loginradius

REPORT

# Consumer Digital Identity Trend Report 2023

By Deepak Gupta and Rakesh Soni

# Table of Contents

# Executive Summary

Our digital identity is a key component of today's digital economy. Consumers expect a seamless, secure ability to prove their identity while accessing their favorite online services. No wonder, the key to establishing trust with brands and businesses, today, is to manage customer identity across multiple channels.

The report offers an exclusive look into the state of global consumer identity trends in 2023. It provides insights into consumer behavior around digital identities, along with a detailed analysis of their behavior trends and lifecycle.

The world is changing, and so are the ways in which consumers interact with their digital identities. Advances in artificial intelligence and the increasing interconnectedness of our global society have transformed businesses and led to a new generation of consumers who expect seamless and intelligent access to products and services.

Businesses that want to stand out in a highly competitive world will need to make a huge improvement in their consumer experience. The experience includes not just your interactions with your consumers but also theirs with your brand, starting from registration to checkout.

To figure out what consumers want, their behavior and pain-points, businesses are increasingly looking for authentication methods they prefer, like passwordless login or multi-factor authentication via email or SMS, or social login.

We analyzed data from the LoginRadius Customer IAM (CIAM) Platform which is used by over 500 brands  around the world. In this report, we will help you understand the **eight core trends around consumer identity**, ranging from the preferred authentication methods, preferred identity verification to industry-standard performance benchmarks.

# Methodology

The data for this research was collected from the LoginRadius CIAM Platform, which empowers businesses to securely manage consumer identities and provide a unified, seamless experience for their consumers.

LoginRadius offers a fully-managed, comprehensive cloud-based CIAM platform that is rated #1 in the identity market and presently used by over 500 brands globally including many Fortune 1000 companies. The platform hosts and manages over 1.17 billion consumer identities.

The research was carried out with data from January 01, 2022 to December 31, 2022. While the actual numbers are not revealed, the report highlights comparative trends.

# About LoginRadius

LoginRadius provides a complete solution to an enterprise's Customer Identity and Access Management (CIAM) needs — including registration, authentication, authorization, single sign-on, security, directory service, and data governance. The platform is designed to provide a secure and privacy-compliant customer experience while freeing up developers from all-things identity.
The LoginRadius CIAM platform is an Identity-as-a-Service (IDaaS) with two core components – Low-code Identity Workflow and No-code Identity Infrastructure. These components make it easy for businesses to create the perfect customer experience on its fully-managed cloud identity infrastructure.

We also offer open-source SDKs, along with integrations with over 150 third-party applications, pre-designed login interfaces, and top-notch data security products. Our developer-friendly CIAM identity platform is easy to deploy and can be managed by organizations with basic technical prowess. The platform is extensible, where enterprises can add their own customizations and integrations as needed.

LoginRadius is recognized by analyst firms like Gartner, KuppingerCole, and Forrester as a leader in the customer identity and access management (CIAM) space. The platform manages to retain its top position as an industry leader every year. Its technology partner Microsoft is also a major investor in the company.

For more information about **LoginRadius**, book a **free personalized demo** or **contact sales**.

***The digital revolution has placed a greater emphasis on customer identity solutions as more businesses recognize the importance of providing secure and streamlined access to their services. We recognized early on how providing hassle-free and seamless onboarding to users is critical for driving conversions and building customer loyalty.***
***We are committed to our ongoing product development and enhancements to meet the evolving needs of our customers. Our success in helping businesses at a staggering rate is a testament to the value we bring to the market and the trust that our customers have in our platform.***

- Rakesh Soni
CEO and Co-Founder, LoginRadius

# Key Terminologies Used

- **Authentication:** Authentication refers to the process of verifying and validating the identity of an individual, ensuring that they are who they claim to be.

- **Business/Companies:** LoginRadius clientele who use our identity platform on their websites or applications. In this report, we use the terms business and companies interchangeably.

- **User/Customer:** The end-user who is registering or logging in to an app/website.

- **Multi-Factor Authentication (MFA):** Multi-factor authentication (or MFA) is a multi-layered security system that verifies the identity of users for login or other transactions. It prevents unauthorized access to a user account in case of any suspicious activity by prompting the user to provide an additional proof of identity for authentication.

- **Passwordless Login:** A passwordless authentication system swaps the use of a traditional password with other frictionless security methods like a magic link, fingerprint, PIN, or a secret token delivered via email or text message.

- **Phone Login:** Phone login allows the user to register or log in to an account using a password and a phone number instead of email.

- **Social Login:** Social login enables users to use existing credentials from various social providers like Facebook, Google, Twitter, and more to register or login with a single click on a website or mobile application.

- **Standard Login:** Standard login is the traditional method of registering or logging in to an account using a password and a unique ID such as a username or email address.

- **Authentication Token:** The token through which a user can authenticate or prove its assertion over a platform.

# Consumer Trends Observed on the LoginRadius CIAM Platform

## A Brief Overview of Standard Login Trends

**Registration Forms**

Everything begins with a user signing up to use your platform, and you only get one chance to make a good impression.

Registration forms can be an intimidating obstacle for most businesses. It is important to keep them easy, quick, and simple to fill out—as lengthy registration can increase bounce rate. There is constant research going on how to design forms that convert and what validations to apply.

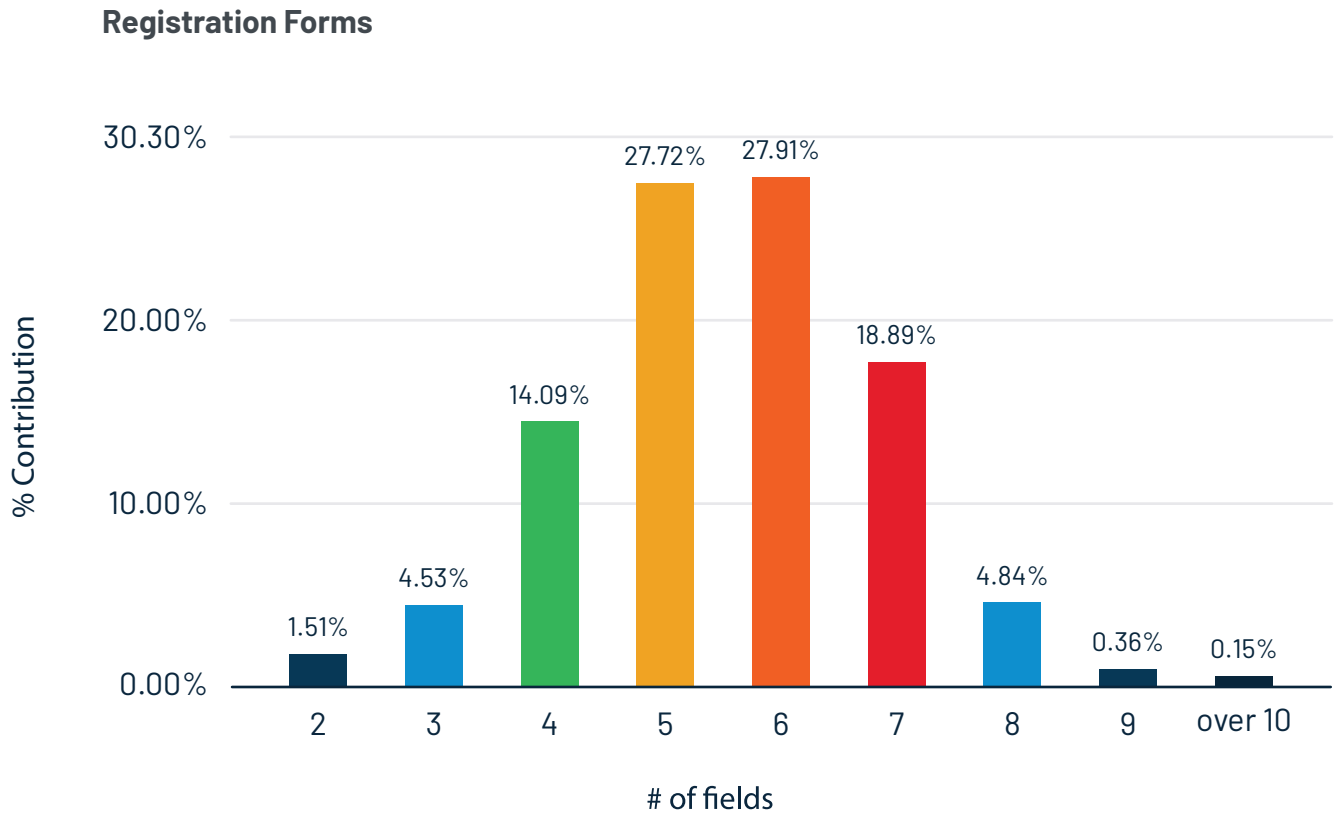
Optimizing a registration form is an art of its own. It needs a certain empathy for a customer and a certain type of creativity. If your registration form is not perfect you're losing a lot of possible new customers.

There's no "right" number of fields to collect, but there is such a thing as too many.

To get a deeper understanding, we have looked at the number of fields in our registration module and tracked the amount of data that is being collected at the start of a customer journey.

During the registration process, the amount of information users are asked to provide has a huge influence on how likely they are to proceed to sign up for an account.

