

Adventures in Recovery Land: Testing the Account Recovery of Popular Websites When the Second Factor is Lost

Eva Gerlitz¹, Maximilian Häring², Charlotte Theresa Mädler²,
Matthew Smith^{1,2}, Christian Tiefenau²

¹Fraunhofer FKIE, ²University of Bonn

Eva, how can I increase the security of my accounts?

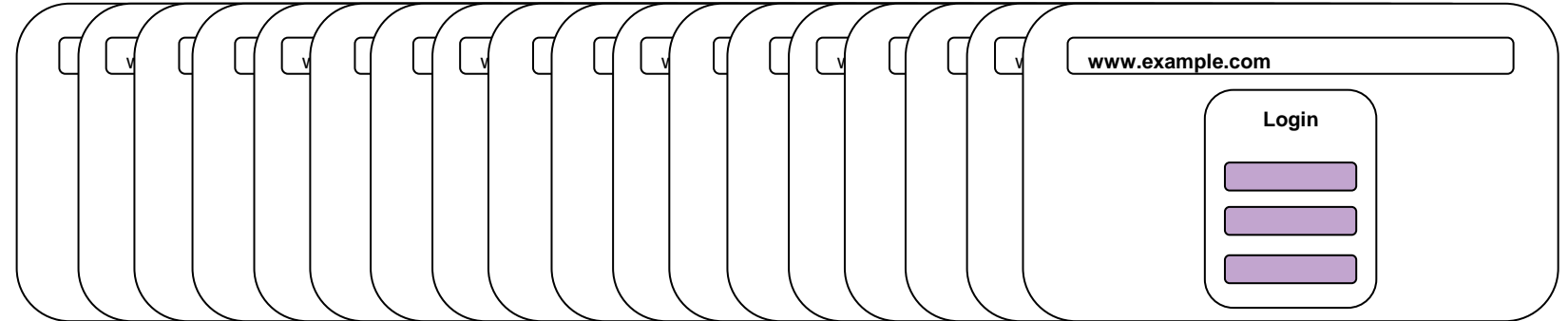
Enable 2FA!

But what happens, if I lose my phone?

...



78 Services



2 Tasks:

1. 2FA Setup

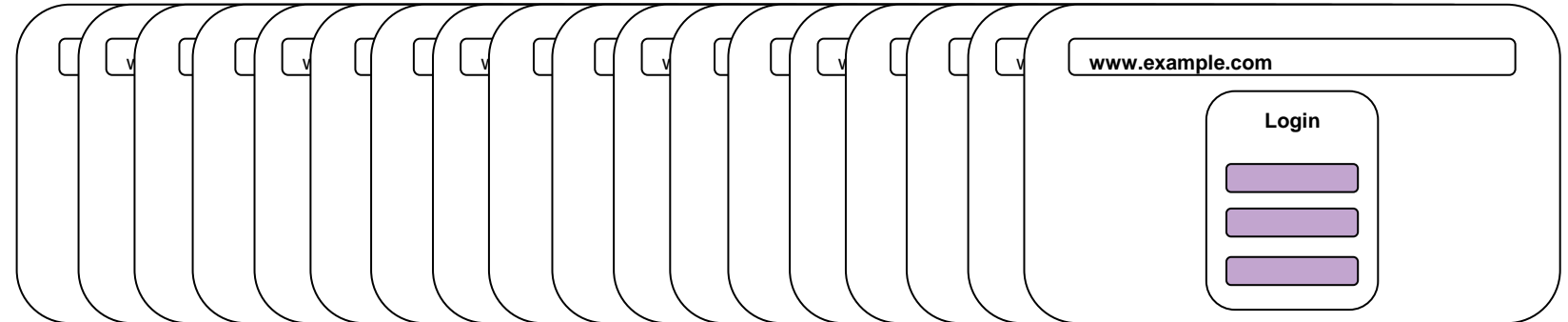


2. Access without second factor

2FA Setup

- Second factor: SMS, Mail, App
- No additional backup

78 Services



2 Tasks:

1. 2FA Setup



2. Access without second factor

Access without second factor

- No access to backup codes
- But: Access to email
- Login screen, Websites FAQs, Google

