

ICICS 2026



南開大學
Nankai University

An Empirical Measurement Study of Authentication Mechanisms in Cloud-Based Password Managers

Yanduo Fu, Qingxuan Wang, Ding Wang

College of Cryptology and Cyber Science, Nankai University, Tianjin, China

October 28, 2026

Background: Managing passwords creates a usability-security dilemma

Increasing account numbers



80-112 accounts^[1-2] before COVID-19



120 accounts^[3] after COVID-19

Password guidelines



Creating **random & unique** passwords for each account



Enhancing password security for web users



High password-management burden!

Using **popular or similar** passwords across multiple accounts



Passwords are **reused** and **guessable**

[1] Leveraging semantic transformation to investigate password habits and their causes. In Proc. CHI 2018, pp. 1-12.

[2] Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In Proc. ACM CCS 2017, pp. 295-310.

[3] Juggling security: How many passwords does the average person have in 2026? <https://nordpass.com/blog/how-many-passwords-does-average-person-have/>

Background: Password managers provide a technical solution

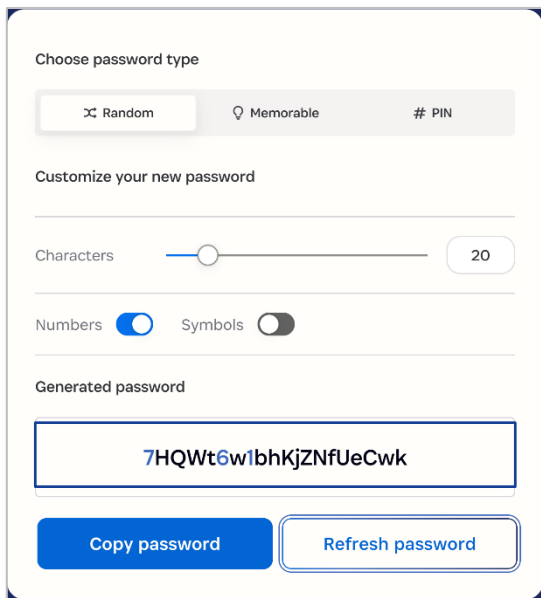


Built-in PMs



Standalone PMs (Cloud-based and Local-Deployed)

