



# An Analysis of the Security, Usability, and Automation Capabilities of Password Update Processes on Top-Ranked Websites

**Alexander Krause**, Jacques Suray, Lea Schmäuser, Marten Oltrogge<sup>†</sup>, Oliver Wiese, Maximilian Golla,  
Sascha Fahl

CISPA Helmholtz Center for Information Security, Hannover · SOUPS 2026



Dr. Alexander Krause



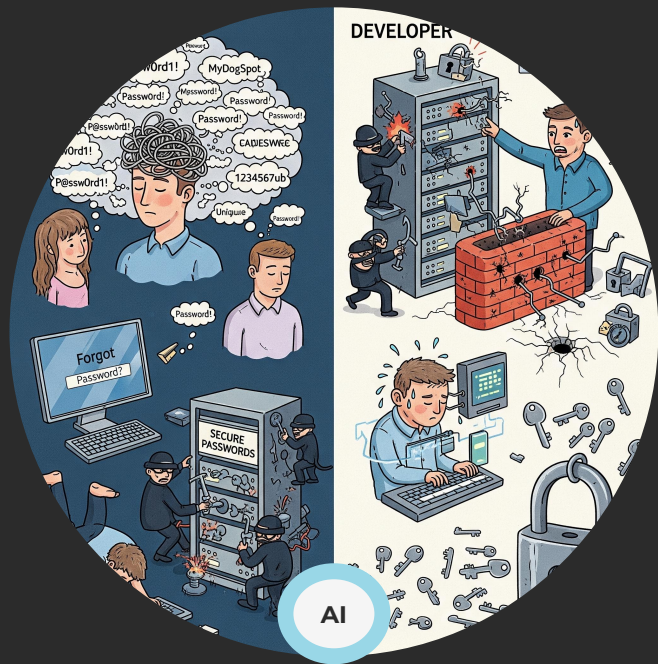
# Passwords still rule the world

- The main way people get into their accounts
- Works for everyone, no extra device or app
- Easy to share and easy to use
- Hard to replace, even with passkeys





# The catch with passwords



- People can not keep strong, unique passwords for many accounts
- Password managers help, but not everyone uses them well
- It is hard for developers to store and check passwords safely
- Many rules push people to make weaker passwords

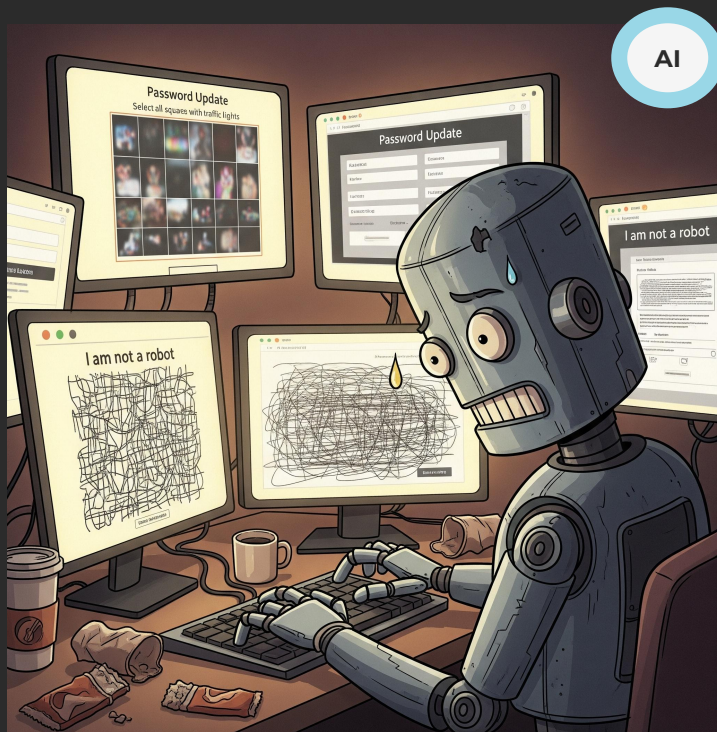




# Why users update their passwords

- They forgot the password, so they reset it
- There was a data breach
- They want to stop sharing access
- They want to be safe, for example after a login warning





- We started by trying to automate password updates for users
  - It did not work. Every site built the flow in its own way
  - A popular password manager, Dashlane, gave up on this in 2022
  - No study had looked at these flows in a systematic way
  - So we asked how these flows really work
- That became this work





# Research Questions

**RQ1** How do websites implement password update processes?

**RQ2** What are common security, usability, and automation challenges and obstacles end-users and password managers face when interacting with password update processes?

**RQ3** How can websites be better supported to deploy more secure, easy-to-use, and more easily automated password update processes?

