card number might only get a hacker **US \$5 on the dark web**¹, if they steal hundreds of thousands of pieces of data in one fell swoop, it adds up. And then those hackers use the information stolen from one site, to gain access to a more important site like online banking. **Don't let your guard down.**

How many people think their accounts aren't worth a hacker's time

42%



YOUR NEED FOR CONTROL IS PUTTING YOU AT RISK

Password reuse is the biggest password security error being committed by our survey respondents. When asked how frequently they use the same password or a variation, **66% answered always or mostly** – which is **up 8% from our 2018 survey findings**.

No change since 2018?

Cognitive dissonance continues to be the trend here. Respondents intellectually know

what they should do, but they aren't taking action. **Why?**

People seem to be numb to the threats that weak passwords pose. Technology like biometrics is making it easier for them to avoid text passwords all together and many people are simply comfortable using the “forgot password” link whenever they get locked out of their accounts.

When asked why they reuse passwords, respondents had almost identical responses as they did in 2018:



60%

I am afraid of forgetting my login information



52%

I want to be in control and know all of my passwords

This need for control is understandable but misguided. While you may feel safe knowing all your passwords are the same, reusing passwords puts you at a much greater risk than when you create a unique password for each account.

Also, trying to remember all your passwords isn't working.



25%

reset their passwords once a month or more because they forgot them

And since we have to remember them, they aren't strong enough and are predictable:



22%

said they could guess their significant other's password



Why is password reuse so risky?

Reusing the same password across all or most of your accounts means that if a hacker gains access to one of your accounts, they have access to all. Also, if you use the same passwords at home and at work, you're putting your organization at risk of breach as well.

WHAT MORE CAN YOU BE DOING TO SECURE YOUR ACCOUNTS?

In addition to creating strong, unique passwords – which is an essential first step – there are other tools that can be used to protect online accounts.

Multifactor authentication (MFA) is an additional layer of security that can be added easily. The good news is there is broad awareness and usage of MFA. **Only 19% of survey respondents** said they **didn't know what MFA** was. **54% of respondents** said they use it for their **personal accounts** and **37% use it at work**.

Respondents are also very comfortable with biometric authentication – using your fingerprint or face to login to devices or accounts. **65% said they trust fingerprint or facial recognition more** than traditional text passwords. The comfort with biometrics is likely due to frequent use on mobile devices.



What is multi-factor authentication?

MFA is a tool that requires you to have more than just your username and password to log in to an account. After you enter your username and password it also requires a second piece of information – like a one-time code or your fingerprint.

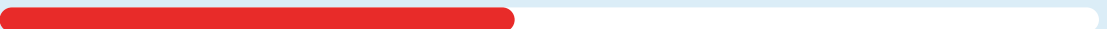
USERS ARE VIGILANT ABOUT THEIR EMAIL AND FINANCIAL ACCOUNTS

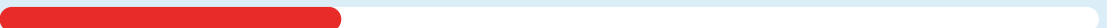
Respondents recognized that email and financial accounts needed extra protection, which is a smart instinct. Your email address is the hub of your online life and often contains information that hackers can use to steal your identity and access other accounts. Your financial accounts are obviously critical because they provide access to your money, credit information and other sensitive data.

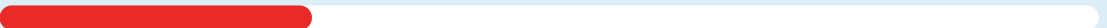


What accounts would you create stronger passwords for?

