VIRGINIA TECH

End-to-End Measurements of Email Spoofing Attacks

Hang Hu, Gang Wang

hanghu@vt.edu

Computer Science, Virginia Tech

Spear Phishing is a Big Threat

- Spear phishing: targeted phishing attack, often involves impersonation
- 91% of targeted attacks involve spear phishing[1]
- 95% of state-affiliated espionage attacks are traced to phishing[2]

1. Enterprise Phishing Susceptibility and Resiliency Report, PhishMe, 2016
2. 2013 Data Beach Investigation Report, Verizon, 2013

Real-life Spear Phishing Examples

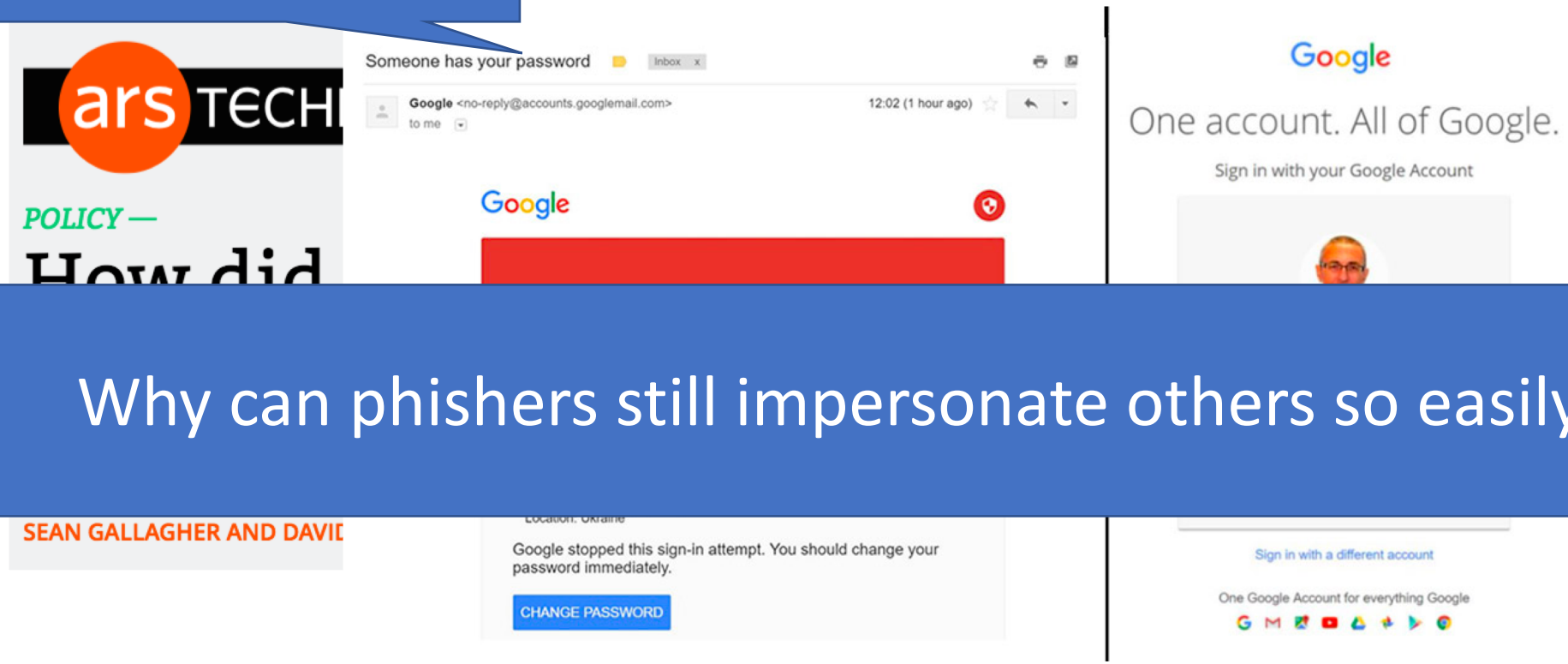
Yahoo Data Breach in 2014

John Podesta's Gmail Account

500 Million Yahoo Users Affected

Hillary Clinton 2016 Campaign Chairman

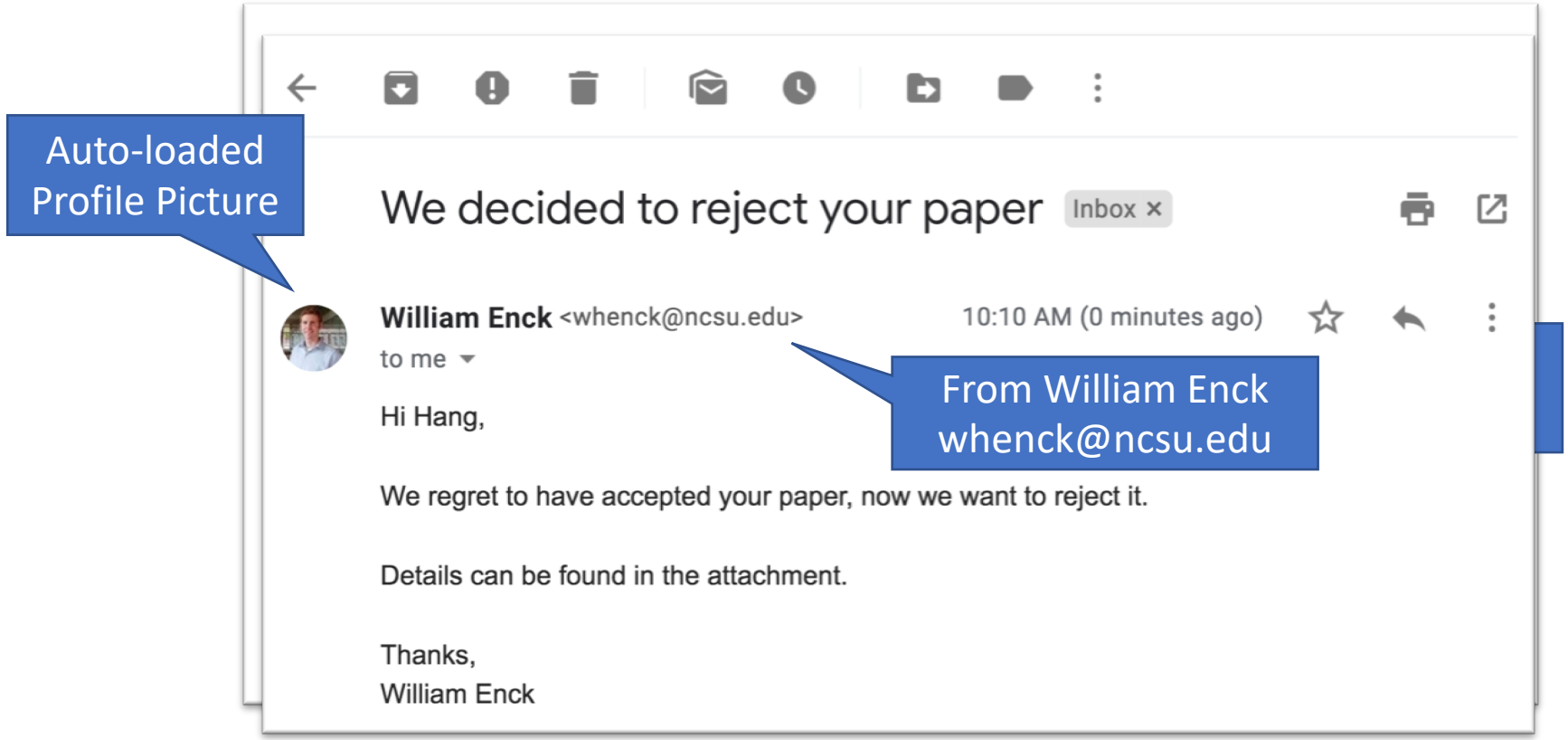
From Google
[accounts.googlemail.com]



Why can phishers still impersonate others so easily?

