PSYCHOLOGY OF PASSWORDS SURVEY

THE PASSWORD PARADOX AND WHY OUR PERSONALITIES WILL GET US HACKED

LastPass •••|

Introduction

Despite high-profile, large-scale data breaches dominating the news cycle - from Mark Zuckerberg's Twitter account to a leak of millions of LinkedIn passwords - consumers have yet to adjust their online behavior. Experts continue to warn against password reuse and encourage strong, unique passwords. However, while consumers consider themselves cautious, their behavior says otherwise.

LastPass wanted to find out if there is a psychological reason behind risky password practices. Are people predisposed to creating weak passwords due to their comfort level with simple, easy to remember names and dates? Is the fear of forgetting a password a stronger motivator than the fear of being hacked? Is it simply a case of user apathy that they either don't care or don't see themselves as being at risk? Or, does it run deeper than that?

To further explore this issue, LastPass partnered with Lab42 to ask 2,000 adults around the world about their password habits, their beliefs and their understanding of what secure online behavior looks like. This summary of the findings underscores what many believe: although we know what safe passwords are, we tend to ignore this knowledge in favor of using easy-to-remember passwords. Furthermore, the traits that normally define us seem to have little bearing on our poor behavior, but do help us rationalize it.

A CLOSER LOOK AT THE ISSUES

» 19 people fall victim to identity theft every minute.[1]

» More than 500 million passwords were leaked so far in 2016 from the recent LinkedIn, Twitter and Myspace hacks.[2, 3, 4]

» It takes an average of 18 months and 200 hours of work to recover from identity theft.[5]

» 110 million American adults had their personal information exposed by hackers in 2014.[6]

» The average cost of a data breach based on a survey of 350 companies globally was $3.79MM in 2015.[7]

FINDINGS AT A GLANCE:

91 percent know there is a risk when reusing passwords, but 61 percent continue to do so

Only 29 percent of consumers change their passwords for security reasons - the #1 reason people change their passwords is because they forgot it

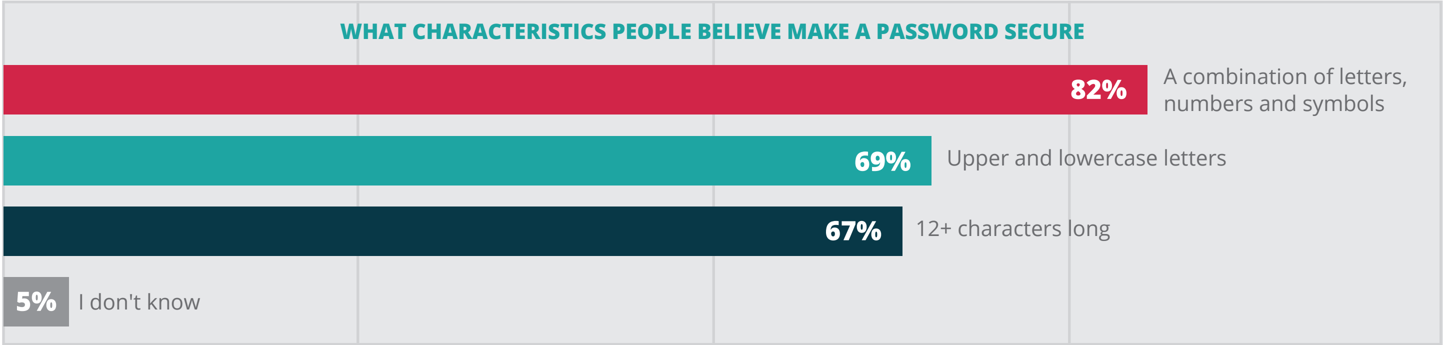
People prioritize their financial accounts (69 percent) over retail (43 percent) social media (31 percent) and entertainment (20 percent)

The Password Paradox

In the physical world, there are certain behaviors that are commonly accepted even though it's known they are bad for your health and well-being: you pick up your phone to answer an important call while driving even though it's dangerous, you overindulge during the holidays even though you know it will be reflected on the scale, or you open a pack of cigarettes to have just one after a particularly stressful day. The data collected through this survey suggests that the theory of **cognitive dissonance** also applies to a user's digital behavior: you know it's bad for you, but you continue to do it anyway.

