The Future of Security in the Hybrid Workplace

Patterns and trends in employees' workplace security habits that will help you futureproof your business—at home, in the office, or on the go

DASHLANE

CONTENTS

01 / Remote work—here today, not gone tomorrow

02 / Key findings and predictions

03 / Frustration? Indifference? A tale of many UXs

04 / So many screens... secure all of them

05 / One workplace, four (SECURITY) personalities

06 / The digital workplace of tomorrow

INTRODUCTION

Following what many have called the year of the great work-from-home experiment, new security concerns and risks have bubbled up, causing organizations to reprioritize their cybersecurity budgets. Remote work environments may be here to stay—but lax security policies need to go.

Nearly a third of Americans are online "almost constantly," according to Pew Research.[1] With the boundaries between work and home lives now blurred more than ever, it's important to understand how employees' internet habits and attitudes impact your company's security culture.

To assess these attitudes and behaviors—and their potential impact on organizations' cybersecurity—we surveyed 1,000 U.S. employees about their feelings toward technology, internet use, and online habits. We've discovered four clusters, ranging from "out of touch" employees to those who are "above it all," and have identified the barriers to creating a more secure culture for each of these groups so that you can stay ahead of these trends in the workplace.

Our research found that feelings toward being online range from enjoyment and appreciation to guilt and annoyance, with a lot of "meh" in between. These feelings influence your employees' actions and security habits. And, as we saw in 2020, explaining the risks of certain behaviors isn't always enough to get people to change their actions and habits.

In this report, we dig into our findings to help you understand what the realities of employee attitudes mean for the future of security in your workplace. We also dive into the implications of the ever-evolving work environment so that you can stay proactive and ensure adoption of your security policies and programs.

1 "About three-in-ten U.S. adults say they are 'almost constantly' online," Pew Research Center, July 2019.

SECTION 01

Remote Work— Here Today, Not Gone Tomorrow

Remote work → coffee shops, parks, beach, train, mountain side, hotel, friend's house, in a forest... the world is your oyster.

— SPOTTED ON TWITTER

Not that long ago, working from home in sweatpants was a perk available only to tech employees, independent workers, and other lucky few. The COVID-19 pandemic turned the workplace on its head, as an estimated 42% of U.S. workers hustled to set up office at home and entire companies went fully remote.[2]

Nearly overnight, working from home became as common in the workplace as emojis and memes. And remote work didn't move from the fringes temporarily. It's here to stay.

[2] "Stanford research provides a snapshot of a new working-from-home economy," Stanford, June 2020

Remote Work—Not Just a New Fad

+500%

forecasted increase of remote workers post-COVID [3]

72%

office workers who would like to work away from the office at least twice a week [4]

74%

chief financial officers who planned to shift some employees to remote work permanently [5]

53%

employees new to remote work who plan to do it more often in the future [6]

2x

increase in the permanently remote workforce expected by chief information officers [7]

3 "Widespread Shift to Remote Work Presents Massive Opportunities for Virtual Meeting Solution Providers," Frost & Sullivan, July 2020

4 "It's time to reimagine where and how work will get done," PwC, January 2021

5 "Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently," Gartner, April 2020

6 "COVID-19 Likely to Usher in "Decade of the Home," Accenture, August 2020

7 "Permanently remote workers seen doubling in 2021 due to pandemic productivity: survey," Reuters, October 2020

The remote or hybrid environment doesn't just mean trading the watercooler for Slack and huddling on Zoom instead of the meeting room.

It creates new risks for your business:

→ **Phishing attacks:** Hackers prefer easy targets—including a remote work environment that is likely less secure than the corporate perimeter. During the pandemic, for example, a quarter of employees surveyed by Deloitte reported a higher number of spam, fraudulent, and phishing emails sent to their corporate accounts.[8]

→ **Unsecure practices:** HaA reliance on cloud-based collaboration and sharing tools creates more instances of employees reusing passwords, connecting via unsecure or public WiFi, and using unpatched devices. That, in turn, creates a bigger attack surface.

8 "Cyber crime – the risks of working from home," Deloitte, April 2020

Not all businesses will give up the office for good. But the pandemic provided the perfect beta test for the virtual office and if nothing else, more employers will embrace a hybrid environment. Looking at the results of our study through the lens of these emerging workplace trends makes it clear that businesses need to rethink their security and address gaps such as laidback, risky processes.

SECTION 02

Key Findings and Predictions

What we make of the survey data

Security is not like a box of chocolates. You should always know what you get.

Our research found that many people have poor security habits, such as using unsecure practices to create and track their passwords and other account information. And they don't feel a significant amount of friction or frustration in doing so.

For businesses, this could mean real danger because it suggests that employees may not necessarily complain about workplace security policies and procedures—they may simply not follow them. Without a strong security culture or the right tools, they may view those policies as an inconvenience at best.

Think of a ‘90s throwback, dial-up internet.

Not a lot of people complained back then about the excruciatingly slow speed. Does that mean everyone was elated about waiting for long minutes for a simple website to load? Hardly. Any inconvenience was rolled into the cost of accessing the internet. Today, the inconveniences of living a digital life are different—such as having to reset passwords—but people view them as necessary pains just the same.

One thing has changed since the dial-up era. Online risks have exploded, leading to increased understanding about security concerns. But, as we saw from our research, even when people acknowledge that security is important, their risky online behavior says they think otherwise. And if your employees aren’t active participants in your security culture, eventually their frustration will lead to shortcuts that compromise your defenses.

Our findings indicate that IT leaders face several barriers to creating a strong security culture. Employee awareness and education is only one step to improving your organization’s security posture. Employee awareness training explains “the why.” What’s missing is “the how.” To implement better security, you need tools that enable employees to align their beliefs about security with their online behaviors—and to maintain good security hygiene.

Without these tools, you’re stuck with old habits. That’s not unlike being stuck with dial-up in the ‘90s. People knew a 56 Kbps connection was slow and inconvenient, but they simply didn’t have any speedier options. Fortunately, today you do have a variety of options that can provide employees convenience without sacrificing security.

