

# Bridging digital identity generational gaps

The digital identity lifecycle and why is it so  
different for each generation of consumers



# Mitek

# Everybody's online

It's an exaggeration to say everybody's online—but not much of one. The pandemic touched off a massive expansion in digital accounts and transactions, reaching widely across all generations.

Even consumers may be underestimating the extent of their digital involvement. [Allstate research](#) found that more than 80% of respondents—from gen Zs to baby boomers—said fewer than 25 companies had access to their personal information, although the actual number of online accounts averaged well over 100.

With digital activity expanding to fill more of everyday life, digital identity becomes hugely important. We need to establish our digital identity to open new accounts for digital products and services (a process called “identity proofing”). It needs to be checked each time we access those accounts (“identity verification”). And sometimes, for risky transactions or just periodically for security's sake, it needs to be rechecked against additional corroborative information (“identity authentication”).

These identity lifecycle processes are among our first and most frequent user experiences with digital providers. Whether they make a positive or negative impression depends partly on if the provider has hit the right balance between ease/convenience and security/privacy. Our attitudes toward this balance are complicated, and vary considerably by generation. There's variation too in generational preferences for identity lifecycle methods.

Still, overall trends are emerging: The [2021 Identity Fraud Study by Javelin Strategy & Research](#) reports that 60% of consumers say they understand physical biometrics, such as voice recognition, facial recognition, and fingerprint scanning to be secure and reliable. And 64% trust biometrics more than passwords.


**90%** 

of US consumers used one or more digital payment methods in 2021

**70%** 

used mobile banking at least weekly (60% say they can't live without it)

[Chase Digital Banking Attitudes Study](#)

**79%** 

of consumers used some form of P2P, such as Zelle, Venmo or ApplePay in 2020

[Fiserv study](#)

**50-98%** 

of US adults use social media, depending on age group

[Pew Research Center 2021](#)

**49%** 

of US consumers shopped for groceries online in 2021

[Mercatus/Incisiv study](#)



# Every organization has to deal with it

With the expansion in digital activity we've also seen an expansion in the number and variety of organizations needing to manage digital identity lifecycles. The success of not only large enterprises, but also of local merchants, nonprofits, and government agencies is affected by how well they handle digital identities. Almost overnight, it's become a fundamental requirement for being in business or providing public services.

The challenge is not just scale—being able to handle growing numbers of digital identities. It's also about specificity—getting granular enough to meet varied needs and preferences rather than trying to force-fit a single solution for all. You have to hit the right balance of ease/convenience and security/privacy for different generations of users. Increasingly, you also have to get it right for individuals within generations (the trend toward customization is one of the things we'll talk about).

**The way to hit the right balance:** Implement a connected, layered digital identity lifecycle solution that supports user choice. With this approach, you can also dynamically invoke the right combination of protections based not only on segment or individual user characteristics, but also on the context and risk associated with historical and real-time user behaviors.

Every organization also needs to protect identity information and build trust. In a [June 2021 Cisco survey of consumers across 12 countries](#), 86% of respondents said they care about data privacy, but 46% said they are unable to effectively protect their personal data today. It turns out trust improves when digital identity lifecycle methods are specific to consumers: A [PYMNTS study](#), in collaboration with Mitek, found that 73% of digital account users say being able to choose their preferred verification method increases their trust in a service provider.

**Massive, sudden growth in digital transactions is creating EXPANDING field of opportunities, challenges and risks for organizations of all types and sizes**



**But success requires NARROWING focus on needs and preferences of generational segments and, increasingly, individuals within them**



