

Yikes! We need you to wait for a bit before trying

To control abuse, we limit the number of attempted logins per hour.

If the password to your account has recently changed, ensure that all 3rd party Twitter accounts using your account have been updated. For more information, please visit this [help article](#).

Please try again in **60** minutes.

Home | Help Center | Terms | Privacy policy | Imprint | Cookies | Ads info | Brand Blog | Status | Press | About

RUB

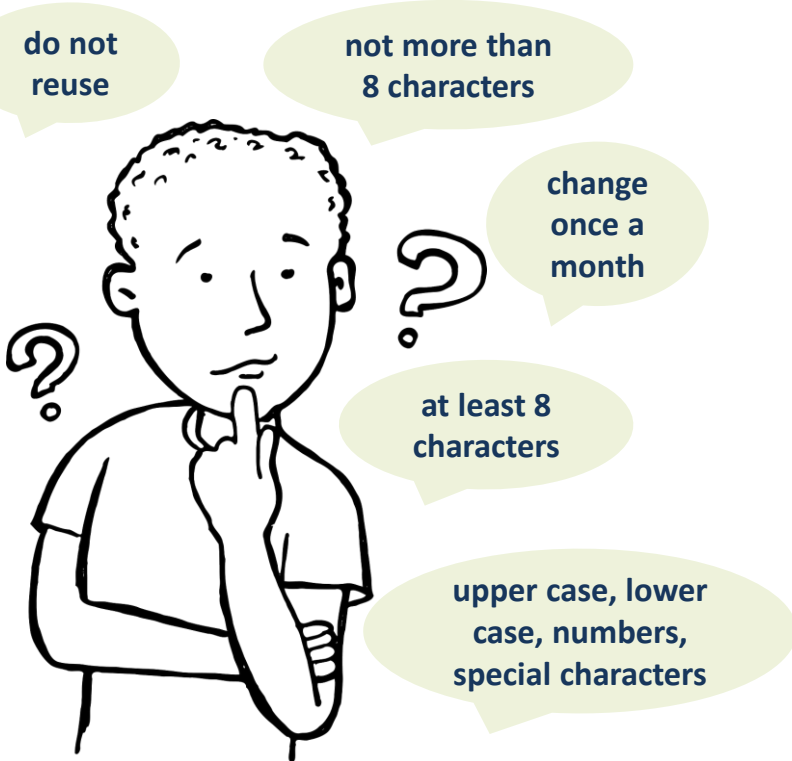
RUHR-UNIVERSITÄT BOCHUM

WILL ANY PASSWORD DO? EXPLORING RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, **Theodor Schnitzler**, Markus Dürmuth

MOTIVATION



Rate-limiting

“... the verifier shall limit attempts on a single account to no more than 100.”

(NIST Special Publication 800-63B)

Research Question

Do real-world websites take appropriate measures to prevent unauthorized accesses to their users' accounts?

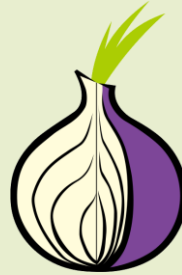
STUDY PROCEDURE

Number of attempts



- Usability: min. 10
- NIST: max. 100
- First impression
- No resource wasting

Tor network



- Hide identity
- Circumvent IP blocking

Final valid attempt



- Correct credentials
- From same Tor session

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

WEBSITES

Existing Accounts

- History & Value

NETFLIX

Google

Dropbox

Don't be evil

- Our own accounts

PLEX



grammarly

amazon.com

YAHOO!

UBER



trainline

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

RUHR
UNIVERSITÄT
BOCHUM

RUB

PASSWORDS

Baseline



- Pwned Passwords v2
- 500 million breached passwords

Composition Policies

Screenshot of a password creation form showing a list of requirements: "At least 1 numeric character [0-9]", "At least 1 uppercase character [A-Z]", "At least 1 lowercase character [a-z]", and "At least 8 and maximum 12 characters". The form also shows a lock icon, a key icon, and a list of allowed symbols: "\$ @ & + - / # _ ? !".

- Remove non-compliant passwords
- Bad practice still in use

Manual Verification

Screenshot of the Google Account creation page showing a "Next" button and a "Sign in instead" link. The page includes fields for First name, Last name, Username, and Password, along with a "Confirm password" field and a "Next" button.