The workplace as we know it will transform and employers will embrace flexibility.

Our survey found that the majority of people spend a great deal of their time online. In our always-on, never-miss-anything culture, this probably doesn't come as a surprise. What's changing is how and where employees are accessing your company data and other business-related resources.

The physical separation between personal and company spaces, devices, and even schedules will completely disappear. This is an opportunity for businesses to embrace flexibility and provide employees with tools and resources that support both personal and work needs and interests.

62%

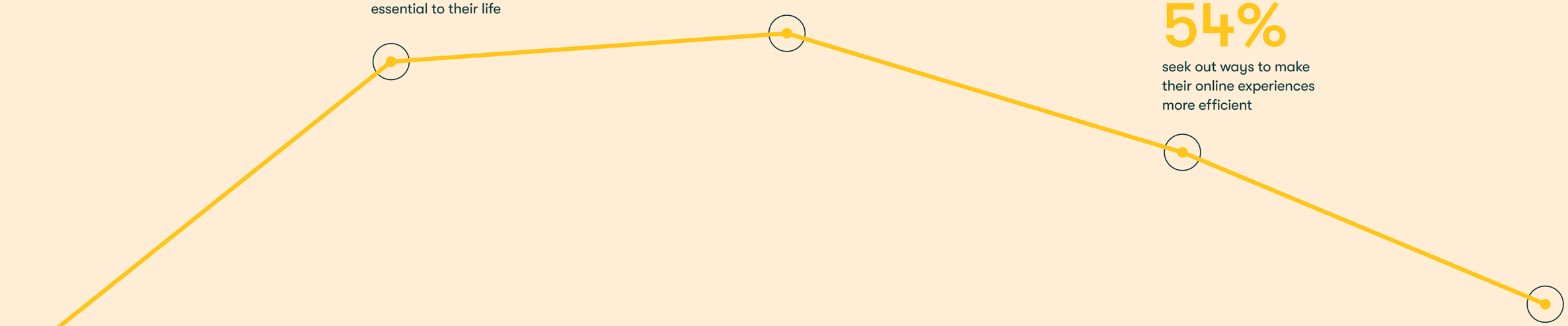
say fast access to online services and information is essential to their life

64%

prefer to take care of things online

54%

seek out ways to make their online experiences more efficient



38%

of our respondents spend a significant amount of their waking hours offline

43%

use their mobile devices more than their laptops and desktop computers

Employees will seek more convenience, and businesses will need to simplify employees' lives.

Our findings show that employees want to make their lives more efficient and convenient. Often, that means taking shortcuts to simplify things and eliminate stress.

As work and personal lives further intertwine, employees' personal online habits and attitudes will continue to bleed into the workplace. Businesses will take a closer look at the blended work/home lifestyles and provide new tools to simplify their employees' digital lives without compromising security.

35%

of respondents feel overwhelmed by keeping track of all their account information and logins

18%

feel they're wasting a lot of time trying to get into online accounts

48%

blame themselves rather than the app or service when they have difficulty logging in

48%

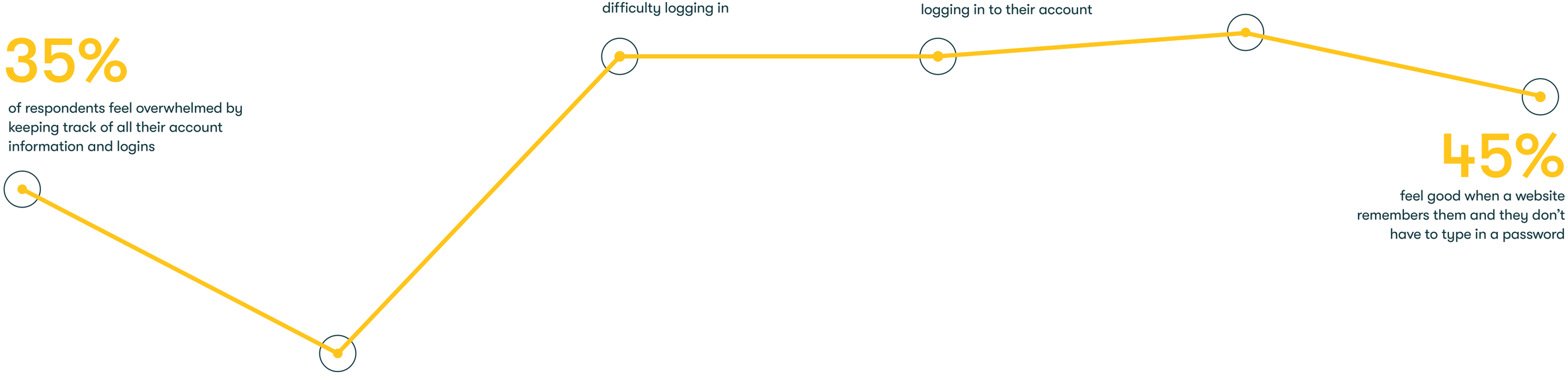
say every website or app they use requires a different set of steps for logging in to their account

49%

create their own tricks and shortcuts for managing logins

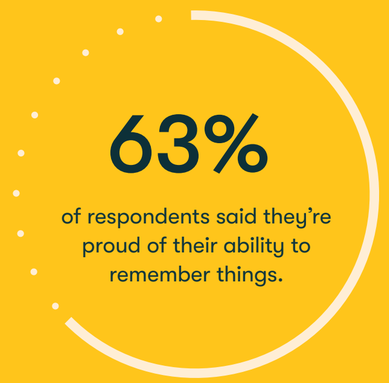
45%

feel good when a website remembers them and they don't have to type in a password



Businesses will pivot their focus to create a security-first culture.