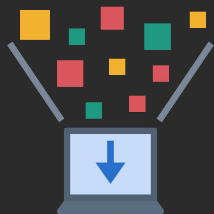




# Method – the sample

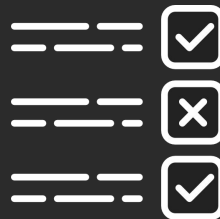
## Data Collection & Sample

- We made fresh accounts on 111 top websites
- We looked at the top 402 sites and kept 111 after exclusions
- We did this from September 2024 to February 2025



## Account Creation

- 96 sites let you change, 109 let you reset
- We used new US and German phone numbers and a VPN
- We did not use any real user account







# Method – the protocol

- We checked 32 points in three steps: start, update, feedback
- Two researchers did each site alone
- We used a new Chrome profile and recorded the screen
- We agreed in 96 percent of the cases
- We also tested the W3C change password URL on every site (example.com/well-known/change-password)



| ID              | Attribute                       | Description                                                                                                                                                                                                   | Process |     |
|-----------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-----|
|                 |                                 |                                                                                                                                                                                                               | PWC     | PWR |
| Initialization  |                                 |                                                                                                                                                                                                               |         |     |
| 1               | RBA Email                       | An additional risk-based e-mail authentication was performed.                                                                                                                                                 | ●       | ○   |
| 2               | RBA CAPTCHA                     | An additional risk-based CAPTCHA authentication was performed.                                                                                                                                                | ●       | ○   |
| 3               | RBA SMS                         | An additional risk-based SMS authentication was performed.                                                                                                                                                    | ●       | ○   |
| 4               | HTML Autocomplete Login Process | Is 'True' if the autocomplete attribute is set to 'email' or 'username' for the user input field and 'current-password' for the password input field.                                                         | ●       | ○   |
| Password Update |                                 |                                                                                                                                                                                                               |         |     |
| 5               | Opposite Process (PWC↔PWR)      | The PWC process references the PWR process and vice versa.                                                                                                                                                    | ●       | ●   |
| 6               | Pre-Verification                | To enter the password update form, the user must verify their identity again.                                                                                                                                 | ●       | ○   |
| 7               | Current PW Field                | The current password is required to update the password.                                                                                                                                                      | ●       | ○   |
| 8               | Confirm PW Field                | To update the password, the new password must be confirmed once again.                                                                                                                                        | ●       | ●   |
| 9               | HTML Autocomplete PWC           | Is 'True' if the autocomplete attribute is set to 'current-password' for the current-password input field and to 'new-password' for the 'new' and 'confirm' password input field in the password update form. | ●       | ○   |
| 10              | PW Policy                       | Website provides information about its own password composition policy.                                                                                                                                       | ●       | ●   |
| 11              | PW Visibility Toggle            | Users have the option to toggle the visibility of the passwords they enter.                                                                                                                                   | ●       | ●   |
| 12              | PW Generator                    | The website has a built-in function to generate a random password.                                                                                                                                            | ●       | ●   |
| 13              | PW Strength Meter               | Website provides feedback about the password strength.                                                                                                                                                        | ●       | ●   |
| 14              | PW Leakage/Breach Check         | Website checks and communicates whether parts of the user data have been part of a data leak or breach.                                                                                                       | ●       | ●   |
| 15              | Secure PW Tips                  | Website provides advice for strong passwords.                                                                                                                                                                 | ●       | ●   |
| 16              | CAPTCHA                         | At least one CAPTCHA had to be solved before or after processing the password update form.                                                                                                                    | ●       | ●   |
| 17              | PW Reuse Prevention             | Updating the password to a previously used password is actively prevented.                                                                                                                                    | ●       | ●   |
| 18              | Logout All Devices              | The website communicates that all active sessions will be terminated when updating the password.                                                                                                              | ●       | ●   |
| 19              | Logout Partially                | The website communicates that some sessions, mostly excluding the user's session, will be terminated.                                                                                                         | ●       | ●   |
| 20              | Expire Current Session          | Without any prior information, the user is logged out after updating their password.                                                                                                                          | ●       | ○   |
| 21              | Automatic Login                 | The user is automatically logged in after updating their password.                                                                                                                                            | ○       | ●   |
| Feedback        |                                 |                                                                                                                                                                                                               |         |     |
| 22              | Visual Feedback                 | The website visually communicates a successful password update.                                                                                                                                               | ●       | ●   |
| 23              | Pop-up                          | The visual feedback is displayed in a temporary or closable pop-up.                                                                                                                                           | ●       | ●   |
| 24              | Short-Display-Time              | The visual feedback is only visible for a very short amount of time.                                                                                                                                          | ●       | ●   |
| 25              | Embedded in Page                | The visual feedback is persistent and embedded in the webpage.                                                                                                                                                | ●       | ●   |
| 26              | Hard to Detect                  | The visual feedback is hard to notice due to the size, arrangement on the webpage, or color scheme.                                                                                                           | ●       | ●   |
| 27              | Redirect                        | There is an automatic redirect after updating the password.                                                                                                                                                   | ●       | ●   |
| 28              | Redirect Main Page              | The redirect leads to the main page.                                                                                                                                                                          | ●       | ●   |
| 29              | Redirect Same Page              | The redirect directs to the same page without changing the URL.                                                                                                                                               | ●       | ●   |
| 30              | Redirect Other                  | The redirect leads neither to the main page nor to the same page.                                                                                                                                             | ●       | ●   |
| 31              | Sign-in Notification            | A sign-in notification is sent to the user's email address.                                                                                                                                                   | ●       | ●   |
| 32              | PW Update Notification          | A password update notification is sent to the user's email address.                                                                                                                                           | ●       | ●   |