Background: Password managers provide a technical solution



Choose password type

☒ Random ☐ Memorable ☐ # PIN

Customize your new password

Characters 20

Numbers ☒ Symbols ☐

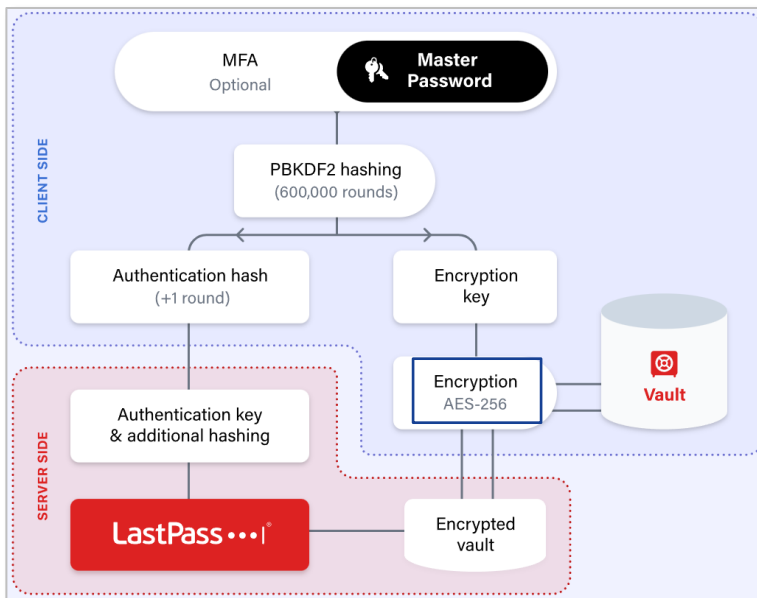
Generated password

7HQWt6w1bhkjZNfUeCwk

Copy password Refresh password

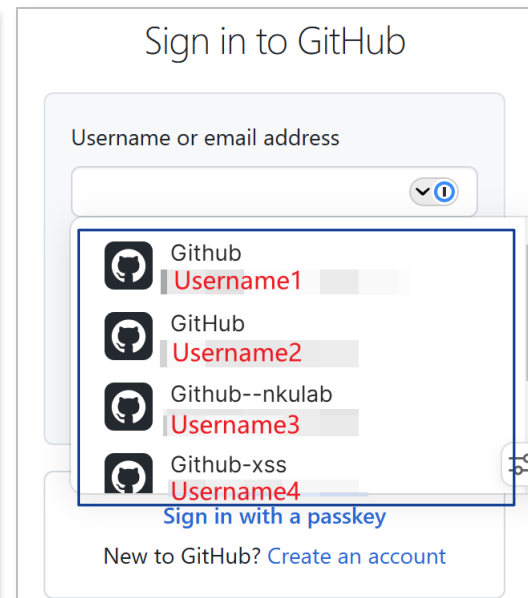
[1Password]

Generate strong passwords



[LastPass]

Encrypted storage



Sign in to GitHub

Username or email address

Dropdown menu showing autofill suggestions:

- Github Username1
- Github Username2
- Github--nkulab Username3
- Github-xss Username4