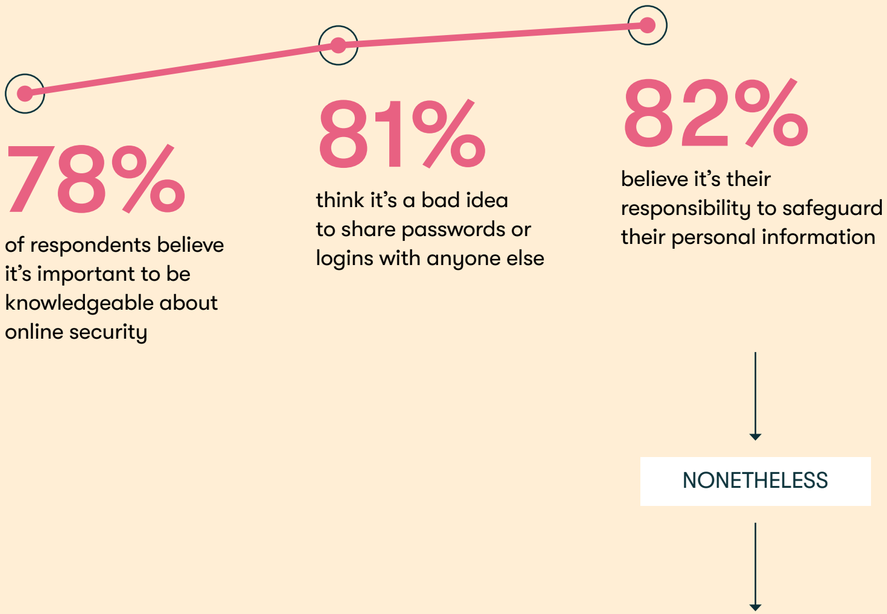
BUT



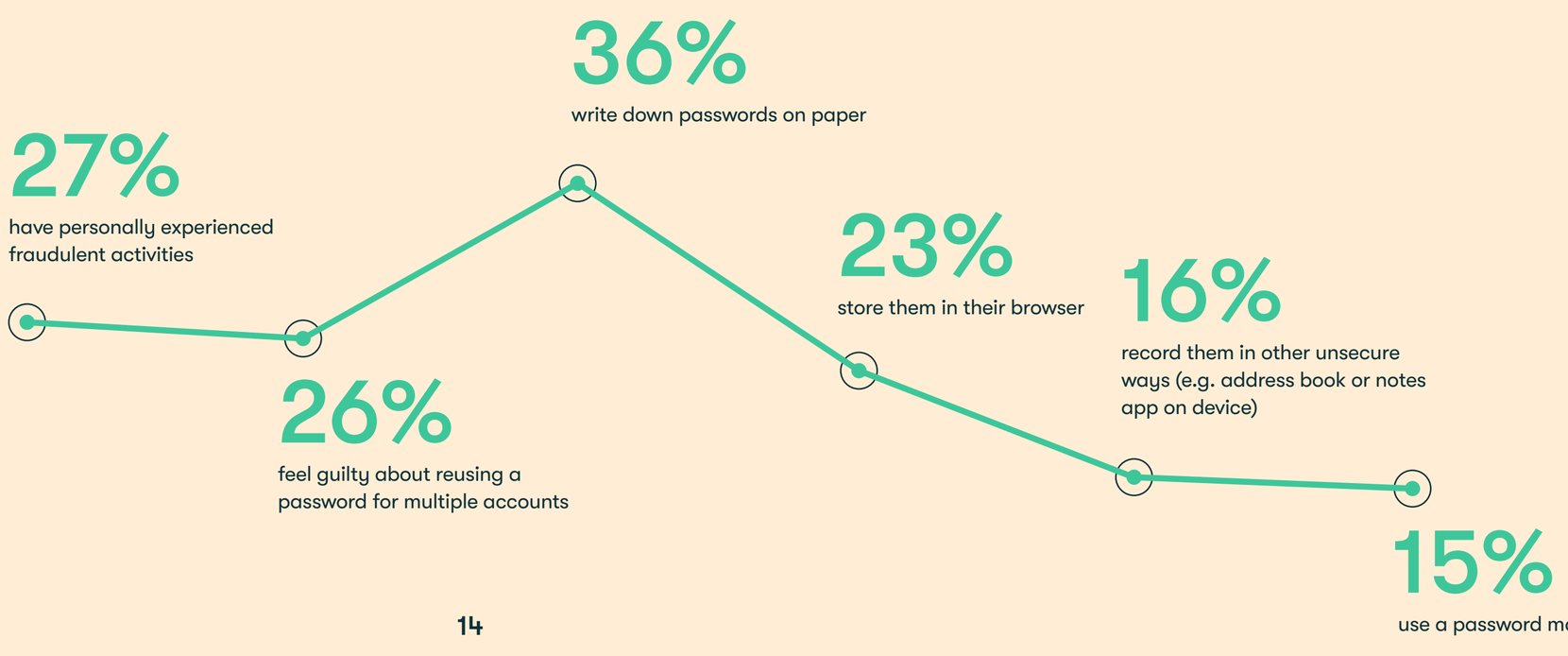
When it came to security, our respondents were a study in contradiction. Their behaviors didn't necessarily reflect feelings and beliefs.

To align attitudes with actions, businesses will change the way they implement and nurture a security mindset across the entire organization. And to support this change, they'll be looking for solutions that can solve security challenges while providing a seamless user experience regardless of where employees are getting their work done.

Start using a password manager today.



NONETHELESS



SECTION 03

Frustration? Indifference? A tale of many UXs

It's a UX jumble out there. Disorder, frustration everywhere. Make the case for a simpler digital future through secure access.

People are constantly online. A smartphone is almost always within reach and anyone with an "office job" is potentially at work at all times, whether they're grabbing a latte, sightseeing in Rome, or chilling on the couch.

People experience the internet as an ambient jumble of sites, services, apps, and devices. For a subset of Americans, accessing the internet feels like watching an episode of "Game of Thrones"—bewildering and confusing. More than a third of our respondents said they're overwhelmed with managing their online credentials. Over half don't want the responsibility of remembering their passwords.