COGNITIVE DISSONANCE
is the psychological conflict resulting from an individual performing an action that is contradictory to their beliefs, ideas or values.

To get a baseline understanding of what people do know about password best practices, respondents were asked about the characteristics of a secure password.



While users understand what a secure password looks like, they are still falling short when it comes to password creation. A number of users use the criteria below to create their passwords.

47% initials, friends or family names

42% significant dates and numbers

26% pet names

21% birthdays

14% hometown

13% school name or mascot

A strong majority (91 percent) of respondents stated that there is inherent risk associated with reusing passwords - yet nearly two thirds of them (61 percent) continue to use the same or similar passwords anyway, and 55 percent do so while fully understanding the risk.

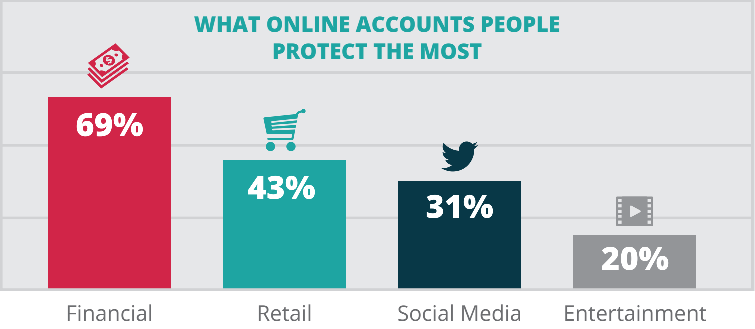
As with any other issue, there needs to be an understanding of how to change their behavior. In today's environment, just as it's important to pay attention to our physical health, we need to maintain a healthy online lifestyle.

KEY TAKEAWAY
We understand what makes a good password and why having one is important, but we continue to exhibit bad password behavior.

What You Prioritize

Cybercrime is most often motivated by opportunity. According to the Verizon 2016 Data Breach Investigation Report,[8] most attacks are opportunistic, indiscriminate and exploit known vulnerabilities. If you make your defenses good enough, attackers will move on to easier targets. Given that 63 percent of breaches in 2015 used weak, default, or stolen passwords, it is incumbent upon all users to create strong and unique passwords that contain a minimum of 12-14 characters made up of numbers, letters and symbols.

It's clear that users still partake in poor password behavior. To better understand how this behavior differs across accounts, respondents were asked about their priorities when protecting their online accounts.



WHAT YOU PROTECT MOST

The Verizon 2016 DBIR states that money remains the main motive for most cyber attacks, with 80 percent of analyzed breaches having a financial motive. When asked about what accounts they create more secure passwords for, the data was consistent with the motivation of cyber attacks.

While it may seem counterintuitive to put your Facebook profile on the same level as your savings account, reports indicate that this should be the case. So far in 2016, 657 businesses including retail and social media sites have reported data breaches compared to just 21 financial institutions.[9] If users are using the same or similar passwords across accounts - which a majority of respondents indicated - then they are also essentially handing the key to hackers to access their most critical information when they attack another, less important account.

PERSONAL VS. WORK HABITS

This poor password behavior also seems to flow into the workplace. More than a third (39 percent) of respondents said they create more secure passwords for personal accounts over work accounts. The first line of defense for businesses in protecting themselves from attacks is informed users. Business leaders should implement policies/tools to ensure users are safely sharing passwords and creating/using strong passwords.

KEY TAKEAWAYS

- Consumers should be protecting all accounts with the same level of security.
- Business leaders should educate employees about safe password practices and put policies around password updates to improve their security posture.

Why Your Personality Will Get You Hacked

To gain more clarity around why people exhibit poor password habits, even though they understand the risks, respondents were asked questions about their personality type. Do Type A personalities have better password behavior than Type B? Or do Type B personalities have more of an understanding around the risks but choose not to change their behavior out of laziness? With our personalities dictating so much of our behavior in the physical world, we wanted to understand if this translated to our lives online.

