NDSS Symposium 2026

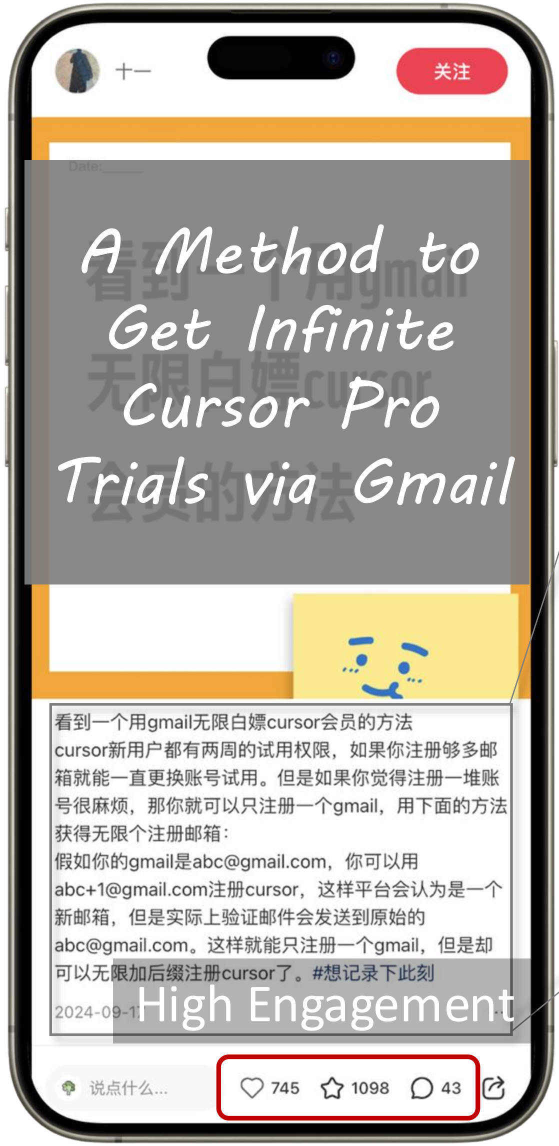
One Email, Many Faces: A Deep Dive into Identity Confusion in Email Aliases

Mengying Wu[†*], Geng Hong[†*], Jiatao Chen[†],
Mingxuan Liu[‡], Baojun Liu[‡], Min Yang[†]

[†]Fudan University, [‡]Tsinghua University

2026/02/26

From "Life Hacks" to Systematic Threats

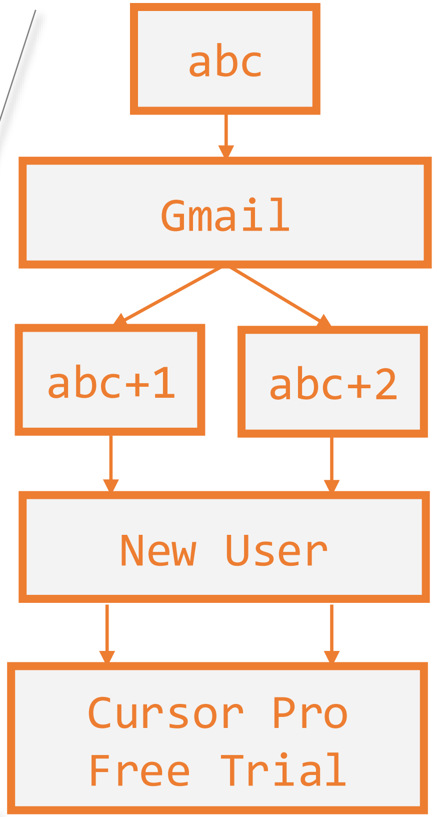


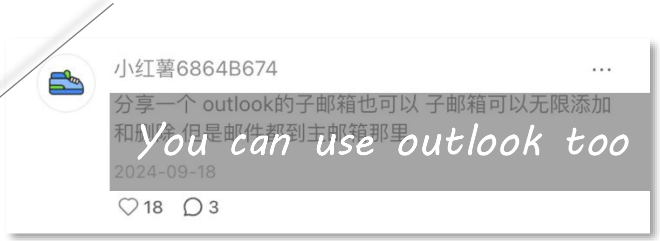
A Method to Get Infinite Cursor Pro Trials via Gmail

看到一个用gmail无限白嫖cursor会员的方法
cursor新用户都有两周的试用权限，如果你注册够多邮箱就能一直更换账号试用。但是如果你觉得注册一堆账号很麻烦，那你就可以只注册一个gmail，用下面的方法获得无限个注册邮箱：
假如你的gmail是abc@gmail.com，你可以用abc+1@gmail.com注册cursor，这样平台会认为是一个新邮箱，但是实际上验证邮件会发送到原始的abc@gmail.com。这样就能只注册一个gmail，但是却可以无限加后缀注册cursor了。#想记录下此刻

