LastPass •••|

Psychology of Passwords

Employee (mis)behaviors that are putting your business at risk.

Increase security and compliance without adding complexity.

With personal and professional lives merging at unprecedented rates, strong password hygiene is critical to your business's success and security. IT teams must adapt to ensure employees' credentials remain secure in a work-from-anywhere world.

The Psychology of Passwords report explores the password behavior of 3,750 professionals worldwide and can help your business:

- **Become more security conscious** and improve password hygiene.
- **Learn best practices** to eliminate password reuse and securely store passwords.
- **Set goals** to achieve comprehensive security awareness in a remote work landscape.

LastPass Business empowers your workforce by removing friction for users and IT teams. **Save time by simplifying employee password management while granting admins actionable oversight,** from advanced reporting to 100+ customizable security policies.

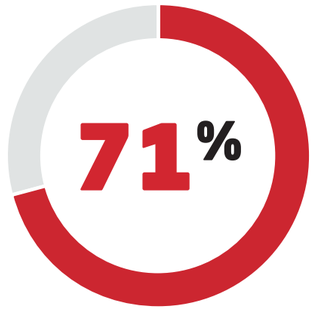
To learn more, visit
lastpass.com/business

Password security in 2021: outsmarting human vulnerabilities.

The COVID-19 pandemic disrupted the workplaces of millions worldwide. Physical offices shuttered. Many people transitioned to working from home. With nowhere to go, they spent more time online.

Individuals and businesses are more at risk than ever.
Hackers are taking advantage and exploiting human vulnerabilities more than ever. The types of attacks have shifted given the large number of people working remotely and spending more time online.

During the pandemic:



Worked wholly or partly remotely.

Spent more time online for personal entertainment and work.

According to the 2021 Data Breach Investigations Report (DBIR), Cybercriminals are increasingly targeting individuals and their devices.

85%

Most data breaches – a staggering 85% – involved a human element (phishing, stolen credentials, and human error).

36%

36% of breaches last year involved phishing – 11% more than before.

Survey Overview

Our Psychology of Passwords report explores the password security behaviors of 3,750 professionals across seven countries. We asked respondents about their feelings and behaviors regarding online security.

Countries surveyed:

- United States
- United Kingdom
- Germany
- France
- Australia
- Singapore
- India

Lots of awareness, not enough action.

What people say.

79%
Agree that compromised passwords are concerning...

92%
Know that using the same password or a variation is a risk...

What people do.

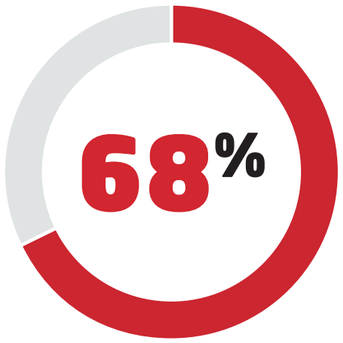
51%
...Rely on their memory to keep track of passwords.

65%
...Always or mostly still use the same password or variation.

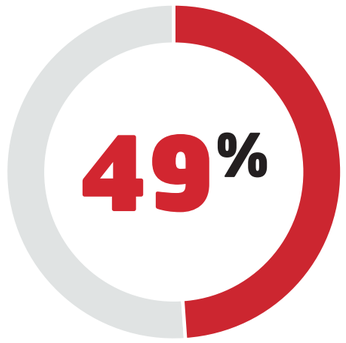
45% DID NOT CHANGE THEIR PASSWORDS

45% of survey respondents did not change their passwords in the past year even after a breach had occurred.

People practice selective password security but would create stronger passwords for:



Financial Accounts



Email Accounts

Work-Related Accounts

Medical Records

8%

Only 8% said that a strong password should not have ties to personal information.

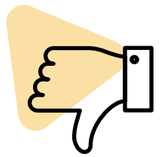
This means most users are creating passwords that leverage personal information that has ties to possible public data, like a birthday or home address.

PRO TIP

Enforce nonsensical phrases peppered with numbers and symbols as opposed to individual words to make your employee passwords longer, stronger, and easier to remember while also more difficult for hackers to crack.