According to our research, the percentage of companies using five (27.72%) to six fields (27.91%) on their registration forms is higher than those who are using two (1.51%) to three (4.53%) fields. Majorly the traditional fields include first name, last name, email, phone number, username, password.




**Key Findings**

After in-depth research, we concluded that if you want to create an engaging website, you need to take your visitor's needs into consideration. The fewer fields you ask for, the more conversions you get along with a better user experience.

When working with LoginRadius clients, we always recommend running A/B tests on new fields to ensure they do not negatively affect the conversion rate.

A progressive profiling method can be a simpler alternative to multiple registration fields. A progressive profiling method is an alternative to multiple registration fields. The method lets users fill out their profiles bit by bit as they are ready. It helps businesses to split a potentially complicated registration process into multiple steps and capture business-critical information like email addresses, usernames, and passwords during the time of registration. Once they sign up for your website, you can ask them for additional information throughout the customer journey.

When customers land on your website, you want to make sure they have a positive experience. The progressive profiling method allows you to gather all the essential information about them with ease. As they interact with your brand, and take part in special events or engage on social media channels, they will transform into loyal customers..

> **For this report, multi-stage registration forms that are set up under progressive profiling are each counted as individual forms.**

## Forgotten Password

A forgotten password is when a user forgets their password and opts to have it invalidated so they can start over. It is a common issue that can happen to any user.

> **We calculated the percentage of customers who opted for the 'forgot my password' module, to get insight into how easily users could retrieve login credentials.**

Many companies are now building digital identity solutions to address the increasing demand for frictionless authentication that is currently being experienced in the digital realm.

We looked at the percentage of customers who use the 'forgot my password' module to gain access to their accounts. Our research showed that 24.14% of active customers use the 'forgot my password' tool. Of those customers, 81.55% actually retrieve their passwords, and 8.11% never reset their passwords.

| | |
|---|---|
| # of users who have forgotten password | 24.14% |
| # of users who actually reset/ retrieved password | 81.55% |
| # of users who never reset/retrieved password | 8.11% |

## Key Findings

The finding could be used as a benchmark for assessing customer satisfaction. If fewer than 24% of customers have used the "forgot password" module compared to 33% in 2022, you can use this gradual decline in customer interest to your advantage. You might want to explore this area further.

With increasingly sophisticated cyberattacks, you cannot afford to put your users' data at risk. One way you can keep hackers out of your system is by implementing an advanced authentication process.

The financial and public sectors, which are more prone to identity theft, can set up **multi-factor authentication**. This extra security layer can counter the threat without hampering the customer experience.

Besides, there is a natural and growing demand for password management solutions as they help both individuals and businesses to handle their security better. Moreover, increasingly complex regulatory and risk management environments in businesses are encouraging the implementation of these solutions among industries across the globe.

If your current authentication methods are not working, you can evaluate different solutions to offer your customers. For instance, if your users frequently forget their passwords when logging in, or not making an attempt to retrieve their passwords at all, you can look into providing alternative methods such as **passwordless login** or social login.

Learn more about alternative **authentication methods** here.

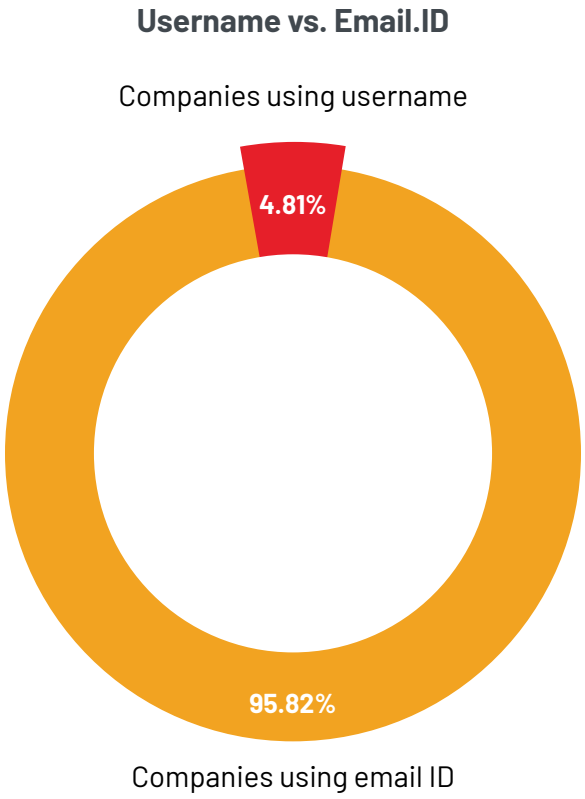
## Username vs. Email ID

According to industry analysts, businesses like the financial sector often use usernames instead of email addresses to identify users.

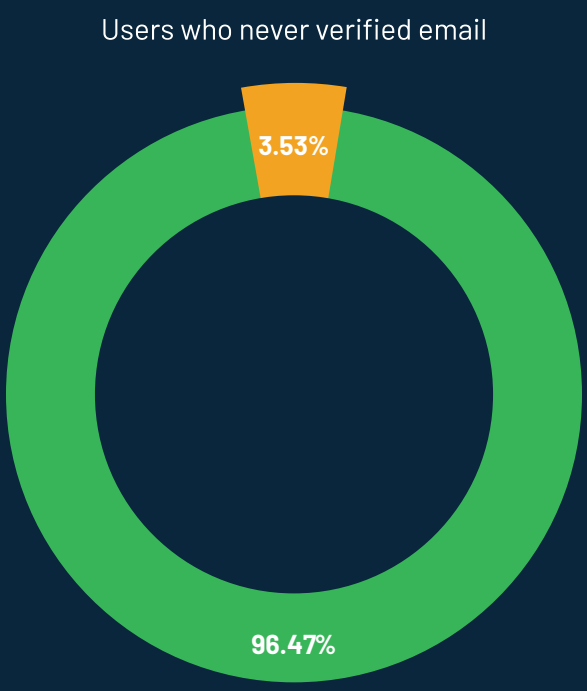
To figure out if our customers are switching their email IDs for usernames, we looked at the number of companies on our platform that allow their customers to log in with a username instead of an email ID.

Then again, many companies in the business environment use standard login in order to authenticate their employees. In this login method, a user registers and logs in with a unique ID and password. This unique ID can either be a username that they create themselves or an existing email address.

In our research too, we closely analyzed the companies on our platform that have deployed standard login with either a username or an email. Our results showed that 95.82% of companies offer standard login using an email ID, and only 4.18% offer standard login using a username. Of those, 96.47% successfully verified their email id and only 3.53% never put an effort to verify the same. However, this number has increased from 2.84% in 2022.



## Email Verification




### Key Findings

When we speak of standard practices, we recommend businesses to offer standard login only via email address. People usually already have an email address, so they can just register with their existing email address. To provide an extra field, businesses can add a username.

Afterall, in order to have a unique username for every account, they have to come up with something that has never been used before. This adds an unnecessary step to the customer journey.

Another option is to ensure that your application allows users to create a screen name. This way, you can still enable them to log in using an email, while giving them the option of creating a unique username.

Learn more about **standard login** here.

# A Brief Overview of Passwordless Login Trends

## Passwordless Login

We have explained how a frictionless login process can change the overall customer experience. By removing the inconvenience of remembering yet another password, passwordless login makes the experience simpler, faster, and less frustrating for end users.

A passwordless authentication system swaps the use of a traditional password with more secure factors. These extra-security methods may include a magic link, fingerprint, PIN, or a secret token delivered via the following medium:

- **Email:**
  The user is asked to enter the email address. A unique code (or magic link) is created and sent to the associated email ID. When the user clicks on the link, the server triggers an action to verify if the code is valid within a certain timeframe (e.g. three minutes) and then swaps it for a long-time validation token. If the authentication is successful, the user is let in.

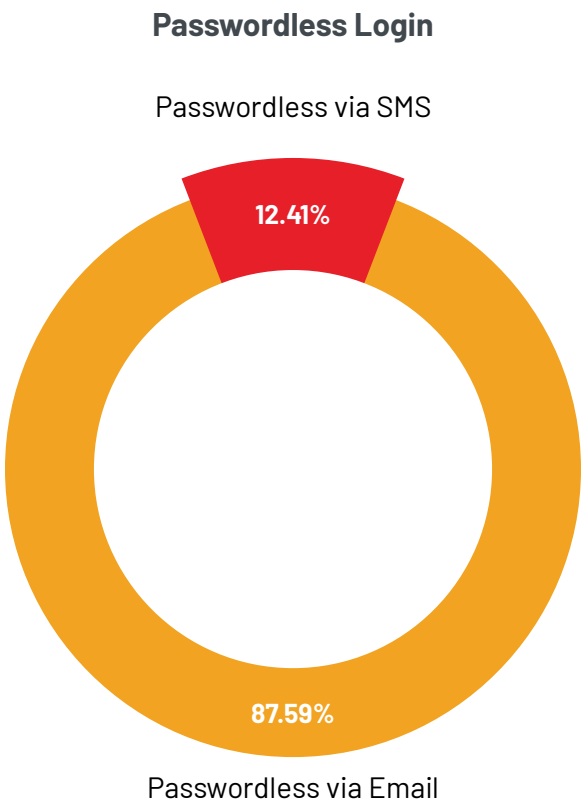
- **Phone:**
  The user is asked to enter a valid phone number; then the server sends a single-use code to that number which the user enters to log in.