2024-09-1

High Engagement





小红薯6864B674

分享一个 outlook的子邮箱也可以 子邮箱可以无限添加和删除 但是邮件都到主邮箱那里

2024-09-18

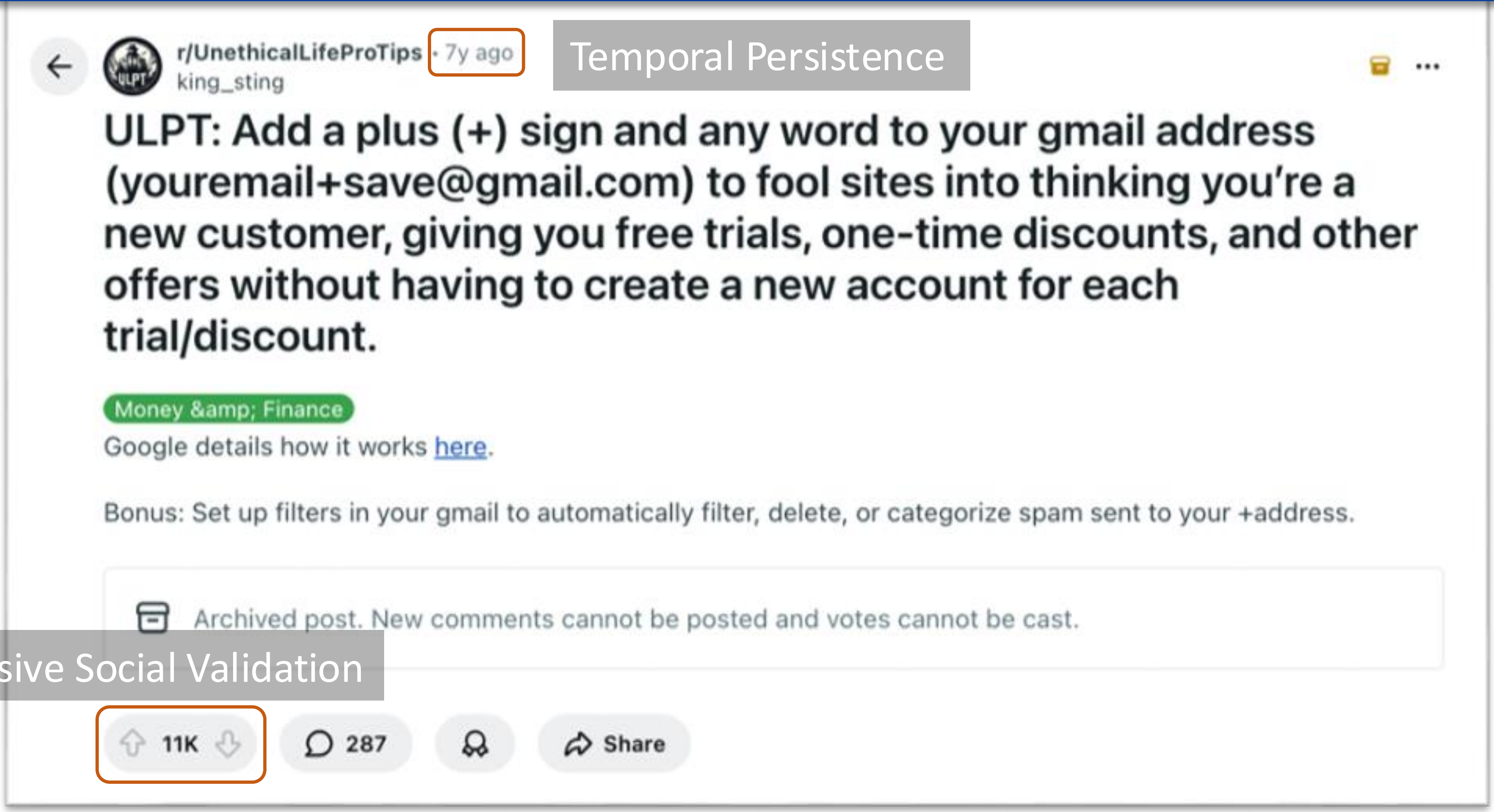
You can use outlook too

Key Observations:

- **Zero Barrier:** No technical skills required
- **Scalability:** One single Gmail account can generate N identities.
- **Persistence:** Users sharing cross-platform tricks

From "Life Hacks" to Systematic Threats

How to get infinite email address effortlessly?



r/UnethicalLifeProTips · 7y ago
king_sting

Temporal Persistence

ULPT: Add a plus (+) sign and any word to your gmail address (youremail+save@gmail.com) to fool sites into thinking you're a new customer, giving you free trials, one-time discounts, and other offers without having to create a new account for each trial/discount.

Money &amp; Finance

Google details how it works here.

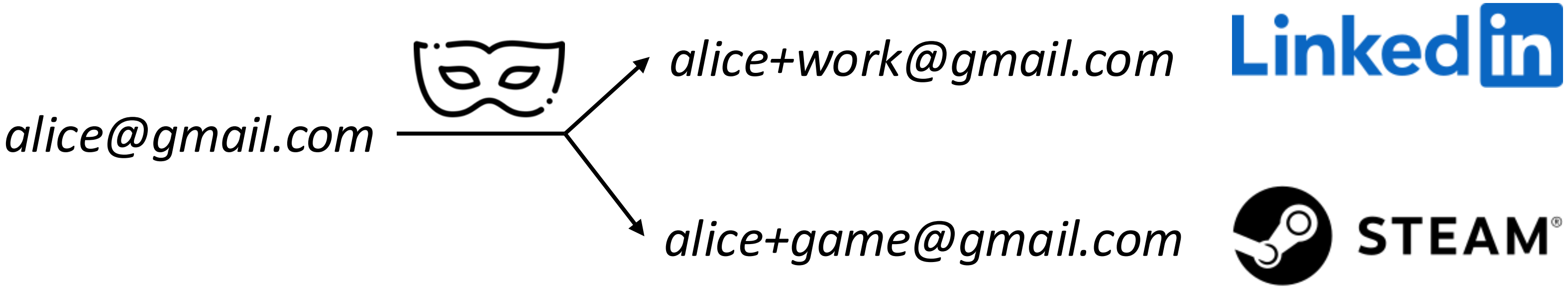
Bonus: Set up filters in your gmail to automatically filter, delete, or categorize spam sent to your +address.

Archived post. New comments cannot be posted and votes cannot be cast.

Massive Social Validation

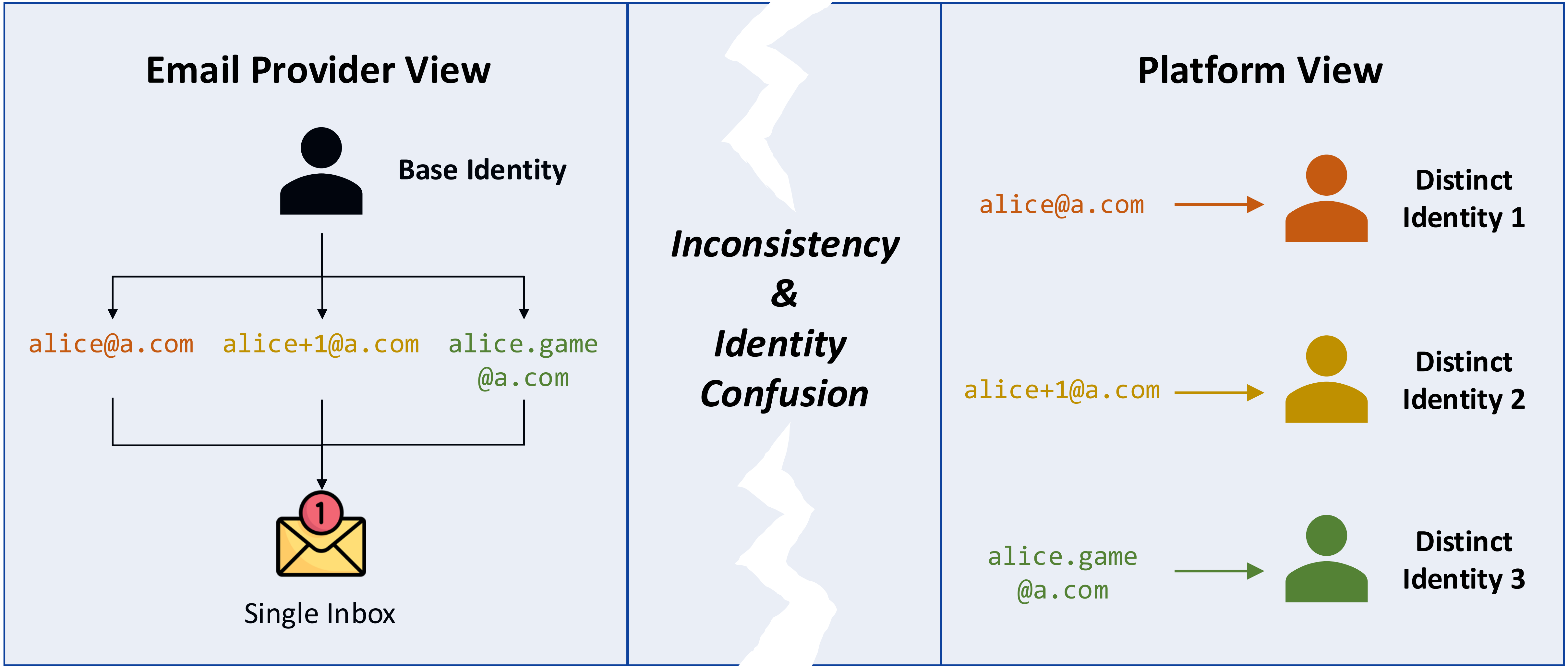
Email Alias

- Redirect the email sending to the alternative addresses to the same inbox as the primary email
- Help users leverage a single email account to separate different activities, such as work or gaming



One Email --->Many Faces, with no extra settings

The Identity Gap



Email Provider View

Base Identity

alice@a.com

alice+1@a.com

alice.game
@a.com

1

Single Inbox

Inconsistency
&
Identity
Confusion

Platform View

alice@a.com → Distinct Identity 1

alice+1@a.com → Distinct Identity 2

alice.game
@a.com → Distinct Identity 3

Our Work

The first systematic analysis of identity confusion caused by email aliasing mechanism inconsistency

01

How do email providers **document** their aliasing mechanisms?