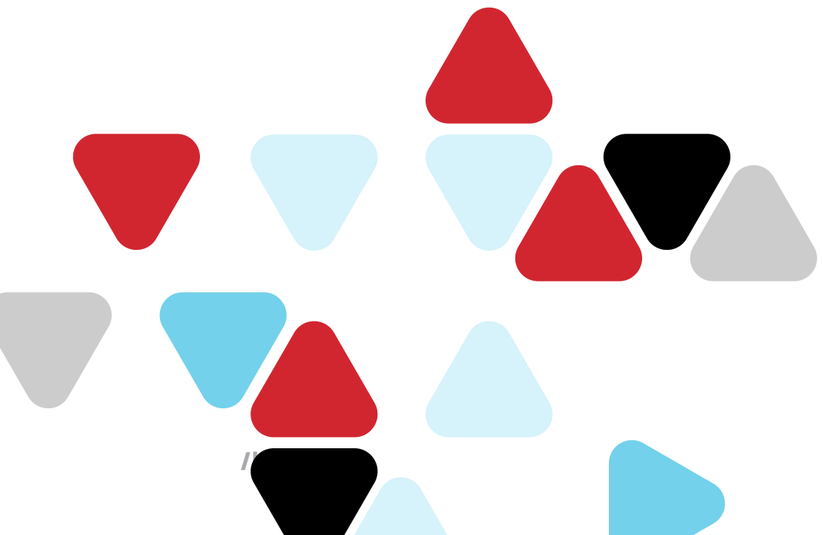
Blind spots and bright spots.

Cognitive dissonance prevails. People pick and choose what information they think is worth protecting. As a result, they knowingly engage in risky password behaviors, even when spending an unprecedented amount of time online for work and entertainment during a pandemic.



83% would not know whether their information was on the dark web.

76% claim to use MFA for both work and personal reasons, a 10% increase from last year.



PRO TIP

Treat all credentials as vulnerable. Your employees might not think their local gym password is valuable to hackers, but if those credentials are identical to those they use at work, a breach at your gym could mean sensitive financial information is exposed too.

Digital life expansion.

More accounts than ever before.

91% of respondents have created at least one new account this year.

90% of respondents indicate they have up to 50 online/app accounts.

50% Respondents have 50% more accounts in 2021 than in 2020.

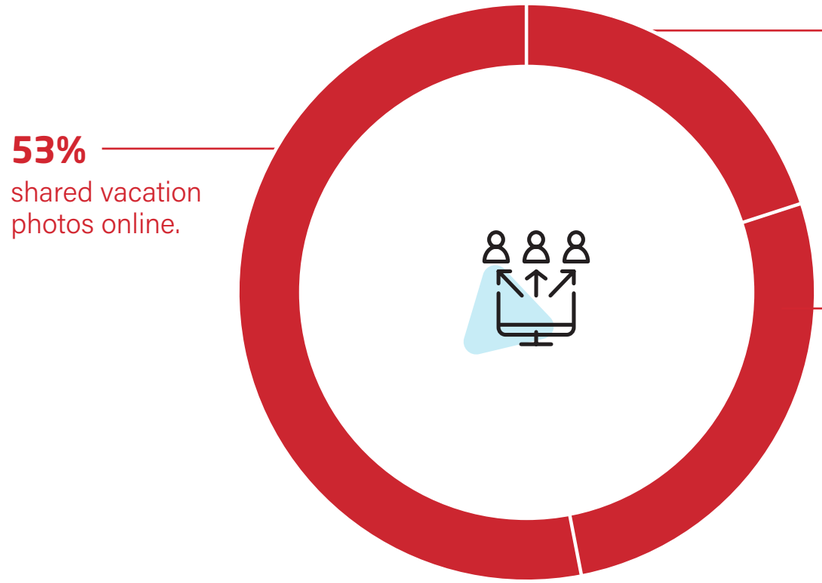
As we grow our digital presence, employees and businesses need more robust protection.