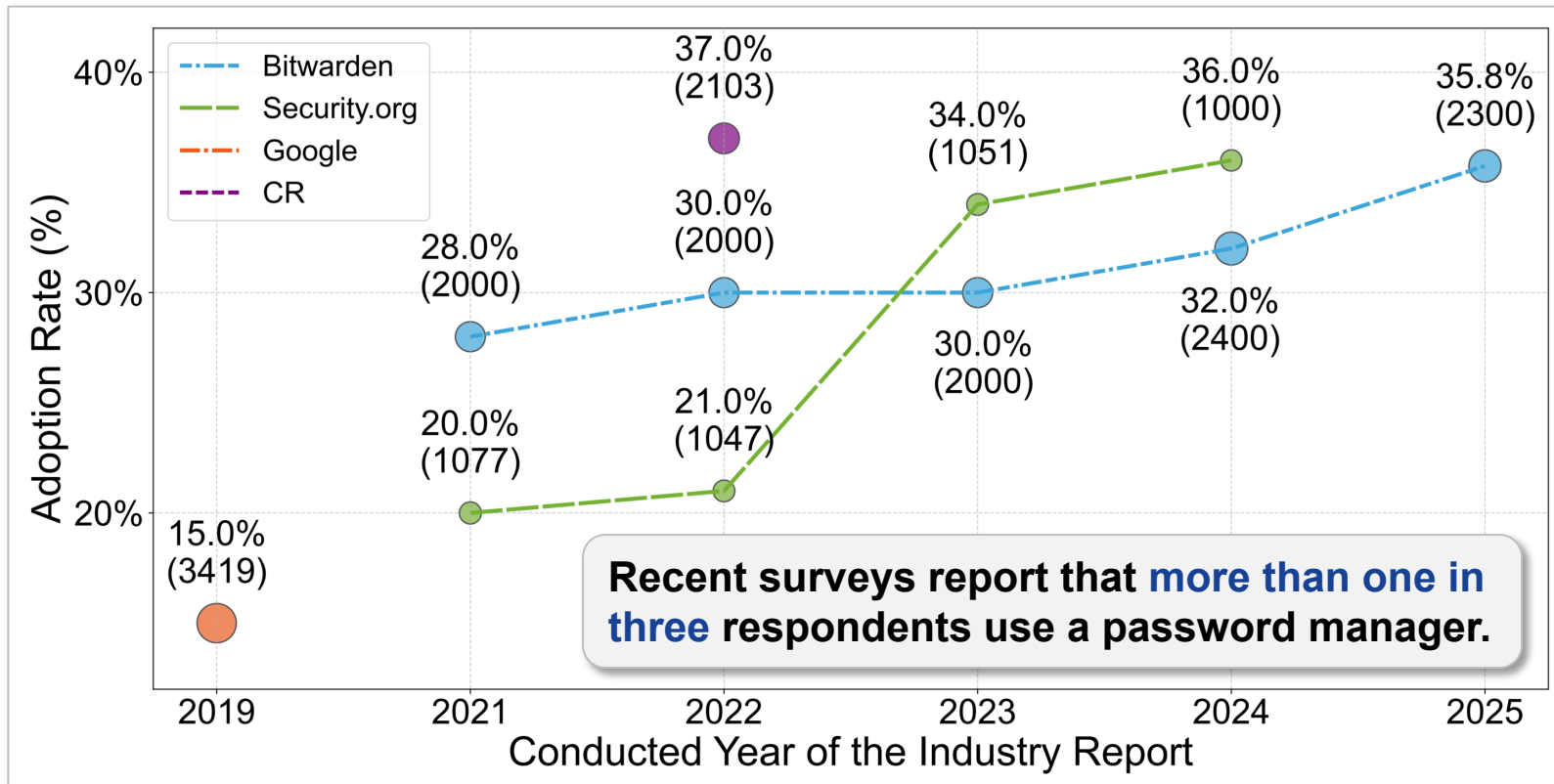
Sign in with a passkey

New to GitHub? [Create an account](#)

[1Password and GitHub]

Convenient autofill

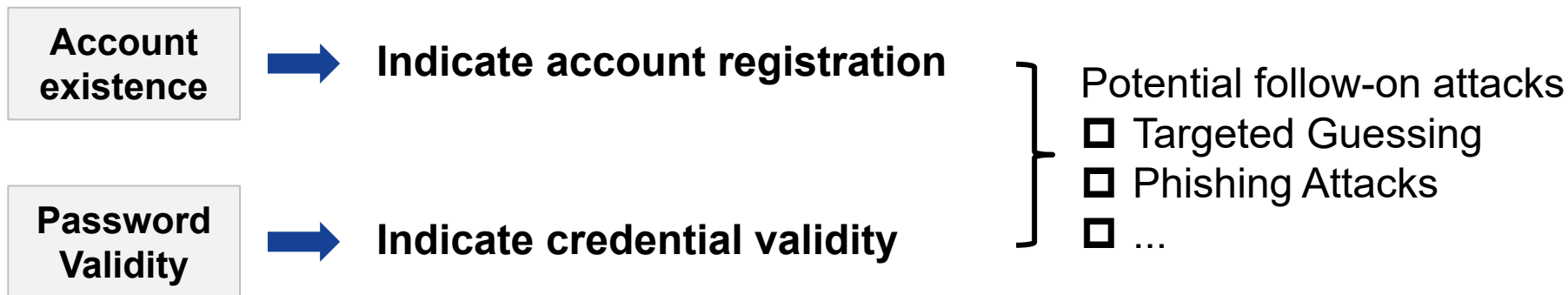
Background: Password-manager use is widespread



Motivation: Cloud access exposes a public authentication workflow



What can public login interface reveal to an attacker?



These signals can identify targeted accounts and confirm password guesses.

Threat Model: A fresh-device attacker observes the workflow

The attacker can:

- ❑ ... access public websites or extensions
- ❑ ... submit candidate identifiers and credentials
- ❑ ... observe UI feedback, network response, and workflow transitions

The attacker cannot:

- ❑ ... complete email / SMS / device verification
- ❑ ... use trusted sessions
- ❑ ... possess required additional keys

RQ1 Does this account exist?

RQ2 Is this credential correct?

RQ3 What happens after repeated failures?