● Attribute analyzed. ○ Attribute not applicable and therefore not part of the analysis.





# Two processes: change vs. reset

- **PWC process**

- you know the password
  - You log in
  - find the form
  - set a new one

- **PWR process**

- you lost access
  - You find the link
  - prove who you are
  - set a new one

→ They look similar, but the start and the checks are different





# Findings



## Systematic Analysis





# Usability: login and the extra checks

- Some websites ask for an extra code at login
- This does not happen every time, it is random
- About 20 percent send an email code, 7 percent a CAPTCHA, 2 percent a text
- Some codes can not be pasted, so you type them by hand
- The CAPTCHAs go from picking a picture to adding dice

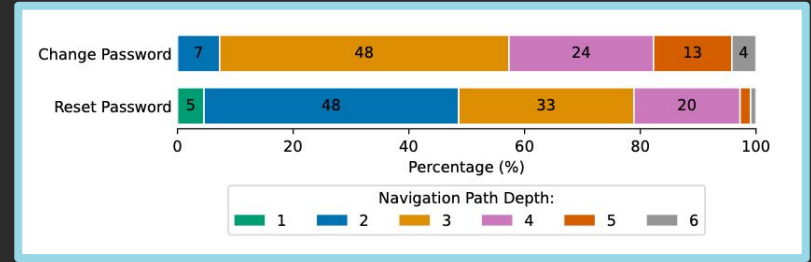
| ID             | Attribute   | Change (N=96) |       | Reset (N=109) |       | Equality |
|----------------|-------------|---------------|-------|---------------|-------|----------|
|                |             | True          | False | True          | False | %        |
| Initialization |             |               |       |               |       |          |
| 1              | RBA Email   | 19            | 77    | n/a           | n/a   | n/a      |
| 2              | RBA CAPTCHA | 7             | 89    | n/a           | n/a   | n/a      |
| 3              | RBA SMS     | 2             | 94    | n/a           | n/a   | n/a      |





# Usability: the path is long

- The change form is 2 to 6 clicks away, most often 3
- The reset form is closer, usually 2 clicks
- The names are completely inconsistent: security, account, edit profile
- On one site we had to use a search engine to find it





# Usability – the forms

- Some change flows just send you to the reset flow (15 of 96)

| Password Update |                            |    |    |   |     |
|-----------------|----------------------------|----|----|---|-----|
| 5               | Opposite Process (PWC↔PWR) | 15 | 96 | 2 | 109 |
|                 |                            |    |    |   | n/a |

- 21 of 96 change forms have no password confirm field
- 43 of 96 have no show or hide button, so you can not see typos
- The form can be a page, a popup, or a small part of the profile





# Security: the controls that are missing

Most sites skip the controls that matter most after a problem.

- Only 1 of 111 checks your new password against leaked ones
- Only 2 of 111 have a generator built into the site
- Only 9 of 111 can fill the form correctly with a password manager (autocomplete attribute)
- Only 8 of 96 end your other sessions after an update
- Many do show a policy and a strength meter, but the active security is missing





# Feedback: did it work

- About 80% show some message
- Many are a small flash for 1 to 2 seconds, easy to miss
- Some sites only redirect you to the home page
- Or nothing at all

Password Change

https://example.com/profile/change\_pw/

Current password

\*\*\*\*\*

New password

\*\*\*\*\*

Confirm new password

\*\*\*\*\*

Change Password

\*Passwords must be at least 8 characters long.

✓ Your password has been changed!

Home

https://example.com

Latest News:

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Non sodales neque sodales ut etiam. Proin sagittis nisi rhoncus mattis. Phasellus egestas tellus rutrum tellus pellentesque eu tincidunt tortor. Varius duis at consectetur lorem donec massa sapien faucibus. Facilisi nullam vehicula ipsum a arcu. Viverra maecenas accumsan lacus vel facilisis volutpat est. Aliquet bibendum enim facilisis gravida neque convallis. Vel risus commodo viverra maecenas accumsan lacus vel. Aliquet nibh praesent tristique magna. Lobortis mattis aliquam faucibus purus in massa tempor. Habitant

✓ Changes saved!