# Fraudsters already get it

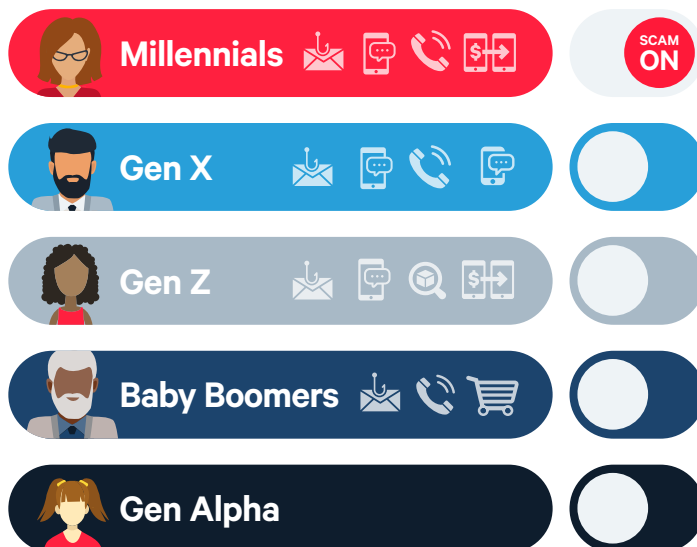
Fraudsters have already become very strategic about customizing their schemes to reflect generational differences in digital activity and attitudes, and to exploit behavioral vulnerabilities. That means every organization also has to take these “customized” tactics into account when deciding on digital identity lifecycle methods.

This ebook provides a survey of generational differences and fraud tactics to help you do that.

“

*“One of the most concerning factors shaping fraud patterns today is not just the digital transformation and the pandemic, but how fraudsters adapt their tactics according to the unique generational personas.”*

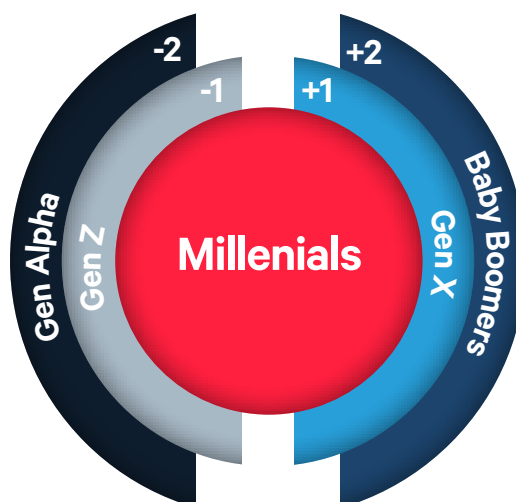
ACAMS Today, Sept 2021



## Generational survey

We start our survey with millennials, who are at the center of the generational spectrum and of their working lives. Already 35% of the global workforce, millennials will amount to 75% by 2025. They're currently the largest group of digital buyers, according to [Statista](#). As such, millennials strongly impact digital products, services, identity authentication, and cybersecurity developments.

From this center of gravity, we'll move outward one step at a time to see what's different about downstream and upstream generations.







# Center of gravity: millennials/bridge millennials

1980 - 1995

EMERGENCE OF  
INTERNET &  
SMARTPHONES

MULTIPLE CONNECTED  
DEVICES

FIRST DIGITAL  
NATIVE GENERATION

If you're a millennial, you were born between 1980 and 1995, a period bookended by the emergence of the Internet and smartphones. Regarded as the first digital native generation, you and your cohorts have multiple connected devices and have enthusiastically adopted digital technologies in the workplace and for home/personal use.

The oldest millennials, often referred to as bridge millennials since they're adjacent to gen X, are currently the biggest online spenders. With peak earning years still ahead, many will also soon be on the receiving end of a massive generational transfer of wealth through inheritances from baby boomers.



emergence of the  
**internet &  
smartphones**



generational  
transfer of  
**wealth**  
from baby boomers



## WHERE THEY'RE COMING FROM



**Savvy users of banking apps, digital payments, online shopping, and social media**

**98%**

use mobile banking apps (89% to view balances; 73% to view statements; 65% to transfer money between accounts)

**31%**

make P2P payments

[Chase's 2021 Digital Banking Attitudes Study](#)

**86%**

shop online

[PowerReviews, 2021](#)

**65%**

of millennials and 53% of bridge millennials used mobile digital wallets in May 2021; 22% of millennials and 27% of bridge millennials used three or more

[2021 Global Payments Report, FIS Inc.](#)

**57%**

of millennials and 70% of bridge millennials say a merchant's digital payment options impact their shopping decisions

[PayPal research, Sept 2020](#)

**80%**

use social media, with most activity on YouTube, Facebook, Instagram and LinkedIn

