transmit security

Gen Z Survey:

Shaping the Future of Passwordless

Gen Z Survey: Shaping the Future of Passwordless

Gen Zers seek flawless digital experiences and have little patience for old methods that should be obsolete. They also want cyber to be secure, but their own bad habits get in the way. It's a challenging mix, yet catering to Gen Z could lead us to a new digital age with expansive business potential.

Gen Z under a microscope

Gen Z, iGen, Zoomers, Zillennials... the post-millennial generation, born after 1996, bears a few monikers. What's beneath the names? It's time to study Gen Z as they gain spending power. What opportunities and obstacles will your company face?

We surveyed Gen Z on topics that directly impact your business:

- Their password habits
- Their login experiences
- How they engage with technology
- Why they abandon websites
- What they prefer

Our prediction:

Gen Z's idealized vision of the digital world, how it should be, will give rise to an ultramodern webscape where business and consumers thrive.

Survey snapshot

Gen Zers **grew up with smartphones** and have little memory of a world without touchscreens. These digital natives interact with devices, websites and apps like no other generation.

When it comes to account access, they're on a quest for logins that are both **easy and secure**. But Gen Z brings added risks with sloppy password habits and a lack of threat awareness that may surprise you.

Companies will **gain Gen Z loyalty** by keeping accounts secure and giving them free-flowing journeys across channels, on any device. It can be done, and we'll tell you how.

"Gen Z's earnings are set to hit $33 trillion by 2030 … more than ¼ of all global income."

— Bank of America[1]

Gen Z's purchasing power

will inspire companies to meet their uncompromising demands.

1 Markets Insider: "Gen Z's surging economic power will permanently change the the investing landscape over the next decade, Bank of America says," Nov. 2020.

Raised on tech, always connected

Gen Zers in our study were ages 4 to 10 when iPhones first landed in their hands. To them, dynamic content and endless options are simply expected.

Most Gen Zers had their own smartphone by age 12.[1] On average, they check social media and text 100 times a day. They fly through options, making decisions in flash.

Gen Zers decide in **8 seconds** if your content is worth their time.[2]

Survey demographics:

600
Respondents in the U.S.

Age 18-24
The oldest Gen Zers

48.83%
Female

51.17%
Male

Survey objectives

Transmit Security collaborated with Pollfish to design a blind survey that would get to the heart of what Gen Zers think about passwords, account setup and all things authentication.

Our goal was to see what drives them forward or turns them away. In this report, we examine the data and offer insights to help your company attract Gen Z and keep them engaged.

Our findings reveal Gen Z is intolerant of bad login experiences. At the same time, they want companies to respect their privacy and protect their accounts.

1 Business Insider: "104 Gen Zs Reveal What They Think About Instagram, Facebook and Life," June 29, 2018.

2 Forbes: "Marketing to Gen Z? Here are 5 Things You Need to Know," Aug. 2021.

Table of Contents

Gen Z stats & insights

Gen Zers want it all: secure, fast and easy identity experiences.[1]
Anything less is costing you business.

49.5%
Abandon a cart if they forget their password

58%
Drop off if registration is too complex

52%
Leave a site if they forget their credentials

Expect more risk: they're reckless with passwords & login choices.

81% of Gen Zers do **not** use a password manager

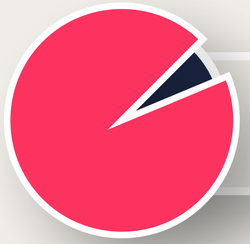
71% don't know what phishing is or how to spot it

Top 3 takeaways

Quick to split
Gen Zers are on the move and want instant results. Don't ask them to take extra steps. If it feels too difficult, you've lost them. They're acutely aware of the endless alternatives online.

Secure accounts for them
They want security, but their password habits show a lack of security know-how. Naive? They admit they're oblivious to the most common threats.

Ease is essential
Gen Z, the one-tap generation, is primed for passwordless. Biometric authentication[2] enables simple and secure access with a single touch.



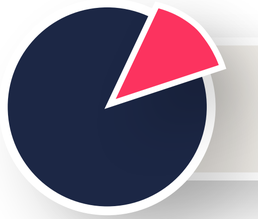
93% of all consumers prefer biometrics over passwords.[3]

Gen Zers won't sacrifice ease for security.