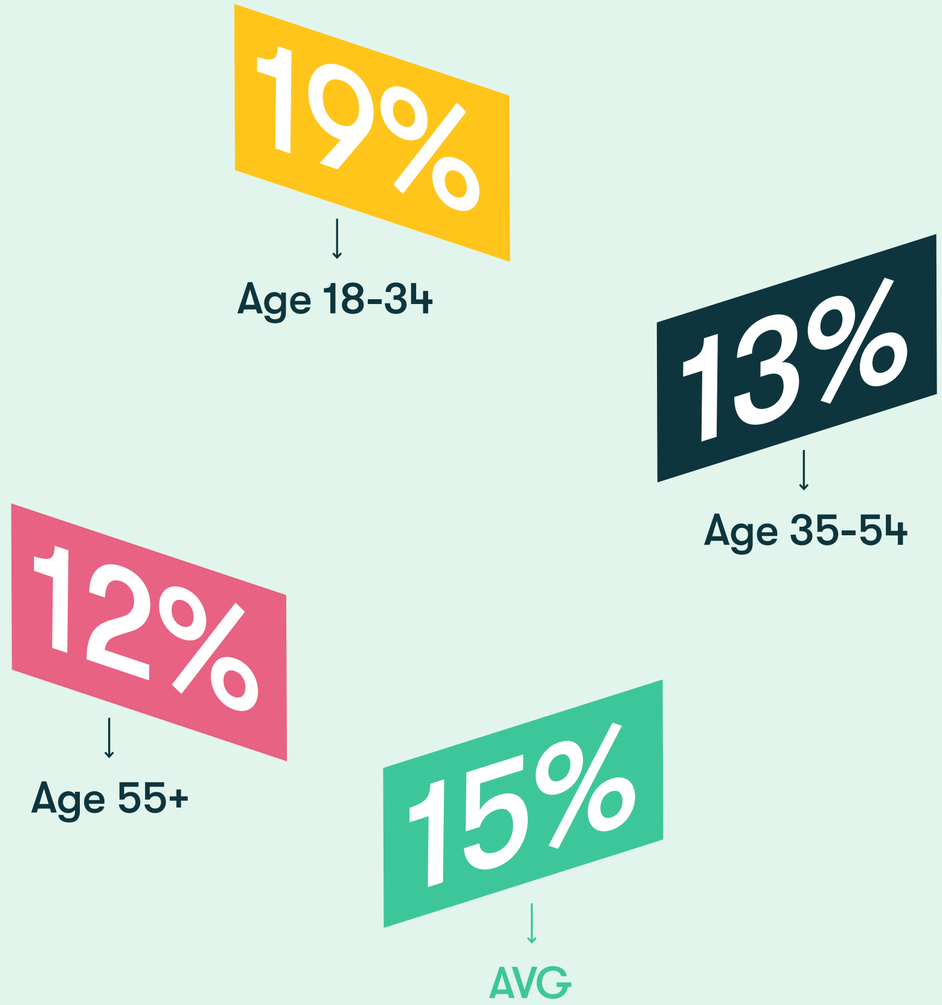
Different generations are not necessarily as different as fire and ice, but they do differ somewhat on their attitudes and habits.

Password Management 101.

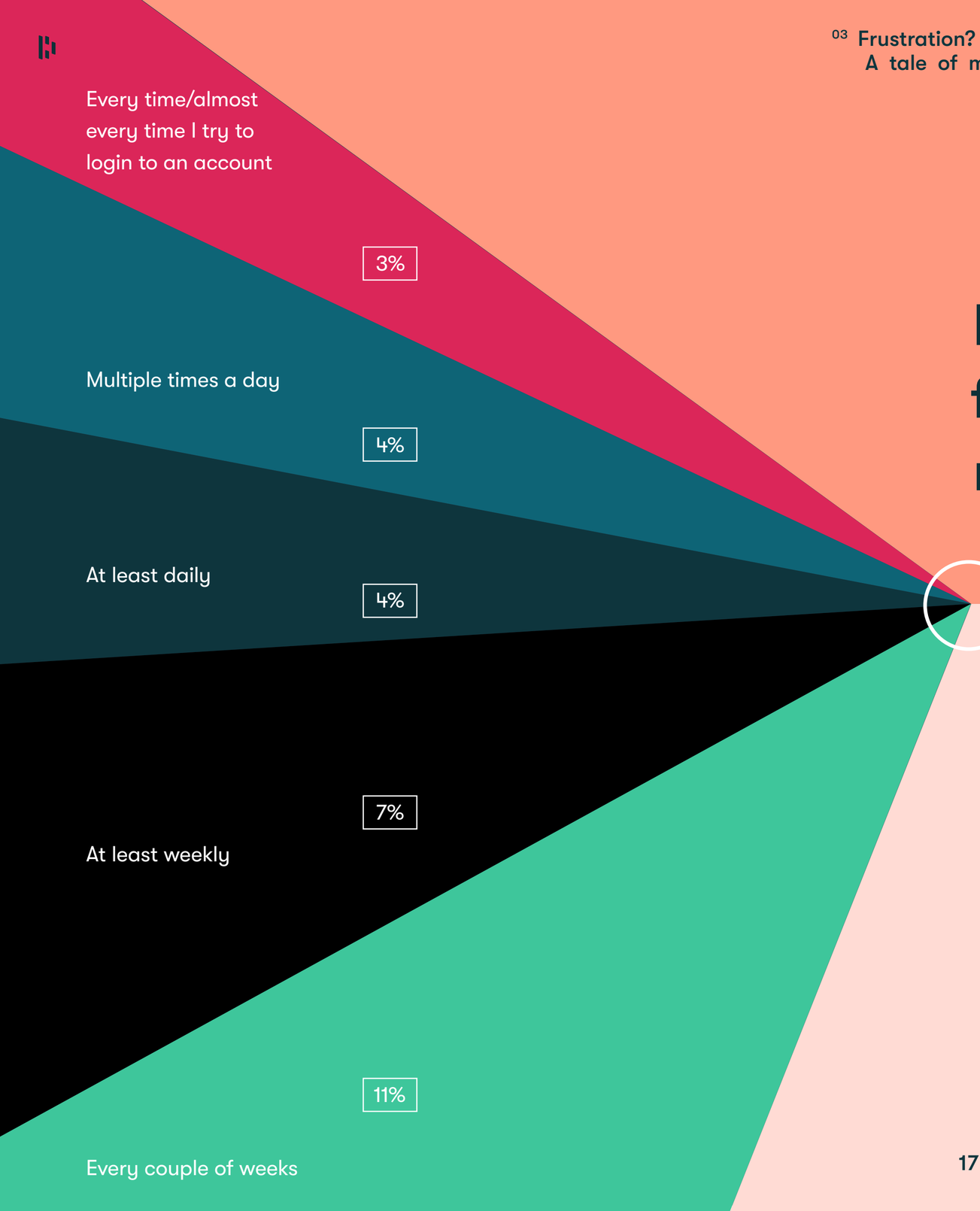
Almost 7 out of 10 respondents retrieve or reset passwords for user accounts at least monthly. Understandably, more than half would feel relieved if they didn't have to remember another password ever again.