- "8 or more characters"
- "12345678" not allowed

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

RESULTS OVERVIEW

| Alexa | Service | Guesses | Time (Min.) | Login | CAPTCHA | Lockout | Blocking | 2nd Step | Notification |
|-------|-----------|---------|-------------|-------|---------|---------|----------|------------|---------------------|
| 1 | Google | 25 | 10 | 0 | • | 0 | • | - | - |
| 3 | Facebook | 25 | 4 | 0 | 0 | • | 0 | - | - |
| 7 | Yahoo | 25 | 5 | 0 | • | 0 | • | Email Code | Suspicious |
| 12 | Twitter | 25 | 4 | • | 0 | 0 | • | Phone No. | Sign-in, Suspicious |
| 30 | Netflix | 25 | 7 | 0 | 0 | • | • | - | - |
| 84 | Amazon | 25 | 15 | • | • | 0 | • | Email Code | - |
| 89 | Dropbox | 25 | 19 | • | • | 0 | 0 | - | Sign-in |
| 285 | IKEA | 7 | 2 | 0 | 0 | • | 0 | - | Account Locked |
| 664 | Grammarly | 13 | 6 | 0 | 0 | • | • | - | - |
| 992 | Plex | 25 | 7 | • | 0 | 0 | • | - | - |
| 1220 | Uber | 25 | 9 | • | • | 0 | • | SMS Code | - |
| 4333 | Trainline | 25 | 3 | • | 0 | 0 | 0 | - | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

RESULTS OVERVIEW

| Alexa | Service | Guesses | Time (Min.) | Login | CAPTCHA | Lockout | Blocking | 2nd Step | Notification |
|-------------|------------------|-----------|-------------|----------|----------|----------|----------|------------|---------------------|
| 1 | Google | 25 | 10 | ○ | ● | ○ | ● | - | - |
| 3 | Facebook | 25 | 4 | ○ | ○ | ● | ○ | - | - |
| 7 | Yahoo | 25 | 5 | ○ | ● | ○ | ● | Email Code | Suspicious |
| 12 | Twitter | 25 | 4 | ● | ○ | ○ | ● | Phone No. | Sign-in, Suspicious |
| 30 | Netflix | 25 | 7 | ○ | ○ | ● | ● | - | - |
| 84 | Amazon | 25 | 15 | ● | ● | ○ | ● | Email Code | - |
| 89 | Dropbox | 25 | 19 | ● | ● | ○ | ○ | - | Sign-in |
| 285 | IKEA | 7 | 2 | ○ | ○ | ● | ○ | - | Account Locked |
| 664 | Grammarly | 13 | 6 | ○ | ○ | ● | ● | - | - |
| 992 | Plex | 25 | 7 | ● | ○ | ○ | ● | - | - |
| 1220 | Uber | 25 | 9 | ● | ● | ○ | ● | SMS Code | - |
| 4333 | Trainline | 25 | 3 | ● | ○ | ○ | ○ | - | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

RESULTS OVERVIEW

| Alexa | Service | Guesses | Time (Min.) | Login | CAPTCHA | Lockout | Blocking | 2nd Step | Notification |
|-------|-----------|---------|-------------|-------|---------|---------|----------|------------|---------------------|
| 1 | Google | 25 | 10 | ○ | ● | ○ | ● | - | - |
| 3 | Facebook | 25 | 4 | ○ | ○ | ● | ○ | - | - |
| 7 | Yahoo | 25 | 5 | ○ | ● | ○ | ● | Email Code | Suspicious |
| 12 | Twitter | 25 | 4 | ● | ○ | ○ | ● | Phone No. | Sign-in, Suspicious |
| 30 | Netflix | 25 | 7 | ○ | ○ | ● | ● | - | - |
| 84 | Amazon | 25 | 15 | ● | ● | ○ | ● | Email Code | - |
| 89 | Dropbox | 25 | 19 | ● | ● | ○ | ○ | - | Sign-in |
| 285 | IKEA | 7 | 2 | ○ | ○ | ● | ○ | - | Account Locked |
| 664 | Grammarly | 13 | 6 | ○ | ○ | ● | ● | - | - |
| 992 | Plex | 25 | 7 | ● | ○ | ○ | ● | - | - |
| 1220 | Uber | 25 | 9 | ● | ● | ○ | ● | SMS Code | - |
| 4333 | Trainline | 25 | 3 | ● | ○ | ○ | ○ | - | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