Digital lives expanded greatly during the COVID-19 pandemic. The disconnection motivated us to connect more online than ever. The result: more accounts created, and more personal information shared online.

PRO TIP

Malicious actors scrape public profiles and can use seemingly harmless information to hack accounts outside of your social media. Encourage employees to keep personal updates and social media private.

The amount of personal information online is increasing:



53%
shared vacation photos online.

20%
shared photos of their pets with their names then used their names in passwords, **up 5% from 2020.**

27%
shared photos of their house/neighborhood, **up 7% from 2020.**

Remote work: employee and employer perspectives.

Employee
remote work habits:

47% Did not change their online security habits since working remotely.

46% Did not strengthen their passwords while working remotely.

44% Shared sensitive information and passwords for professional accounts while working remotely.

Employer
remote work habits:

39% Made sure employees logged on the company network via secure networks while working remotely.

35% Made employees update their passwords more regularly.

35% Enhanced authentication methods.

IT admins must pay attention. The presence of risk does not inherently motivate people to adopt better security. Almost half of employees engage in risky password behavior while working remotely.

IT admins must rethink their security strategies just as their employees reshape and reassess the way they work.

PRO TIP

Invest in a **password management** solution to improve password hygiene and security. Implement **SSO** and **MFA** to secure all points of access. Launch security trainings to educate and evangelize.

Regional snapshot:

United Kingdom

61% know that a strong and unique password does not have ties to personal information.

They were also the least likely to share personal information online **(41%).**

Germany

Germany leads the way when it comes to dark web knowledge **(79%).**

But, only **14%** would know if their personal information was on the dark web.

France

Only **15%** of French respondents worked remotely during COVID.

Only **43%** changed their online security habits if working remotely.

Singapore

Singapore is the most concerned when it comes to compromised passwords **(93%).**

They also lead the way when it comes to knowing what to do if they have been hacked **(74%).**

India

India is significantly more likely to use a password manager or browser to store passwords than other countries **(64%).**

Indian respondents led the way when it came to changing their online security habits while working remotely **(81%).**

Australia

71% of Australians always/mostly use the same password variation.

However, Australians spent less time online overall during the pandemic **(61%).**

United States

Americans were more likely to use credit monitoring services if their account was compromised **(31%).**

However, **39%** felt they didn't need to change their online security habits when working remotely because they were already strong.

Connecting the dots.

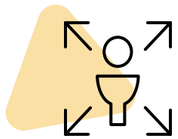
Why do people engage in bad password behaviors (when they clearly know better)?

68% Who reuse their passwords are afraid of forgetting them.

52% Who reuse want to be in control of all their passwords.

36% Do not consider their accounts valuable enough for hackers.

Why is password reuse so dangerous, especially as our digital lives expand?



One stolen username and password combination gives a hacker access to many accounts.

When a cybercriminal gets access to a device used for personal and work, they can quickly gain access to a corporate network to steal data or money.

PEOPLE ENGAGE IN BAD PASSWORD BEHAVIOR

With ever-expanding digital lives and lack of cybersecurity support, a combination of habits, emotions and lack of urgency keep people from changing their online behaviors.

Combatting password (mis)behaviors.

The COVID-19 pandemic brought unprecedented change in the way we work and interact. We spend more time online. We share more digitally. If we know why people are behaving the way they do, how can we fix this behavior?

What does good password behavior look like?

- Make every password unique.
- Use nonsensical combinations of characters.
- Turn on multi-factor authentication.
- Update passwords when notified of a breach.

Combat fear.

Use a **password manager** to manage and secure passwords. Let a password manager do the work of creating, remembering and filling in passwords.

Combat anxiety.

Add a layer of security with **multi-factor authentication (MFA)** to ensureyour employees are the only ones accessing business information and applications.

Combat apathy.

Monitor data and make sure you know when information has been compromised with **dark web monitoring.**

LastPass

LastPass Business reduces friction for employees while increasing control and visibility with a password management solution that is easy to manage and effortless to use.

LastPass Business empowers employees to generate, secure, and share credentials seamlessly, ensuring protection through LastPass' zero-knowledge security infrastructure.

Learn More