How do these compare to the **actual** aliasing behaviors?

02

How do online **platforms** interpret and handle email aliases?

Do their practices **align with** those of email providers?

03

How can adversaries **abuse** email aliasing mechanisms in real-world **attacks**?

Identity in Email Providers

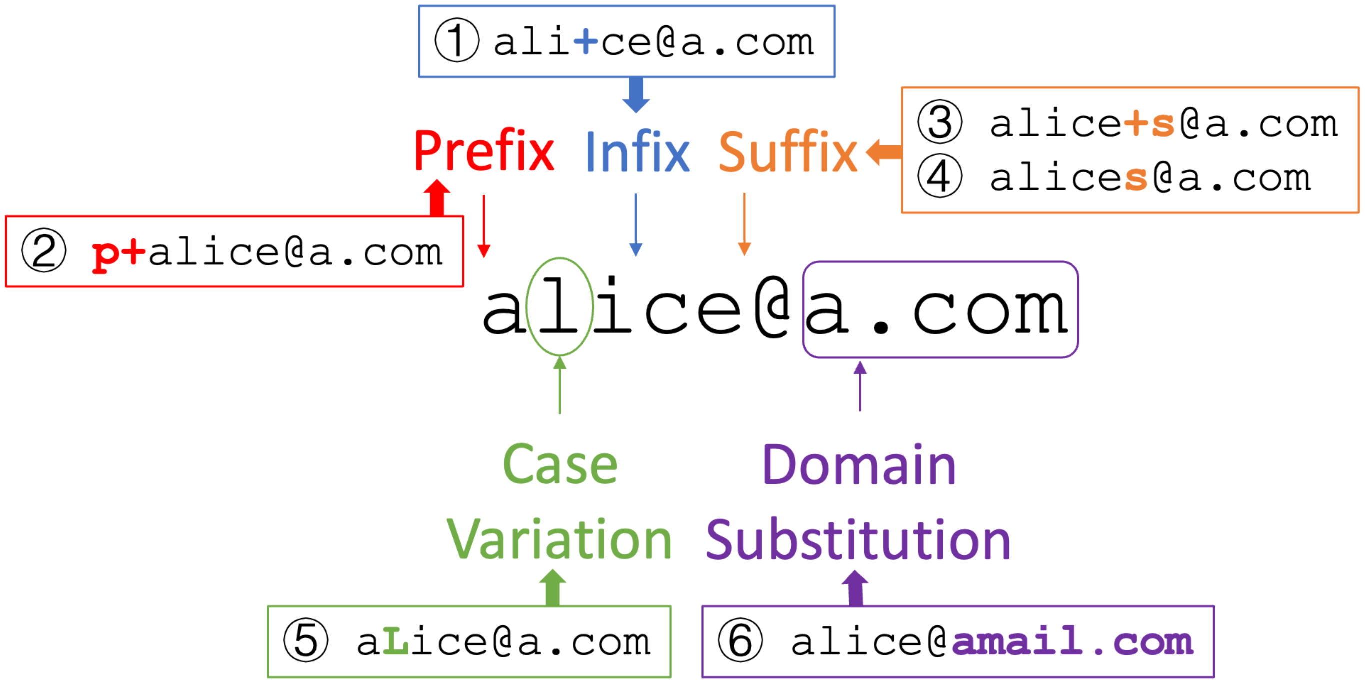
- Target 28 email providers
  - 12 have non-case alias
- Protocol-level inconsistency