ACCOUNT LOCKOUT

| Alexa | Service | Guesses | Time (Min.) | Login | CAPTCHA | Lockout | Blocking | 2nd Step | Notification |
|-------|-----------|---------|-------------|-------|---------|---------|----------|------------|---------------------|
| 1 | Google | 25 | 10 | ○ | ● | ○ | ● | - | - |
| 3 | Facebook | 25 | 4 | ○ | ○ | ● | ○ | - | - |
| 7 | Yahoo | 25 | 5 | ○ | ● | ○ | ● | Email Code | Suspicious |
| 12 | Twitter | 25 | 4 | ● | ○ | ○ | ● | Phone No. | Sign-in, Suspicious |
| 30 | Netflix | 25 | 7 | ○ | ○ | ● | ● | - | - |
| 84 | Amazon | 25 | 15 | ● | ● | ○ | ● | Email Code | - |
| 89 | Dropbox | 25 | 19 | ● | ● | ○ | ○ | - | Sign-in |
| 285 | IKEA | 7 | 2 | ○ | ○ | ● | ○ | - | Account Locked |
| 664 | Grammarly | 13 | 6 | ○ | ○ | ● | ● | - | - |
| 992 | Plex | 25 | 7 | ● | ○ | ○ | ● | - | - |
| 1220 | Uber | 25 | 9 | ● | ● | ○ | ● | SMS Code | - |
| 4333 | Trainline | 25 | 3 | ● | ○ | ○ | ○ | - | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

ACCOUNT LOCKOUT

The image shows a browser window with the Netflix login page. The browser's address bar displays "https://www.netflix.com/nl-en/login". The Netflix logo is visible on the left. The main heading is "Sign In". A red rectangular box highlights a grey message box that reads: "We are having technical difficulties and are actively working on a fix. Please try again in a few minutes." Below this message are input fields for "Email" (containing "XXXXXXXXXX@gmail.com") and "Password".

| 2nd Step | Notification |
|------------|---------------------|
| - | - |
| Email Code | Suspicious |
| Phone No. | Sign-In, Suspicious |
| - | - |
| Email Code | - |
| - | Sign-In |
| - | Account Locked |
| - | - |
| SMS Code | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

SUCCESSFUL LOGIN


| Alexa | Service | Guesses | Time (Min.) | Login | CAPTCHA | Lockout | Blocking | 2nd Step | Notification |
|-------|-----------|---------|-------------|-------|---------|---------|----------|------------|---------------------|
| 1 | Google | 25 | 10 | ○ | ● | ○ | ● | - | - |
| 3 | Facebook | 25 | 4 | ○ | ○ | ● | ○ | - | - |
| 7 | Yahoo | 25 | 5 | ○ | ● | ○ | ● | Email Code | Suspicious |
| 12 | Twitter | 25 | 4 | ● | ○ | ○ | ● | Phone No. | Sign-in, Suspicious |
| 30 | Netflix | 25 | 7 | ○ | ○ | ● | ● | - | - |
| 84 | Amazon | 25 | 15 | ● | ● | ○ | ● | Email Code | - |
| 89 | Dropbox | 25 | 19 | ● | ● | ○ | ○ | - | Sign-in |
| 285 | IKEA | 7 | 2 | ○ | ○ | ● | ○ | - | Account Locked |
| 664 | Grammarly | 13 | 6 | ○ | ○ | ● | ● | - | - |
| 992 | Plex | 25 | 7 | ● | ○ | ○ | ● | - | - |
| 1220 | Uber | 25 | 9 | ● | ● | ○ | ● | SMS Code | - |
| 4333 | Trainline | 25 | 3 | ● | ○ | ○ | ○ | - | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