The results indicated that when it comes to online security, personality type does not seem to impact your behavior. Both Type A and Type B personalities had similar bad password habits. However, your personality does reveal how you rationalize this behavior. Our research uncovered the following character traits of both Type A and Type B personalities and the role these personality makeups play in creating or preventing stronger password habits. It appears that the driving factors around the cognitive dissonance toward passwords is rooted in our personalities.

TYPE A

Bad password behavior in Type A personalities stems from their need to be in control. Even though they reuse passwords, they don't believe they are personally at risk because of their own organized system and proactive efforts.

CONTROL

35% reuse because they want to remember all passwords

DETAIL-ORIENTED

49% have a personal "system" for remembering passwords

DELIBERATE

2/3 are proactive to help keep personal info secure

DRIVEN

86% having a strong password makes you feel like you're protecting yourself and your family

TYPE B

Type B personalities rationalize their bad behavior by convincing themselves that their accounts are of little value to hackers. This enables them to maintain their casual, laid-back attitude toward password security.

NONCHALANT

45% believe your accounts aren't valuable enough to make them worth a hacker's time

LAID BACK

43% prioritize a password that is easy to remember over one that is secure

FLEXIBLE

1/2 feel that you need to limit your online accounts and activities due to fear of a password breach

PREOCCUPIED

86% feel other things outside of a weak password could compromise your online security

KEY TAKEAWAY

Personality types don't seem to impact our online behavior, but do drive our rationalizations of poor password habits.

Conclusion & What's Next

Users generally understand the importance of having strong and distinct passwords. Three-quarters (75 percent) of our respondents indicated that they consider themselves informed on password best practices. However, much like with other known vices, they seem ill-prepared to effectively enforce good habits on their own.

Most admit to knowing better, but still implementing poor choices and tactics in creating and managing passwords for their digital lives. It further enforces the message that knowing the right thing to do and actually doing the right thing are completely separate discussions when it comes to password habits. There are many factors driving these behaviors, increasing complexity, growing numbers of accounts, and overall password/security fatigue. However, these breakdowns are what hackers count on to create easy opportunities to breach an account. If we are serious about establishing more effective defenses, we need a system that makes it easier for the average user to better manage their password behavior.

Looking ahead, we plan to take a deeper dive into the psychology behind what makes us avoid changing this behavior, even though we know it's bad for us.

About The Survey

The Psychology of Passwords survey was commissioned by LastPass and fielded by independent panel research firm Lab42 from May 4-18, 2016. The responses were generated from a survey of 2,000 adults, ages 18+ who have at least one online account. Survey respondents represented the United States, Germany, France, New Zealand, Australia and the United Kingdom.

SOURCES:

1. Clements, Nick. "How To Protect Your Credit Score When You Are An Identity Theft Victim." Forbes, 24 Aug. 2015, http://www.forbes.com/sites/nickclements/2015/08/24/how-to-protect-your-credit-score-when-you-are-an-identity-theft-victim/#72fd9d633f18.
2. Shu, Catherine. "Passwords for 32M Twitter Accounts may have been hacked and leaked." TechCrunch, 8 June 2016, https://techcrunch.com/2016/06/08/twitter-hack/.
3. McMillan, Robert. "Mark Zuckerberg's Twitter and Pinterest Accounts Hacked." The Wall Street Journal, 7 June 2016, http://www.wsj.com/articles/mark-zuckerbergs-twitter-and-pinterest-accounts-hacked-1465251954.
4. Meyer, David. "If You Ever Had a Myspace Account, This Hack May Affect You." Fortune, 30 May 2016, http://fortune.com/2016/05/30/myspace-data-hack/.
5. Federal Trade Commission. "Latest Data Breach Spotlights Need for Identity Restoration." BusinessWire, 7 October 2016, http://www.businesswire.com/news/home/20151006006149/en/Latest-Data-Breach-Spotlights-Identity-Restoration.
6. Pagliery, Jose. "Half of American adults hacked this year." CNN Money, 28 May 2014, http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/.
7. "2015 Cost of Data Breach Study: Global Analysis." Ponemon Institute and IBM, May 2015, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF.
8. "2016 Data Breach Investigations Report." Verizon Enterprise, April 2016, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.
9. "Identity Theft Resource Center 2016 Data Breach Stats." Identity Theft Resource Center, 9 September 2016. http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2016.pdf.