Whitepaper

Innovating with the basics: **Reduce fraud with low-friction QR code log-in**

Improve user experience and security practice with easy-to-use passwordless log-in

Zumigo
Mobile in Context

Whitepaper

Innovating with the basics: Reduce fraud with low-friction QR code log-in

Kai wants to log into his online banking to pay his bills. However, it's been a while since he has accessed the website. He tries using the five passwords he has in rotation but they are all wrong, so the website locks him out. He requests a password reset and checks the email inbox several times before it arrives. He quickly resets the password, scrambling to find a piece of paper to write down his new password. Finally, he succeeds at accessing his account. But he is now frustrated that he has spent an additional 10 minutes on this password debacle which should have been a simple task.

Using passwords to log into online accounts or make payments is the common method, but as evidenced by the many stories of hacks and breaches, it's unsecure, cumbersome, and expensive to maintain. Passwords are vulnerable and easy to crack, accounting for over 60% of breaches due to hacking[1].

Security notwithstanding, passwords can create friction and frustration for users and administrators. They degrade user experience as passwords can be lost, forgotten or impacted by breaches. Businesses have inconsistent requirements for password strength and the frequency of change. Reset requests are usually unavoidable.

This complexity results in increased help desk calls and open tickets to be resolved, thereby increasing IT security operational costs to a business. Multi-factor authentication can be added to improve security and prevent fraud, but additional resources are required for implementation.

As expected, the marketplace is moving away from using passwords in order to avoid user friction and to reduce operational costs. According to Gartner, more than 20% of customer authentication transactions will be conducted without passwords by 2025, up from less than 10% today[2].

The Simplicity and Security of QR Codes

The marketplace offers different types of verification that avoids using passwords, some more secure than the others. The most secure methods include hardware security token, biometrics, and QR code. However, these methods can increase user friction. Less secure methods include SMS-based or email-based links, are generally used as an additional method in multi-factor authentication, not by itself.

> "By 2025, more than **50%** of the workforce and more than **20%** of customer authentication transactions will be passwordless, up from less than 10% today."
>
> *- Gartner: Take 3 Steps Toward Passwordless Authentication, Refreshed 22 February 2023, Published 19 October 2021 - ID G00745034*

1. 2021 Data Breach Investigation Report, Verizon.
2. Gartner: Take 3 Steps Toward Passwordless Authentication, Refreshed 22 February 2023, Published 19 October 2021 - ID G00745034

Zumigo
Mobile in Context

Out of the different methods, the QR code-based method utilizes existing systems that the general population is familiar with, making it easier to implement and guaranteeing usage adoption.

QR codes – a machine-readable barcode made of black and white squares – are commonly used to convey information including menus, bus schedules, product packaging, banners and advertisements and business cards, or for customers to take the next step, including order fulfillment and making a payment. They are easily recognized and can be read by a camera-equipped smartphone.

QR code log-in can be used as an additional authentication method, and is compliant with the requirements for multi-factor authentication (MFA)[3] and Strong Customer Authentication (SCA)[4]. It replaces passwords, thereby eliminating the associated challenges, including weak passwords, frustrating user experience, and costly IT operations and management resources to reset passwords. Without passwords, enterprises can expect better security, fewer breaches and higher trust with customers.

Basic Understanding of QR Code Log-in Method

From the user perspective, the process is easily understood and can be carried out with a laptop or tablet and a smartphone. After entering a mobile number as an user ID to log-in, the user is then presented with a QR code on the screen of the laptop or tablet. The user scans the code with the smartphone that has the same mobile number. Upon scanning, the authenticated trusted identity gets passed from the phone to the laptop or tablet, allowing the user to continue with the log-in process. Most users are used to receiving a one-time password (OTP) to their phone when accessing the website on the laptop or tablet so this process is seamless and easy to understand.

For the backend, the business or service provider's web server responsible for managing account access requests asks for a mobile number as the log-in ID. With the mobile number, a request is then sent to the Zumigo platform for authentication. Zumigo generates a QR code for the web server to present back to the user. When the user scans the QR code with the smartphone associated with the mobile number, Zumigo uses its mobile identity network (that includes mobile carrier networks) to validate the mobile number, and determines whether there is a match. If so, then the user is authenticated, and a message is transmitted to the web server that the user is permitted to access the account. Otherwise, the user is denied access.

The smartphone needs to be connected to a mobile carrier network for the process to work, even globally. This technology can be integrated with any platform via API. It can also be combined with other existing biometric methods for two-factor authentication where a high level of security is required.

The Versatility of the QR Code Log-in Method

QR code log-in method of authentication is versatile and can be applied across many different use cases along a customer's digital engagement journey.

Safely originate a new account: Fraud occurs when a bad actor opens a new account – including credit card, bank, insurance, utility, or ecommerce – using someone else's personal information. Because of data breaches, much of this information has been leaked and is easily accessible to career criminals. This usually allows the fraudulent application to pass traditional identity verification checks. Businesses can send a QR code to be scanned with a smartphone that the applicant has to validate the identity.

3. National Institute of Standards & Technology Computer Security Resource Center: https://csrc.nist.gov/glossary/term/multi_factor_authentication
4. European Union Revised Payment Services Directive (PSD2): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

Prevent online purchase fraud: Online purchases made with stolen payment card information cost merchants millions in chargeback expenses. Such card-not-present transactions are risky and easy for bad actors to take advantage of. Ecommerce stores can validate the identity of the purchaser and the payment method by presenting a QR code to be scanned with a smartphone.

Improve conversion rate and purchase process with pre-fill form: To speed up the account opening or express checkout process, businesses can present a pre-filled online form when the user scans a QR code from the screen with a smartphone to validate identity and payment method. Auto form fill can save users time and effort by automatically populating the required personal information, thereby increase rate of conversion, speed of checkout, and user satisfaction.

Enhance security with multi-factor authentication: Passwords are not the most secure way of protecting accounts. Two-factor or multi-factor authentication is designed to keep accounts safe from password hacking and breaches. Upon logging in with a password, businesses can present a QR code to be scanned by the user's smartphone to further authenticate the identity to prevent unauthorized access.

Summary

Logging into accounts without passwords can be even simpler and more secure than the current way of managing account access. QR code authentication can become popular because it relies on equipment and processes that most consumers are already familiar with – a laptop or tablet with a smartphone. QR codes are versatile and can be easily applied to many different use cases along the digital engagement journey. It is an effective tool in the continuous fight against fraud.

Leila has just enough time to log into her online bank to pay her bills before she has to run off to pick up her child from school. When she navigated to the website and entered her mobile number, the webpage showed her a QR code. She quickly uses the camera on her smartphone to scan it. Within seconds, her account is loaded on her screen. She pays her bills quickly and is able to take some extra time to get a latte before the pickup.

About Zumigo

Zumigo is the frontline of digital identity verification that helps the world's largest enterprises secure transactions, devices and accounts. With a multi-layer approach, Zumigo validates users against a unique identity network that spans global carrier providers, third-party data analytics and databases, and payment information. **Learn more at www.zumigo.com**.