SUCCESSFUL LOGIN

Alexa  Verify your identity English ▾ Notification

1 C Help us keep your account safe.

3 F

7 V

12 T Verify your identity by entering the phone number associated with your Twitter account.

30 P [Why am I being asked for this information?](#)

84 A Hint: **Your phone number ends in 22**

89 E

285 I

664 C

992 P

1220 L

4333 T

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

BLOCKING

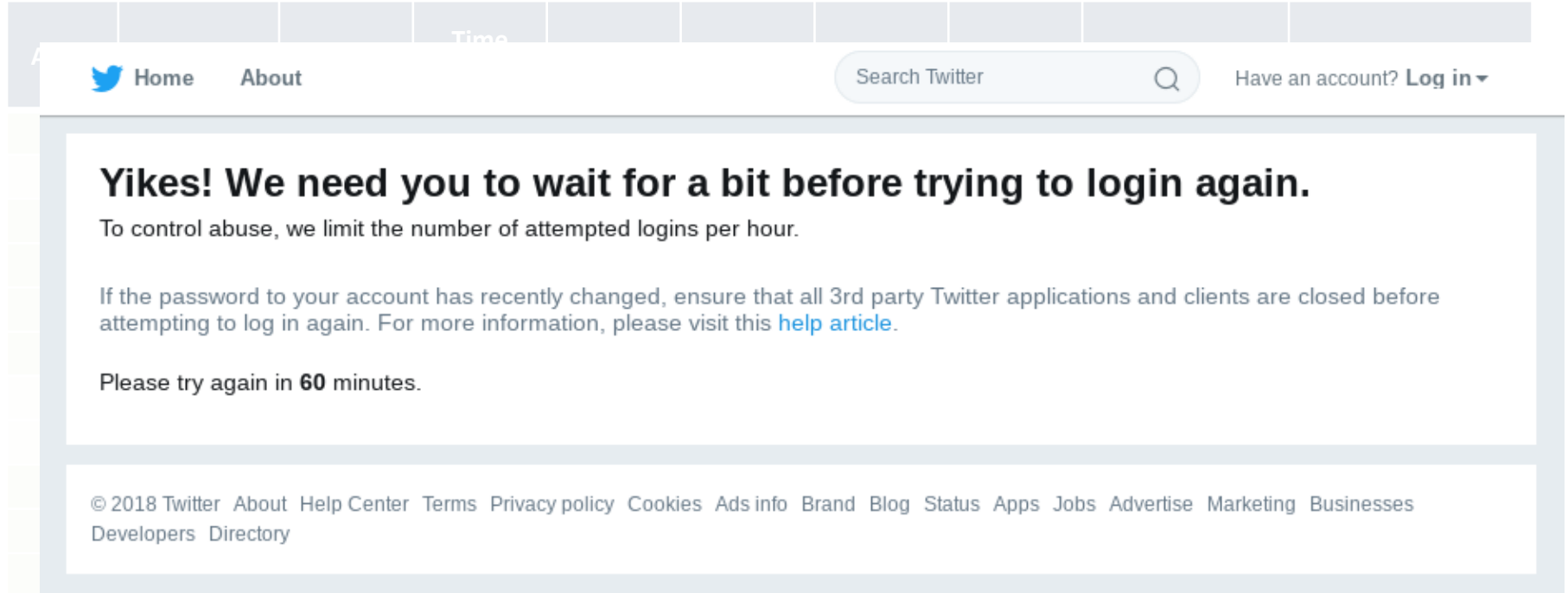
| Alexa | Service | Guesses | Time (Min.) | Login | CAPTCHA | Lockout | Blocking | 2nd Step | Notification |
|-------|-----------|---------|-------------|-------|---------|---------|----------|------------|---------------------|
| 1 | Google | 25 | 10 | ○ | ● | ○ | ● | - | - |
| 3 | Facebook | 25 | 4 | ○ | ○ | ● | ○ | - | - |
| 7 | Yahoo | 25 | 5 | ○ | ● | ○ | ● | Email Code | Suspicious |
| 12 | Twitter | 25 | 4 | ● | ○ | ○ | ● | Phone No. | Sign-in, Suspicious |
| 30 | Netflix | 25 | 7 | ○ | ○ | ● | ● | - | - |
| 84 | Amazon | 25 | 15 | ● | ● | ○ | ● | Email Code | - |
| 89 | Dropbox | 25 | 19 | ● | ● | ○ | ○ | - | Sign-in |
| 285 | IKEA | 7 | 2 | ○ | ○ | ● | ○ | - | Account Locked |
| 664 | Grammarly | 13 | 6 | ○ | ○ | ● | ● | - | - |
| 992 | Plex | 25 | 7 | ● | ○ | ○ | ● | - | - |
| 1220 | Uber | 25 | 9 | ● | ● | ○ | ● | SMS Code | - |
| 4333 | Trainline | 25 | 3 | ● | ○ | ○ | ○ | - | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

BLOCKING



The screenshot shows the Twitter login page with a navigation bar at the top containing 'Home', 'About', a search bar, and a 'Log in' link. The main content area features a large error message: 'Yikes! We need you to wait for a bit before trying to login again.' Below this, it explains that logins are limited to control abuse and provides instructions for users who have recently changed their passwords. A 60-minute wait time is specified. At the bottom of the page, a footer contains various links such as 'About', 'Help Center', 'Terms', 'Privacy policy', 'Cookies', 'Ads info', 'Brand', 'Blog', 'Status', 'Apps', 'Jobs', 'Advertise', 'Marketing', 'Businesses', 'Developers', and 'Directory'.