With data breaches becoming more and more common in recent years, businesses are looking to alternative solutions that can serve the same purpose and ultimately replace the legacy of passwords.

Passwordless login provides endless benefits; some of which are greater convenience and better security. This solution is proving to be a better fit for enterprises because it meets all their authentication needs. The security provided by passwordless login is hard to beat.

In our research, we gathered data on how comfortable customers are with the passwordless login method. We then looked at the percentage of customers that prefer to use their email versus phone number when authenticating.

We found that, of the customers that use passwordless login, 87.59% prefer to log in with their email address, and 12.41% prefer to log in with their phone number.



## Key Findings

Based on our analysis, we see that passwordless login via email is more frequently used than passwordless login via a phone.

It is also important to keep in mind that the data we have used is predominantly from North America and Western Europe. These locations have had email login options available for much longer than phone options.  In developing nations, this order was reversed, as phone registration came before email login options were set up.

We expect to see more users opt for passwordless login via phone in the coming years. This trend should continue as more people become aware of its availability. We should also see a move towards passwordless logins overall.

As demand for a single sign-on solution grows because of the increasing use of multiple devices to access digital services, users will seek out frictionless logins. And even more popular will be passwordless login.

# A Brief Overview of Multi-Factor Authentication Trends

Multi-factor authentication is an additional layer of security that can be added to user accounts. Unlike 2FA authentication, which enables two layers of security, multi-factor authentication enables three or more layers of security.

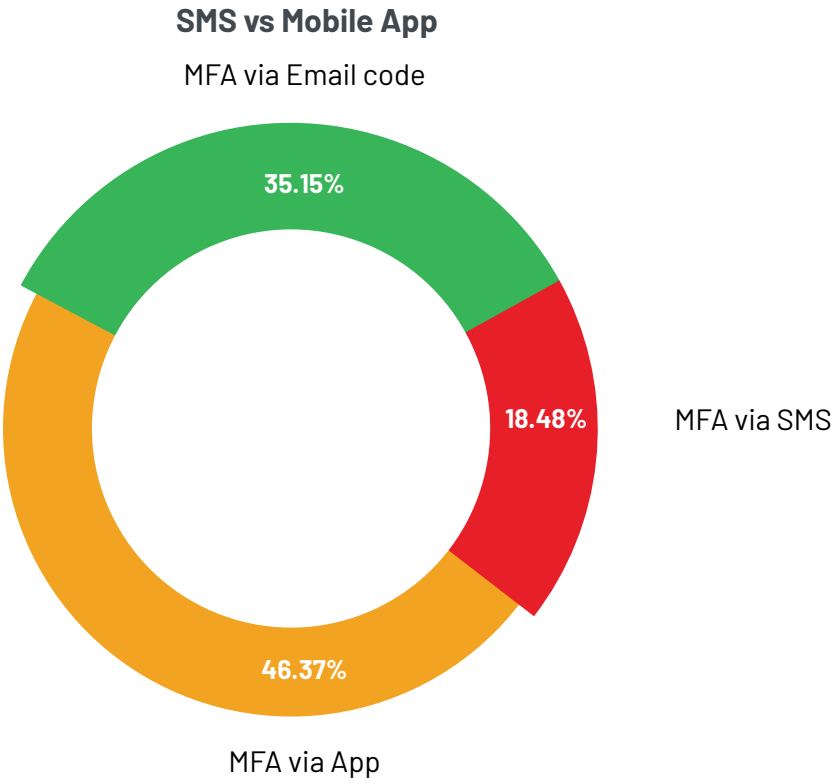
## SMS vs. Mobile App

> **To determine whether SMS messaging or authenticator apps were more popular, we analyzed users' preferences by studying their selections.**

The growing instances of security breaches and cyberattacks, along with a significant increase in online frauds, are among the key factors driving the growth of the market. Businesses are quickly adopting new methods of authentication to limit risk and win customer trust.

MFA provides customers with additional security in the form of an authentication code they must enter in addition to entering their credentials. For example, whenever a customer logs into your site, they are asked for their username and password. They are then sent an authentication code that must be entered before they are logged in to the account.

Based on our research, the three  most common verification methods are SMS messaging, authentication apps, and email codes. To further determine which verification method was the most popular, we compared the percentage of users that use SMS messaging over an authenticator app and email code. Our results showed that of the customers that use multi-factor authentication, 46.37% use MFA via an authenticator app, while 18.48% use MFA via SMS messaging, and 35.15% use MFA via an email code.




## Key Findings

There are three ways for a company to offer multi-factor authentication. One is via the company's own app; the second is through a third-party app like Google Authenticator or Microsoft Authenticator, and the third is via an email code.

We predict companies will continue to adopt multi-factor authentication via an authenticator app, since it is the simpler method of the three.  For one thing, an app doesn't require cell phones or internet service. That's a huge positive especially for customers who travel. As long as they have their devices with them, they can easily verify their identities. We've already seen our clients leverage the LoginRadius white-labeled authenticator app, in anticipation of the new trend.

The popularity of MFA via email code is also on the rise among users, likely due to the familiarity and convenience of email as an authentication method. As a result, we can expect to see more users opting for email-based MFA in the coming months.

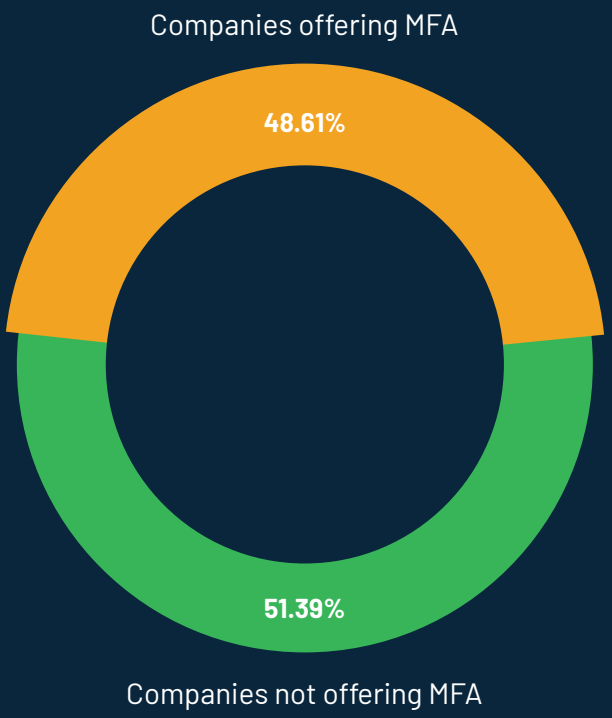
## Multi-Factor Authentication Adoption

> **We examined the percentage of companies that have implemented multi-factor authentication across their customer base.**

As we've discussed, MFA is a great option for companies to ensure data security while still providing a seamless customer experience.

To assess the adoption rate of MFA, we look at the percentage of companies offering it. Our data shows that 51.39% of companies do not offer MFA, but 48.61% of companies do.

### MFA Adoption



## Key Findings

> **Our results show that many companies still do not offer MFA.**

The primary reason behind this is the fact that businesses want to keep their authentication process as simple as possible; they do not want to add an additional step that will slow down or reduce conversions. Also, they are worried that the costs may be high, and implementation complexities make this option unworkable for some companies. For example, MFA via SMS requires a company to pay a fee for every message.

However, with data breaches becoming more sophisticated by the minute, MFA is a valuable tool to protect your customer's identity.

It is a simple yet powerful tool that allows businesses to protect their digital assets while ensuring that their customers are who they say they are. It is also the least disruptive method in regards to the customer journey.

We believe that in the next few years, MFA will become more common, especially for businesses in the financial sectors that deal with sensitive data and critical services. **Learn more about MFA here**.

