IDENTIFY YOUR SUBJECT

ENTER YOUR TITLE (thesis.subject@edu.ch.com...)

forgot title?

THE LOGIN FORTRESS - How can we redesign login experiences to build new relationships between platforms and users?

ENTER YOUR SECRET DATA

What IS a login experience? What is a login? Can I talk about logins without talking about logging out? Where am I logging in? From where? Into what? For whom? New and different relationships?

“How many times in a day do we face hacking attempts? Millions of times”.

“He assumed that design had already solved security. “

“Your system sucks! I do not control access here, THE IT DEPARTMENT does.”

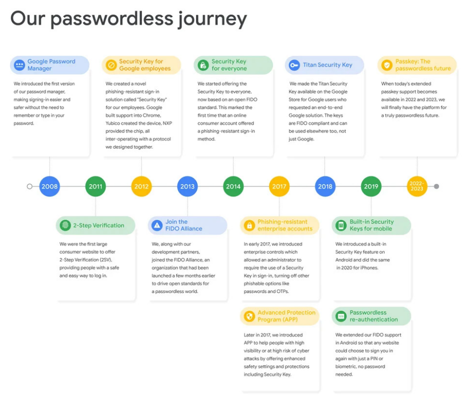
“The site asked me, after one attempt “Are you not Selin Yildirim?”... and I felt betrayed”

“If you don’t have much affinity with technology, it’s really hard to use that stuff once it doesn’t work the way it should.”

PASSWORD MUST INCLUDE QUOTES ABOUT YOUR INTERVIEWS, BE COMPLICATED, AND MAKE YOU FEEL ALIENATED.

Observe the following phenomenon: a person wants to enter a place. In order to do so, they need to go through a door, which, for one reason or another, is locked by a key they own. The concept is simple: use the key, enter through the door. Simple, but not enough anymore. In recent times, the login experience has developed a trend of increasing security, generating seamless interactions and externalizing the moment of authentication outside of platforms users are on. This trend presents itself in email verification, 2FA, captcha, “Prove you are human” prompts, accessing one’s smartphone...

SELECT ALL BOXES THAT CONTAIN RESEARCH EVIDENCE



Our passwordless journey

2008 — Google Password Manager: We introduced the first version of our password manager, making signing-in easier and safer without the need to remember or type in your password.

2011 — 2-Step Verification: We were the first large consumer website to offer 2-Step Verification (2SV), providing people with a safe and easy way to log in.

2012 — Security Key for Google employees: We created a novel phishing-resistant sign-in solution called "Security Key" for our employees. Google built support into Chrome, Yubico created the device, NXP provided the chip, all inter-operating with a protocol we designed together.

2013 — Join the FIDO Alliance: We, along with our development partners, joined the FIDO Alliance, an organization that had been launched a few months earlier to drive open standards for a passwordless world.

2014 — Security Key for everyone: We started offering the Security Key to everyone, now based on an open FIDO standard. This marked the first time that an online consumer account offered a phishing-resistant sign-in method.

2017 — Phishing-resistant enterprise accounts: In early 2017, we introduced enterprise controls which allowed an administrator to require the use of a Security Key in sign-in, turning off other phishable options like passwords and OTPs.

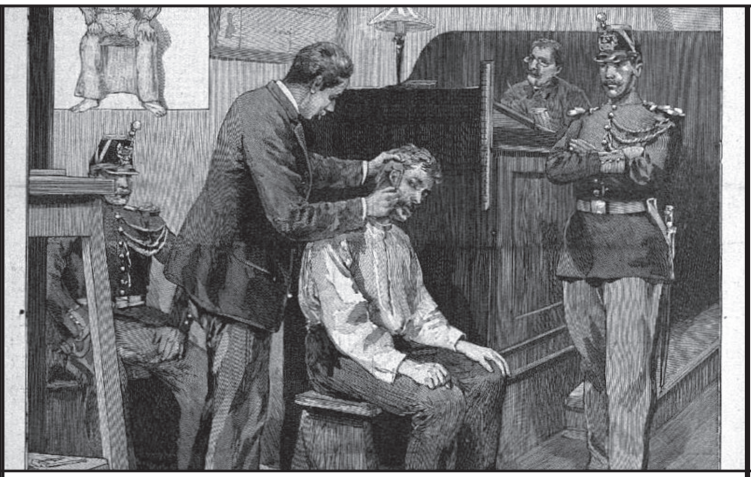
2017 — Advanced Protection Program (APP): Later in 2017, we introduced APP to help people with high visibility or at high risk of cyber attacks by offering enhanced safety settings and protections including Security Key.