Home About Search Twitter Have an account? Log in ▾

Yikes! We need you to wait for a bit before trying to login again.

To control abuse, we limit the number of attempted logins per hour.

If the password to your account has recently changed, ensure that all 3rd party Twitter applications and clients are closed before attempting to log in again. For more information, please visit this [help article](#).

Please try again in **60** minutes.

© 2018 Twitter About Help Center Terms Privacy policy Cookies Ads info Brand Blog Status Apps Jobs Advertise Marketing Businesses Developers Directory

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, **Theodor Schnitzler**, Markus Dürmuth

CAPTCHA

| Alexa | Service | Guesses | Time (Min.) | Login | CAPTCHA | Lockout | Blocking | 2nd Step | Notification |
|-------|-----------|---------|-------------|-------|---------|---------|----------|------------|---------------------|
| 1 | Google | 25 | 10 | ○ | ● | ○ | ● | - | - |
| 3 | Facebook | 25 | 4 | ○ | ○ | ● | ○ | - | - |
| 7 | Yahoo | 25 | 5 | ○ | ● | ○ | ● | Email Code | Suspicious |
| 12 | Twitter | 25 | 4 | ● | ○ | ○ | ● | Phone No. | Sign-in, Suspicious |
| 30 | Netflix | 25 | 7 | ○ | ○ | ● | ● | - | - |
| 84 | Amazon | 25 | 15 | ● | ● | ○ | ● | Email Code | - |
| 89 | Dropbox | 25 | 19 | ● | ● | ○ | ○ | - | Sign-in |
| 285 | IKEA | 7 | 2 | ○ | ○ | ● | ○ | - | Account Locked |
| 664 | Grammarly | 13 | 6 | ○ | ○ | ● | ● | - | - |
| 992 | Plex | 25 | 7 | ● | ○ | ○ | ● | - | - |
| 1220 | Uber | 25 | 9 | ● | ● | ○ | ● | SMS Code | - |
| 4333 | Trainline | 25 | 3 | ● | ○ | ○ | ○ | - | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

NOTIFICATIONS

| Alexa | Service | Guesses | Time (Min.) | Login | CAPTCHA | Lockout | Blocking | 2nd Step | Notification |
|-------|-----------|---------|-------------|-------|---------|---------|----------|------------|---------------------|
| 1 | Google | 25 | 10 | ○ | ● | ○ | ● | - | - |
| 3 | Facebook | 25 | 4 | ○ | ○ | ● | ○ | - | - |
| 7 | Yahoo | 25 | 5 | ○ | ● | ○ | ● | Email Code | Suspicious |
| 12 | Twitter | 25 | 4 | ● | ○ | ○ | ● | Phone No. | Sign-in, Suspicious |
| 30 | Netflix | 25 | 7 | ○ | ○ | ● | ● | - | - |
| 84 | Amazon | 25 | 15 | ● | ● | ○ | ● | Email Code | - |
| 89 | Dropbox | 25 | 19 | ● | ● | ○ | ○ | - | Sign-in |
| 285 | IKEA | 7 | 2 | ○ | ○ | ● | ○ | - | Account Locked |
| 664 | Grammarly | 13 | 6 | ○ | ○ | ● | ● | - | - |
| 992 | Plex | 25 | 7 | ● | ○ | ○ | ● | - | - |
| 1220 | Uber | 25 | 9 | ● | ● | ○ | ● | SMS Code | - |
| 4333 | Trainline | 25 | 3 | ● | ○ | ○ | ○ | - | - |

WILL ANY PASSWORD DO? RATE-LIMITING ON THE WEB

WAY'18, Baltimore, MD, USA, 12 August 2018

Maximilian Golla, Theodor Schnitzler, Markus Dürmuth

TAKEAWAY

Combine mechanisms



- Large services take most effort
- CAPTCHA, Blocking, multiple steps, security notifications

Trade-off usability



- Smaller websites lock down accounts
- Requires user effort to regain access

No rate-limiting detected



- No protection on provider side
- Leave account security solely to users
- Not recommendable