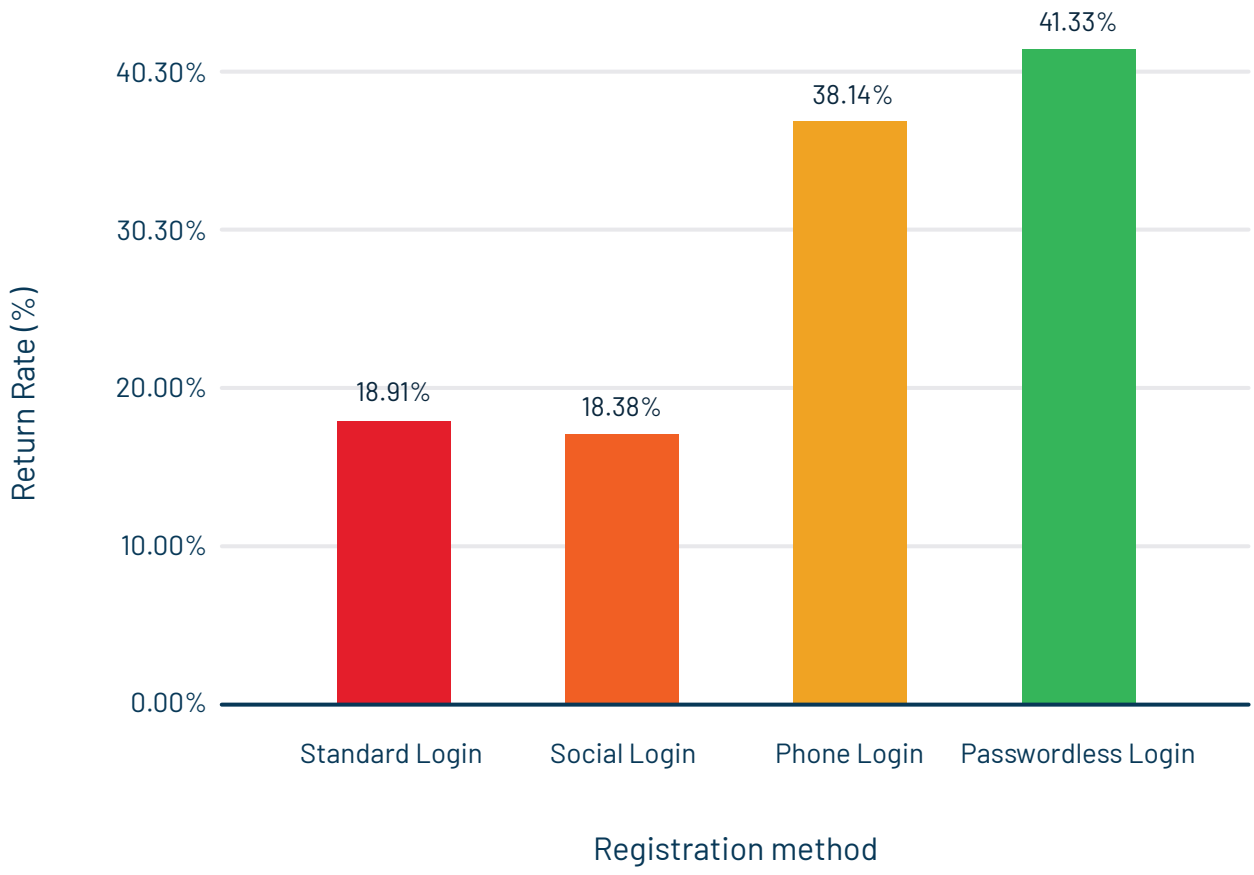
# A Brief Overview of Return Rate Comparison

> **We used our data to find out which authentication method provided the highest return rate.**

Your customer return rate is affected by the experience a user has throughout their journey with your product. If any part of that experience is not seamless, the customer may not return.

To better understand the effect of authentication methods on user retention, we compared the return rates for users who used different methods when signing in. Our research showed that users who used passwordless login had the highest return rate of 41.33%. Next is phone login with 38.14%, followed by standard login with 18.91%, and finally social login with 18.38%. This is in sharp contrast to last year's data that ranked phone login in the first spot, followed by passwordless, standard login, and finally social login.

**Return rate comparison**



## Key Findings

Our data indicate that passwordless login has the highest return rate; phone login is still close behind.

Passwordless authentication options are becoming more popular with consumers because they are the simplest form of verification. It swaps the use of a traditional password with easier and more frictionless methods like  a magic link, fingerprint, PIN, or a secret token delivered via email or text message.

Passwordless login eliminates the need to generate passwords altogether. There's a lot of good in this method of authentication for both users and organizations. Since users need not type passwords anymore, it leads to a better screen time experience. And for organizations, it leads to fewer breaches and support costs.

These findings indicate that the less friction caused by an authentication method, the higher the likelihood that a customer will return.

# A Brief Overview of Login Preference Trends

## Login Preference by End-Users

We analyzed data based on end-user demographics to determine login patterns.

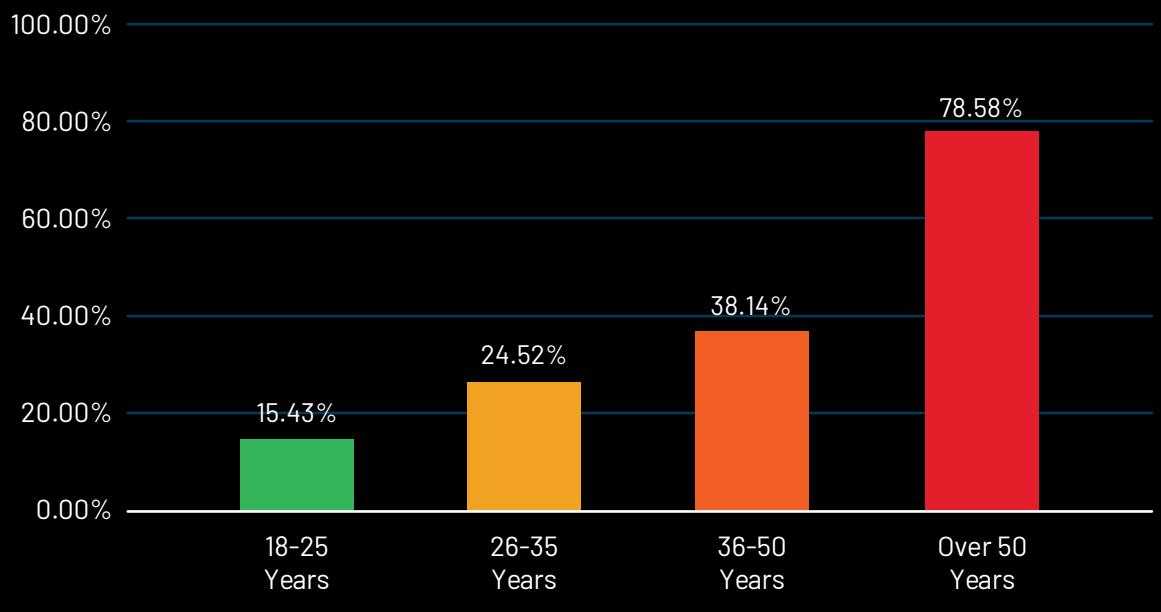
In the previous section, we discussed how new authentication methods like passwordless login and phone login are becoming increasingly popular and how businesses are opting for these options. While standard and social login remain common methods of authentication among users, businesses have begun to rely on newer ways to verify identities.

In the past few years, social login has increased in popularity, but standard login still tends to be one of the most used. We also analyzed audience demographics to determine which method of authentication is more widely used by different segments of the population.

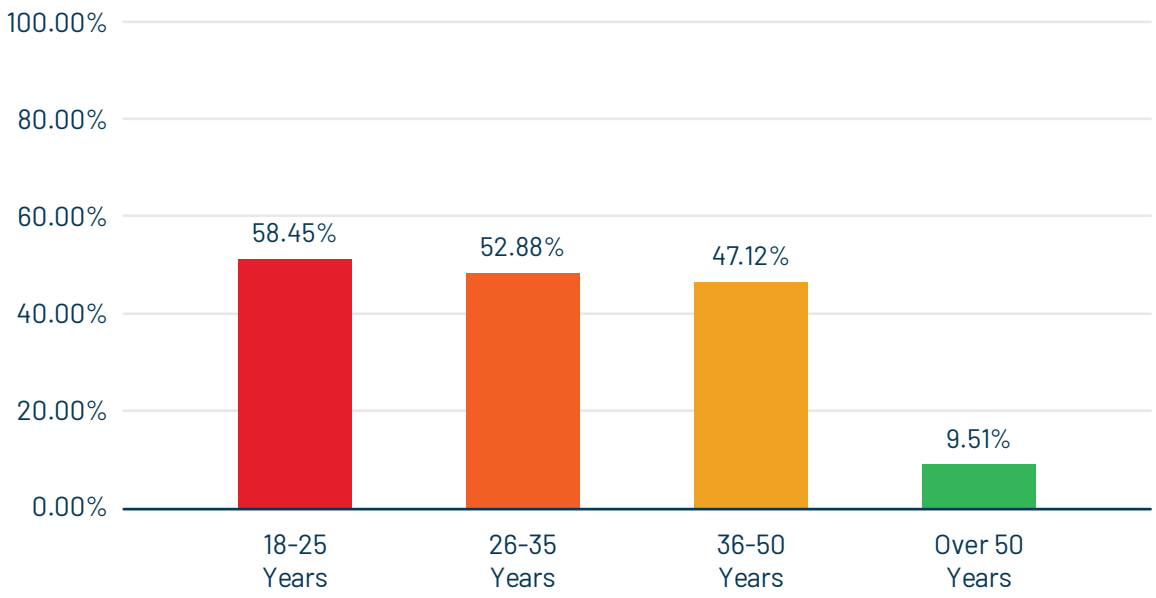
When comparing login preference by age, our results showed that as the age increases, so does the preference for standard login. For example, only 15.43% of 18-25 year-olds prefer standard login compared to 78.58% of over 50s. When looking at the data, we can see that this is the reverse for social login. 58.45% of 18-25 year olds prefer social login compared to 9.51% of over 50s.