Method: 15 PMs, 20 Entry points, controlled black-box probes

Measured products

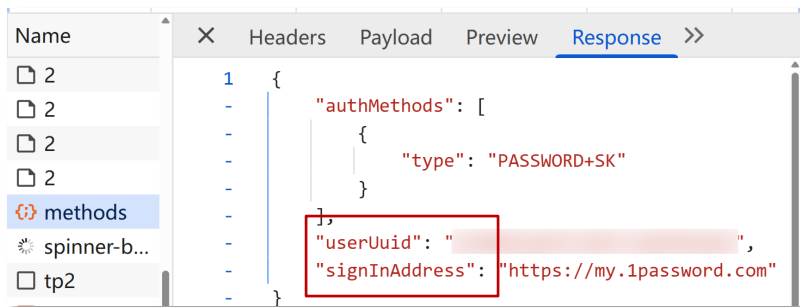
- ❑ 8 single-master password:
LastPass, Bitwarden, Proton Pass,
Dashlane, Keeper, True Key,
RoboForm, DualSafe
- ❑ 5 two-stage:
Avira, NordPass, Norton,
Kaspersky, Zoho Vault
- ❑ 2 compound (with additional keys)
1Password, MultiPassword

Probe	Controlled Comparison
Account Existence	❑ Registered / Unregistered ❑ Same incorrect credentials
Credential Validity	❑ Correct / Incorrect ❑ Same registered identifier
Repeated Failures	❑ ≤ 15 incorrect submissions ❑ ≥ 5 seconds between attempts

RQ1: Six PMs expose a stable account-existence signal

6 / 15 PMs with a stable signal

- ❑ **Workflow:** LastPass
- ❑ **UI:** DualSafe, True Key, Zoho Vault
- ❑ **Network:** 1Password, MultiPassword



1Password Example:

same HTTP status, different response fields

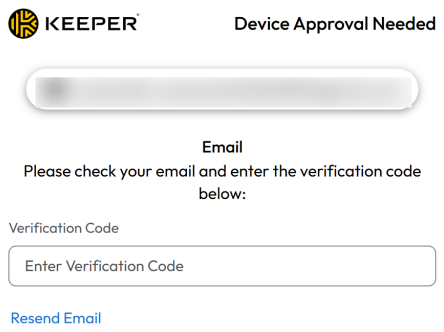
- ❑ **Registered:** userUuid and signInAddress
- ❑ **Unregistered:** those fields are absent



Account-existence signals could help tailor product-specific phishing.

RQ2: 15 entry points expose a credential-validity signal

Outcome	Entry Points	Meaning
Stable Signal	15	☐ Correct and incorrect candidates differ
Blocked	3	☐ Verification prevents validity exposure ☐ Dashlane, Keeper: Verification before inputting the password ☐ LastPass: Same email-verification responses for both candidates
Compound	2	☐ Additional key prevents isolation ☐ 1Password and MultiPassword



KEEPER Device Approval Needed

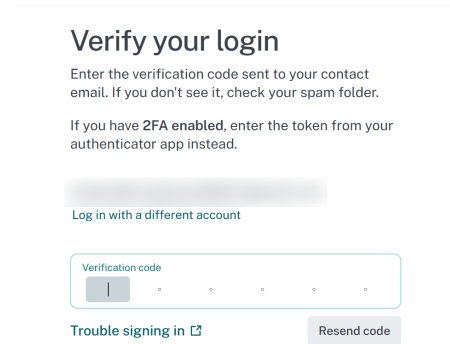
Please check your email and enter the verification code below:

Email

Verification Code

Enter Verification Code

Resend Email



Verify your login

Enter the verification code sent to your contact email. If you don't see it, check your spam folder.

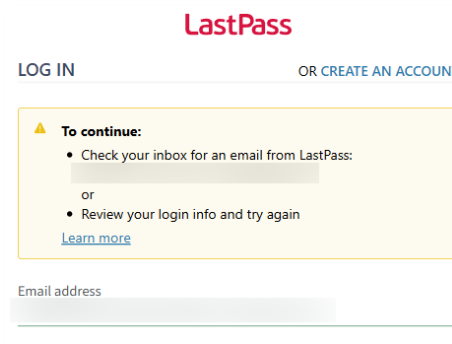
If you have 2FA enabled, enter the token from your authenticator app instead.