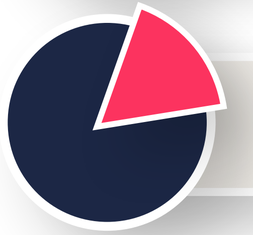
1 Transmit Security Identity Hub: What are Identity Experiences?
2 Transmit Security Identity Hub: What is Biometric Authentication?
3 Mastercard, "Mobile Biometrics in Financial Services: A Five Factor Framework"

The smartphone generation

Our survey revealed Gen Z relies heavily on mobile phones — more than any other generation.



22.7% of Gen Zers **only** have one device, a **mobile phone**. It's their #1 choice.



34.6% have **more than one mobile** phone number. That's 1 out of 3 Gen Zers!

Juggling devices

More than **77%** of Zoomers hop between multiple devices. What's unique is their **clear preference for mobiles**. More than **1/3** own multiple mobile phones with different numbers.

Multi-device management is essential
When using biometric authentication, your customers must be able to link any number of devices to a single, unified account. If you can achieve this, Gen Z can log in with any device they choose.

If not, you'll break their flow
It's not just devices … it's channels and apps too. Consumers are often forced to have several accounts with the same business: one for an app, one for the store and a third for support. This creates a fragmented, frustrating CX that Gen Z won't tolerate.

Gen Zers want to explore everything your business offers without disruption.

Using mobiles to shop and bank online

Modus operandi: mobile

Unlike previous generations, these young adults use their smartphones for everything from financial transactions to shopping online.

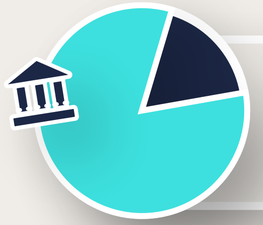
Meet your customers where they are

They want convenience and security, so put those built-in biometric scanners to use. When they're banking and shopping on their mobiles, they can most easily authenticate with a biometric, proving their identities with a single tap.

Shopping online

85.3% use a mobile phone to do some or all of their online shopping. 28% only use a phone.

Banking online



83.3% use a mobile phone for online banking and payments. 37% only use a mobile for banking.

Pushing the easy button

When given third-party login options ...

68% log in with Google, Facebook or Apple. That's nearly 2 out of 3 Gen Zers.
Only 32% log in with an email address & password.

Balancing security & ease

Gen Z is split when given a choice ...

46% opt for more security: "A website that asks for authentication every time."

54% chose ease: "A website that doesn't ask for my password every time."

More than 2 out of 3 choose to simplify registration and logins by using a pre-existing account like Google, Facebook or Apple.

Top 3 findings

Social logins = keys to the kingdom

Hackers steal social logins to gain access to nearly every account. Social logins also create privacy risks by collecting data to target your customers with ads.

Their ease is your complexity

As you offer more login options to customers, your authentication stack grows more complex and expensive.

Give them ease & security

Attract Gen Z with stronger security and ease of use. If you sacrifice one for the other, you could lose half of your Gen Z customers.

Gen Z Password Mismanagement

- **34.2% trust their memory**
- 29.5% use an app, like Notes
- 19% use a password manager
- 17.3% write it down on paper

Oversharing hurts business

Gen Z has a bad habit of **sharing devices and passwords**. It negatively impacts your business in two ways:

1. Password sharing[1] makes accounts more vulnerable
2. Fewer customers are paying for your services

74% have logged into a site using **someone else's device.**

48.5% say someone else has **shared a password** with them.

It's a hassle

No matter which method they use, password management degrades the customer experience.

To make it easier...

58% reuse the same password for many accounts. Hackers know we're lazy, so they hit sites with lists of stolen credentials to break into other accounts.

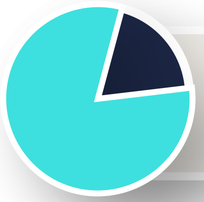
Companies pay the price

Account takeovers are costly and ruin customer trust.

1 Transmit Security Identity Hub: MFA for Shared Accounts

Blindspots create security gaps

Gen Z's lack of threat knowledge makes securing their accounts even more difficult. Granted, companies cannot expect any customer to guard against fraud. It's simply imperative for companies to secure accounts for customers.