## Login Preference by Age

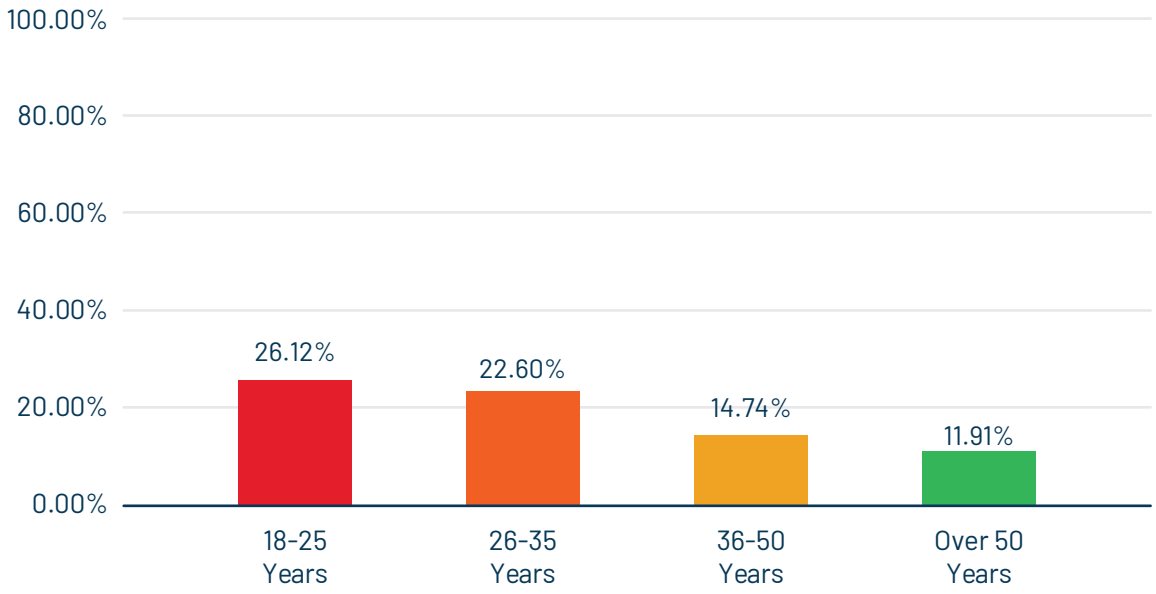
### Standard Login



## Social Login

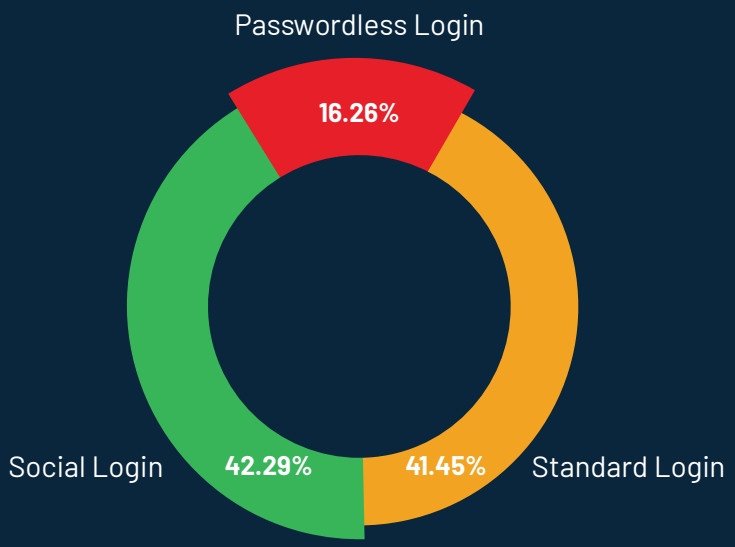



## Passwordless Login

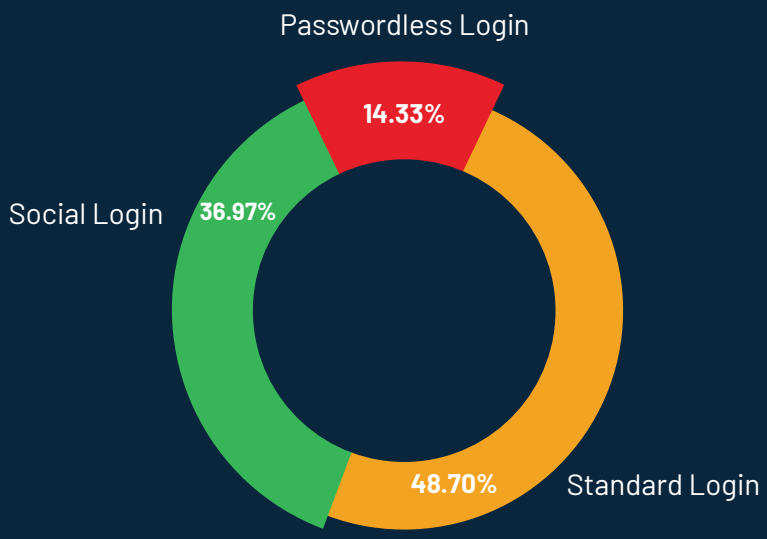


When comparing login preferences by gender, we can analyze by our data that there is no real significant difference. For standard login, 48.70% of females prefer this authentication method and 36.97% prefer social login. Similarly, 41.45% of males prefer standard login, and 42.29% prefer social login.

**Login Preference by Male**




**Login Preference by Female**




## Key Findings

Our data shows that the younger demographic is more likely to use social networks, but as age increases social network usage decreases. Gender, however, does not appear to be a significant factor influencing login preference.

These results suggest that social login may be more appealing to younger users than other registration methods. Thus, if your site has a high percentage of users in this demographic, you may want to consider offering social login as an option along with the standard registration process.

**Learn more about social login here.**

## Social Login Preference by End-Users

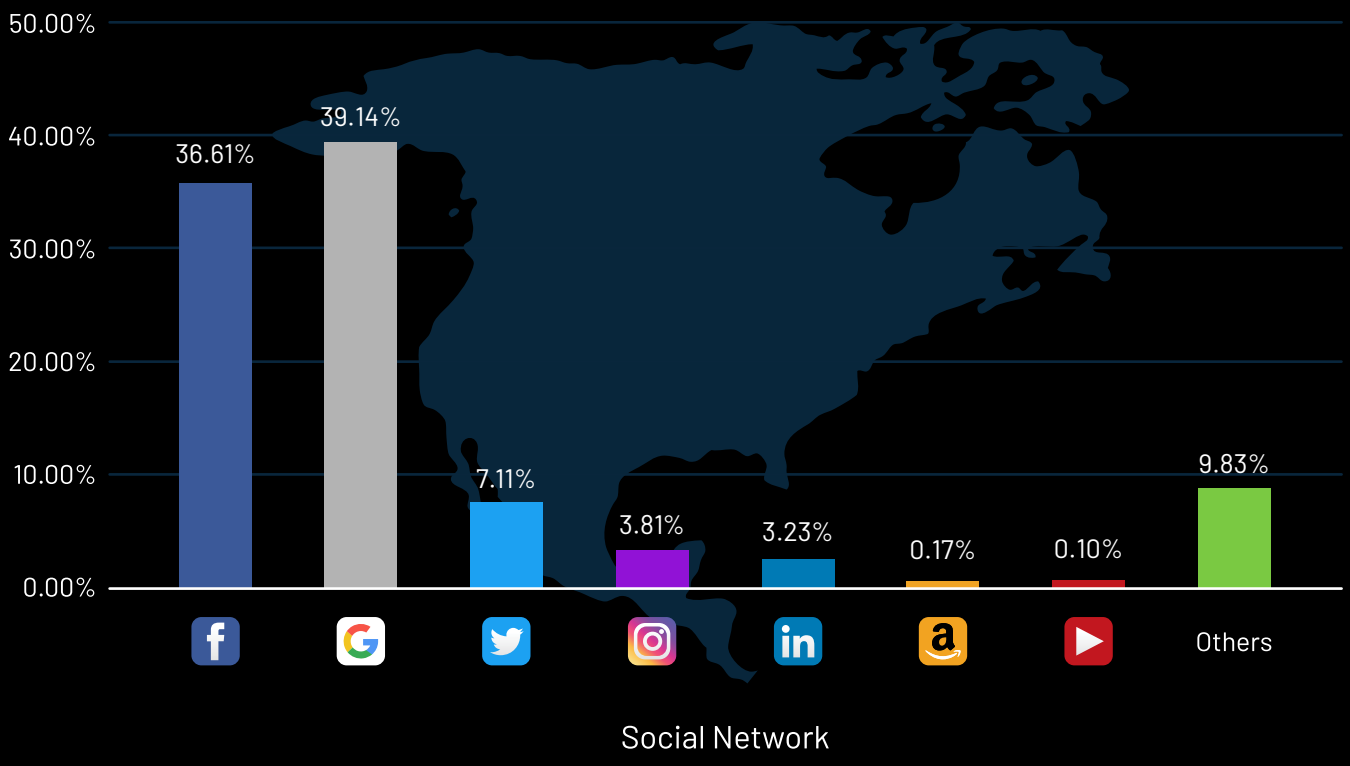
> **We looked at the social login preferences based on end-users' geographic locations.**

Social login is one of the most popular authentication methods, as it provides users with a quick and easy way to authenticate and gain access. It is also very convenient for customers, as they can use existing social network accounts such as Facebook, Twitter, Google, and LinkedIn to log in.

To compare the popularity of social networks in different countries, we looked at which social networks were most popular among people in each country.