SMTP: username **must be** case-sensitive

Alice@ ≠ alice@

All providers (28/28): case-insensitive

Alice@ = alice@



① ali+ce@a.com

② p+alice@a.com

③ alice+s@a.com

④ alices@a.com

Prefix Infix Suffix

alice@a.com

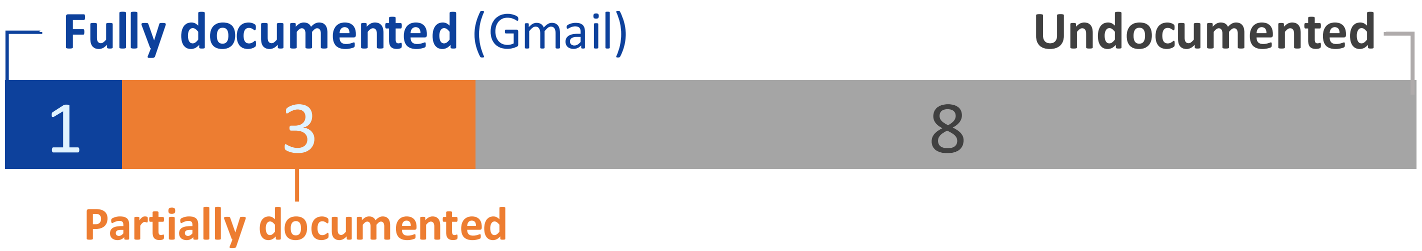
Case Variation

Domain Substitution

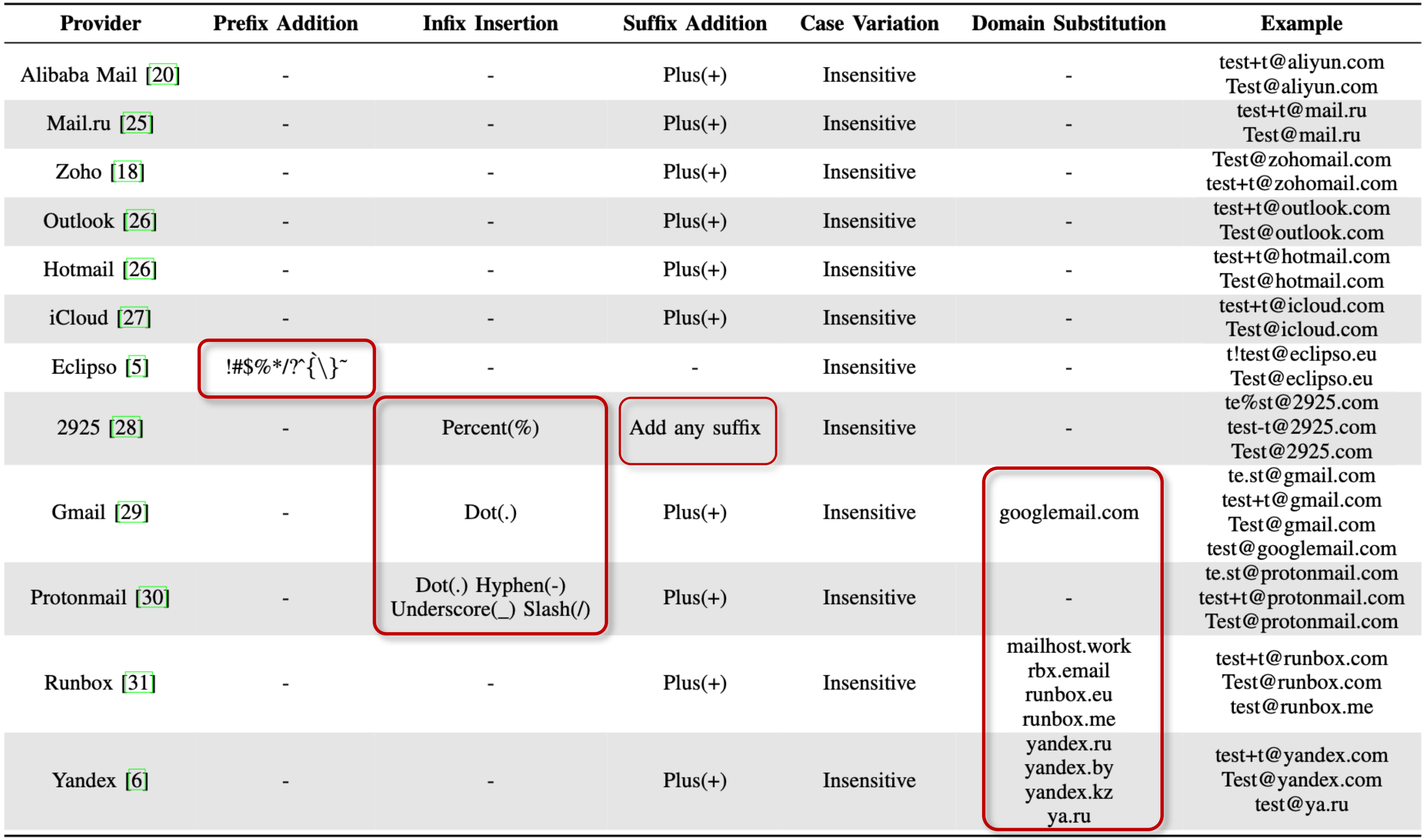
⑤ aLice@a.com

⑥ alice@amail.com

- Documents lack transparency



Alias Implementation of Email Providers



Provider	Prefix Addition	Infix Insertion	Suffix Addition	Case Variation	Domain Substitution	Example
Alibaba Mail [20]	-	-	Plus(+)	Insensitive	-	test+t@aliyun.com Test@aliyun.com
Mail.ru [25]	-	-	Plus(+)	Insensitive	-	test+t@mail.ru Test@mail.ru
Zoho [18]	-	-	Plus(+)	Insensitive	-	Test@zohomail.com test+t@zohomail.com
Outlook [26]	-	-	Plus(+)	Insensitive	-	test+t@outlook.com Test@outlook.com
Hotmail [26]	-	-	Plus(+)	Insensitive	-	test+t@hotmail.com Test@hotmail.com
iCloud [27]	-	-	Plus(+)	Insensitive	-	test+t@icloud.com Test@icloud.com
Eclipso [5]	!#$%*/?^{`\}~	-	-	Insensitive	-	t!test@eclipso.eu Test@eclipso.eu
2925 [28]	-	Percent(%)	Add any suffix	Insensitive	-	te%st@2925.com test-t@2925.com Test@2925.com
Gmail [29]	-	Dot(.)	Plus(+)	Insensitive	googlemail.com	te.st@gmail.com test+t@gmail.com Test@gmail.com test@googlemail.com

Protonmail [30]	-	Dot(.) Hyphen(-)
		Underscore(_) Slash(/)
			Plus(+)	Insensitive	-	te.st@protonmail.com
						test+t@protonmail.com
						Test@protonmail.com

Runbox [31]	-	-	Plus(+)	Insensitive	mailhost.work rbx.email runbox.eu runbox.me	test+t@runbox.com Test@runbox.com test@runbox.me
Yandex [6]	-	-	Plus(+)	Insensitive	yandex.ru yandex.by yandex.kz ya.ru	test+t@yandex.com Test@yandex.com test@ya.ru

Unique alias making users hard to consistently normalize alias

Email as Identity in Platforms

- Target 18 platforms in top 100 domain which allows email registration
- Test registering with variant emails when base email has been registered

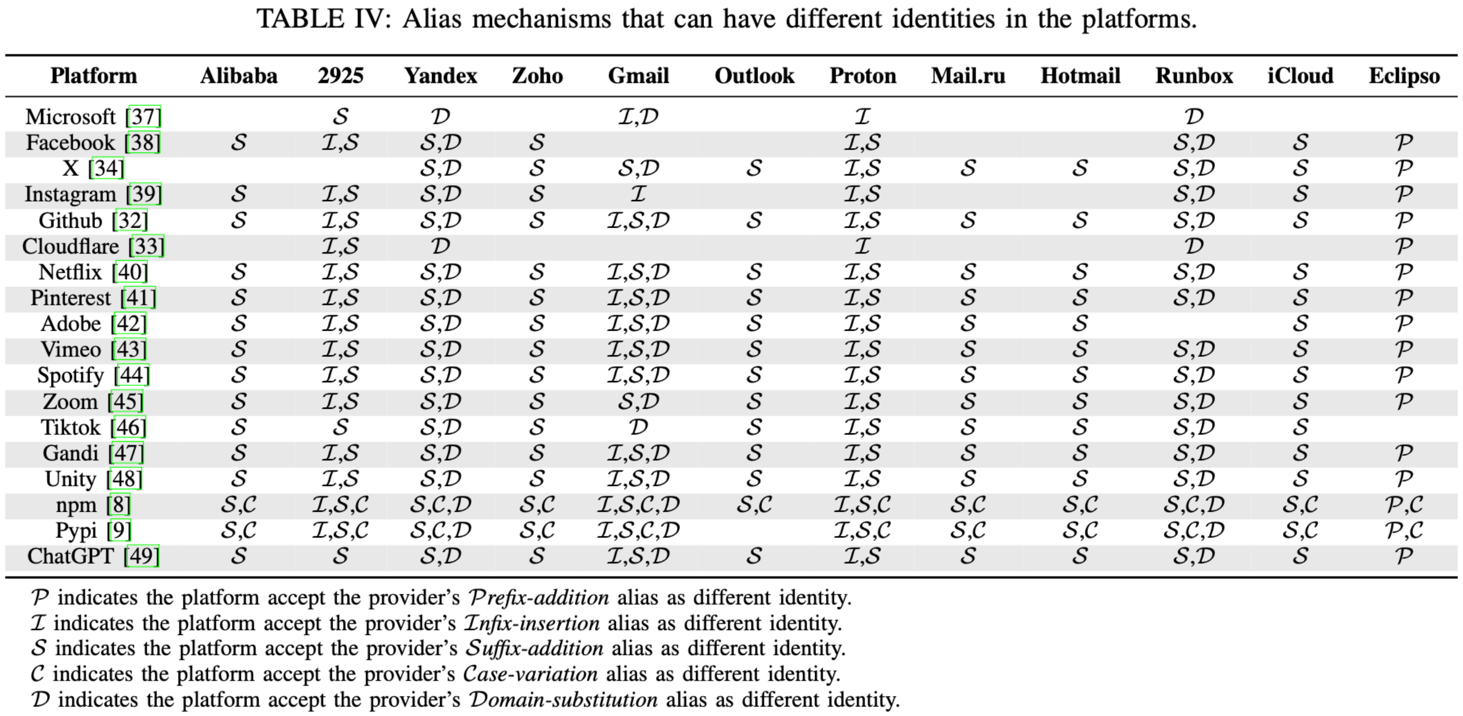


TABLE IV: Alias mechanisms that can have different identities in the platforms.