71% either don't know what **phishing** is or don't know how it works. Stunning, right?

Gullible targets

Gen Z can easily be tricked by deceptive emails or sites that lure them to enter their login credentials. The only way to prevent this is to **eliminate passwords completely**.

74% of organizations in the U.S. experienced a phishing attack in 2020 (Statista).

Passwordless is the only cure

Only native passwordless[1] authentication removes all passwords, even from the account recovery process.

Keeps biometrics safe

Biometrics verify customers locally on their devices. Identifying data is never sent over the web or stored in a database. Without shared secrets, there's nothing to steal.

No shared secrets = No account takeovers[2]

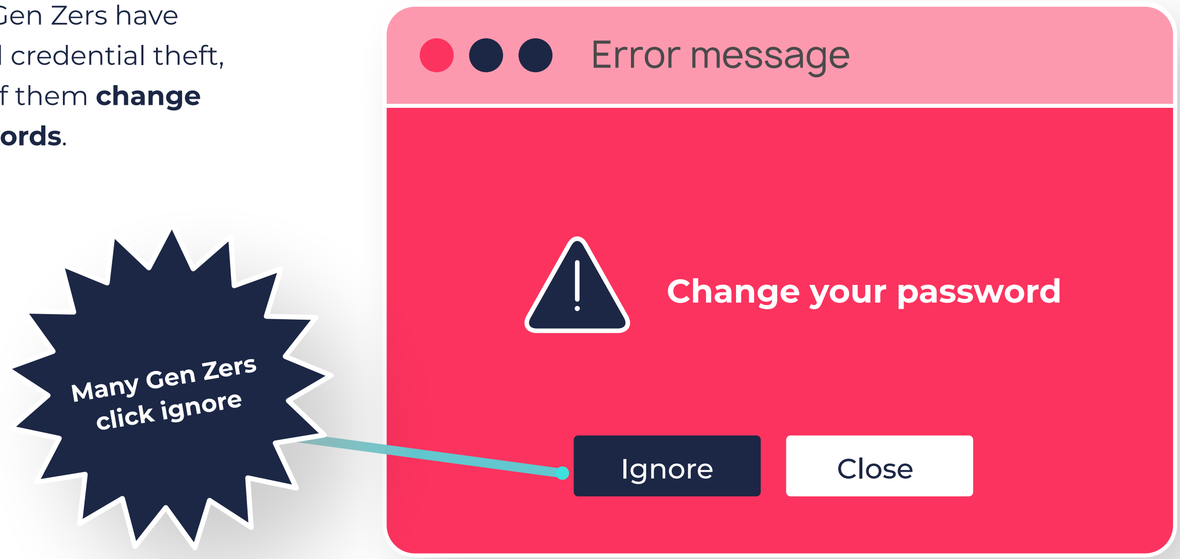
- ✕ Brute force
- ✕ Password spraying
- ✕ Phishing, sprear phishing
- ✕ Smishing
- ✕ Credential stuffing
- ✕ Keyloggers
- ✕ SIM swapping
- ✕ Man-in-the-middle

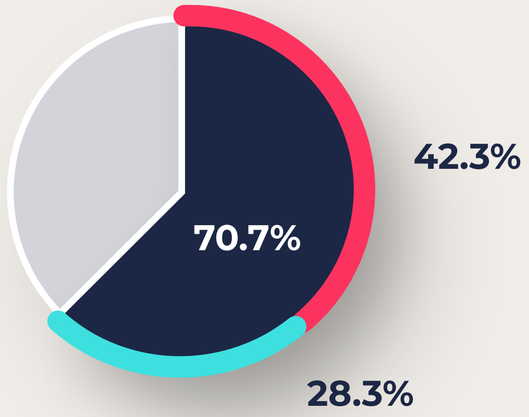
1 Transmit Security Identity Hub: Passwordless Authentication

2 Transmit Security Identity Hub: Account Takeover Prevention

Alerted to stolen credentials

7 out of 10 Gen Zers have experienced credential theft, but not all of them **change their passwords**.





70.7% have **received an alert** to change their password.

42.3% took action by changing their passwords.