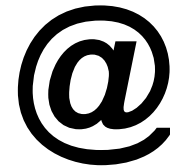
Used second factors



46



25



5



2

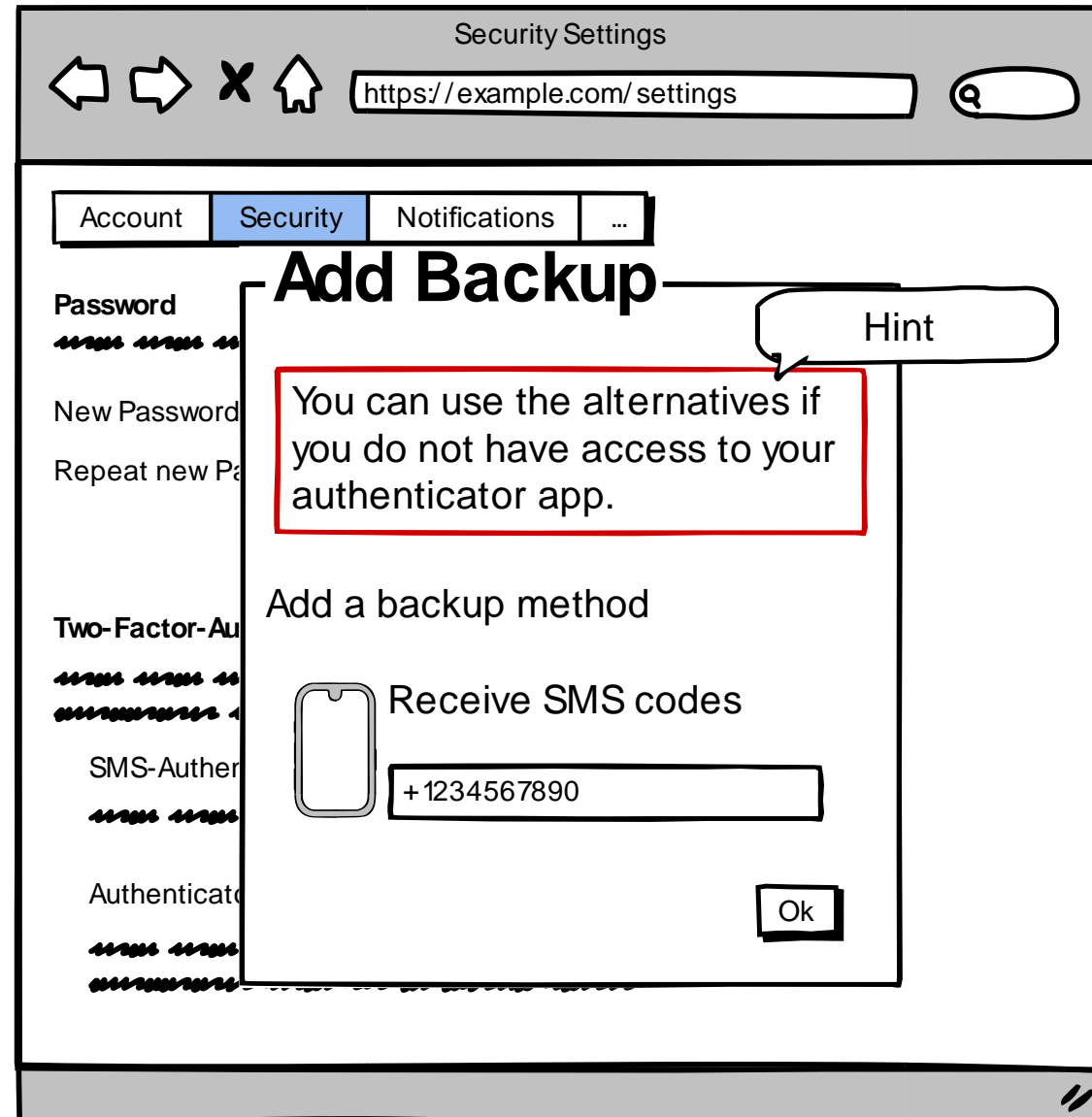
2FA Setup

(How) do popular services **communicate the issue** of losing the second factor to their users?

Cues during 2FA Setup

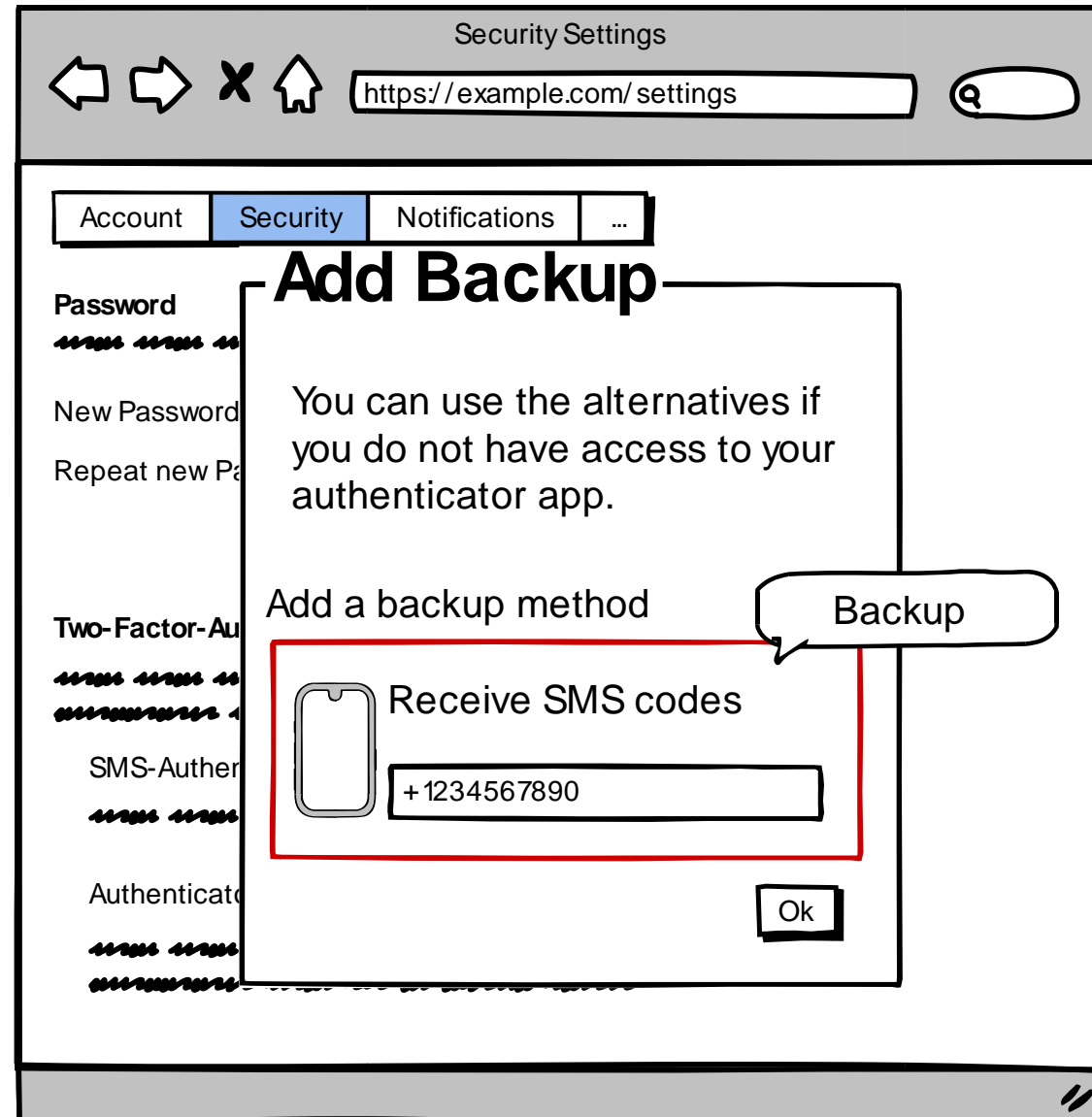
Three different cues:

1) Hint



Three different cues:

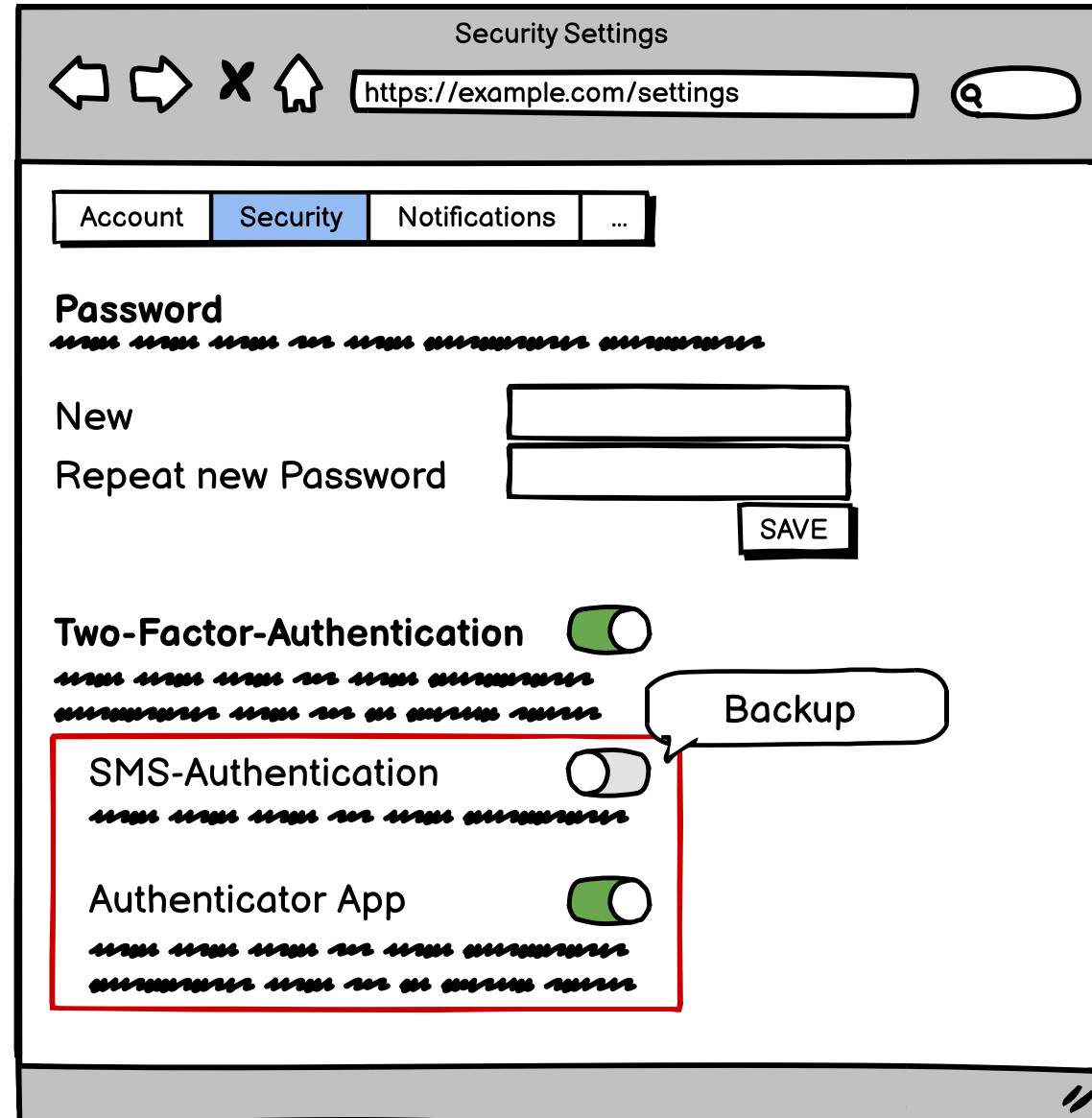
- 1) Hint
- 2) Backup possibility



Cues during 2FA Setup

Three different cues:

- 1) Hint
- 2) Backup possibility



The screenshot shows a web browser window titled "Security Settings" with the URL "https://example.com/settings". The browser's address bar contains navigation icons (back, forward, close, home) and a search icon. Below the address bar is a navigation menu with "Account", "Security" (highlighted), "Notifications", and "...".