Platform	Alibaba	2925	Yandex	Zoho	Gmail	Outlook	Proton	Mail.ru	Hotmail	Runbox	iCloud	Eclipso
Microsoft [37]		$\mathcal{S}$	$\mathcal{D}$		$\mathcal{I}$,$\mathcal{D}$		$\mathcal{I}$			$\mathcal{D}$		
Facebook [38]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$			$\mathcal{I}$,$\mathcal{S}$			$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
X [34]			$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Instagram [39]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$		$\mathcal{I}$,$\mathcal{S}$			$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Github [32]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Cloudflare [33]		$\mathcal{I}$,$\mathcal{S}$	$\mathcal{D}$				$\mathcal{I}$			$\mathcal{D}$		$\mathcal{P}$
Netflix [40]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Pinterest [41]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Adobe [42]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$		$\mathcal{S}$	$\mathcal{P}$
Vimeo [43]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Spotify [44]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Zoom [45]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Tiktok [46]	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	
Gandi [47]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
Unity [48]	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$
npm [8]	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{C}$	$\mathcal{S}$,$\mathcal{C}$,$\mathcal{D}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{C}$,$\mathcal{D}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{C}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{S}$,$\mathcal{C}$,$\mathcal{D}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{P}$,$\mathcal{C}$
Pypi [9]	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{C}$	$\mathcal{S}$,$\mathcal{C}$,$\mathcal{D}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{C}$,$\mathcal{D}$		$\mathcal{I}$,$\mathcal{S}$,$\mathcal{C}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{S}$,$\mathcal{C}$,$\mathcal{D}$	$\mathcal{S}$,$\mathcal{C}$	$\mathcal{P}$,$\mathcal{C}$
ChatGPT [49]	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{I}$,$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$	$\mathcal{S}$,$\mathcal{D}$	$\mathcal{S}$	$\mathcal{P}$

$\mathcal{P}$ indicates the platform accept the provider's *Prefix-addition* alias as different identity.
$\mathcal{I}$ indicates the platform accept the provider's *Infix-insertion* alias as different identity.
$\mathcal{S}$ indicates the platform accept the provider's *Suffix-addition* alias as different identity.
$\mathcal{C}$ indicates the platform accept the provider's *Case-variation* alias as different identity.
$\mathcal{D}$ indicates the platform accept the provider's *Domain-substitution* alias as different identity.

No platform fully defends against aliasing rules across all 12 providers

Alias Defense Strategies of Platforms

Explicit Alias Detection

- Provider-specific alias check
  - 5 platforms can identify alias of 4 providers, but only plus-suffix
- Provider-independent Alias Check
  - Cloudflare reject **all** plus-suffix
  - npm and PyPI are case-sensitive for both local-part and domain

Alice@example.com

≠ = ≠

alice@example.com

≠ = =

alice@EXAMPLE.com

npm PyPI | Others | SMTP

Implicit Character Defense

- Symbol Sanitizer
  - Three platforms have strict restrictions
  - Microsoft only allows hyphen (-), dot (.), and underscore (_) in email usernames
- Domain-level Restrictions
  - Adobe explicitly blocks runbox.com, reporting “This email address is not allowed.”
  - Vimeo rejects both sina.com and qq.com