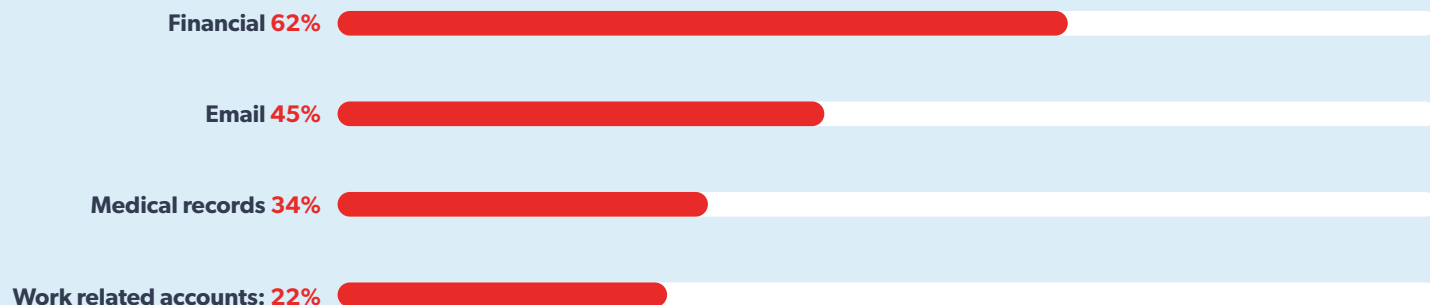
Financial 69% 

Email 47% 

Medical records 31% 

Work related accounts: 29% 

For which accounts do you have multi-factor authentication enabled?



It's encouraging to see that people understand how critical it is to protect their email accounts and financial data. However, it's imperative that everyone extends these protections to all their accounts.

Businesses take note!

Respondents are protecting their work accounts at a lower rate than their personal. We can see that security behaviors are flawed for personal data, and these bad habits extend into your business.

REGIONAL SNAPSHOT

Our report so far has been considering global data, but do the trends change if we look at them by country?



Germany is aware of the risk

While **GDPR** may be highlighting the risk of poor data privacy protection, it's not encouraging the right behaviours.

94% know the risk of using the same or similar password yet 30% use a variation of 1 or 2 passwords and a further 30% are not concerned about having their password compromised.



Brazil is showing promise

Pending **LGPD** regulation will increase vigilance online.

94% of Brazilians are concerned about having their passwords comprised and 64.8% agree that their accounts are valuable to a hacker.

With 78% trusting biometrics more than traditional passwords – MFA could be the additional layer of security they need.



Singapore is leading by example

Given the focus on creating and sustaining a vibrant **digital economy**, it's no surprise that 88% of people know that using the same or a variation of the same password is a risk. This could be the reason why:

40% create a stronger, more complex password for their work accounts.

MFA is actively used across work and personal accounts – 58% and 70% respectively!

**The UK has the most online accounts**

Even with the **NCSC** driving awareness of online best practice, it is not hitting home as 58% did not change their password even after a breach in the news!

92% know that using the same or similar password is a risk, but they do it anyway

64% of people reuse passwords due to the fear of forgetting them.

**Australia has the greatest work and personal overlap**

With the high profile **NDB** reports detailing data breaches and their sources, its positive to see that 80% consider themselves well informed on password best practice, but:

Only 18% create a complex, unique password for their work account, and for 36% there is no difference between work and personal passwords.

And while 90% know it's a risk, 69% mostly or always use the same or a variation of the same password.

**United States password behavior is poor, but MFA use is strong**

60% are afraid of forgetting their login information and therefore 33% write them down

67% trust biometrics more than traditional text passwords

42% use MFA for work accounts and 58% for personal accounts – the highest of any region except Singapore

STOP PUTTING YOURSELF AT RISK

You have a lot on your plate trying to keep yourself and your family safe. It may not have occurred to you to extend those efforts to your online life – but doing so does not have to be difficult.

Let this year be the tipping point for a change in behavior

Let a password manager remember and fill your passwords. We know you want to be in control – but it's safer to create strong, unique passwords for each account and store them in an encrypted vault. You no longer have the stress of remembering them and you know they are safely stored for when you need them.

Use multi-factor authentication. Start with the essential and most-used accounts like email, banking, credit cards, taxes, social media. Then each time you sign up for a new account check if it offers MFA and enable it if so.

Monitor your data. Whether you use credit monitoring through your credit card or bank or enable dark web monitoring services, make sure you know when your information has been compromised.

LastPass is trusted by over 17 million users and 61,000 businesses to store and fill passwords, credit cards and other personal information. Use LastPass to generate strong passwords for you and fill them automatically when you visit sites and apps – across all of your devices.

Learn more about LastPass for individuals, families and businesses of all sizes at www.lastpass.com.



Sources:

1 <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>