[Pew Research Center, April 2021](#)



**Favor 2FA and biometrics**

**70%**

of US millennial digital account users agree that biometric authentication is faster and more convenient than other methods

**65%**

say they feel comfortable using biometrics more than other methods

**83%**

of millennials and 82% of bridge millennials are willing to use 2FA (36%/34% want to use it only when logging in from a new device; 29%/30% want to use it for every login)

[Identity Verification in the Connected Economy, a PYMNTS/Mitek collaboration, Oct 2021](#)



**Willing to share personal data and somewhat resigned to loss of privacy**

**70%**

are willing to share personal data with an app in exchange for more relevant, personalized, and/or convenient services.

**37%**

say don't believe they have much control over their data

[Entrust research reported in HelpNetSecurity, Feb 2021](#)





## WHERE THEY'RE VULNERABLE



**Millennials are certainly feeling some vulnerability:**

**44%**

have experienced a cyber threat

**25%**

have had their identities stolen (the highest incidence rate of all generations)

[Cybersecurity Attitudes and Behaviors Report 2021, National Cybersecurity Alliance/CybSafe](#)

**53%**

say they experienced significant to severe stress related to identity fraud (highest among generations—almost double that of gen X)

[Javelin 2021 Identity Fraud Study](#)



**Although:**

**57%**

have been locked out from an account due to account takeover fraud and...

**46%**

have had unauthorized charges on their bank or credit card accounts (both stats are lowest of all generations)

[Allstate US survey, 2021](#)



**Some of the causes of vulnerabilities can be found in poor security behavior:**

**23%**

admit to sharing their online credentials with a non-family member

[Infosecurity-magazine, Jan 2021](#)

**55%**

are using corporate email for their personal social media logins

[SailPoint Trust Issues Survey, 2021](#)

**22%**

use the same password for all accounts

**45%**

use 2-5 password variants for all accounts

**8%**

use a password manager or generator

[Liminal Consumer Digital Identity Landscape 2021](#)

(These vulnerabilities may be of decreasing importance in the near future, though, as millennials embrace biometrics in droves. Currently only 25% of millennials favor username/passwords for identity authentication in browsers, and only 18% in mobile apps.)



## WHERE THEY'RE VULNERABLE



### Fraudsters are targeting millennials through:

**Phishing emails, mobile texts, or robocalls** impersonating a retailer (offering rewards, promotions, parcel tracking), a P2P transfer confirmation, a potential employer, or business communications. Fraudsters may leverage phishing kits that enable them to impersonate leading cloud-based email services. Once they fool consumers into revealing email account credentials, they may sell these on the dark web. Or they may rapidly try them on other digital services. In fact, the [Javelin study](#) found that in 59% of consumers victimized by identity fraud in 2020 experienced takeovers across multiple accounts and that these often occurred within just a couple of days.

Even worse (though not surprising given the use of corporate emails for personal logins), Javelin found that 15% of victims lost both personal and business information—a trend that's grown by 150% since 2017.

**Cloud-based platforms and videoconferencing services** with security holes or no identity proofing at onboarding. When fraudsters are allowed to join platforms like Amazon, Etsy, and eBay, they can use them to approach other members from a seemingly trusted environment. There's also the increasing risk of being targeted from a trusted environment by a deepfake (tech-generated synthetic voice or video impersonation) requesting identity credentials, payments, or reimbursements.

**Gig economy apps**, which seem less risky than financial accounts and therefore usually have lighter security. Also, many consumers sign up for them casually, often using an existing credential like their Facebook or Google login. But such accounts are increasingly being targeted as a way into

other accounts. In fact, according to the Javelin study, services like Uber, Instacart, and Grubhub represented 18% of account takeovers in 2020, and social media accounts were at 15%.

Social media, a goldmine of personal information fraudsters piece together to craft very convincing phishing scams. Through tricks or impersonation, they get victims to disclose login credentials, download malware, and/or send money.

