PasswordlessDay
23 June

Toolkit

#passwordless

Thank you for being a part of the first ever Passwordless Day!

We're here to declare that there is a better way to do user security. We're here to unburden ourselves of clunky, annoying passwords and the vulnerable systems that support them.

We're here because logging in should be **faster**, user data should be **safer**, and the entire architecture of internet privacy should be **more affordable** to companies.

The first ever Passwordless Day, organised by MIRACL, will be observed on June 23, 2021 -- the 102nd birthday of mathematician Alan Turing. Passwordless Day presents an opportunity to bring attention to the new realities of internet security and the opportunities we have to address them with solutions inspired by Turing's work.

We are calling on companies to embrace more secure, forward-thinking user authentication technology.

This campaign is being organized by MIRACL. We are a company dedicated to securing the people, knowledge, and things needed to run a digital business. Our MIRACL Trust multi-factor authentication system makes logging in easier, more secure, and smoother. It also does away with those pesky passwords.

The Problem with Passwords

- In theory, passwords are our best defense against somebody stealing our personal information. But in practice, they are a cumbersome obstacle to actually *enjoying* the internet.
- The rules of proper password keeping and the reality of our digital lives don't match up. We're told to use random passwords, change them consistently, and never repeat them. But who really does this? Real world password maintenance looks a lot like adding extra excl@mat1on p0int$ to the end of our current pa55words!

  Or worse yet, hitting the "remember my password" button and relying on the magic of cookies until it's finally time to hit the "forgot password" button.
- Passwords are excruciatingly slow to input, especially on mobile devices.
- No matter how careful an individual user is about their passwords, once they get into the hands of a digital business, they are immediately vulnerable. Usually passwords are stored all together in a single file behind layers of expensive security. But hackers have proven again and again that they can beat even the best traditional security infrastructure, leaving users vulnerable. All they have to do is say *Open Sesame*.
- Despite being proven to be fallible, all this easily hackable security infrastructure is *expensive*.
- Sure, there are some decent password-related options out there like two-factor authentication that relies on separate hardware. (Think SMS messages to your phone). But these options are *even more expensive and even more burdensome*. We've all become conditioned for instant gratification in our digital lives -- this can dissuade us from taking extra steps like signing up for 2FA, even if those steps can keep our data safer.

If Not Passwords...

Okay, we've established that passwords are antiquated and vulnerable. How then might companies authenticate their users in a secure and seamless way? Here are some alternatives:

Biometrics

Anybody with a newer mobile phone has likely experienced the magic of biometric authentication. The beauty of these options -- which rely on recognition of each individual's unique physical properties is that you can't "forget" your own self; you are also very hard to replicate. Biometric authentication can include recognition of fingerprints, faces, irises, voices, and even heartbeats.

Biometric authentication is fast and effective. Some users, however, might fear sharing their unique personal data with tech companies; and if compromised, that data presents an even bigger risk. You can change a password, but you cannot change your fingerprint.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is exactly what it sounds like. Instead of just using a password to log in, you add a second "test." Traditionally, that's entering a one-time code sent by SMS or email; other times it can be entering an app and responding to a prompt. But, MFA doesn't have to include a password or a second user step at all! The MFA process can also include biometrics or unique cryptography. A Zero-knowledge proof protocol allows users to prove their identity without actually sharing vulnerable information. In some cases all it takes is a 4-digit pin and the magic of a cryptographic token stored in a browser or mobile app.

Why June 23?

Because on June 23, 1912 a baby was born in London who would change the world of mathematics, cryptography, and computing forever. His name was Alan Mathison Turing.

Turing first came to notoriety in the 1930s for his invention of the Turing Machine -- a hypothetical device with vast computational power. During World War II, Turing worked as a codebreaker, deciphering complex German cryptography including the famous Enigma code.

After the war, Turing designed some of the world's first computational machines, theorised about artificial intelligence, and introduced the concept that we now call the Turing Test, which sought to recognise the difference between machine intelligence and human intelligence.

During his life, Turing called these tests "imitation games," because computers were programmed to imitate human beings. Even in the 1940s and 50s, Turing was very optimistic about the ability of computers to eventually outwit humans. These questions, and Turing's thinking, are now fundamental to the task of user authentication and security.

Tragically, Turing did not live to see his influence take hold as one of the forefathers of computer science. In the decades since his passing, Turing's work has become increasingly relevant -- and he has found himself as the namesake for many prizes, products, and more. In 2021, he will become the first openly gay person to appear on a British banknote.

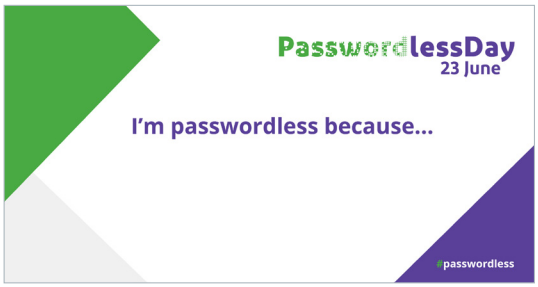
This 23rd June:

Tell your community that you are done with passwords! Use the #passwordless hashtag on social media to share your journey to safer, smarter, verification options.

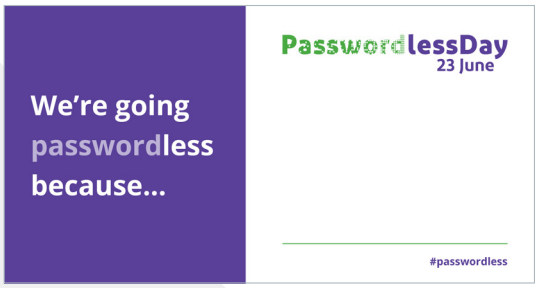
Talk to your users directly about why your company chooses #passwordless user verification.

Reach out to colleagues and learn about their best #passwordless practices. The journey to a safer internet starts with a single conversation.

Here are some assets to fill in why you're going #passwordless:



- I'm #passwordless because I love my users.
- I'm #passwordless because it's 2021, not 2001 anymore.
- Did you know that account takeovers cost businesses a combined $25 billion (!) in 2020, according to Juniper Research? I'm protecting my customers and going #passwordless.



- We're #passwordless because we value the time and security of our users.
- We're #passwordless because we know that real safety is more important than the illusion of safety.
- HALF of all help desk calls are to deal with simple password resets, according to research by OKTA. Is your company ready to save resources and go #passwordless?

- I'm #passwordless because my brain has more important things to remember.
- More than 1/3 of online transactions are abandoned at checkout because users forget their passwords, Mastercard has found. This June, go #passwordless and see your online transactions soar.