2018 — Titan Security Key: We made the Titan Security Key available on the Google Store for Google users who requested an end-to-end Google solution. The keys are FIDO compliant and can be used elsewhere too, not just Google.

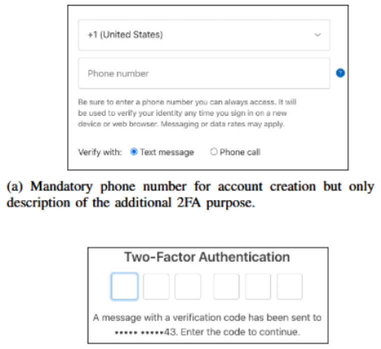
2019 — Built-in Security Keys for mobile: We introduced a built-in Security Key feature on Android and did the same in 2020 for iPhones.

2019 — Passwordless re-authentication: We extended our FIDO support in Android so that any website could choose to sign you in again with just a PIN or biometric, no password needed.

2022-2023 — Passkey: The passwordless future: When today's extended passkey support becomes available in 2022 and 2023, we will finally have the platform for a truly passwordless future.



Ramzy thinks... seamless = good, but behaviour shows that it lead to security concerns.
Selin thinks... Friction = tiring, but reassuring. Suspicion hurts trust.
Emma believes... Friction = stressful for non-experts. Seamlessness OK, but only up to a point. Ownership of accounts is ambiguous.
Military context is,uh... Security is externalised, total lack of internal control...?



+1 (United States)

Phone number

Be sure to enter a phone number you can always access. It will be used to verify your identity any time you sign in on a new device or web browser. Messaging or data rates may apply.

Verify with: ● Text message ○ Phone call

(a) Mandatory phone number for account creation but only brief description of the additional 2FA purpose.

Two-Factor Authentication

□ □ □ □ □ □

A message with a verification code has been sent to ••••• •••••43. Enter the code to continue.

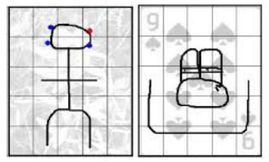
(b) Phone number denoted clearly as 2FA on login.

IF WE REMOVE SECURITY NEEDS FROM LOGIN DESIGN,

WHAT IS LEFT OF THE EXPERIENCE?

By the late twentieth century, passwords had also entered popular culture. Hollywood made the login a dramatic trope: in WarGames (1983), Matthew Broderick hacks into a military simulation with the backdoor password “Joshua.” In Mission: Impossible (1996), Ethan Hunt slips into CIA headquarters with the code “AW96B6.” In The Matrix Reloaded (2003), Trinity resets a power plant’s password to “Z1ON0101.”

LOCIMETRIC LOGIN? DUOPASS? BUILDING RELATIONS TOGETHER? IMAGES? MEMORIES?



(a) (b)

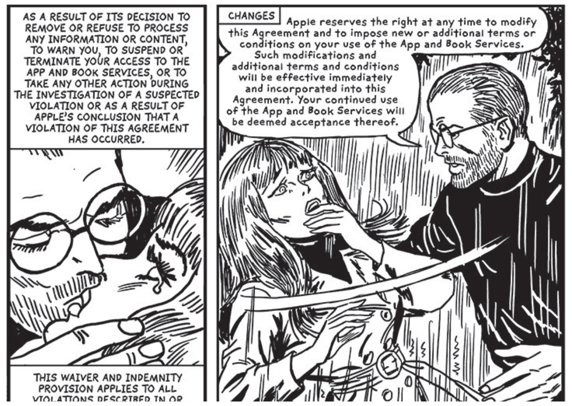
“For example, current password policies create user frustration (e.g., when users forget the passwords or reset the passwords frequently due to strict policies); biometric authentication schemes entail privacy threats (e.g., biometric data could be used in impersonation attacks, the data cannot be revoked in case they are compromised or leaked); unusable password policies increase maintenance costs (e.g., password resets increase labor costs of an organization)...”