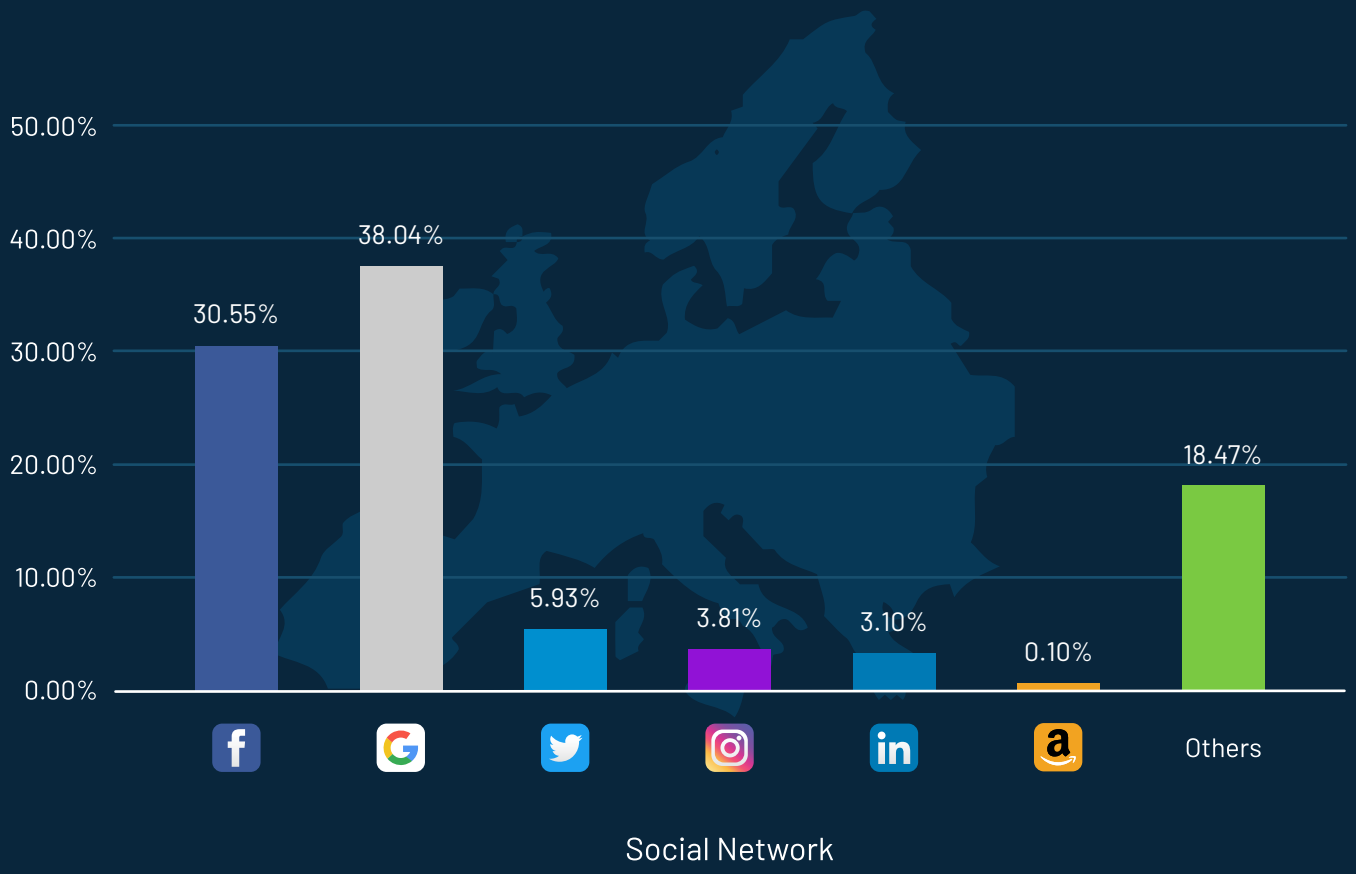
Based on our data, we can see that in North America, Google and Facebook are the most popular social networks to use when logging in with social accounts. Google is being preferred by 39.14% of users, and Facebook by 36.61%.

### North America Trends



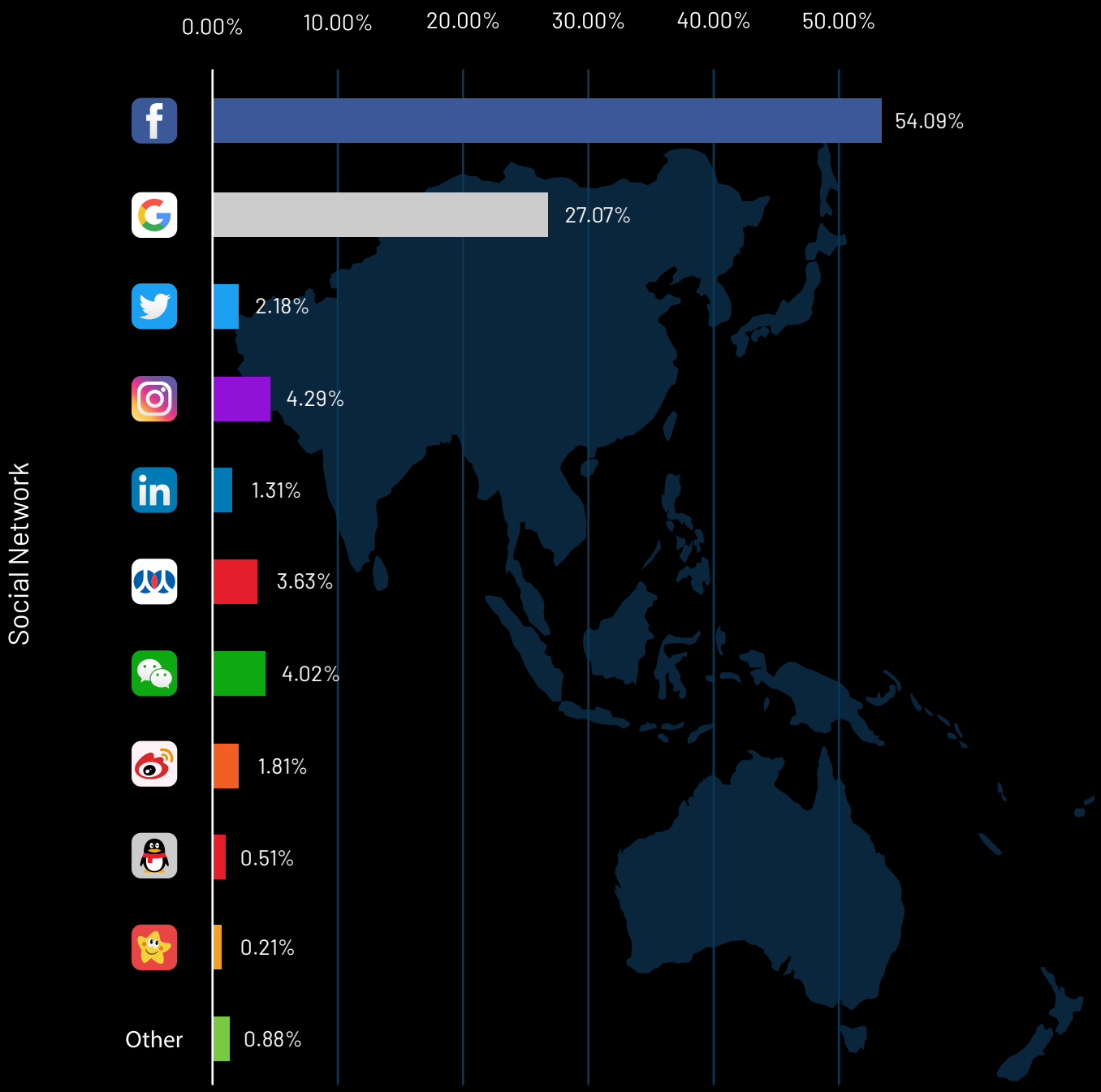
In Europe, we can see a similar trend. Google is preferred by 38.04% of users, and Facebook by 30.55%.

**Europe Trends**



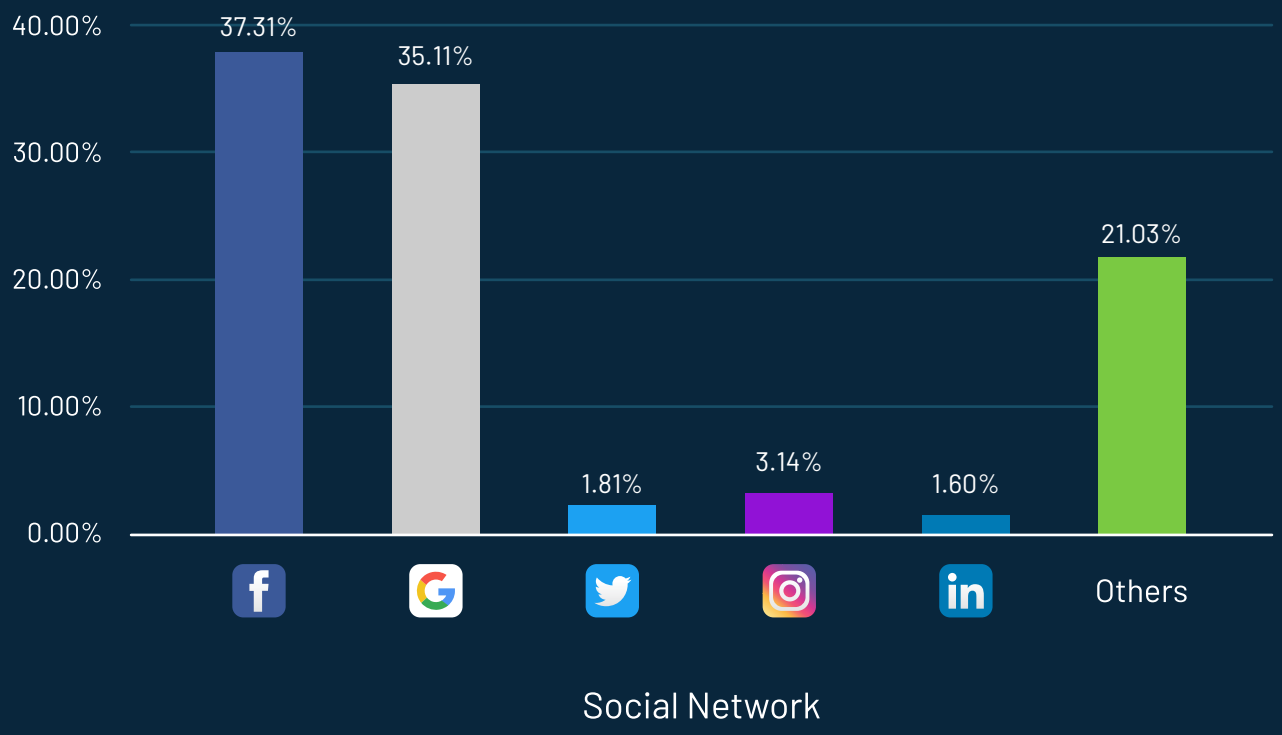
In the APAC region, we can see other social networks increasing in popularity. Facebook is still preferred by 54.09% of users and Google by 27.07%. However, our data shows that while Chinese-based social networks like RenRen are also showing strong results, WeChat's popularity has slightly dropped since last year. WeChat is preferred by 4.02% of users in 2023, and RenRen is preferred by 3.63% of users.