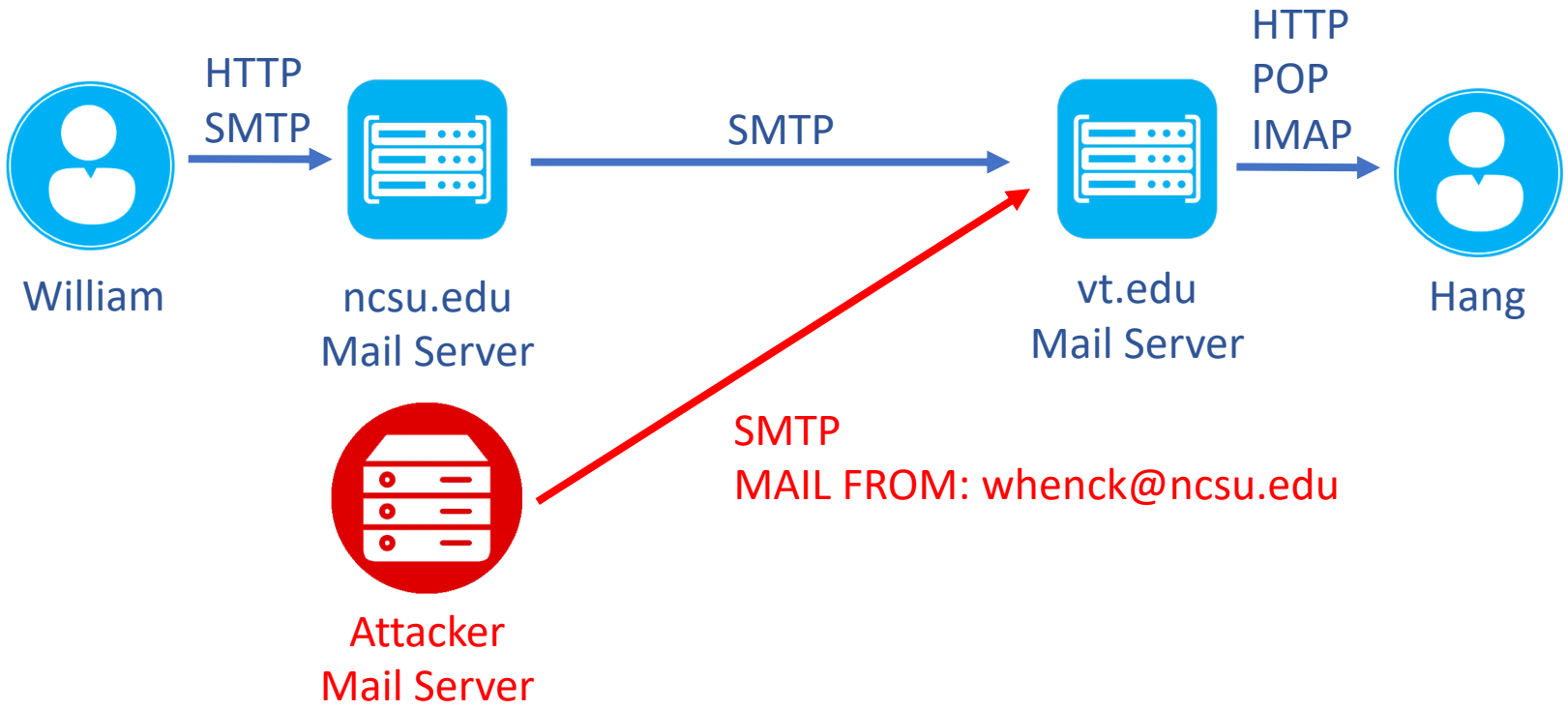
I Performed a Spear Phishing Test

- I impersonated USENIX Security co-chairs to send spoofing emails to my account (hanghu@vt.edu)



Background: SMTP & Spoofing

- Simple Mail Transfer Protocol (SMTP) defined in 1982
- SMTP has no built-in authentication mechanism
- Spoof anyone by modifying MAIL FROM field of SMTP