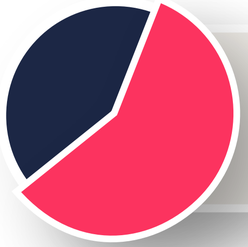
28.3% didn't change their password.

Key takeaway:

They say they want security but don't always take precautions, even when advised to do so.

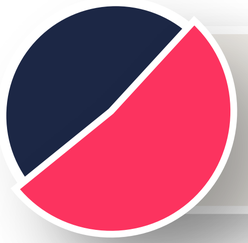
Lost business

Registration complexity leads to drop offs



58.2% of Gen Zers have stopped enrollment because registration was too complex.

Forgotten passwords cause drop offs



52% have stopped using a website because they couldn't remember their password.

Each step can be a point of failure:

1. Registering for the first time
2. Logging in to make a transaction
3. Waiting for or entering an OTP
4. Resetting a password

Abandoned carts = lost sales

49.5% of Gen Zers abandon an online purchase if they forget their password.

According to Mastercard, 1/3 of all sales are lost due to forgotten passwords. That seemed high until now. You could lose 1/2 of all Gen Z sales.

Passwords are cutting into profits.

‘Forgot my password’

is costing you business

78.5% have used ‘Forgot my password’ within the past few months.

Failing to recover passwords

59% were unable to recover their credentials on at least one occasion. It’s a high failure rate.

Lockouts and password resets increase support costs

of all support requests are password resets.[1]

A single password reset costs $70 or more.

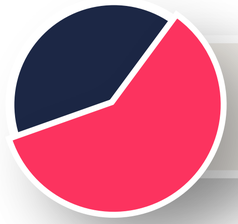
1 Gartner, "Are Password Resets Overwhelming Your Service Desk?"

Friction-filled 2FA

OTPs: Often Too Painful

One-time passcodes (OTPs)[1] add a second factor of authentication (2FA) on top of passwords. But SMS OTPs frustrate customers and can be intercepted by hackers. Plus you're still using passwords!

Failing to authenticate



62% of Gen Zers say an SMS OTP didn't arrive even after clicking "send again."

Too many mobiles?

It complicates 2FA when 35% of Gen Zers have more than one mobile phone. If an SMS OTP is sent to the wrong phone, the process is broken.

4 pain points of SMS OTPs:

1. It's not secure - hackers can intercept SMS OTPs
2. 2FA still uses passwords - fails to remove your #1 risk
3. It's bad for CX - Gen Z is annoyed by extra steps
4. It leads to drop offs - 62% failed to receive an OTP

Replace 2FA with passwordless MFA

With passwordless authentication, customers can prove their identities with fingerprint or facial recognition plus the possession of a private key on their device. You'll achieve multi-factor authentication (MFA)[2] in one step.

1 Transmit Security Identity Hub: One-Time Passcodes (OTP)

2 Transmit Security Identity Hub: Multi-Factor Authentication (MFA)

Shaping the future of passwordless

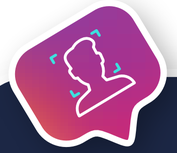
Ready for passwordless

Gen Z is on a quest for fast and easy digital experiences — from login to checkout. Authenticate them directly on any device they're using. After a quick scan, they're in! And you'll **know who they are with confidence**.

Native passwordless

Transmit Security's BindID™ is the only **passwordless customer authentication service** that eliminates all passwords from the customer journey. No more passwords anywhere, not in browsers, the user store nor the recovery process. And no more frustrating OTPs.

To do this, you must **say "no"** to solutions that stack biometric authentication on top of passwords. They all do, except one. Only BindID fully eradicates passwords. Your #1 security risk and leading cause of revenue loss is **completely gone**.



By removing passwords you'll:

- Fuel business growth
- Slash support costs
- Prevent ATO fraud
- **Dazzle Gen Z with the automagical experiences they crave**

Passwordless is transformational

The shift in identity will extend beyond Gen Z to all generations. **Passwordless authentication simplifies logins** and removes those points of failure for every customer. It's fast, easy, private and secure.

With the **BindID service**, your customers never create or use a password, and they enroll only once. As the first **app-less** biometric solution, BindID removes a barrier to entry for all customers, especially Gen Z, least likely to download an app.