**APAC Trends**



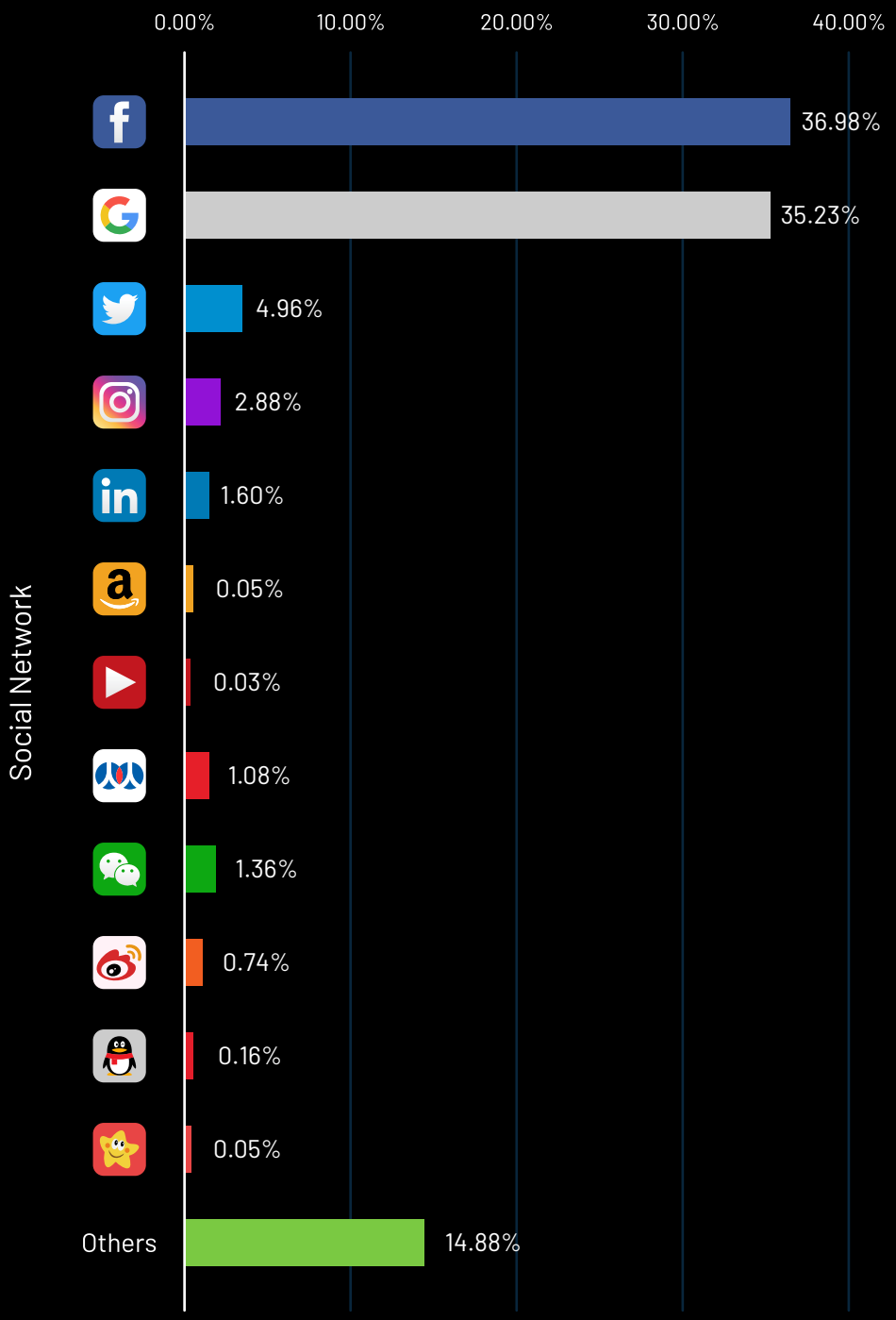
In the Rest of the World (RoW), we can see the login preference trends favor the North American based social networks. Facebook is preferred by 37.31% of users, and Google by 35.11%.

**RoW Trends**



When combining all the data, regardless of the user's region, we can see that Facebook and Google are dominant. Facebook is preferred by 36.98% of users, and Google by 35.23%.

**Overall Social Login Preferences**



## Key Findings

Based on our research, we can safely say that North American networks have become the dominant social login methods. Facebook and Google are by far the most popular.

However, if we look at the APAC region, we can see slight differences in trends when comparing China, Taiwan and India. Here we see WeChat and RenRen are popular social networks in China and Taiwan, but not as much in India.

The social media platforms Facebook, Google, Twitter, and Instagram are all banned in China. This may explain why they are not as popular in the APAC region.

Learn more about the future of social login by reading our white paper, **Social Login Reconsidered**.

# A Brief Overview of Login Preference by Businesses

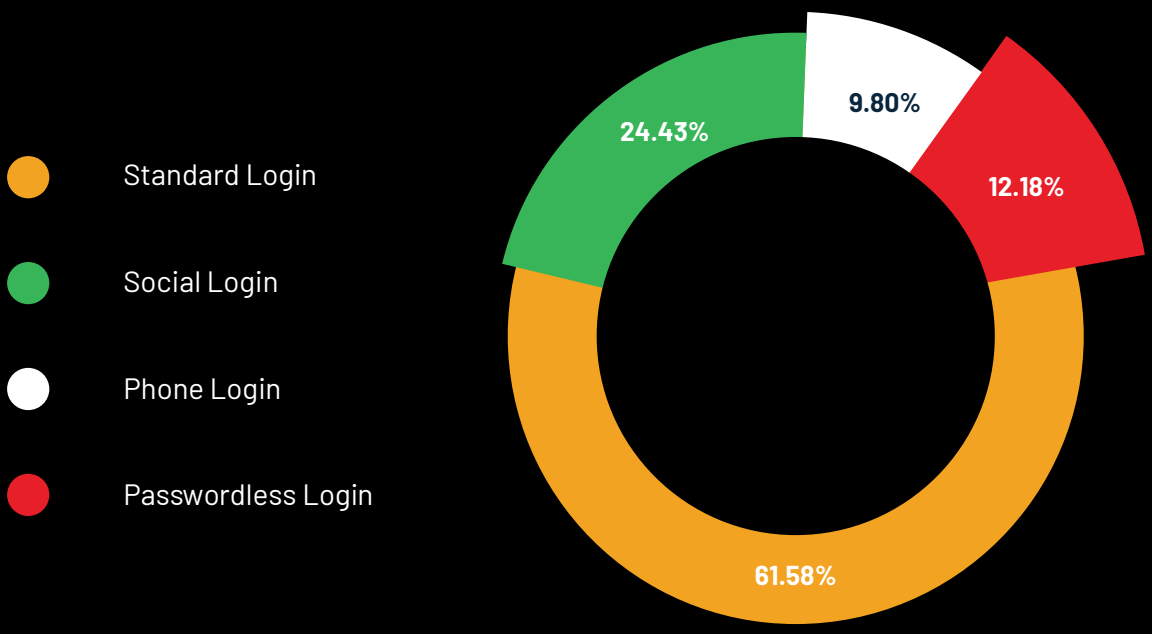
**We surveyed businesses to see which login method customers prefer.**

Choosing the right authentication method for your users is important. It's not just about whether it is secure or easy to use—you also have to consider how popular it is with your customers.

In order to determine which login options businesses offer, we looked at the most popular option from a business point of view.

We found that 61.58% of businesses prefer to offer standard login, whereas 24.43% like to offer social login, 9.80% phone login, and 12.18% passwordless login.

**Login offering preference by businesses**



## Key Findings

The overall data indicate that standard login is still the most popular authentication option among businesses. This is because it is considered the core of any identity system.

