BEYOND IDENTITY

Passwordless customer authentication – Reduce friction and increase security

WHITEPAPER | MAY 2022

technology leaders club

The explosion of consumers transacting online and accelerated digital transformation has left companies trying to keep up with modern experiences, infrastructure and products to serve their digital users. But what has been the impact on consumers of moving digital?

Online security has failed to keep up with the speed of digital transformation, leaving challenges that need to be dealt with in order to provide a frictionless yet secure experience for users.

We hosted a roundtable that brought together of security architects, IT, network & security operations directors, process & innovation professionals to discuss:

- Whether password requirements stop consumers from creating accounts, therefore transactions
- Whether consumers forget or make too simple passwords, so they don't forget
- Consumer loyalty – are consumers more loyal to companies where they have accounts?
- How account issues affect consumer transactions
- Whether consumers favour products where they have an account over similar products

> Rela8 Group's Technology Leaders Club roundtables are held under the Chatham House Rule. Names, organisations and some anecdotes have been withheld to protect privacy.

About Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in – eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication. Their invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements and improve the user experience and conversion rates.

Their revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device and continuously analyses hundreds of risk signals for risk-based authentication.

Customer authentication

Account authentication can be many and varied, from social logins to national identity card links, username and password to trusted device. Some organisations could use a separate method of MFA like a one-time code delivered via SMS or email or even single sign-on. There can even be federated sign-on, where the organisation links into another system that handles the authentication for them. Some businesses may incorporate many different authentication systems, facing horizontal authentication challenges, especially with complicated supply chains. So what kind of options are organisations offering their customers?

Security challenges

Many organisations, especially those in finance and health, recognise that username and password sign-on can be exploited, so are looking towards MFA. Companies operating in a forex trading environment need real-time data, accuracy and security, so username and password is never enough.

The security challenge can be difficult in businesses like residential homes, where customers may be more old-school, preferring everything on paper. Employing smart technology and setting up a portal for customers is particularly challenging when users are less technologically conversant or have cognitive or visual impairments. In fact, authentication should be easy and as smooth as possible for those who are less tech savvy. The opportunity to go one step beyond MFA, passwordless authentication without additional technologies, is beneficial in this industry.

Alongside security challenges, authentication is also an accessibility issue. It can be thought of as a door to let some people in while keeping others out. Balancing friction and security authentication is difficult - not every interaction is created equal. Accessing a forex trading account is a high risk event, whereas a consumer accessing an ecommerce account is lower risk. Friction can therefore be used to adapt authentication to the type of risk, keeping low risk transactions simple then graduating to higher levels of authentication e.g. MFA or one-time code verification.

Password complexity

There can be issues around password complexity. Most organisations, if given the choice, would prefer users to have complicated passwords to make the life of a hacker more difficult. But this depends on the type of user? For example, children may find it difficult to remember complicated passwords, no matter how good they are at using devices. Other users may be illiterate or have impairments. Above all, security has to allow users access to what they need. One solution is to create different levels of user, so for example administrators may have a corporate user ID. So there is always a trade-off between security and usability. There is also the additional complication of dealing with local regulations or cultural issues in a lot of instances.

Security is a state of mind, or culture. You can put lots of different measures in place, but it is also important that people are committed and participate with security measures. Winning hearts and minds, educating people so they don't have their password on a post-it on the keyboard, write it in a book or keep the ID and password next to each other. The organisation and mindset of users is as important as technical measures – humans are a key security component.

> "Humans are a key security component"

Password protocol

Until recently, the advice was to enforce password rotation, but this is very inconvenient for users. They will find a way around it by incrementing a number at the end of their password whenever they need a new one, nullifying security. If organisations place complex constraints on what constitutes a password, adding enforced rotation will annoy users, who will work around it, rendering the extra-secure password useless.

Many organisations have now moved away from the enforced rotation in favour of MFA. As long as a password is 12+ characters and there is conditional access with at least two factor authentication in place, password rotation isn't required. But MFA is not without its pitfalls. If organisations use push factors like SMS, they have to pay for every text message, and changing phones can cause problems because the trusted device has changed.

There is going to be a time when creating a password is going to be difficult because of the high number that have been hacked. One option for passwordless is leveraging the secure enclaves of modern devices. User biometrics are combined with asymmetric cryptography where a private key is generated and never leaves the tpm on the phone or device. This verifies the identity and device of the user at the same time, with little friction.

Weighing up the options

Security challenges are many and varied. Security can also be seen as an access issue, with multiple levels of risk attribution. Not all users are equal as some are more tech savvy and others may have educational gaps or other types of impairment. A 'one solution fits all' scenario is therefore not possible.

Security has to allow people to access what they need, so there has to be a balance between it and usability. The mindset of organisations and users is just as important as technological solutions, and they need to be educated and advised on how to keep their passwords safe. Security needs to win over the hearts and minds of those using it.

There is little point in organisations implementing complicated password protocols because the more friction for the end user, the more ways they will find to work around it. User biometrics combined with asymmetric cryptography can verify both the user identity and trusted device, with little or no friction for the user.

> "There is going to be a time when creating a password is going to be difficult"

Rela8 Group serves the technology leaders community by giving executives a platform to identify challenges, connect with key innovators and understand where their business is going next. Based on these three pillars, we create engaging and stimulating B2B programs as well as custom gatherings for senior leaders and solution providers.

technology **leaders club**

rela8 group