Log in with a different account

Verification code

Trouble signing in

Resend code



LastPass

LOG IN OR CREATE AN ACCOUNT

To continue:

- Check your inbox for an email from LastPass:
- or
- Review your login info and try again

Learn more

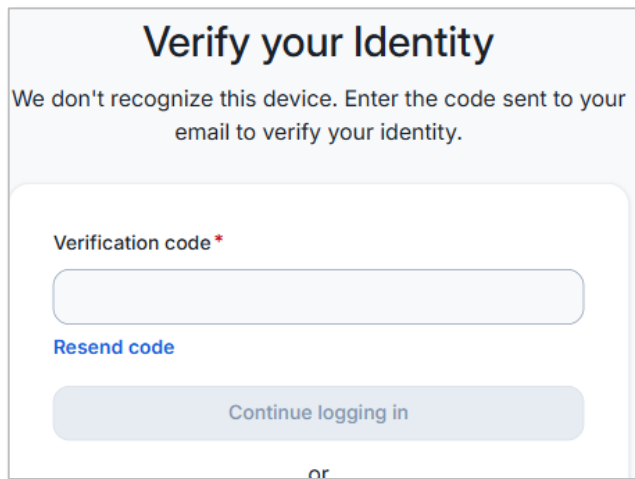
Email address

Victim verification stops attackers before inputting the password.

Same email verification

RQ2: Login feedback can reveal credential validity before vault access

Correct master password



Verify your Identity

We don't recognize this device. Enter the code sent to your email to verify your identity.

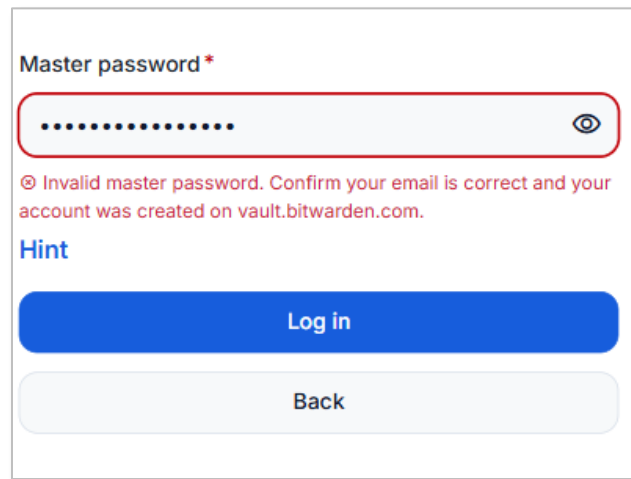
Verification code *

[Resend code](#)

[Continue logging in](#)

or

Incorrect master password



Master password *

© Invalid master password. Confirm your email is correct and your account was created on vault.bitwarden.com.

[Hint](#)

[Log in](#)

[Back](#)

The responses differ before the vault is unlocked.

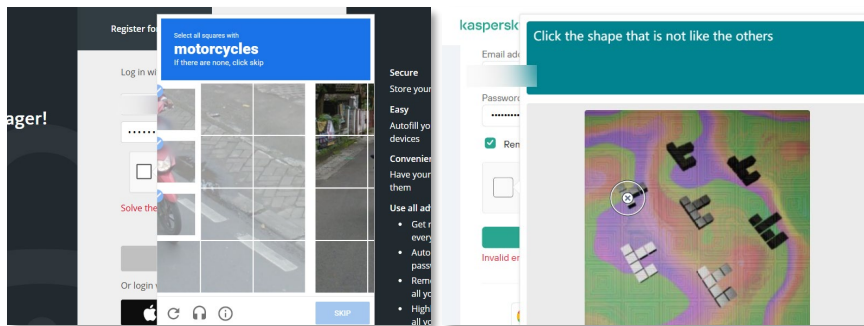
RQ3: Interventions observed during repeated failures

Bounded Result	Entry Points
Visible intervention	12
None observed within budget	6
Credential submission unreachable	2