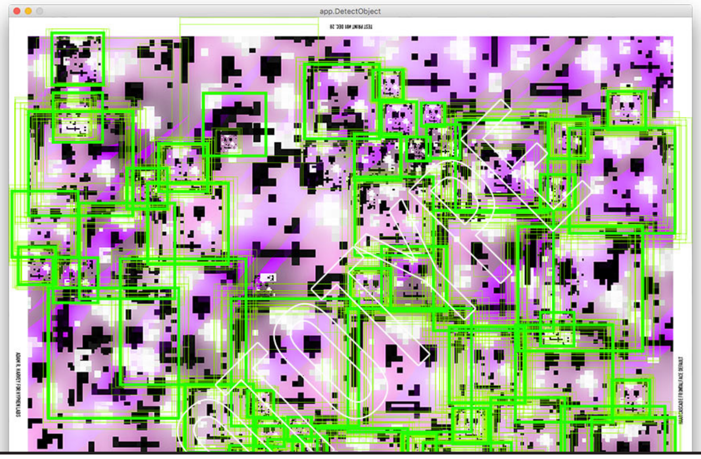
Niemimaa, Marko, et al. “Security and Usability of a Personalized User Authentication Paradigm: Insights from a Longitudinal Study with Three Healthcare Organizations.” Proceedings of the ACM on Human-Computer Interaction

“Both conceptually and thematically, these interfaces offer their users a way to map and engage an increasingly complex world allegedly driven by invisible laws of late capitalism. Most strongly, they induce the user to map constantly so that the user in turn can be mapped. They offer a simpler, more reassuring analog of power, one in which the user takes the place of the sovereign executive “ source,” code becomes law, and mapping produces the subject.“

(Programmed Visions, Wendy Chun, 2 Daemonic Interfaces, Empowering Obfuscations, page 59)

NOW WHAT


AS A RESULT OF ITS DECISION TO REMOVE OR REFUSE TO PROCESS ANY INFORMATION OR CONTENT, TO WARN YOU, TO SUSPEND OR TERMINATE YOUR ACCESS TO THE APP AND BOOK SERVICES, OR TO TAKE ANY OTHER ACTION DURING THE INVESTIGATION OF A SUSPECTED VIOLATION OR AS A RESULT OF APPLE'S CONCLUSION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED.
THIS WAIVER AND INDEMNITY PROVISION APPLIES TO ALL VIOLATIONS DESCRIBED IN OR
CHANGES
Apple reserves the right at any time to modify this Agreement and to impose new or additional terms or conditions on your use of the App and Book Services.
Such modifications and additional terms and conditions will be effective immediately and incorporated into this Agreement. Your continued use of the App and Book Services will be deemed acceptance thereof.



Another insight we noticed is that people were aware that passwords are not as secure as other authentication schemes but preferred to use them anyway. Some even believed passwords to be safer than other methods of authentication.

”Password is the most easiest and safest of the three.”
As mentioned earlier with security friction, people will exchange security for convenience if the security seems too overbearing or complicated for every day use.
Alvi, Muneeb. Authentication Schemes and Their Impact on User Security Perceptions. California State University, 2023. ScholarWorks,