“

*“By using corporate email for personal use, employees are inadvertently expanding the threshold for malicious actors to enter into a corporate network, completely unnoticed.”*

[SailPoint global Trust Issues Survey, Nov 2021](#)

“

*“The customer-first culture of the [food delivery] business, together with the need to fulfill orders quickly, means that transactions are less likely to be questioned... Additionally, fraud prevention is deprioritized because average order values are relatively low.”*

[The Dark Side of Delicious: Decoding Food Delivery Fraud on the Dark Web, Riskified blog, Aug 2020](#)

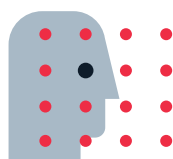




## DIGITAL IDENTITY LIFECYCLE—BEST PRACTICES FOR MILLENNIALS



**Make sure you know who you're letting in.** Use document-centric identity proofing at onboarding to ensure individuals opening new accounts are who they say they are. Let consumers know why you're asking them, for example, to submit a snapshot of a government-issued ID along with a selfie. Explain the security advantages for them of taking just a few extra minutes to do it.



**Take a biometrics-first approach to verifying the identities of active users.** While offering a range of identity methods, lead with biometrics, such as facial and/or voice recognition, since most millennials embrace these as both easy and secure. For millennial users who aren't into biometrics (a dwindling number), offer other quick and easy methods. Verify identities, for example, using password-less logins via push apps.



**Auto-invoke context- and risk-sensitive extra protections where appropriate.** Using linked and layered security technologies, step up identity confidence with additional identity authentication for high-risk transactions or at specific points in customer journeys. For example, passive behavioral biometrics and/or fraud analytics working invisibly in the background can spot unusual or risky consumer activity, triggering a 2FA identity authentication request before a particular transaction (funds transfer, login from a new device, account settings change, reinstatement of dormant account, etc.) goes through.



**Help them resolve account takeovers and identity thefts.** Even financial accounts, where the stakes are highest, have a poor record here. The [Javelin study](#) found that 69% of customers who experienced identity fraud said their financial institutions did not resolve the issue, and 38% of them closed their accounts. Understanding that consumers are stressed and emotional when account takeovers occur, every type of digital service should be prepared to be helpful. Provide information and guidance on the steps consumers should take as well as clear explanations of what the service will do, the process that will be followed, and what to expect in terms of resolution time.



## M+1: Gen X

1965 - 1980

One step downstream from millennials is gen X. If you're in gen X, you were born between 1965 and 1980. The oldest among you entered the working world just as Macs and PCs were transforming it. The youngest among you grew up with MTV and Sony Walkmans, graduating to MP3 players in young adulthood. As a generation, you're comfortable with new technology, having rapidly moved to the internet and cell phones as they emerged. You're keen on social media and digital services, but have adopted a narrower range of them, at lower rates than younger generations. You still watch a lot of video, but now it's YouTube.

MTV  
TECH BOOM  
FIRST MACS & PCS  
SONY WALKMANS  
EMERGING  
CELL PHONES

Gen Xs have more money, but also more debt, than other generations. Initially building careers during the tech boom, gen Xs had to withstand the tech bust and multiple economic recessions. And while gen Xs suffered worst during 2008 global financial crisis, they've done best during the pandemic, seeing their wealth rise by 50% over the past two years ([Bloomberg](#)).



**2008**  
suffered the worst  
global financial  
crisis



rising wealth by  
**50%**  
over the past two years





## WHERE THEY'RE COMING FROM

Compared to millennials, gen X is:

### Similar

**Similar** in willingness to use 2FA and biometrics, and resigned to, though not happy about, having their personal data tracked as part of the terms and conditions of using apps ([Entrust](#)).

### Less likely

**Less likely** to use Twitter, TikTok, Instagram, and Snapchat, though almost as present on Facebook (which gen Xs use more for staying in touch than for self-broadcast) ([Pew](#)). Significantly lower use of P2P payments and digital wallets. And while they use mobile banking apps almost as much as millennials, gen Xs use them less for depositing checks and transferring funds between accounts ([Chase](#)).

Gen Xs are less willing than millennials (60% compared to 70%) to share their personal information with an app to get more relevant, personalized, and/or convenient services ([Entrust](#)). They're also much less likely to reuse passwords ([Liminal](#)), use corporate emails for personal social media logins ([SailPoint](#)), experience stress around identity theft, or say they've been victimized by cyber threats ([National Cybersecurity Alliance](#)).