> Find out why passwords, but more importantly employees' password habits, are the weakest link in your company security in "Password Management 101: Why Passwords are the Weak Link in Company Security."

Password manager use among different generations



How frequently do you find yourself retrieving or resetting passwords?



Workplace takeaways

Among our respondents,

42% said they have a high tolerance for frustration. But high tolerance doesn't equal zero impact. When faced with a login issue, employees will have to find a workaround. That usually means a tradeoff between productivity and security.
More than one-fifth of respondents did acknowledge they get easily frustrated when trying to do things online. Given these sentiments and the hodgepodge of employee UXs, we believe change is inevitable for businesses.

Recycling your old internet modem? Thumbs up. Recycling passwords? Ugh.

In a separate study by Dashlane and Harris Poll, of 1,200 U.S. employees:

30% said they reused business passwords

22% reused personal passwords for business accounts

Are your employees reusing and recycling passwords as a workaround?

You can make the digital workplace a little simpler and a whole lot more secure with tools such as single sign-on (SSO) and password managers that autofill credentials. You get better security controls. Employees get a simple way to strengthen password security without impacting their productivity.

SECTION 04

So many screens... secure all of them

One device, two device. Big device, small device. Devices in the morning, devices at night. Devices in the house, devices outside.

The days of 9-to-5 office hours have gone the way of the office cubicle. These days, work is only a smartphone away. And if that smartphone is not in employees' hands, it's in their pocket, on a surface next to them, or under their pillow.

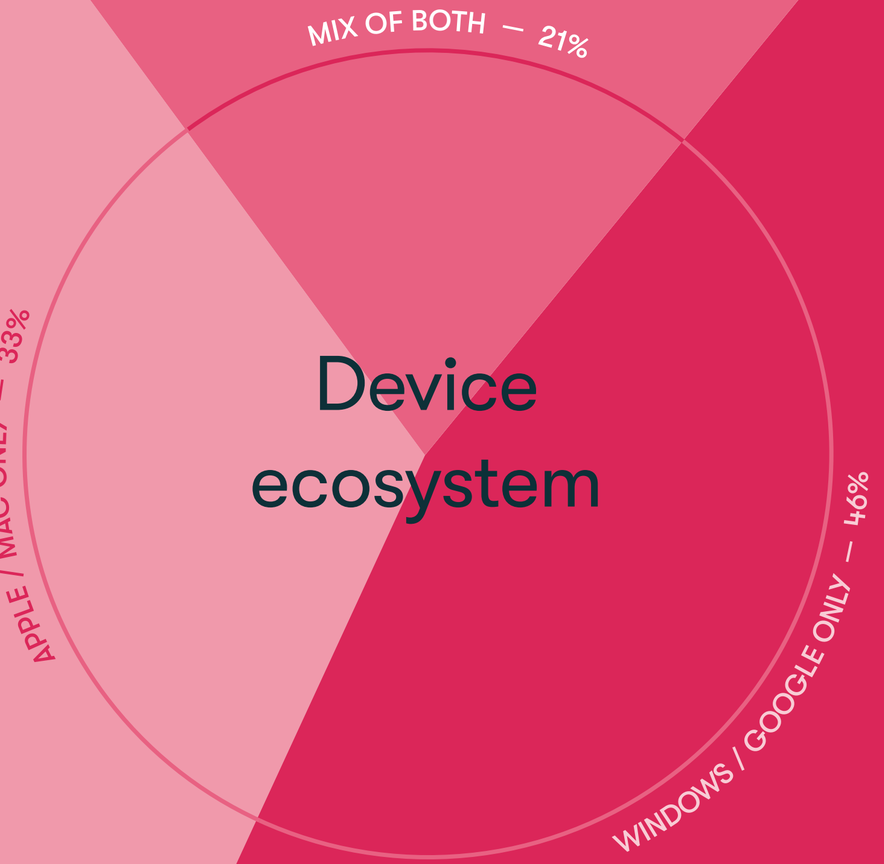
Nearly 90% of our respondents own a smartphone, but that's just for starters. From tablets, to laptops, to wearables, many people own multiple devices for their work and personal lives.

Workplace takeaways

Employees want convenience and efficiency. And let's face it, many have a hard time leaving work behind. Whether they're accessing sensitive data on personal devices or using a company laptop on public WiFi, they're exposing your business to security risks. This is especially a concern in the work-from-home environments that have no boundaries between personal and workspaces—employees may be downloading a sensitive corporate file on a laptop one minute and binge-watching Netflix the next.

Although security budgets shrunk in 2020, more than 70% of chief security officers surveyed by McKinsey & Co. planned to ask for significant increases for 2021.[9] One of the priority areas where they planned to spend more was identity and access management (IAM). This change in focus is not unexpected, considering the lessons learned during the pandemic and the expansion of remote work. An IAM solution can help you provide employees with secure access to your corporate resources regardless of what device they use—or where.