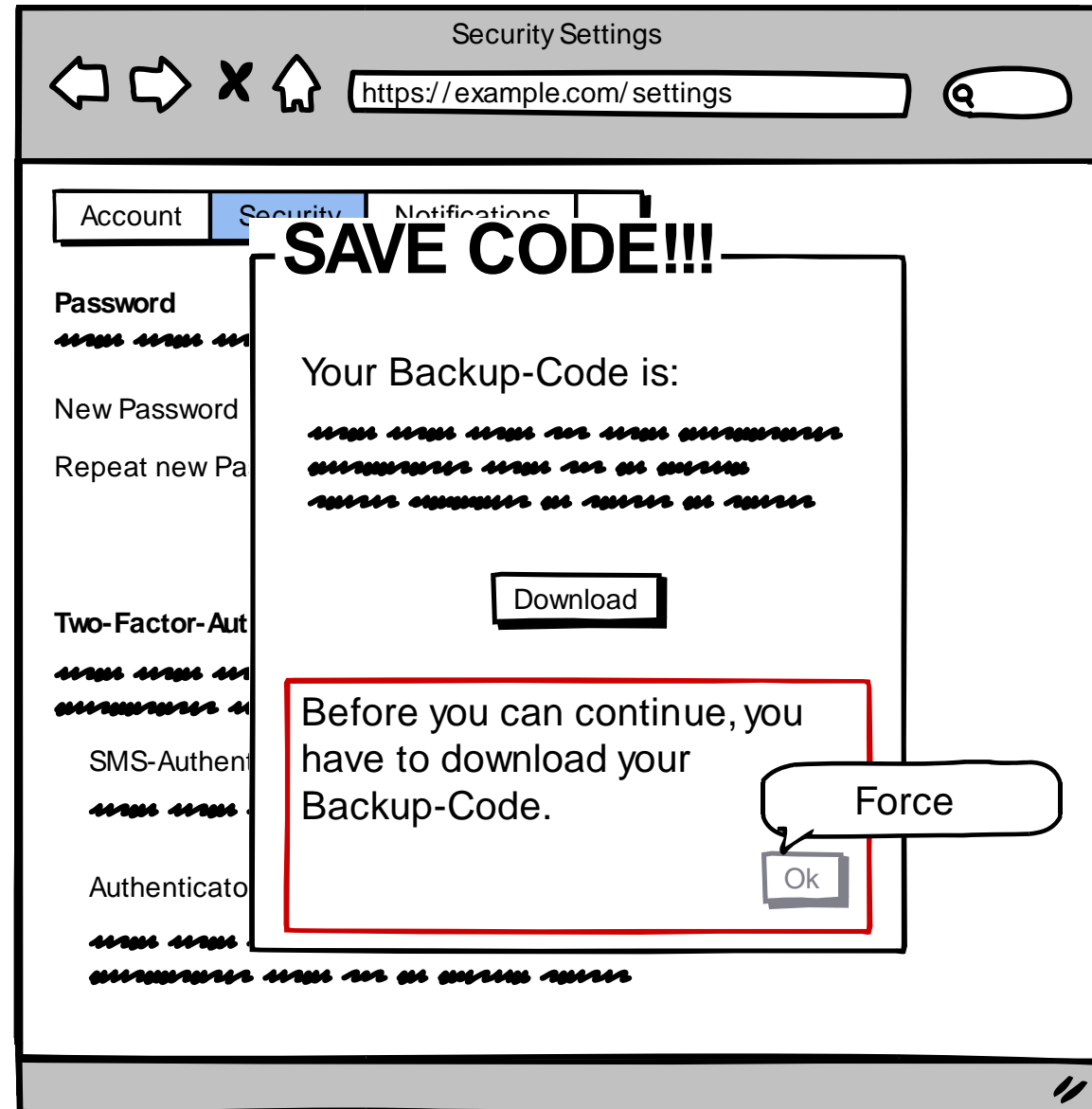
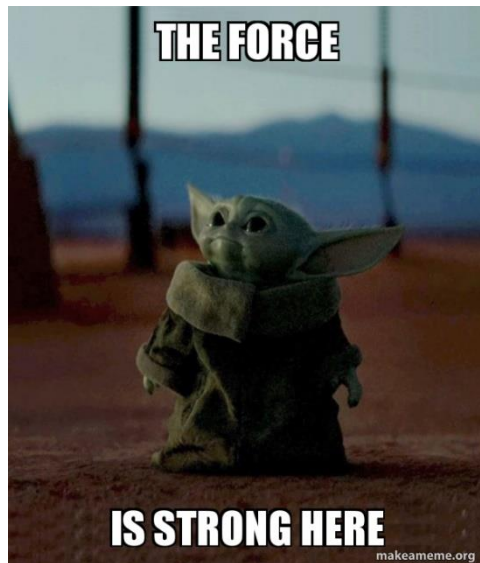
The "Security" section is titled "Password" and contains two input fields: "New" and "Repeat new Password", followed by a "SAVE" button.

The "Two-Factor-Authentication" section is titled "Two-Factor-Authentication" and has a green toggle switch. Below it, there are two options: "SMS-Authentication" (with a grey toggle switch) and "Authenticator App" (with a green toggle switch). A red rectangular box highlights the "SMS-Authentication" and "Authenticator App" options. A speech bubble labeled "Backup" points to the "SMS-Authentication" option.

Cues during 2FA Setup

Three different cues:

- 1) Hint
- 2) Backup possibility
- 3) Force

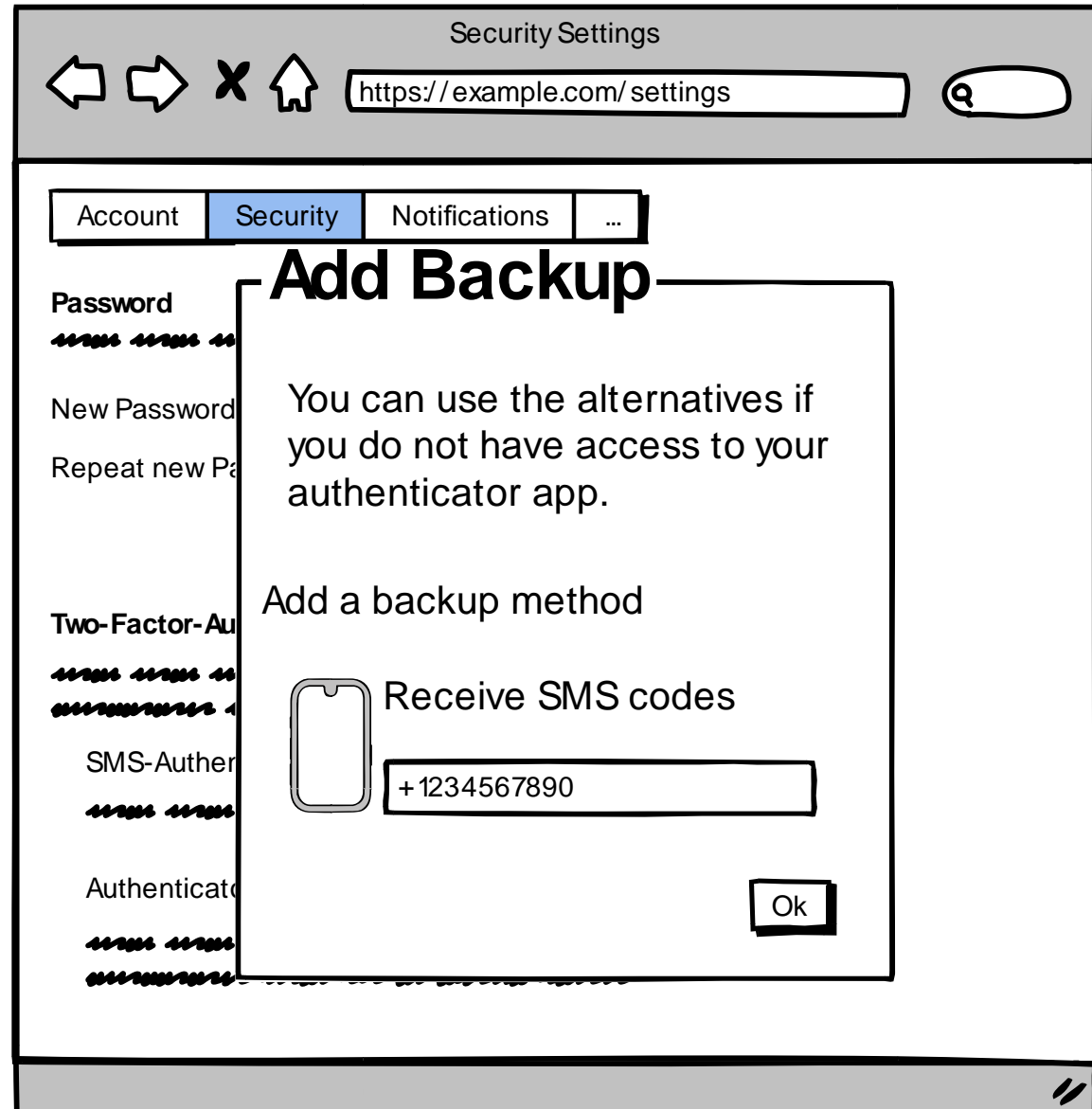


Cues during 2FA Setup

Three different cues:

- 1) Hint
- 2) Backup possibility
- 3) Force

Shown in popup
.. or in settings

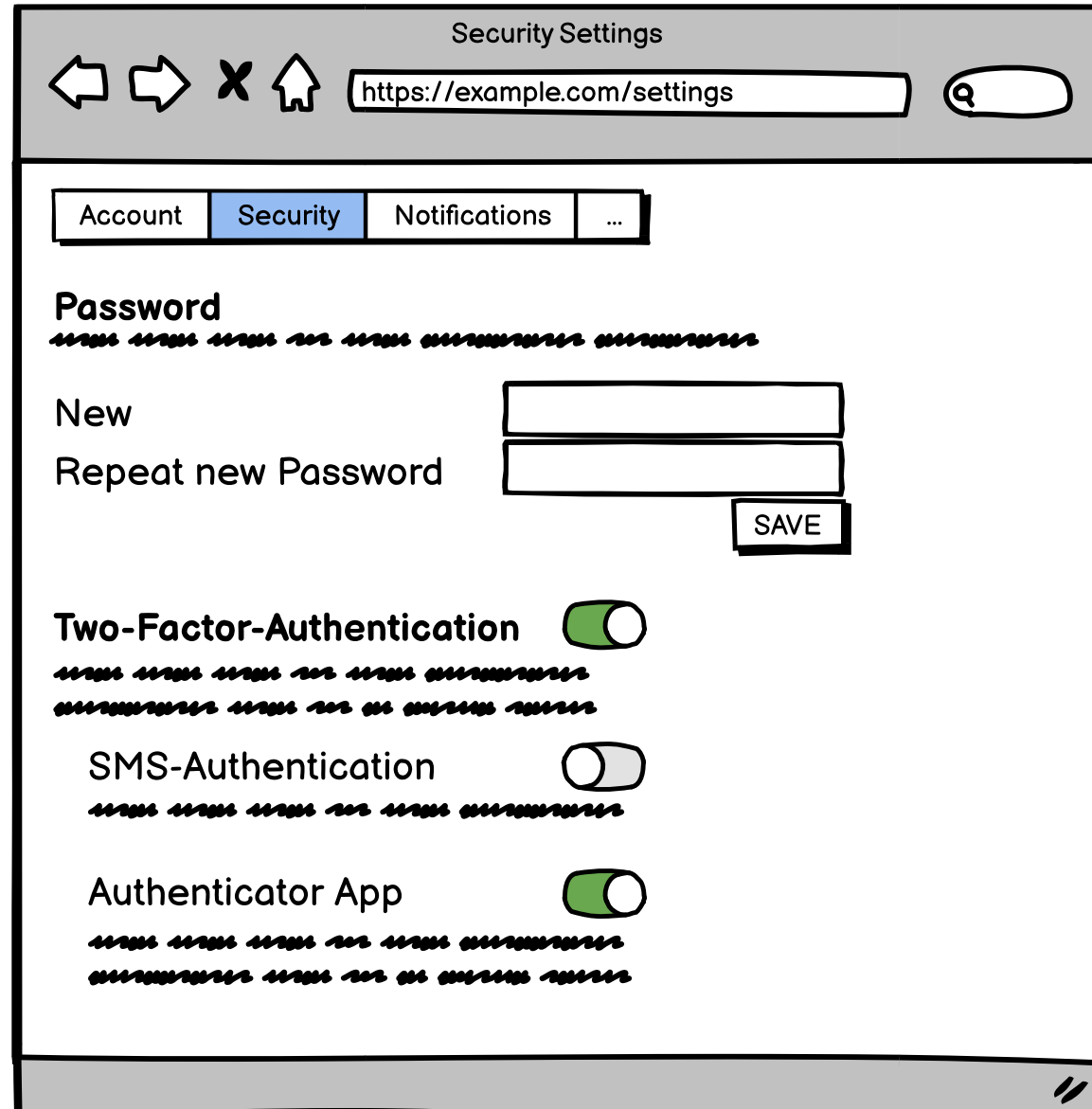


Cues during 2FA Setup

Three different cues:

- 1) Hint
- 2) Backup possibility
- 3) Force

Shown in popup
.. or in settings



The screenshot shows a mobile application interface for 'Security Settings'. At the top, there is a browser-like header with navigation icons (back, forward, close, home) and a URL bar containing 'https://example.com/settings'. Below the header is a tabbed menu with 'Account', 'Security' (selected), and 'Notifications'. The main content area is divided into sections: 'Password' with a strength indicator and two input fields labeled 'New' and 'Repeat new Password', followed by a 'SAVE' button; 'Two-Factor-Authentication' with a green toggle switch and a strength indicator; 'SMS-Authentication' with a grey toggle switch and a strength indicator; and 'Authenticator App' with a green toggle switch and a strength indicator. The bottom of the screen shows a home indicator bar.

Cues during 2FA Setup – Results

● Used ○ Not used

Hint	Backup	Force	Shown in	Number of sites
●	●	○	Popup	29
○	○	○	-	16
●	●	●	Popup	15
64.1%	79.5%	20.5%		

➔ Nothing a user can assume by default or rely on!

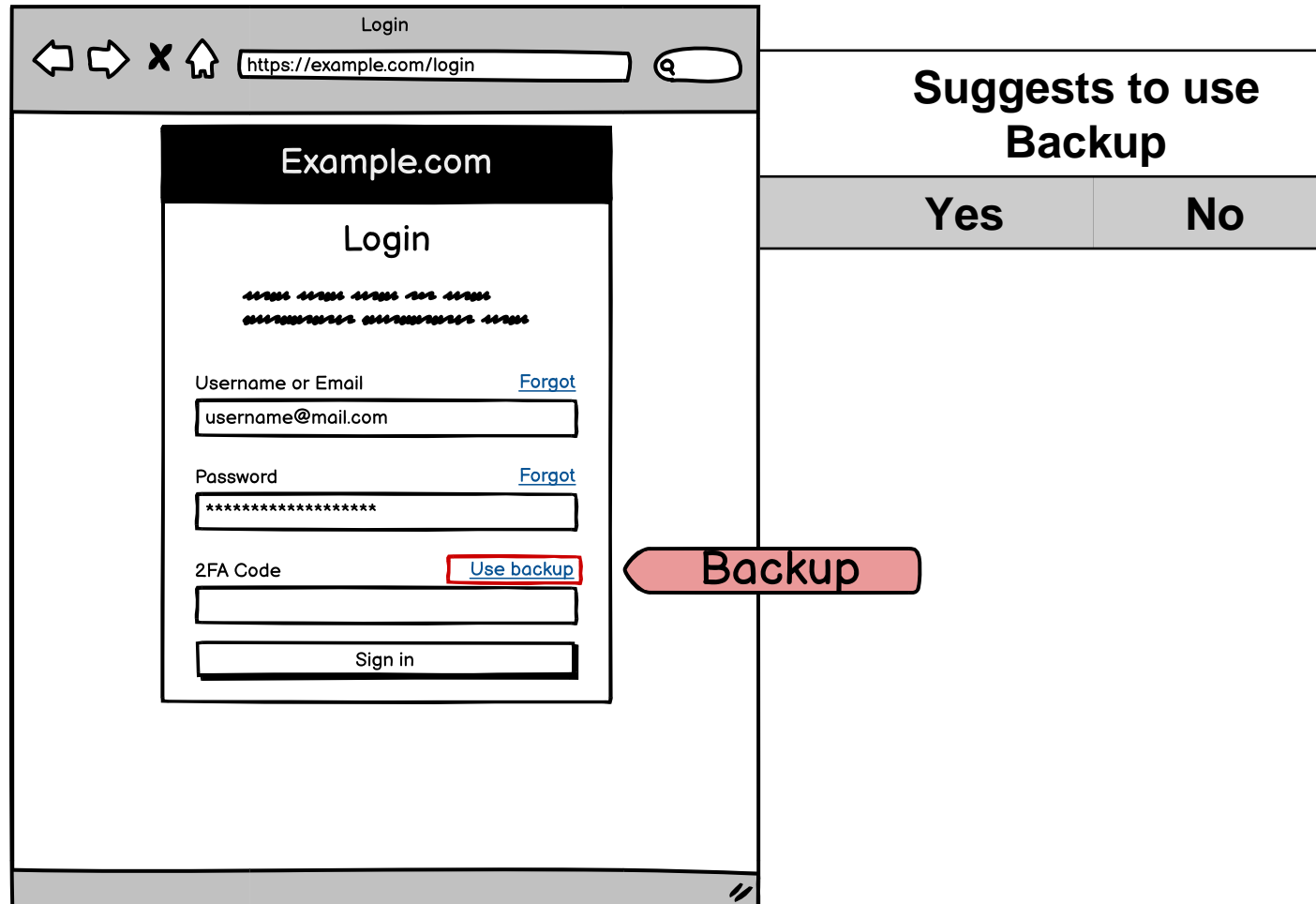


Recovery

How well are users **supported** through the services' recovery protocol when they try to **log in** but the second factor is lost?