### More likely

**More likely** to report cybercrimes and identity thefts, and to say they've been locked out by an account takeover and had unauthorized charges on their accounts ([Allstate](#)). They use password managers a little more than millennials ([Liminal](#)). They have significantly more trust in brands to keep their data safe ([Fluent](#)).

Another thing to know about gen Xs is that many of them are parenting teenagers or young adults. So they're concerned with protecting the digital identities of their children and interested in tools and services that can help them do it in easy, low-friction ways. At the same time, they're influenced by their children's attitudes toward digital life (such as the strong preference for customization and desire to craft one's own digital identity discussed in the section on gen Z). Some gen Xs are also sandwiched—simultaneously caring for aging parents. And even if they're not active caregivers, they're likely involved with helping baby boomer family members make the transition to digital life and adopt good cyber hygiene practices.



## WHERE THEY'RE VULNERABLE



Gen Xs have better security behavior in general, and password hygiene in particular, than younger generations. Some of them may be exposing personal information, however, by oversharing on Facebook. Smart TVs that track searches and viewing, voice-enabled digital assistants, and fitness/health wearable devices and apps can also present data privacy issues and be points of vulnerability for identity fraud.

### Fraudsters are targeting gen X through:

**Phishing emails, texts, and robocalls.** These methods are the same as with millennials; the messages they target to gen X tend to be around financial information, better interest rates on credit cards, or parcel tracking.

**Cloud-based platforms, videoconferencing services, gig economy, and social media.** These vulnerabilities, described in the millennials section, are also relevant to gen X. But because gen Xs manage their passwords better, while also being in favor of 2FA, the threat to them may be lower.

## DIGITAL IDENTITY LIFECYCLE—BEST PRACTICES FOR GEN X

Same measures as for millennials, but with a couple of twists:



### Promote biometrics, but also continue to support good password hygiene.

Encourage gen Xs to enhance their already responsible behaviors and layer on added protections.



### Provide tools/services enabling them to oversee digital identity and data privacy

**for minor-age children.** What can your business do to help parents guide their children in making good privacy settings choices? How can you alert them to account settings changes or unusual user behavior indicative of fraud risk? Do you have a process in place for rapidly notifying them of any data breaches affecting their family?





## M-1: Gen Z

1995 - 2010

One step upstream from millennials are gen Zs. If you're gen Z, you were born between 1995 and 2010, and many of you have never known a world without smartphones and social media. Chances are you've grown up playing videogames featuring immersive worlds, online social interaction, and numerous opportunities for customization. Your online experiences are providing the inspiration and momentum for the emerging Metaverse. This comprehensive digital realm blends social, games, and shopping with virtual reality (VR) and

augmented reality (AR) to create new possibilities for economic transaction and social interaction. Gen Zs will be Metaverse builders and first adopters.

Gen Z's economic impact is large and growing: Already gen Zs makes up more than 40% of global consumers ([McKinsey](#)), although they're only the third-largest group of digital buyers ([Statista](#)).

In less than a decade, gen Z workforce participation will increase by 300% ([Bloomberg](#)), with combined earnings surmounting that of millennials ([BoA](#)).

SMARTPHONES

ONLINE SOCIAL  
INTERACTION

IMMERSIVE WORLDS

EMERGING  
METAVERSE



**40%**  
of global  
consumers



**300%**  
increase of  
workforce



## WHERE THEY'RE COMING FROM

Compared to millennials, gen Zs are:



### Similar

**Similar** in generally favorable attitude toward biometrics and 2FA. They're also similar in willingness to share personal information with an app in return for better products and services. Although in the case of gen Zs, there's a more explicit expectation of a commensurate exchange. Gen Zs want to know: "What's in it for me?" About 2/3rds of gen Zs say it's okay for companies to collect their data as long as they're transparent about what they're doing with it. And get this—91% actually believe access to such information is a human right! ([ViacomCBS](#)). Still, like millennials and other generations, gen Zs are unsure how to exercise this right; 54% say it takes too much time to manage their data across every app and service ([Entrust](#)).