9 "COVID-19 crisis shifts cybersecurity priorities and budgets," McKinsey & Company, July 2020



DEVICES OWNED

Smart TV — 31%

Smart Home Device — 39%

Desktop Computer — 73%

Laptop Computer — 41%

Android / iPhone Smartphone — 89%

SECTION 05

One workplace, four (security) personalities

When it comes to workplace security, are your employees:

- DESENSITIZED
- OUT OF TOUCH
- ON TOP OF IT
- ABOVE IT ALL

Everyone loves a good personality quiz. Why wouldn't someone want to know what chocolate bar matches their personality or which city they should really be living in? We didn't ask our respondents if they preferred the seaside or lakeside, but we did ask questions that identified four clusters of users. Each of these clusters has distinct traits and attitudes toward technology. And each of them could present different barriers to creating a more secure culture in the workplace.

A: ALL OF THE ABOVE

→ DESENSITIZED:

OUT OF TOUCH

ON TOP OF IT

ABOVE IT ALL

Desensitized — 38%

Desensitized employees are not only extremely forgetful but also get easily frustrated when trying to get things done online. They feel overwhelmed by keeping track of all their online account information logins and waste a lot of time trying to access their online accounts.

For the Desensitized, reusing passwords or using weak passwords may feel like the best way to deal with these frustrations. They have a need for speed, and that means shortcuts. To get this cohort to adopt good cybersecurity habits, you'll need to provide tools like a password manager that simplify how they're accessing things on the internet without adding more frustration.

Comprising the largest of our segments, these employees experience the most pain but care about it the least. While they live mostly online, they don't think hard about technology or things like password management or security.

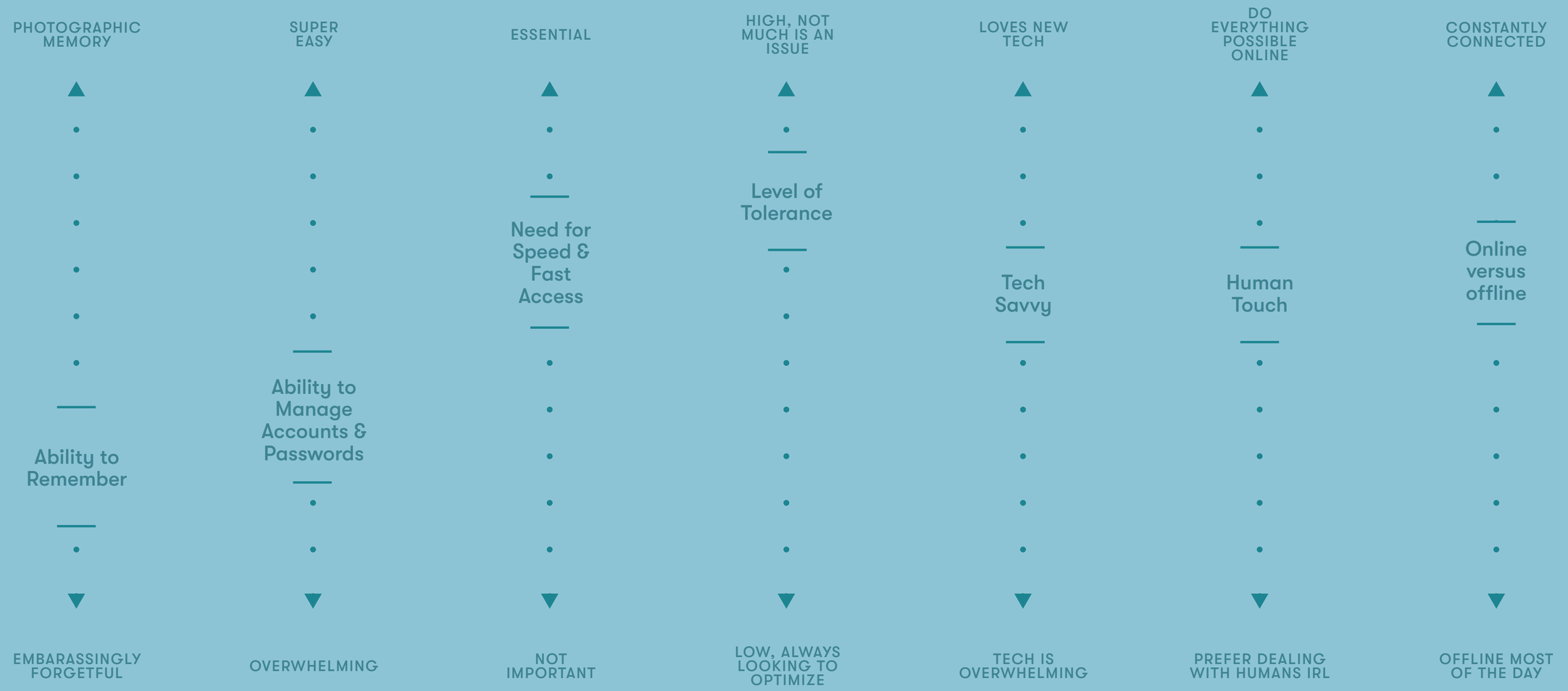
→ DESENSITIZED:

OUT OF TOUCH

ON TOP OF IT

ABOVE IT ALL

Potential barriers to your security culture:



DESENSITIZED

→ OUT OF TOUCH:

ON TOP OF IT

ABOVE IT ALL

Out of touch — 21%

This group isn't online as much. They don't inhabit the online world, so they just care less about it. With a lower level of tech savvy, they have a higher preference for doing things in person.

Out-of-touch employees don't frequently share online logins with anyone. They're most likely to write down their passwords and least likely to lock their devices with a code.

With the Out of Touch, the lack of awareness and the shunning of technology are big barriers to security culture. To encourage change, you'll need to start with a basic employee education program and then use security technologies that have a very small learning curve and require minimal user interaction. A seamless onboarding experience is essential for this category. Consider cybersecurity tools that have video tutorials and guides that can help with adoption and use.