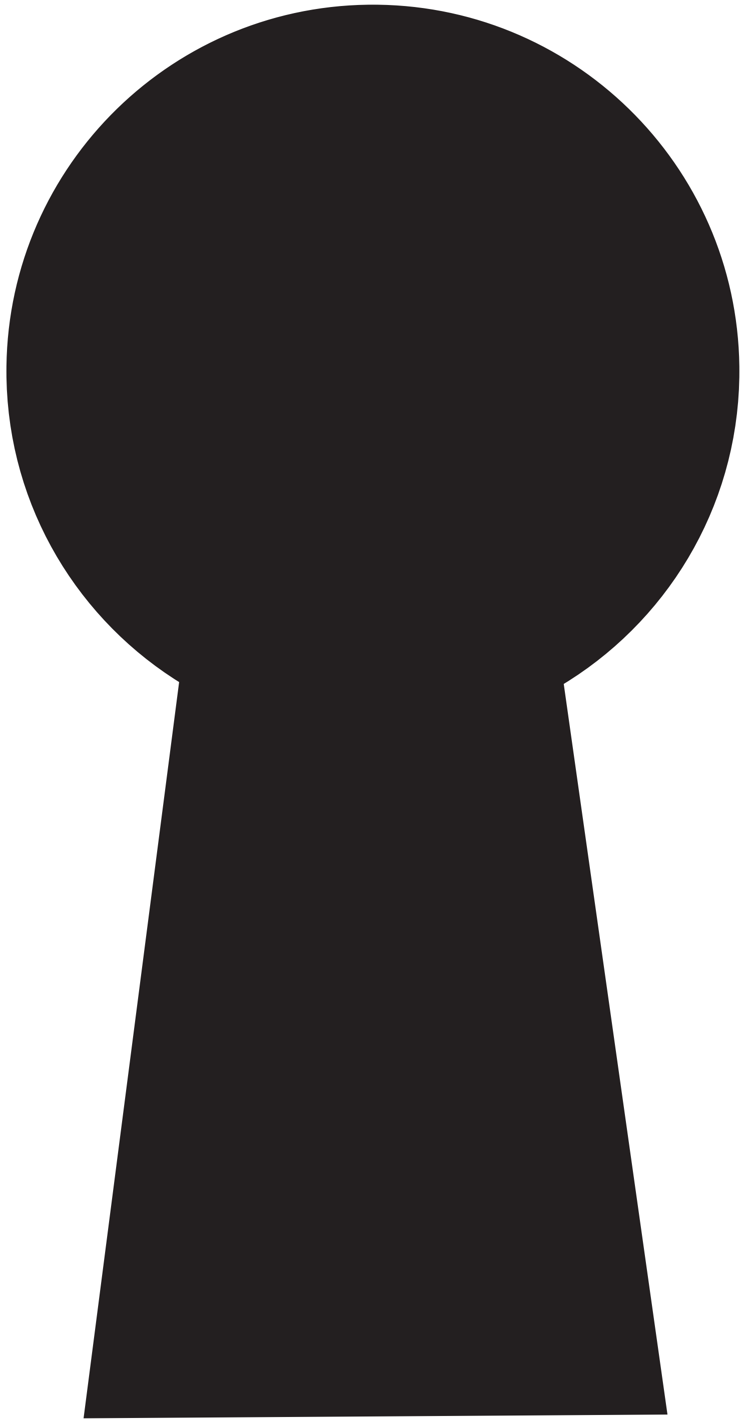
NEW LOGIN RELATIONS BUT ALSO RELATIONS FROM USERS, STATE, PEOPLE, RELATIONSHIPS, SERVICES, HOW LOGIN DICTATES THOSE RELATIONSHIPS and how CAN WE REDEFINE THEM....