Profile Settings

https://example.com/profile

01/01/70

Gender

Prefer not to say

Time zone

GMT-05:00 Eastern

Email

user@example.com

Promotional emails

Phone

123-456-789

New password

\*\*\*\*\*

Confirm new password

\*\*\*\*\*

Settings Saved

Home

https://example.com

Latest News:

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Non sodales neque sodales ut etiam. Proin sagittis nisi rhoncus mattis. Phasellus egestas tellus rutrum tellus pellentesque eu tincidunt tortor. Varius duis at consectetur lorem donec massa sapien faucibus. Facilisi nullam vehicula ipsum a arcu. Viverra maecenas accumsan lacus vel facilisis volutpat est. Aliquet bibendum enim facilisis gravida neque convallis. Vel risus commodo viverra maecenas accumsan lacus vel. Aliquet nibh praesent tristique magna. Lobortis mattis aliquam faucibus purus in massa tempor. Habitant

303 Redirecting: https://example.com







## Risk: silent changes

- 34 of 96 change flows and 45 of 109 reset flows send no email
- No message and no email means a bad change goes unseen
- Add sessions that do not end, and the old access stays
- This is the line between I changed it and someone changed it

|           |                        |    |    |    |     |    |
|-----------|------------------------|----|----|----|-----|----|
| <b>31</b> | Sign-in Notification   | 17 | 79 | 6  | 103 | 80 |
| <b>32</b> | PW Update Notification | 62 | 34 | 64 | 45  | 85 |





# Automation: why password managers struggle

- Only 6 of 111 sites, that is 5 percent, use the W3C change password URL

|   |                                 |    |    |     |     |     |
|---|---------------------------------|----|----|-----|-----|-----|
| 4 | HTML Autocomplete Login Process | 43 | 68 | n/a | n/a | n/a |
| 9 | HTML Autocomplete PWC           | 15 | 96 | n/a | n/a | n/a |

- 92 percent have a broken autocomplete, one field is missing or wrong
- The field names change, sometimes between two page loads
- The flow is blocked by codes and CAPTCHAs anyway
- So the manager gives up and you type the password yourself





# What we would change





## Recommendations – the security -critical ones

- End the other sessions when the password changes
- Always send a separate email or text, with a fix link
- Show the user the next steps: 2FA, recovery, active sessions
- Make the form clear: a confirm field or a show password toggle button, plus a real update confirmation message
- Test the autofill before you go live





# Recommendations – standards and the ecosystem

- Developers: follow the form rules.  
Frameworks: put the right HTML in by default
- Use the W3C change password URL, it removes the long click hunt
- Make it a guarded API that still keeps 2FA and the checks against abuse
- Browsers can push it, the same way they marked HTTP as not secure





# Open questions

- We measured, but a user test should show if long paths and missing feedback cause real errors
- How much automation will people accept before they feel unsafe
- Why do clear best practices see so little use





- 111 top sites, one pattern: complex, different, hard to automate
- The hard part is not the password, it is the flow around it
- Updates are security work: direct path, clear yes, a separate email, end old sessions

„So what makes changing a password hard?" – It's not the password. It's everything around it.





## Dr. Alexander Krause

CISPA Helmholtz Center for Information Security

Hannover, Germany



[alexander.krause@cispa.de](mailto:alexander.krause@cispa.de)



<https://akrause.de>



Dr. Alexander Krause

### Research Questions

**RQ1** How do websites implement password update processes?

**RQ2** What are common security, usability, and automation challenges and obstacles end-users and password managers face when interacting with password update processes?

**RQ3** How can websites be better supported to deploy more secure, easy-to-use, and more easily automated password update processes?



Dr. Alexander Krause

6

### Method – the protocol

- We checked 32 points in three steps: start, update, feedback
- Two researchers did each site alone
- We used a new Chrome profile and recorded the screen
- We agreed in 96 percent of the cases
- We also tested the W3C change password URL on every site (example.com/well-known/change-password )



Dr. Alexander Krause

### Method – the protocol

- We checked 32 points in three steps: start, update, feedback
- Two researchers did each site alone
- We used a new Chrome profile and recorded the screen
- We agreed in 96 percent of the cases
- We also tested the W3C change password URL on every site (example.com/well-known/change-password )



Dr. Alexander Krause

### Recommendations – standards and the ecosystem

- Developers: follow the form rules.
- Frameworks: put the right HTML in by default
- Use the W3C change password URL, it removes the long click hunt
- Make it a guarded API that still keeps 2FA and the checks against abuse
- Browsers can push it, the same way they marked HTTP as not secure



Dr. Alexander Krause

20