### Less likely

**Less likely** to shop primarily online; gen Zs shop fluently across all commerce formats and are more inclined to make in-store purchases than millennials. In general, they see less distinction between the physical and digital worlds than other demographics and want to be able to move seamlessly between them.

Gen Zs are less likely to use digital wallets, although usage is up 50% since 2020 ([Digital Transactions](#)). In addition, they're currently less likely to use a mobile banking app for paying bills, transferring money between accounts, depositing checks, and viewing account statements—which could simply reflect their stage in life.

A lower percentage of gen Zs (39%) than any other demographic say they trust brands to keep their data safe ([Fluent](#)).





WHERE THEY'RE COMING FROM  
Compared to millennials, gen Zs are:

## More likely

**More likely** to prefer face scan authentication when using mobile apps. And gen Zs have the highest willingness to use 2FA for both mobile and web. That's especially the case when logging in from a new device, where the top preference of gen Z is for face scan + PIN code ([PYMNTS](#)).

Gen Zs are more likely than millennials to use mobile banking apps for creating/tracking budgets and savings goals. They're the biggest users of Apple Pay for digital purchases ([eMarketer](#)) and though behind millennials in usage of other digital payment services, including P2P, they're catching up ([Chase](#)).

Gen Zs are the largest cohort of TikTok, Instagram, Snapchat, and Twitter users, in preference over Facebook ([Pew](#)). In the vanguard of the creative economy, they're more likely to approach social media as not only a means of connecting with others, but a platform for entertainment, content generation, and self definition, expression, and promotion.

More than any other demographic, gen Zs (75%) say they're more likely to buy a product if they can customize it ([Center for Generational Kinetics](#)). They tend to see the brands they choose as extensions of who they are.

A related characteristic, gen Zs regard their digital identity as something they should be able to create and control, and that should be coherent across platforms (vs. presenting a different identity to different services).

In regard to security, gen Zs are more likely to say they've been locked out of accounts by account takeover and to report unauthorized charges on an account ([Allstate](#)). They're also the most likely of all generations to say they've experienced a cyber threat ([National Cybersecurity Alliance](#)).

This generation is the most likely to use a single password for all online accounts ([Liminal](#)), while worrying less about their passwords being stolen or hacked. At the same time, they're more concerned about webcam and social media hacking, and location sharing. ([AVAST/YouGov](#)). More than 75% of gen Zs are using corporate emails for logging into social media—significantly higher than any other demographic ([SailPoint](#)).



## WHERE THEY'RE VULNERABLE



Gen Zs are vulnerable to theft of digital credentials and account takeovers partly because of the fluidity with which they engage in digital activity. Often they're complacent about these interactions, especially when it comes to non-financial accounts that appear less risky, but could be used by fraudsters as a gateway to bigger things. They may be less risk-aware because at this stage of life they have less to lose. But gen Zs are nevertheless vulnerable through security holes in social media platforms and digital services. And, contrary to widespread presumptions, gen Zs are more vulnerable to phishing than any other demographic, including—by a large margin—baby boomers!

### Fraudsters are targeting gen Z through:

**Phishing emails and texts.** The SailPoint study found that 46% of gen Zs said they would open a suspicious looking link or attachment.

**Impersonation of digital services.** Fraudsters pose as a digital service offering rewards, parcel tracking, or P2P transfer confirmations. Gen Zs may be more likely to fall for such schemes because of their willingness to share personal information if there's something in it for them.

Or fraudsters may imitate a P2P payment platform such as PayPal, Square, or Venmo, to try to get the victim to make a payment, supposedly to a known contact or service.

**Social media requests and chatbots.** Fraudsters pretend to be acquaintances or friends of friends looking to connect.



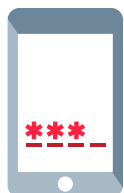


## DIGITAL IDENTITY LIFECYCLE—BEST PRACTICES FOR GEN Z

Same as for millennials, especially in regard to biometrics, plus:



**Educate them on how to handle phishing.** Give gen Zs fast, easy steps for what to do with an email or text that looks suspicious (and a checklist showing what to look for). Explain why it's so important to follow these steps (rising incidence rates of blindingly fast total account takeover, etc.).