Help during 2FA Recovery

Two levels of supports:



Two levels of supports:

Link to support

Yes – Direct form

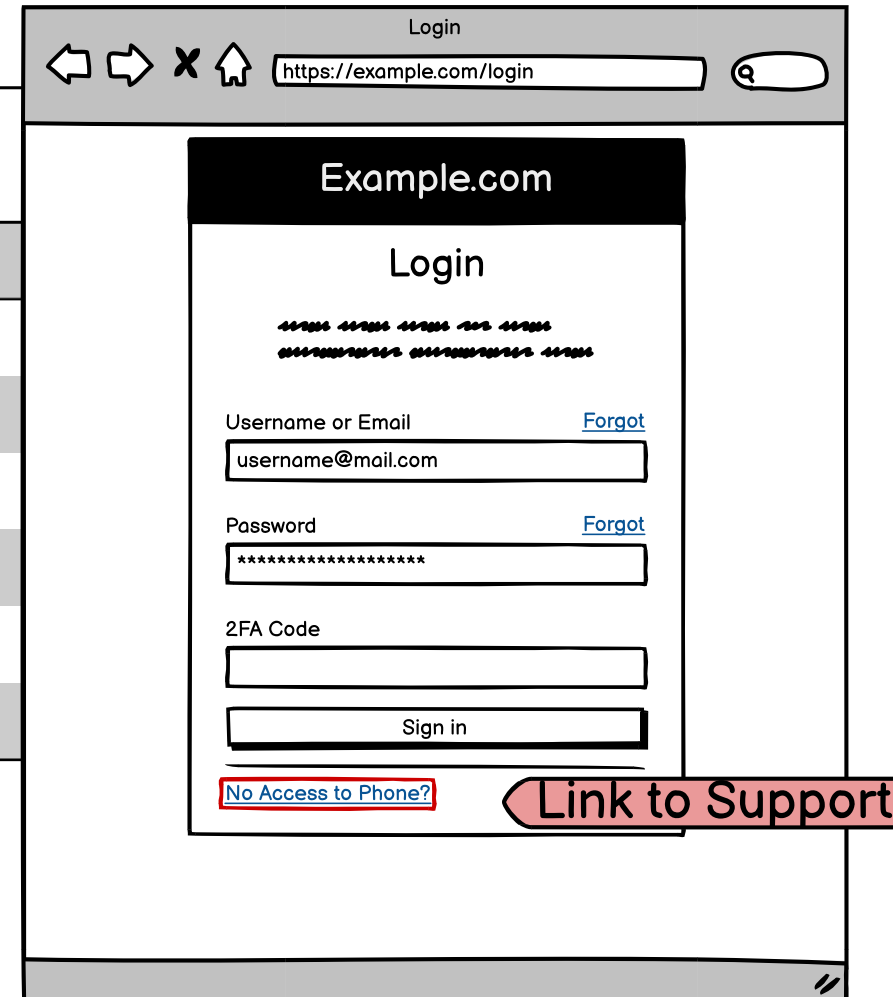
Yes – Specific FAQ

Yes – General FAQ

Yes – Unusable

No – But UI

No – Nothing



The screenshot shows a web browser window titled 'Login' with the URL 'https://example.com/login'. The page content includes the 'Example.com' header, a 'Login' title, a QR code, and input fields for 'Username or Email' (containing 'username@mail.com'), 'Password' (masked with asterisks), and '2FA Code'. There are 'Forgot' links for both the password and 2FA code fields, and a 'Sign in' button. A red callout box labeled 'Link to Support' points to a blue link at the bottom of the page that reads 'No Access to Phone?'.

Two levels of supports:

Link to support

Yes – Direct form

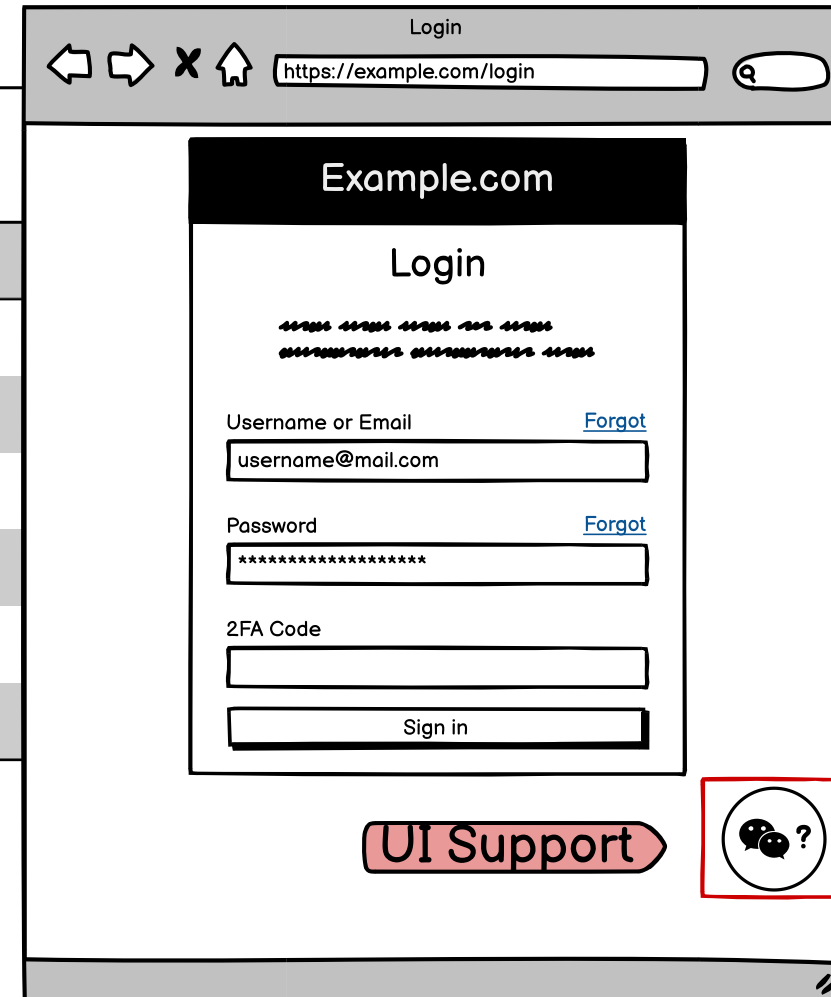
Yes – Specific FAQ

Yes – General FAQ

Yes – Unusable

No – But UI

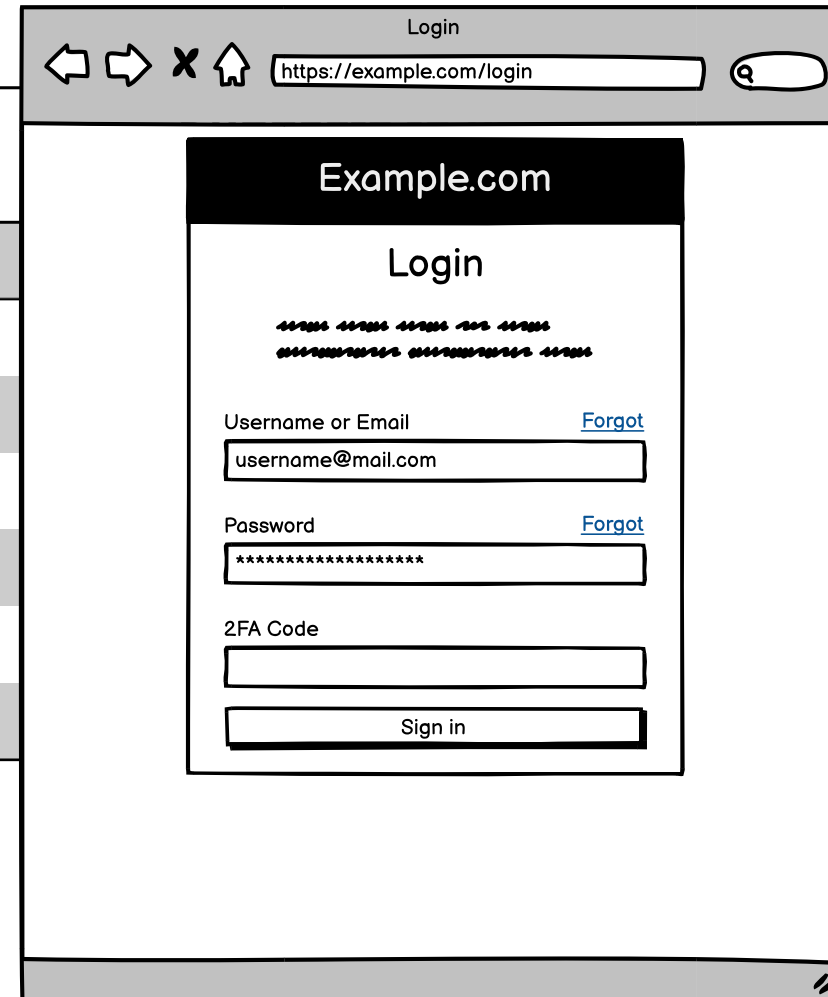
No – Nothing



The screenshot shows a web browser window titled "Login" with the URL "https://example.com/login". The page content includes the "Example.com" header, a "Login" title, a decorative separator, and three input fields: "Username or Email" (containing "username@mail.com"), "Password" (masked with asterisks), and "2FA Code". There are "Forgot" links next to the first two fields. A "Sign in" button is at the bottom. A red box highlights a "UI Support" button and a help icon (two speech bubbles with a question mark) in the bottom right corner.

Two levels of supports:

Link to support
Yes – Direct form
Yes – Specific FAQ
Yes – General FAQ
Yes – Unusable
No – But UI
No – Nothing



The screenshot shows a web browser window titled "Login" with the address bar containing "https://example.com/login". The page content includes the "Example.com" header, a "Login" title, a QR code, and three input fields: "Username or Email" (with a "Forgot" link), "Password" (with a "Forgot" link), and "2FA Code". A "Sign in" button is located at the bottom of the form.

Help during 2FA Recovery - Results

Link to support	Suggests to use Backup	
	Yes	No
Yes – Direct form	15	5
Yes – Specific FAQ	6	1
Yes – General FAQ	6	1
Yes – Unusable	3	2
No – But UI	10	5
No – Nothing	10	14

Link to support	Suggests to use Backup	
	Yes	No
Yes – Direct form	15	5
Yes – Specific FAQ	6	1
Yes – General FAQ ... but specific available	6	1
Yes – Unusable	3	2
No – But UI	10	5
No – Nothing ... but specific available	10	14
	6	14



➔ No common practice, not always equivalent to “forgot password”

Recovery

What **information** do users need to provide to **regain access** to accounts?

Regaining access



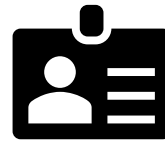
52.6 %

How we regained access

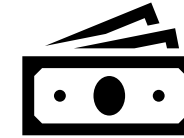
Personal Info



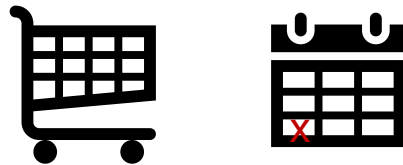
Upload ID



Basic Account Info



Extended Account Info



Access to mails



Summary

- No common practice in any step of 2FA
- Users are often left alone



Open question:

- Who should be responsible?

Adventures in Recovery Land: Testing the Account Recovery of Popular Websites When the Second Factor is Lost

Eva Gerlitz¹, Maximilian Häring², Charlotte Theresa Mädler²,
Matthew Smith^{1,2}, Christian Tiefenau²

¹Fraunhofer FKIE, ²University of Bonn



gerlitz@cs.uni-bonn.de