Alias Multiplicity Abuse in the Wild

Threat Scenarios

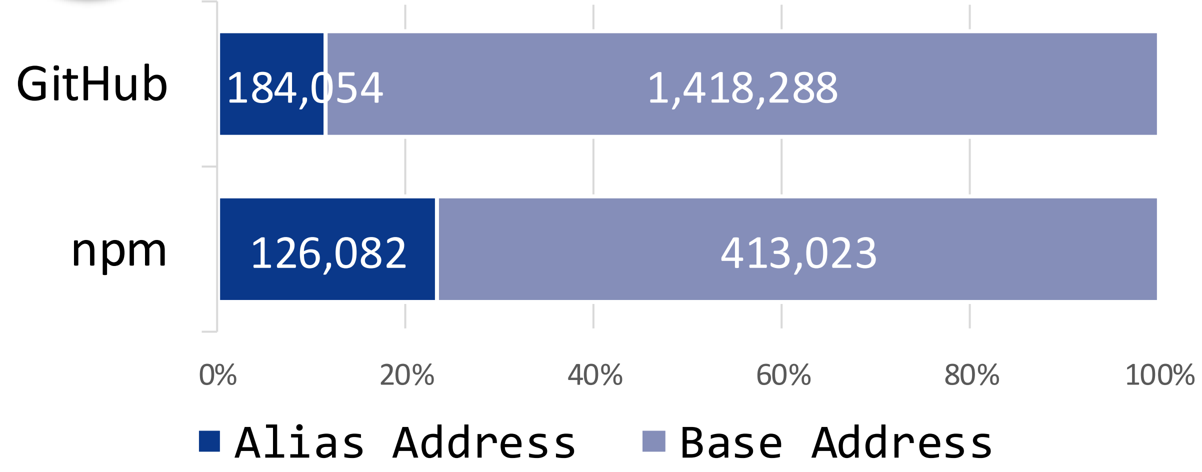
Free trial abuse

Bypassing resource limits

Fake accounts for social manipulation

Real-world Usage

1,007 Base addresses in npm have multiple accounts



umekiyanai@gmail.com

↓

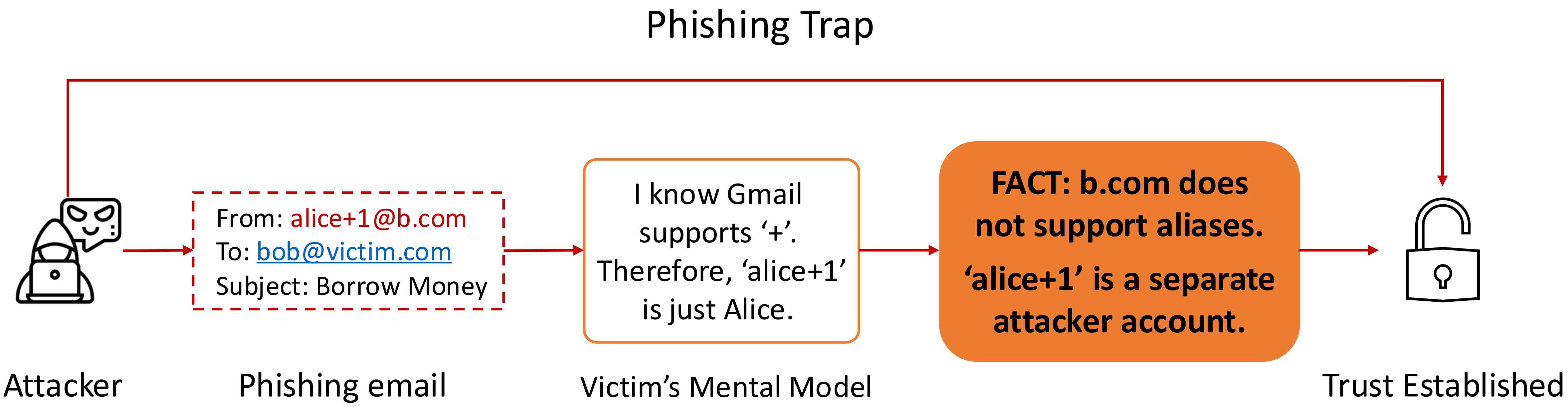
139 Alias accounts

Email Address	Username
j.ulayera@gmail.com	bujalsokao
ju.layera@gmail.com	nuilaopmei
jul.ayera@gmail.com	nualosomuina
jula.yera@gmail.com	ikapikangsua
julay.era@gmail.com	nikakulpaliindi
julaye.ra@gmail.com	limaospoiukas
julayer.a@gmail.com	ukarilaopsiwa

RepSEO[1] Campaigns in npm

[1] Wu et al., Exposing the Hidden Layer: Software Repositories in the Service of Seo Manipulation, ICSE’25

Alias Misidentification Attack



Phishing Trap

From: alice+1@b.com
To: bob@victim.com
Subject: Borrow Money

I know Gmail supports '+'. Therefore, 'alice+1' is just Alice.

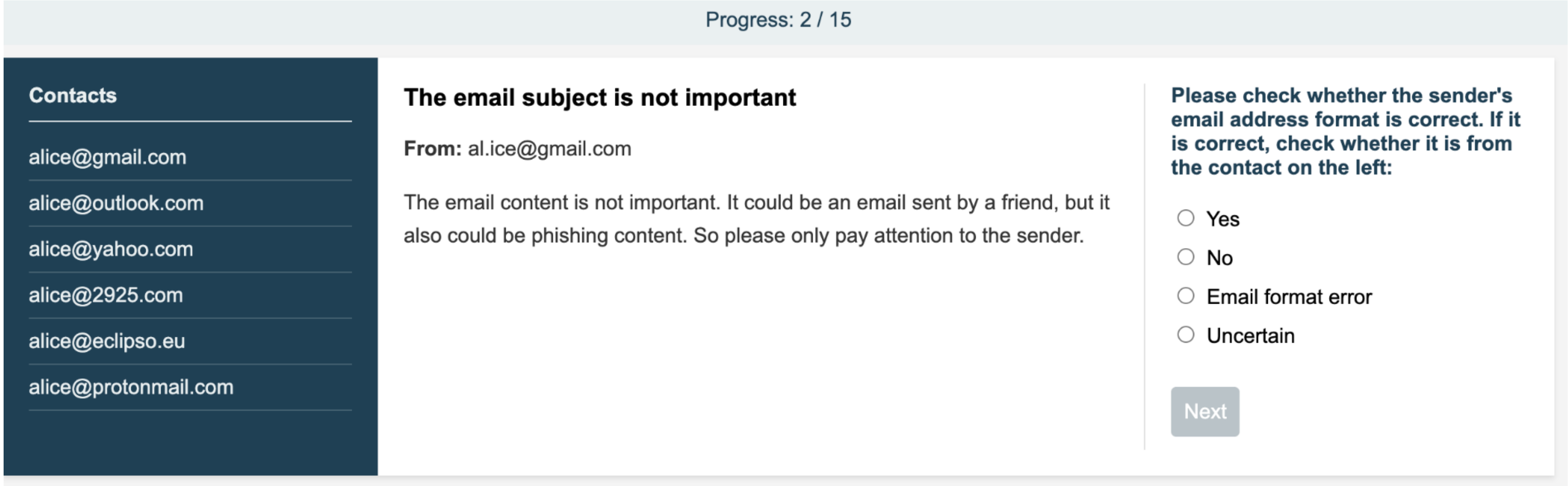
FACT: b.com does not support aliases.

'alice+1' is a separate attacker account.

The vulnerability lies in the user's assumption of universal rules.

Alias Misidentification Attack

- User Study ! (N=304)
  - To evaluate users’ understanding of email aliases
  - Sender may be friend’s alias, or non-alias phishing email address (but seems like)
  - Participants were asked to determine whether the sender was a known contact



Progress: 2 / 15

Contacts

- alice@gmail.com
- alice@outlook.com
- alice@yahoo.com
- alice@2925.com
- alice@eclipso.eu
- alice@protonmail.com

The email subject is not important

From: al.ice@gmail.com

The email content is not important. It could be an email sent by a friend, but it also could be phishing content. So please only pay attention to the sender.

Please check whether the sender's email address format is correct. If it is correct, check whether it is from the contact on the left:

○ Yes
○ No
○ Email format error
○ Uncertain

Quiz Time

Is this Alice’s address?

alice+friend@outlook.com

ali.ce@outlook.com

al-ice@protonmail.com

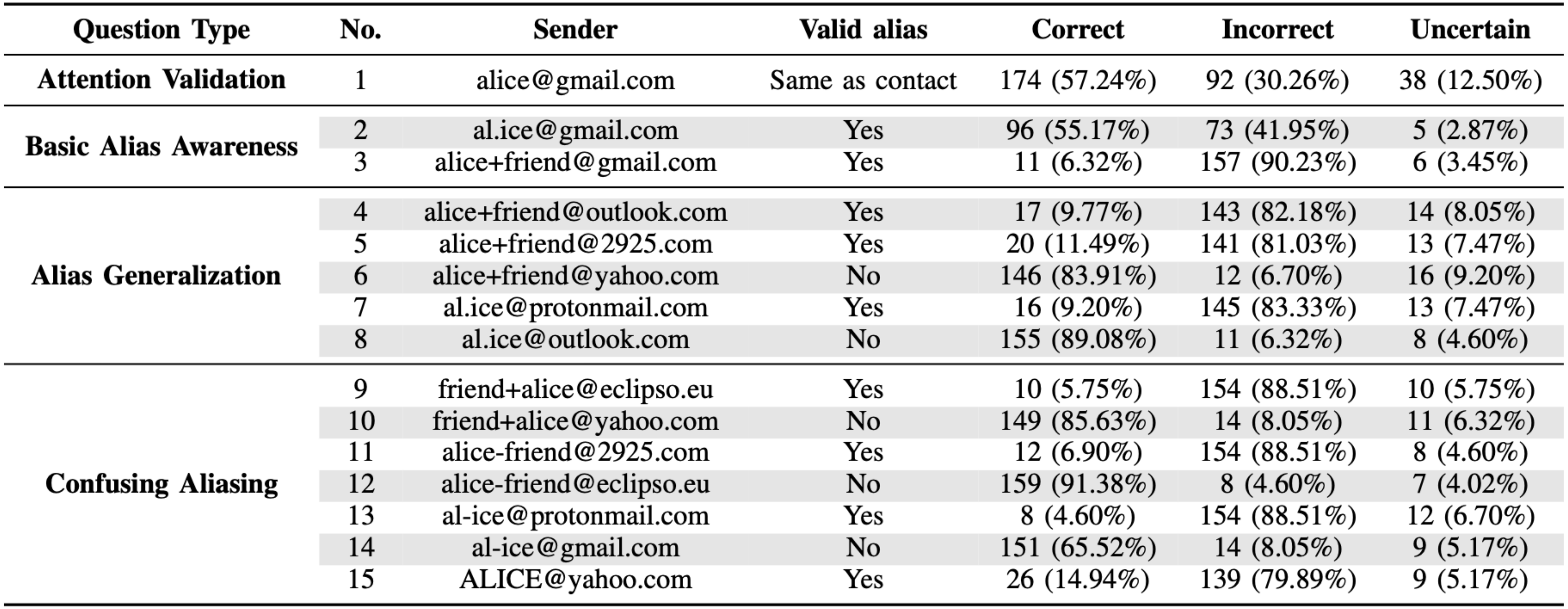
Quiz Time

Is this Alice’s address?