**Let them customize identity verification.** Offer plenty of choices, such as which 2FA methods and when to invoke them. Provide gen Zs with information about the relative risk of various digital activities and guidance on how to match up risk with the right level of protection.



**Create seamless authentication transitions between digital and physical.**

Without having to re-authenticate, for example, consumers should be able to make purchases from their phone on a company's web site and in its stores. And consumers who've been researching loan rates on a mobile banking app should be able to use that app to verify their identities if they drop by a branch for assistance.



**Safely span business and personal interactions.** Encourage consumers not to use their business email for setting up personal accounts and tell them why. At the same time, use backend intelligent automation to create invisible, secure links between business and personal accounts, providing time-saving umbrella features.



**Introduce AI-based security layers.** Gen Zs generally have a positive attitude toward new technologies, such as machine learning and other AIs. In fact, the [Center for Generational Kinetics](#) found that 64% of gen Zs think AI will have a positive impact.



## M+2: Baby boomers

1945 - 1965

MAINFRAMES

MINICOMPUTERS

DROVE DEVELOPMENTS

ADOPTED EMAIL &  
WEB BROWSERS

FIRST WEBSITES

Two steps downstream from millennials are the baby boomers. If you're a baby boomer, you were born between 1945 and 1965. Many boomers are a lot more comfortable with technology than their generation is given credit for. First to use mainframes, minicomputers and personal computers in the workplace, they kept at and drove developments during a time when usage and troubleshooting were far more problematic than today. In the '90s, they adopted email and web browsers in large numbers, with many boomers managing or creating first web sites for their businesses.

While baby boomers have been slower to adopt mobile apps and digital services, usage has surged since the pandemic. Bank and brokerage branch closings, necessitating remote transactions, along with growing interest in touchless payments have motivated boomers to move more aspects of their daily lives to digital. According to a [Harris Poll, conducted for Plaid](#), the highest demographic growth rate in fintech usage from 2020 to 2021 was among baby boomers.



**'90s**  
adopted email &  
web browsers in  
large numbers

usage of mobile  
& digital services

**surged**







## WHERE THEY'RE COMING FROM

Compared to millennials, baby boomers are:

### Similar

**Similar** in willingness to use 2FA.

### Less likely

**Less likely** to favor biometric authentication methods. Boomers are still leaning heavily toward username/password, although this isn't as evident with mobile app users. Some of the resistance may be because boomers think there's a technical learning curve they'll need to traverse with biometrics and/or because they don't trust the technology.

Boomers use a narrower range of social media and spend less time with it. According to the [Pew Research Center](#), about 50% of baby boomers were on Facebook in early 2021, and 49% used YouTube. Boomers value social media most as a way of keeping in touch with family and friends—and, according to [Statista](#), they're far less likely to rely on it as a news source than any other generation. Only 40% of baby boomers, reports [SproutSocial](#), view social media as essential to their lives.

They're also 40% less likely to use mobile banking (although they're the largest demographic for online banking). Even fewer use mobile digital wallets (boomers are almost three times less likely than millennials), according to research by investment intelligence firm [Capco research reported by eMarketer](#). Usage of P2P payment methods is also relatively low—at 14.5%, half the usage rate of millennials.

Baby boomers are less likely than millennials to experience stress around identity theft or to say they've been victimized by cyber threats. According

to FTC complaint numbers, they're also much less likely than millennials to be duped by fake check scams or email scams. The [Sailpoint study](#) also found that boomers are better than millennials at avoiding phishing emails.

### More likely

**More likely** to be victimized by online fraud, such as fake ecommerce sites. Same goes, according to an [2021 Allstate US survey](#), for getting locked out of an account by account takeover fraud and finding unauthorized charges on their bank or credit card accounts. Yet baby boomers are also more likely to follow good password hygiene practices and to use a password manager ([Liminal](#)).

Boomers have the highest level of trust among all demographics that brands will protect their data ([Fluent](#)). Yet, because they trust technologies less than companies, they're cautious about sharing their personal information with apps.