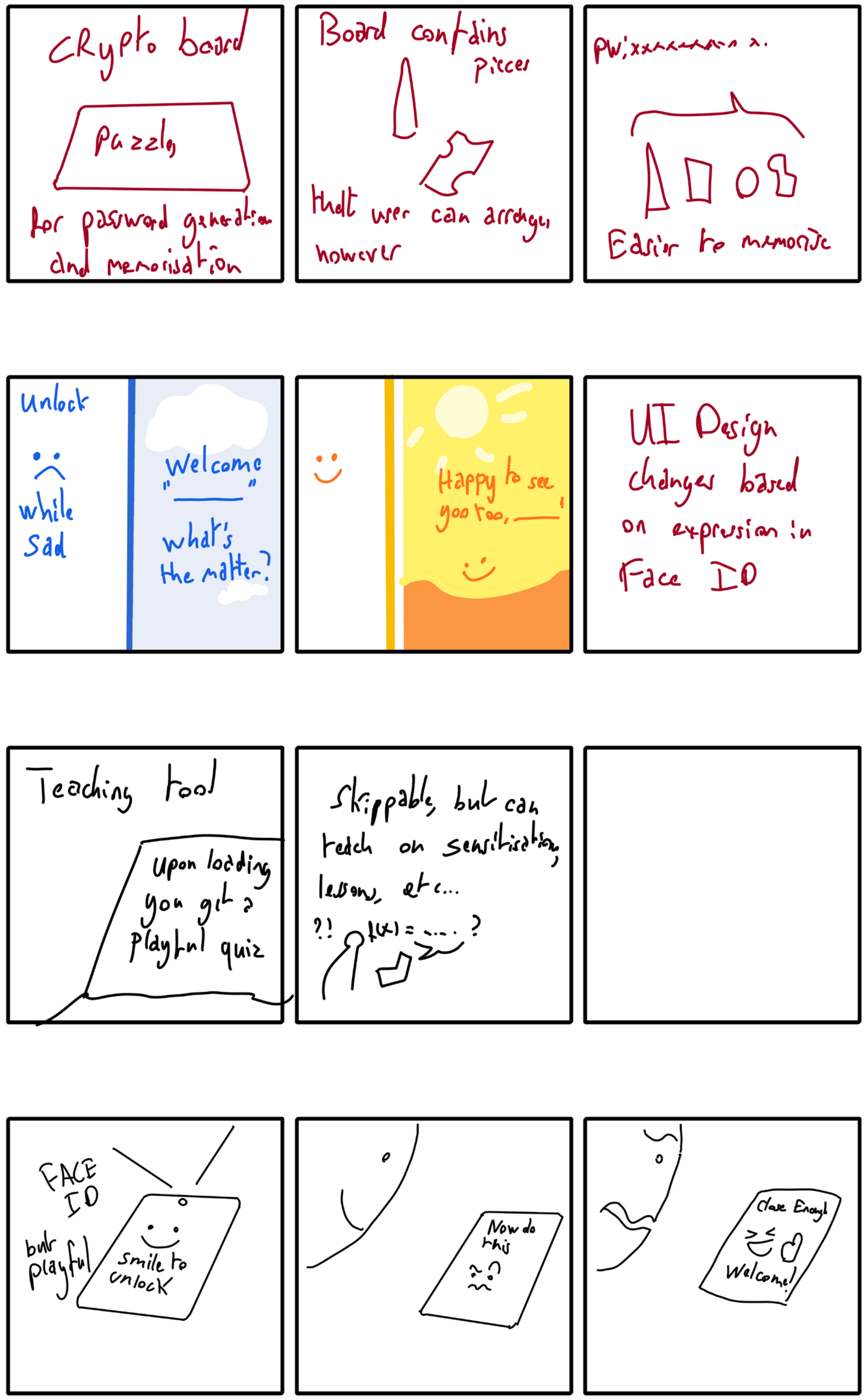
WELCOME HOME, HERE IS WHAT MIGHT INTEREST YOU NOW...

Logins today are externalized...
They are closer to the body...
And they shape feelings and thus behaviours...

But more importantly, how can we create new and better relationships between users and platforms, within the login experience, using technologies already available?

If the present oscillates between seamlessness and friction, this questioning allows us to ask what else login could become. Today's systems are designed under suspicion: "prove that you are not an intruder, prove that you are not a machine, prove that your body is truly your body". Yet if login is a moment of entry, there is no reason it must always express suspicion. The act of recognition could instead become relational or even playful, and not be bound to the body and centuries of bertillonage.





cRypto board
Puzzle
for password generation and memorisation
Board contains pieces
that user can arrange, however
PW: xxxxxxxxx x.
Easier to memorise
Unlock
while sad
Welcome
" ____ "
what's the matter?
Happy to see you too, ____!
UI Design changes based on expression in Face ID
Teaching tool
upon loading you get a playful quiz
Skippable, but can teach on sensitisation, lessons, etc...
?! f(x) = ... ?
FACE ID
but playful
smile to unlock
Now do this
Close Enough
Welcome!