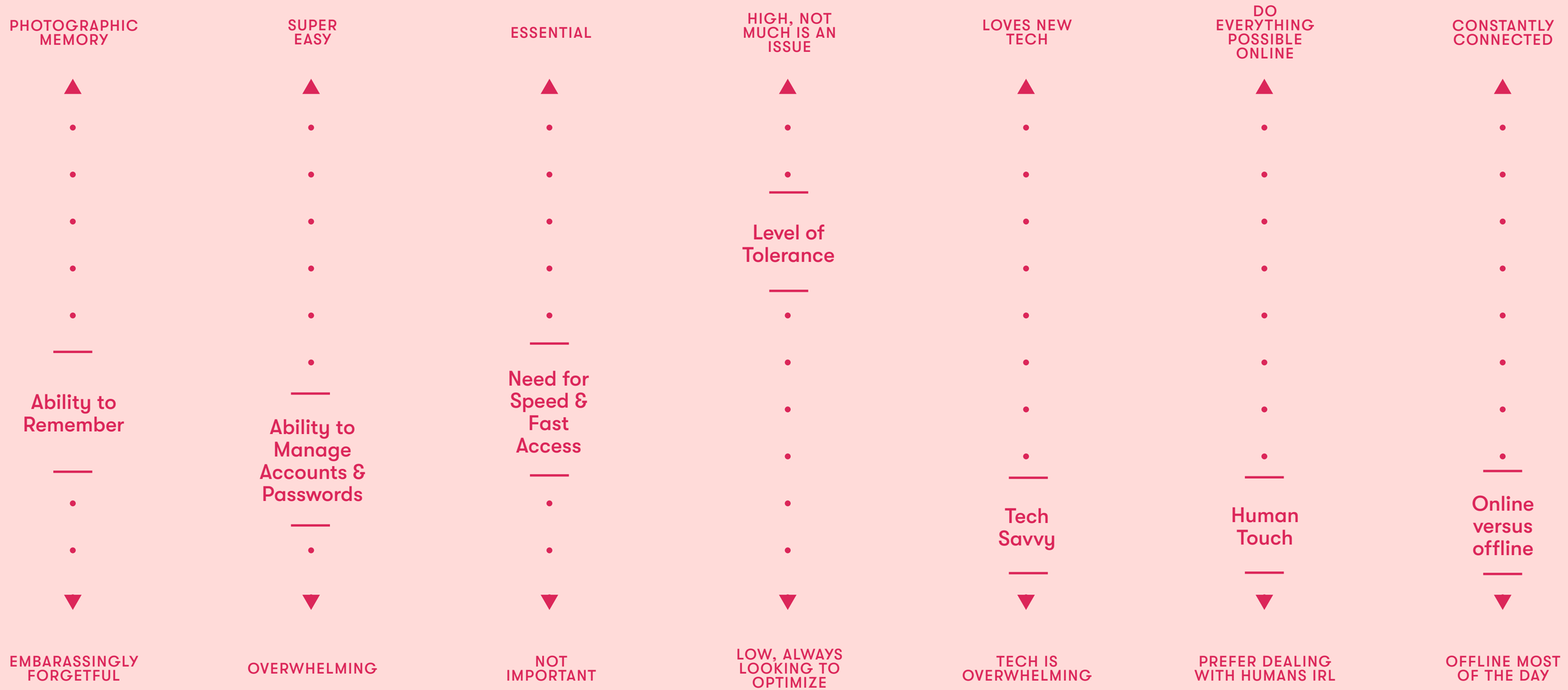
DESENSITIZED

→ OUT OF TOUCH:

ON TOP OF IT

ABOVE IT ALL

Potential barriers to your security culture:



DESENSITIZED

OUT OF TOUCH

→ ON TOP OF IT:

ABOVE IT ALL

On top of it — 21%

Employees who are “on top of it” prefer to do everything online, and consequently are more likely to own multiple devices. While they’re the group with the highest ownership of password managers, however, they also frequently use less secure methods—anything that lets them not remember their password. This includes reusing passwords for multiple accounts and storing them in the browser.

Lack of awareness is not a big barrier for this cluster. But since these employees are looking for efficiencies, it won’t be easy to change their habits if you’re asking them to take an extra step. To boost security culture, you’ll need to provide cybersecurity tools that offer a seamless UX with zero impact on their productivity and speed.