## WHERE THEY'RE VULNERABLE



Baby boomers are vulnerable to online fraud because, as a whole, they are less digitally savvy and comfortable than younger generations. Some may also be exposing personal information by oversharing or not properly configuring access settings on Facebook. Like other generations, boomers are concerned about data privacy. But unlike younger people, their reason for inaction isn't generally time constraints, a bias toward convenience, or even resignation; it's incomprehension. Many boomers admit they don't know where to start in terms of controlling privacy and protecting their digital identity.

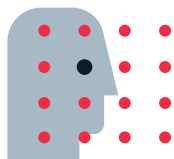
### Fraudsters are targeting baby boomers through:

#### **Robocalls, phishing emails, and ecommerce scams.**

Pitches aimed at baby boomers are often around investments, life insurance, healthcare, and fake products or product warranties. Fraudsters may trick boomers through email offers into making purchases at a fraudulent web site (Amazon tops the FTC's list of impersonated businesses). They may also pretend to be a government agency, such as the IRS or SSA. Although, according to 2021 research by [ACI Worldwide](#) and [YouGov](#), boomers had a lower incidence rate of phone scams during the last tax season than millennials—a flip from the previous year.

## DIGITAL IDENTITY LIFECYCLE—BEST PRACTICES FOR BABY BOOMERS

Same measures as for millennials, but with a few additional services:



#### **Help baby boomers understand and try out biometrics.**

Provide information and step-by-step guidance (text and large, clear pictures).



#### **Always have human assistance available.**

Baby boomers are much more comfortable with digital processes when they know they have the option of talking or chatting with a real person.





## M-2: Gen Alpha

2010 - PRESENT

AI NATIVES  
TECH-SAVVY  
INSTANTANEOUS  
INFORMATION  
PERSONALIZED  
LEARNING

Two steps upstream from millennials, is gen alpha. It's too soon to write this section. Born 2010 to present, the oldest individuals in this generation are just 12 years old. But we can indulge in a bit of speculation.

One way to think about gen alpha: They're the first digital identity natives. As their leading edge enters the teenage years, the concept of digital identity—which has been an emerging, evolving idea even for gen Z—is rapidly becoming a widely understood bedrock of daily life. Most gen alphas won't be able to remember or imagine a world without it.

What will that mean for the digital identity lifecycle? We don't know, although we can expect gen alpha

to accelerate trends we see with gen Z, such as demand for customization and desire to create and control one's own digital identity. With access to ever more powerful tools for manipulating software according to user preference and self-expression, gen alphas are likely to expect interactions with digital service providers of all kinds to offer similar latitude and freedom. Meeting these expectations will present new challenges in balancing user experience with security. And because gen alphas will grow up in the Metaverse, interactions with AI, VR, and AR will likely become increasingly important elements in digital identity lifecycles as well.



desire to  
**create  
& control**  
one's own digital identity



**AI · VR · AR**  
digital ID lifecycles must evolve



# Think bigger and smaller

Across all generations, digital activity is now the fabric of daily life. This is an opportunity for organizations of all types to think bigger in terms of potential customer base and types of services to offer. Opportunity comes not only from being able to interact with more consumers, but also from the ability to collect and analyze transactional data to understand more about them. Even local shops and restaurants can now operate more like e-commerce merchants.

Organizations also have to think smaller, focusing, like e-commerce leaders, on the needs and preferences of granular consumer segments and even individuals. This big-scale/small-focus approach requires a connected, layered solution for digital identity lifecycle management—now a fundamental aspect of consumer experience.

To learn more about biometrics and authentication solutions for all generations visit, [www.miteksystems.com](http://www.miteksystems.com)



A NASDAQ® company | miteksystems.com Copyright © 2022 Mitek Systems, Inc. Confidential. All rights reserved.

This document is for general information purposes only and is not intended to be and should not be taken as legal and/or regulatory advice on any specific facts or circumstances. All information provided in this document is provided "as is" without warranty of any kind, whether express or implied. Contents contained in this document may not be quoted or referred to for any purpose without the prior written consent of Mitek or its affiliates.