`alice+friend@outlook.com`	✅
`ali.ce@outlook.com`	❌
`al-ice@protonmail.com`	✅

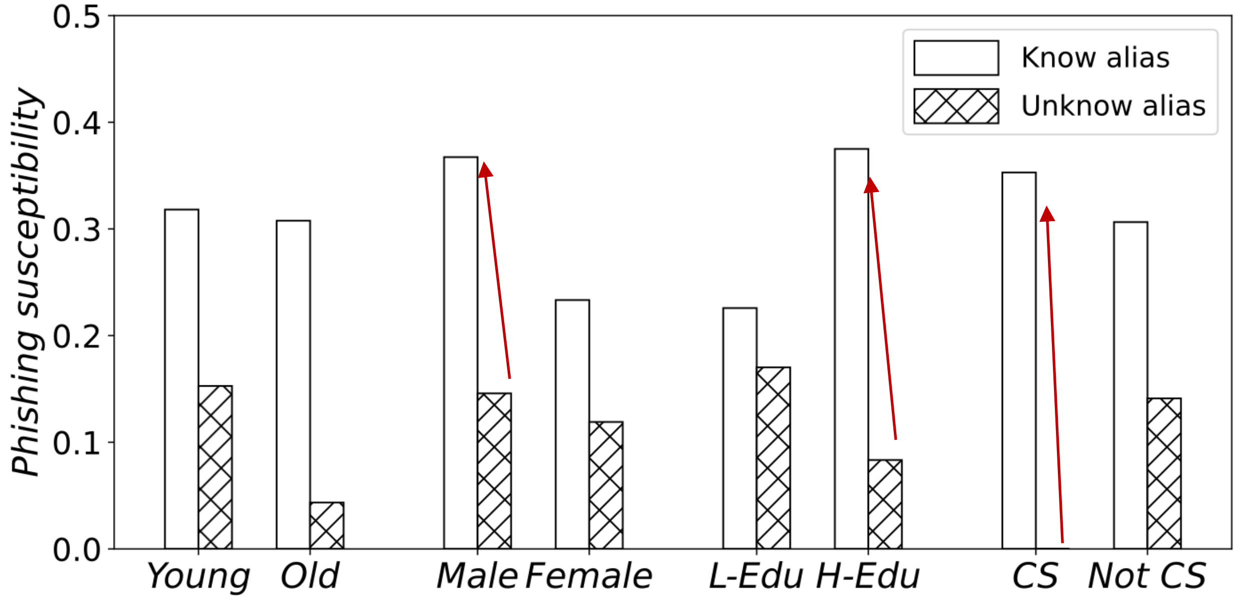
User Study Result

- 29.89% users have little familiarity with alias mechanisms
- Unexpected Hyper-vigilance: 42.76% failed to pass attention validation
  - Defaulted to distrust, prioritizing "safe" rejection over accuracy



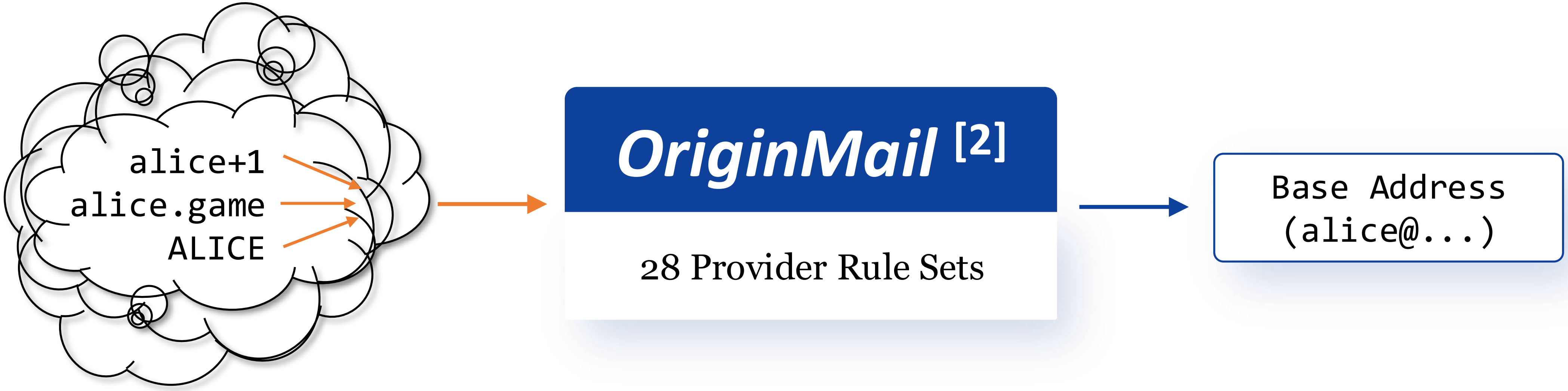
Question Type	No.	Sender	Valid alias	Correct	Incorrect	Uncertain
Attention Validation	1	alice@gmail.com	Same as contact	174 (57.24%)	92 (30.26%)	38 (12.50%)
Basic Alias Awareness	2	al.ice@gmail.com	Yes	96 (55.17%)	73 (41.95%)	5 (2.87%)
	3	alice+friend@gmail.com	Yes	11 (6.32%)	157 (90.23%)	6 (3.45%)
Alias Generalization	4	alice+friend@outlook.com	Yes	17 (9.77%)	143 (82.18%)	14 (8.05%)
	5	alice+friend@2925.com	Yes	20 (11.49%)	141 (81.03%)	13 (7.47%)
	6	alice+friend@yahoo.com	No	146 (83.91%)	12 (6.70%)	16 (9.20%)
	7	al.ice@protonmail.com	Yes	16 (9.20%)	145 (83.33%)	13 (7.47%)
	8	al.ice@outlook.com	No	155 (89.08%)	11 (6.32%)	8 (4.60%)
Confusing Aliasing	9	friend+alice@eclipso.eu	Yes	10 (5.75%)	154 (88.51%)	10 (5.75%)
	10	friend+alice@yahoo.com	No	149 (85.63%)	14 (8.05%)	11 (6.32%)
	11	alice-friend@2925.com	Yes	12 (6.90%)	154 (88.51%)	8 (4.60%)
	12	alice-friend@eclipso.eu	No	159 (91.38%)	8 (4.60%)	7 (4.02%)
	13	al-ice@protonmail.com	Yes	8 (4.60%)	154 (88.51%)	12 (6.70%)
	14	al-ice@gmail.com	No	151 (65.52%)	14 (8.05%)	9 (5.17%)
	15	ALICE@yahoo.com	Yes	26 (14.94%)	139 (79.89%)	9 (5.17%)

The Expert Paradox: Knowledge Increases Susceptibility



- Users who **believe** they understand email aliasing are **more** susceptible to being phished
  - Especially those highly educated, male, and technical participants
  - Overall susceptibility rate rising to **31.65%**
  - **CS student: 0% -> 35.29%!!!**

Closing the Gap: *OriginMail*



Recommendations

Providers:

Increase collaboration.