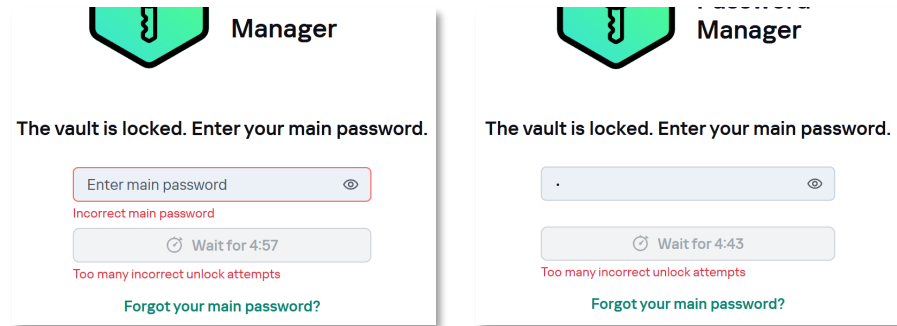
Mechanisms among 12 entry points

- ❑ CAPTCHA: 5 entry points
- ❑ Temporary Lockout: 5 entry points
- ❑ UI Reset: 2 entry points
- ❑ Rate Limiting: 1 entry point

CAPTCHA / UI Reset: Attempts remain possible



Temporary Lockout: Block legitimate access



Existence signals, validity signals, and stopping boundaries differ

Table 2: Account-Existence and Credential-Validity Signals, Repeated-Failure Responses, and Stopping Boundaries Across the Tested Entry Points*.

Password Manager	Entry Point	Account Existence [†]	Credential Validity [†]	Failure [‡] Response(≤ 15)	Stopping Boundary [◊]	Process Mode [*]
LastPass	Website	✓	Blocked	Lockout	Email	A
Avira-AP	Website	✗	✓	CAPTCHA	None	A+M
Avira-MP	Website	-	✓	Not Observed	None	M
NordPass-AP	Website	✗	✓	CAPTCHA + Rate Limit	None	M
NordPass-MP	Extension	-	✓	UI Reset	None	M
1Password	Website	✓	Compound	Not Observed	Compound	A
Bitwarden	Website	✗	✓	Not Observed	Email	A
Norton-AP	Website	✗	✓	CAPTCHA	None	M
Norton-MP	Extension	-	✓	Lockout	None	M
Kaspersky-AP	Website	✗	✓	CAPTCHA	None	A+M
Kaspersky-MP	Extension	-	✓	Lockout	None	M
Keeper	Website	✗	Blocked	-	Email	A
Dashlane	Extension	✗	Blocked	-	Email	M
MultiPassword	Website	✓	Compound	Not Observed	Compound	A
Proton Pass	Website	✗	✓	Not Observed	None	A
True Key	Extension	✓	✓	Not Observed	Email	M
RoboForm	Extension	✗	✓	Lockout	Email	M
DualSafe	Extension	✓	✓	Lockout	None	M
Zoho Vault-AP	Website	✓	✓	CAPTCHA	Email ^s	A+M
Zoho Vault-MP	Extension	-	✓	UI Reset	None	M

For remote attackers in our experiments:

- ❑ In 7 PMs, victim-controlled verification blocks vault access; while 3 PMs reveal credential validity.
- ❑ In 2 PMs, additional keys prevent us from isolating Mpw validity.

For the other six PMs:

- ❑ NordPass shows **rate limiting**; Norton, Kaspersky, DualSafe show **temporary lockouts**.
- ❑ For Avira, **CAPTCHA** is the only visible intervention we observe.
- ❑ Proton Pass shows no visible intervention within 15 attempts.

Implications: Defenses control feedback before stopping boundaries

Observed Behavior	Design implication
Same UI, different network fields	Review all attacker-visible feedback
Only a correct password reaches verification	Check what is disclosed before stopping boundaries
CAPTCHA or UI reset permits continuation	Measure continuation, not just defense presence
Lockout also blocks correct credentials	Evaluate legitimate-user access and recovery

Scope: measured versions and states; bounded online probes; no distributed guessing.

Thank you!

An Empirical Measurement Study of Authentication Mechanisms in Cloud-Based Password Managers

Yanduo Fu, Qingxuan Wang, Ding Wang, Nankai University

6 / 15

PMs reveal account
existence signal

15 / 20

Entry points reveal
credential validity signal

12 / 20

Entry points show a
visible intervention