Another trend we are witnessing is the dramatic increase in the use of passwordless login for enterprises. With data breaches and cyber attacks becoming more sophisticated, password-based authentication methods are no longer considered adequate to protect sensitive information. Passwordless authentication methods, such as biometric and multi-factor authentication, offer more secure alternatives that are harder to compromise.

Additionally, passwordless authentication methods provide a more seamless and convenient user experience, which can improve user adoption rates and productivity. As a result, more and more enterprises are adopting passwordless login to enhance their security posture while providing a better user experience.

# Performance Benchmarks

> **We compared our platform's performance with industry standards so businesses would have a benchmark.**

A successful customer experience requires the right combination of factors. For example, it is important to ensure that your identity pages load quickly, your login and registration process is easy to follow, your system is available when needed and can handle peak loads without crashing. This will protect your brand reputation and increase customer retention—both of which are key factors in driving revenue growth.

To give companies a way to measure their performance, we should start by looking at our own statistics. And here's how we stack up.

| Performance Benchmark | The LoginRadius Platform Performance |
|---|---|
| Landing page load speed | 409ms |
| System uptime | 100% |
| Peak load | 208,000 logins/sec |

## Key Findings

100% system availability is critical to the growth of your company. If your system isn't, customers may grow frustrated and take their business elsewhere.

The digital age has changed the way consumers interact with businesses. Today's customers expect to be able to reach companies at any time, so if you don't provide services when they need them, these customers may leave and never return.

Speed is also an important benchmark for your identity pages. For example, if your registration page takes too long to load, you run the risk of losing customers before they can make a purchase.

Next is peak performance, and  the common scenarios where it becomes critical include:

- Organizations with large customer bases like more than 3 million.
- Heavy traffic loads during periods of busy seasonal activities.
- Heavy traffic due to a new product or service launch.

This data could be used as a baseline for comparing the reliability of identity systems. For example, if your internal systems cannot match a 100% uptime, this might indicate areas where you can improve.

# Authentication Token

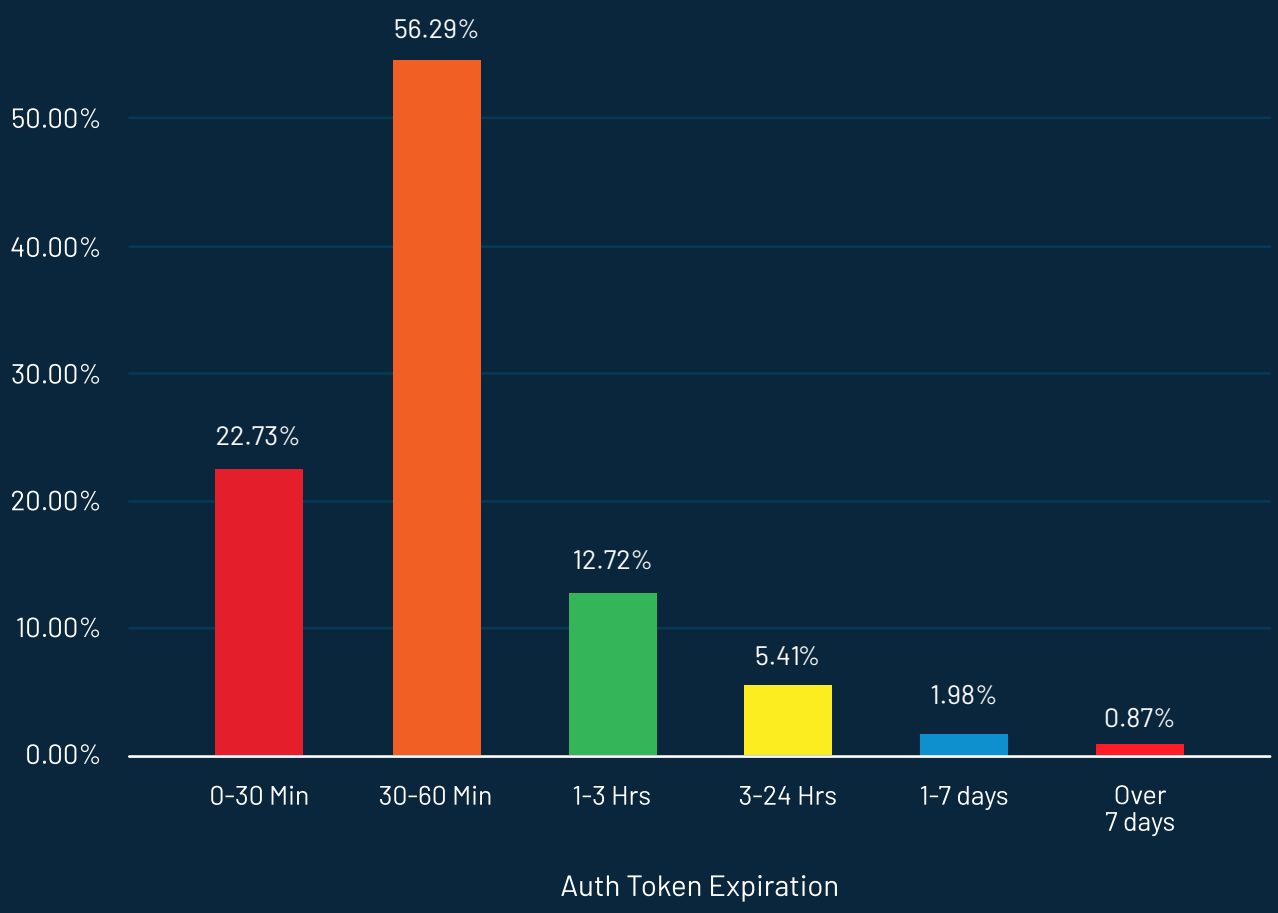
A token can be defined as a digitally encoded signature used to authenticate and authorize a user to access specific resources on a network.

Token-based authentication lets users verify their identity, and in return they receive a token that provides access to certain resources for a set period of time.

When we looked into the LoginRadius platform, we concluded that the percentage of companies setting Auth token for 30 - 60 min is 56.29%, followed by companies that set for 0 - 30 min, which is 22.73%. On the other hand, companies that set Auth Token for more than 7 days is only 0.87%, which is the least on the list.

By analyzing the data, we conclude that the ideal time for Auth Token lifetime is somewhere around 30 - 60 min.

**Authentication Token**



# Conclusion

In today's marketplace, businesses must make a lasting impression on every customer. A modern customer identity solution will not only provide customers with assured security but also give businesses the opportunity to use that data for future marketing opportunities.

In this report, we conducted an in-depth data analysis on customer behavior observed in the LoginRadius Identity Platform. The following is a summary of our findings:

- 74.52% of companies are using five to seven fields on their registration forms, with 27.72% using five, 27.91% using six, and 18.89% using seven.
- 24.14% of active customers use the 'forgot my password' tool. Of those customers,
- 81.55% actually retrieve their passwords and 8.11% never reset their password.
- 95.82% of companies offer standard login using an email ID.
- Of the customers that use passwordless login, 87.59% prefer to log in with their email address.
- Of the customers that use multi-factor authentication (MFA), 46.37% use MFA via an authenticator app. 35.15% of companies offer multi-factor authentication via an email code.
- The passwordless login has the highest return rate of 41.33%. Next is phone login with 38.14%, then social login with 18.38%, and finally standard login with 18.91%.
- 78.58% of over 50 year-olds prefer using standard login. 58.45% of 18-25-year-olds prefer social login.
- 48.70% of females prefer standard login over social login. Similarly, 41.45% of males prefer standard login over social login.
- Facebook is preferred by 36.98% of users, and Google is preferred by 35.23% of users globally.
- 61.58% of businesses adopted standard login, whereas 24.8434% like to offer social login, 9.80% phone login, and 12.18% passwordless login.

# Learn More About Customer IAM with LoginRadius

LoginRadius is an easy-to-implement, adaptable, and secure customer identity management platform that has been adopted by more than 500 brands across a wide range of industries. While the implementation can vary based on the goals of the organization, the capabilities remain consistent.

While there are many platforms available for your CIAM requirements, the cloud-based LoginRadius is uniquely positioned to meet your customers' needs with minimal implementation time.

For more information about **LoginRadius**, book a **free personalized demo** or **contact sales**.

# Authors

**Rakesh Soni**
**CEO, LoginRadius**

Rakesh Soni is a visionary leader, who has led his team to build a platform that makes it easier for millions of people to access technology and place identity at the forefront of security. Soni brings nearly two decades of experience to the company with his expertise in business development, board and investor relationships, fundraising, sales, and marketing. He holds an engineering degree from the Indian Institute of Technology and an MSc from the University of Alberta.

**Deepak Gupta**
**CTO, LoginRadius**

Deepak Gupta brings more than 15 years of experience in application and platform development. He leverages his expertise as a product visionary by creating user-centric solutions across the cybersecurity space. Deepak has helped LoginRadius establish itself as a leader in the CIAM space, and continues to drive the company's growth and success. Deepak holds an engineering degree from the University of Rajasthan and an MS in IT and Management from the Illinois Institute of Technology.

loginradius

LoginRadius is a leading provider of cloud-based Customer Identity and Access Management solutions for mid-to-large sized companies. The LoginRadius solution serves over 3,000 businesses with a monthly reach of over 1 billion users worldwide.