Standardize aliasing rules.

Document hidden rules.

Platforms:

Normalize before registration.

Sync client-server validation.

Alert base email on alias use.

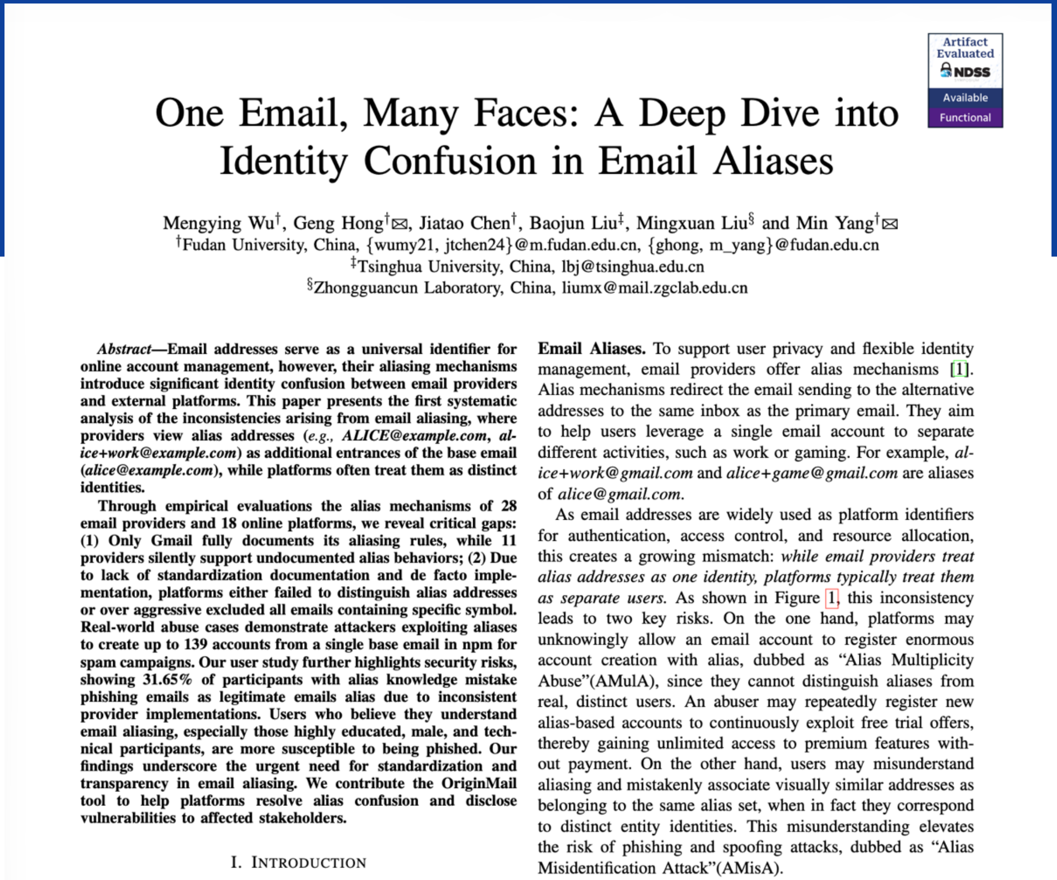
[2] https://doi.org/10.5281/zenodo.16735091.

復旦大學 FUDAN UNIVERSITY

清華大學

Thank you for your Audience!

For more details, welcome to follow our paper.



Artifact Evaluated NDSS
Available
Functional

One Email, Many Faces: A Deep Dive into Identity Confusion in Email Aliases

Mengying Wu†, Geng Hong†✉, Jiatao Chen†, Baojun Liu‡, Mingxuan Liu§ and Min Yang†✉
†Fudan University, China, {wumy21, jtchen24}@m.fudan.edu.cn, {ghong, m_yang}@fudan.edu.cn
‡Tsinghua University, China, lbj@tsinghua.edu.cn
§Zhongguancun Laboratory, China, liumx@mail.zgclab.edu.cn

***Abstract*—Email addresses serve as a universal identifier for online account management, however, their aliasing mechanisms introduce significant identity confusion between email providers and external platforms. This paper presents the first systematic analysis of the inconsistencies arising from email aliasing, where providers view alias addresses (*e.g., ALICE@example.com, alice+work@example.com*) as additional entrances of the base email (*alice@example.com*), while platforms often treat them as distinct identities.**

Through empirical evaluations the alias mechanisms of 28 email providers and 18 online platforms, we reveal critical gaps: (1) Only Gmail fully documents its aliasing rules, while 11 providers silently support undocumented alias behaviors; (2) Due to lack of standardization documentation and de facto implementation, platforms either failed to distinguish alias addresses or over aggressive excluded all emails containing specific symbol. Real-world abuse cases demonstrate attackers exploiting aliases to create up to 139 accounts from a single base email in npm for spam campaigns. Our user study further highlights security risks, showing 31.65% of participants with alias knowledge mistake phishing emails as legitimate emails alias due to inconsistent provider implementations. Users who believe they understand email aliasing, especially those highly educated, male, and technical participants, are more susceptible to being phished. Our findings underscore the urgent need for standardization and transparency in email aliasing. We contribute the OriginMail tool to help platforms resolve alias confusion and disclose vulnerabilities to affected stakeholders.

I. Introduction

Email Aliases. To support user privacy and flexible identity management, email providers offer alias mechanisms [1]. Alias mechanisms redirect the email sending to the alternative addresses to the same inbox as the primary email. They aim to help users leverage a single email account to separate different activities, such as work or gaming. For example, *alice+work@gmail.com* and *alice+game@gmail.com* are aliases of *alice@gmail.com*.

As email addresses are widely used as platform identifiers for authentication, access control, and resource allocation, this creates a growing mismatch: *while email providers treat alias addresses as one identity, platforms typically treat them as separate users.* As shown in Figure 1, this inconsistency leads to two key risks. On the one hand, platforms may unknowingly allow an email account to register enormous account creation with alias, dubbed as “Alias Multiplicity Abuse”(AMulA), since they cannot distinguish aliases from real, distinct users. An abuser may repeatedly register new alias-based accounts to continuously exploit free trial offers, thereby gaining unlimited access to premium features without payment. On the other hand, users may misunderstand aliasing and mistakenly associate visually similar addresses as belonging to the same alias set, when in fact they correspond to distinct entity identities. This misunderstanding elevates the risk of phishing and spoofing attacks, dubbed as “Alias Misidentification Attack”(AMisA).