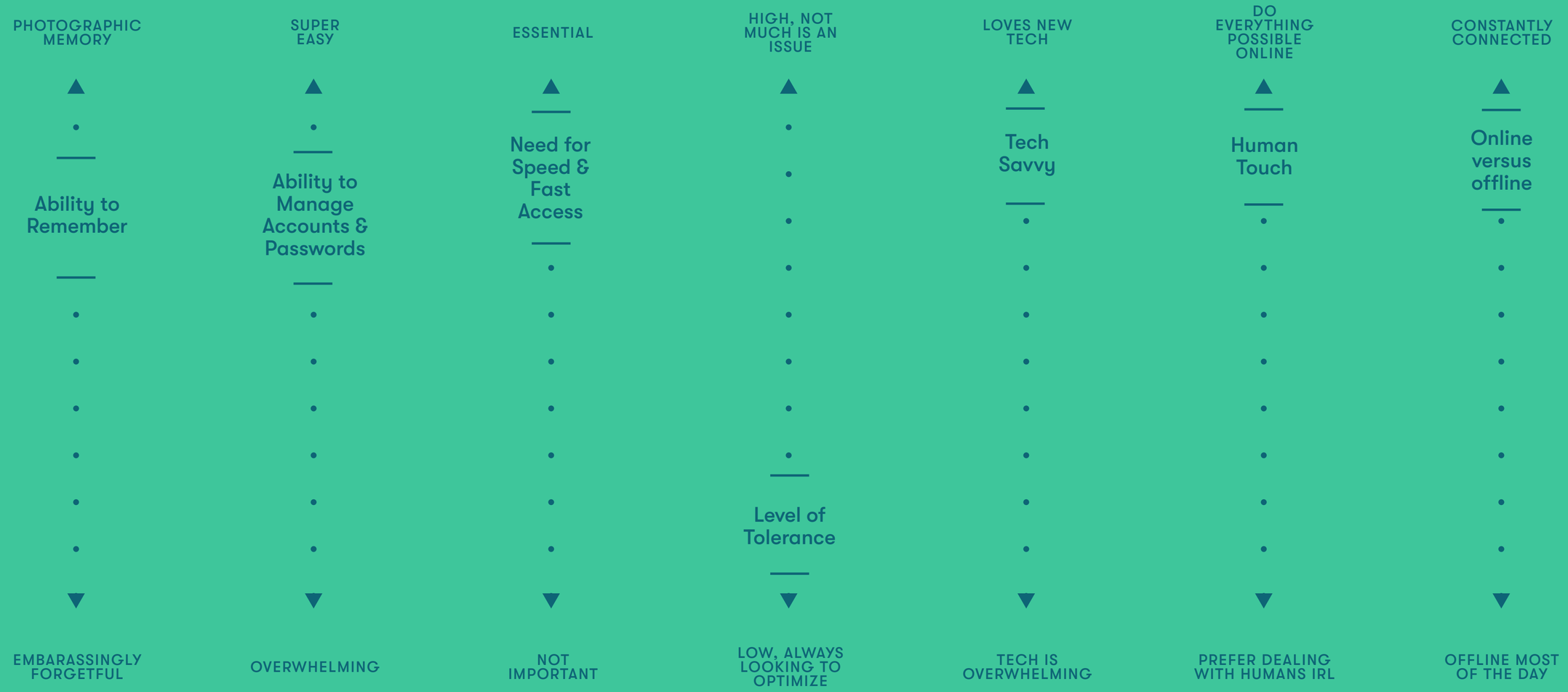
DESENSITIZED

OUT OF TOUCH

→ ON TOP OF IT:

ABOVE IT ALL

Potential barriers to your security culture:



DESENSITIZED

OUT OF TOUCH

ON TOP OF IT

→ ABOVE IT ALL:

Above it all — 22%

With a higher pride and tolerance for frustration, this segment is most likely to be among the earliest adopters of a digital life. The Above it All are proud of their ability to manage technical challenges. They're the least overwhelmed by keeping track of online accounts and the least likely to have experienced fraud or a personal data leak.

This group actively take steps to reduce stress in their daily life. They're proud of their ability to remember things and they don't waste much time accessing their online accounts. But while this cohort seem to have it all under control, they also have slightly lower use of password managers.

If employees in this segment perceive the user experience for your security solutions is too stressful, you'll have a tough sell. Because they're tech-savvy, you may risk them turning to their own preferred tools. Consider cybersecurity tools that offer personal benefits or separate work and business spaces they can toggle between as they maintain fluid boundaries between work and home life. And since these employees are the most likely to carefully read instructions for new services and products, make sure you're providing them plenty of resources to learn aboutthe security solutions you're implementing.

DESENSITIZED

OUT OF TOUCH

ON TOP OF IT

→ ABOVE IT ALL:

Potential barriers to your security culture:

Do the segmented groups overlap?

It's important to note that segments can overlap. Employees can be "borderline," possessing attributes of adjacent segments. They can also move between segments as they grow or mature, or as their situation changes.

What does that mean for your business? Implement a comprehensive, ongoing security awareness campaign that provides continuous education about threats and your employees' role in maintaining a strong security culture. This keeps security on their minds and avoids complacency, even as they become savvier and improve habits.

CONCLUSION

The digital workplace of tomorrow

There's no doubt that the future of the workplace is digital. COVID-19 was a sneak peek at the advantages of the brave new world of remote work. It was also a preview of new security risks, giving businesses an opportunity to better understand and prepare for the future of the workplace.

One of the many lessons we learned during the pandemic is that messaging is not enough—people need tools that will help them change behaviors. Applying that lesson to your security efforts makes it clear that mandating new policies and procedures is not enough to achieve success.

We may not know if hand sanitizers are going to be permanent on the office supply list, but we do know that businesses are reprioritizing cybersecurity budgets and focusing on IAM solutions. Succeeding in the digital workplace of tomorrow requires building better defenses today.

Survey methodology

We distributed our survey to 1,299 potential respondents via U.S.-based consumer research panels and received 1,001 qualified responses. Respondents were distributed across the U.S. Represented vocations included professional, clerical, technical, science, sales, design, and software development. We excluded anyone who currently works, or has worked at any time, in cybersecurity-related roles.

Respondents included 51% women and 49% men. One third fell within the age range of 18-34 and just over 60% were age 55 or younger. We applied an initial screening to ensure a balance of demographic profiles and representation. The data analysis included an evaluation of key demographics (such as age, gender, geography, children in the household, relationship status, income, etc.) to understand how these factors affect behavior, attitudes, and perceptions.

To segment the audience, we performed a cluster analysis on the collected data set, grouping respondents into unique and identifiable audience groups that highlighted different attitudes, behaviors, and demographic profiles. We focused on internet users in their peak working years in order to understand the technology choices and behavior of people making their own financial decisions.

About Dashlane

Dashlane offers businesses a password management solution that is as easy to use as it is secure. Admins can easily onboard, offboard, and manage their employees with the assurance that company data is safe. And employees can enjoy a way to manage their work and personal accounts that's already loved by millions. Our team in Paris, New York, and Lisbon is united by our passion for improving the digital experience and the belief that with the right tools, we can help everyone realize the promise of the internet. Dashlane has empowered over 15 million users and over 20,000 companies in 180 countries to dash across the internet without compromising on security.

dashlane.com

Inspired by the results?
Start practically implementing better cybersecurity no matter where your employees or your new office is with a password manager. Learn more in our latest guide.

Learn more
For more information on Dashlane plans for business, sign up for a trial or visit dashlane.com/business.

LinkedIn:
https://www.linkedin.com/company/dashlane
Twitter:
https://twitter.com/dashlane
Instagram:
https://www.instagram.com/dashlane
Blog:
https://blog.dashlane.com/category/simple-security/business

DASHLANE