Most importantly, you'll instantly prove the customer's identity with multiple factors: a biometric and a private key on their device. **One-touch MFA** delivers effortless experiences, higher conversion rates and rock-solid security.

Challenges only BindID can solve

Broken flows

With other passwordless solutions, users must register and log in with a different account for every device and every channel. This creates **fragmented, frustrating experiences** that Gen Z won't tolerate.

Security gaps

These same solutions leave security holes. If a Gen Z customer switches to another website, uses a browser in a social media app, clears their cookies, uses privacy mode … or if they simply switch devices, you have to **rebind them with a password**, the very problem you must eliminate.

The solution:

BindID carries Gen Z down any path

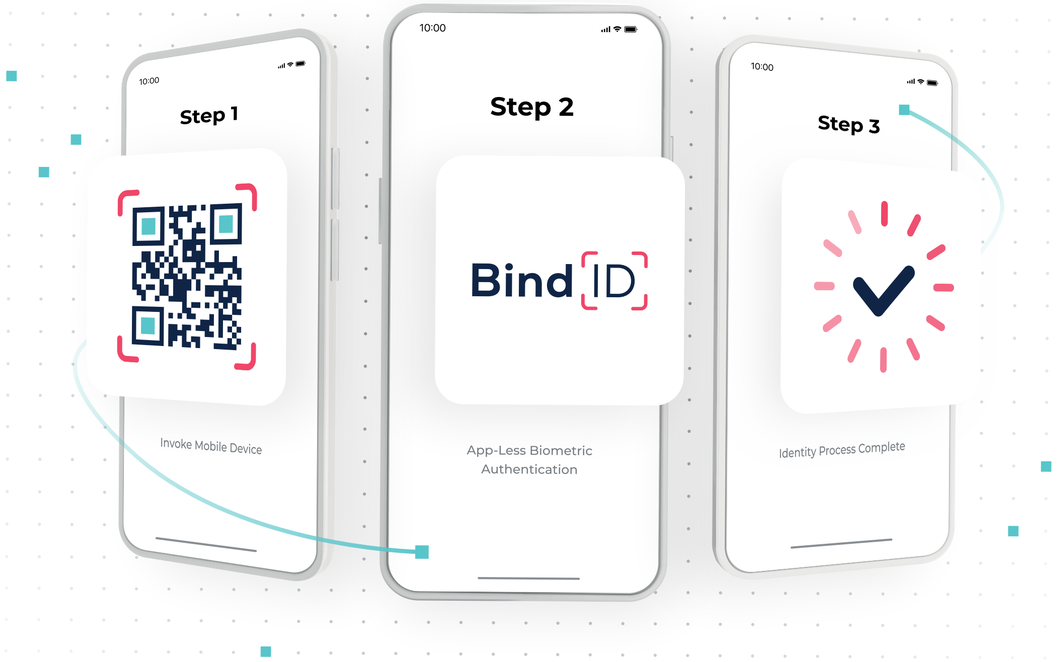
Let them use **any device** to access **any channel** — across web and mobile apps, online stores, call centers and kiosks. Only BindID creates one, unified identity that gives customers seamless cross-channel journeys every time.

Companies that evolve now will be the first to reach the new digital age and reap the rewards.

Discover what you can do with BindID

BindID is the only ...

customer authentication service that completely removes passwords and enables cross-channel journeys on any device. By eradicating passwords, you'll prevent fraud and captivate customers with elegantly simple identity experiences.



About Transmit Security

Transmit Security, the identity experience company, is on a mission to rid the world of passwords. We work with some of the largest, most innovative global enterprises and Fortune 500s to keep their identity stack secure and scalable.

In June 2021, Transmit Security raised a $543 million — the largest Series A in cybersecurity history. The investment was led by Insight Partners and General Atlantic. Since the initial announcement, Citi Ventures and Goldman Sachs have joined as additional investors. Transmit Security's pre-money valuation is estimated to be $2.2 billion.

Transmit Security was co-founded by serial entrepreneurs and investors, Mickey Boodaei and Rakesh Loonkar in 2014 with the aim of changing the security identity landscape.

Join our mission to make passwords obsolete