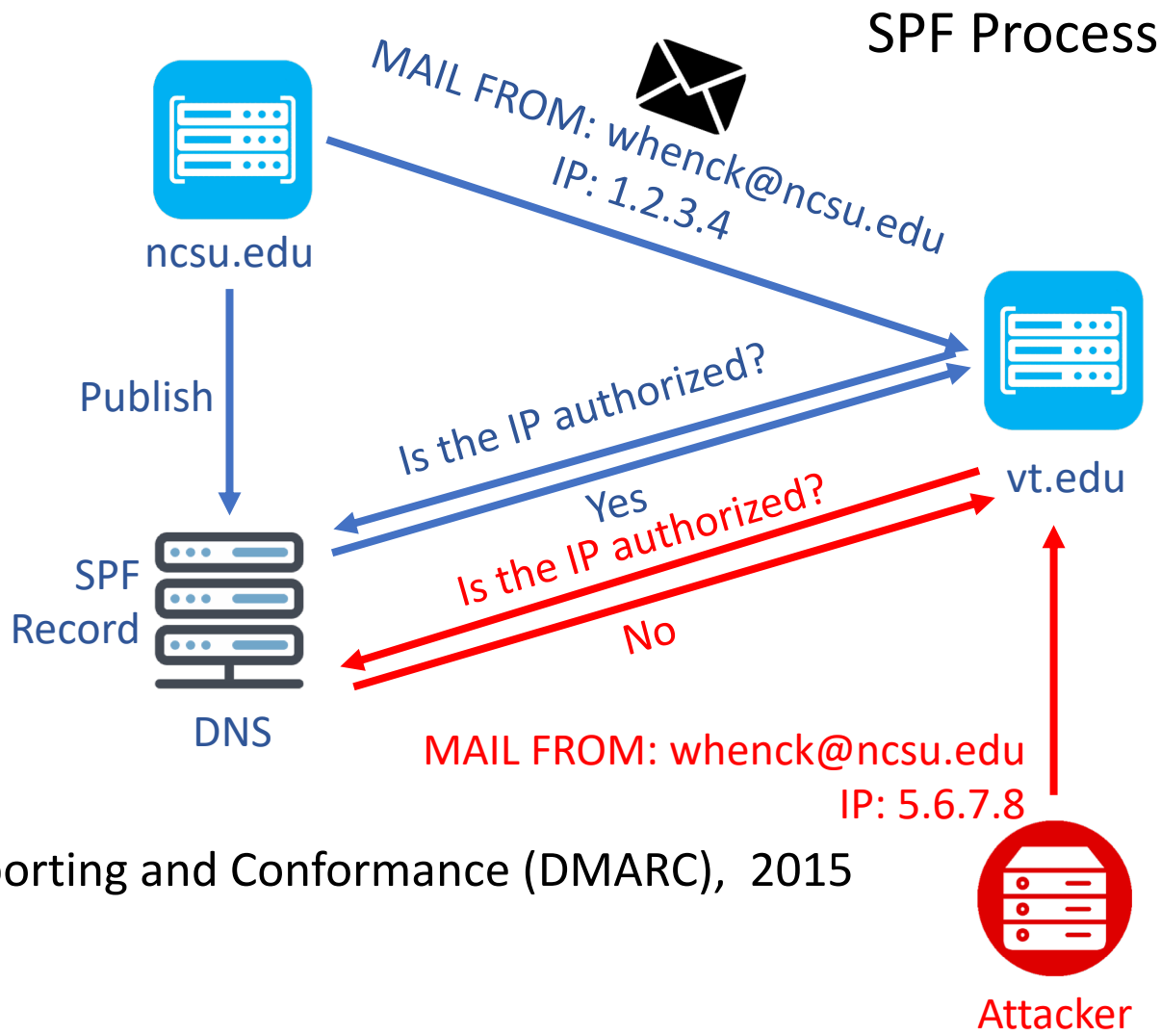
Existing Anti-spoofing Protocols

SMTP, 1982

Sender Policy Framework (SPF), 2002
- IP based authentication

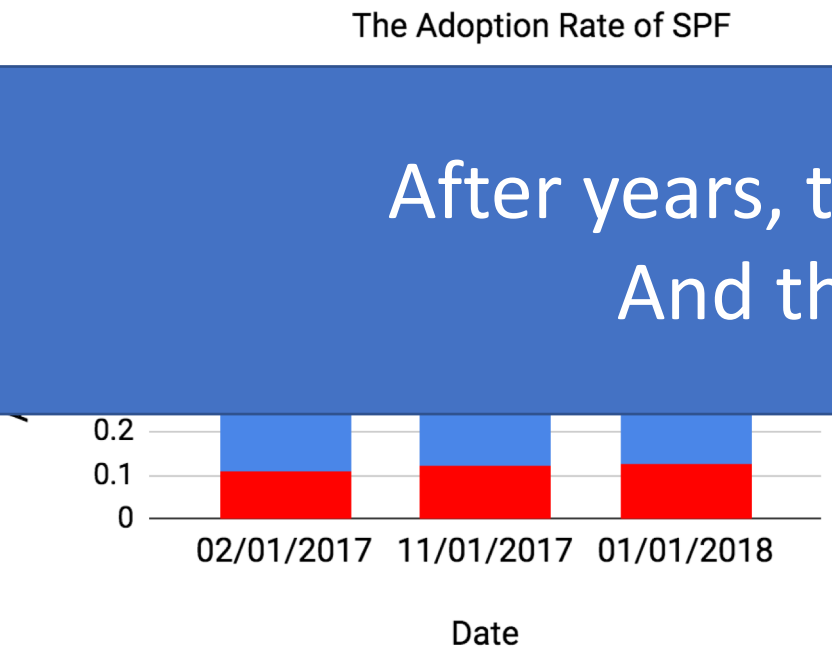
DomainKeys Identified Mail (DKIM), 2004
- Public key based authentication

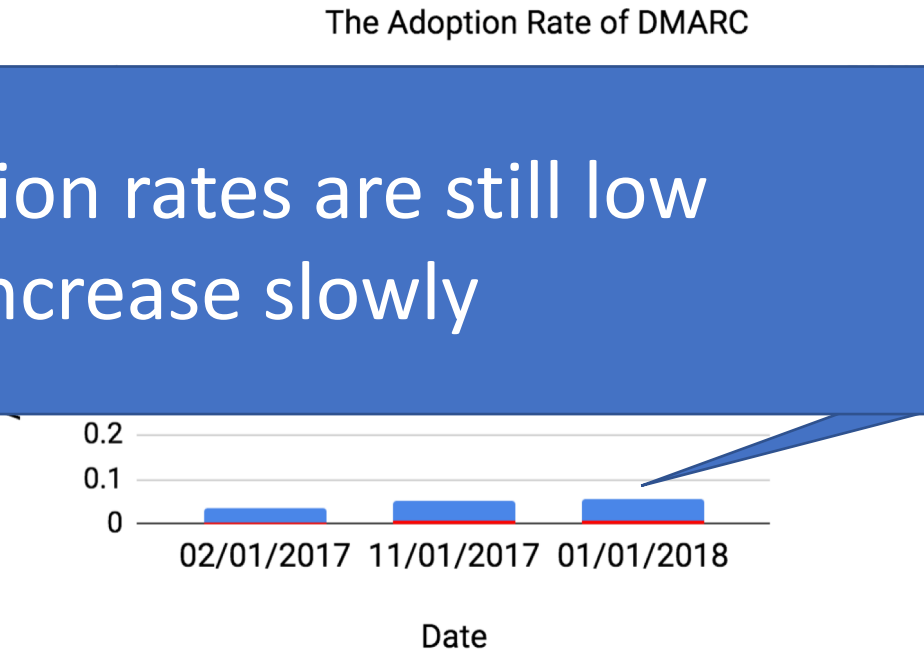
Domain-based Message Authentication, Reporting and Conformance (DMARC), 2015
- Based on SPF and DKIM
- Publish policy



How Widely are Anti-spoofing Protocols Used?

- Scanned SPF and DMARC records of Alexa top 1 million domains
- When an email fails SPF/DMARC:
  - Relaxed: No recommending policy
  - Strict: Rejecting failed emails





After years, the adoption rates are still low
And they also increase slowly

This Study

- Research questions
  - How do email providers detect and handle spoofing emails?
  - Under what conditions can spoofing emails penetrate the defense
  - Once spoofing emails get in, how do email providers warn users?

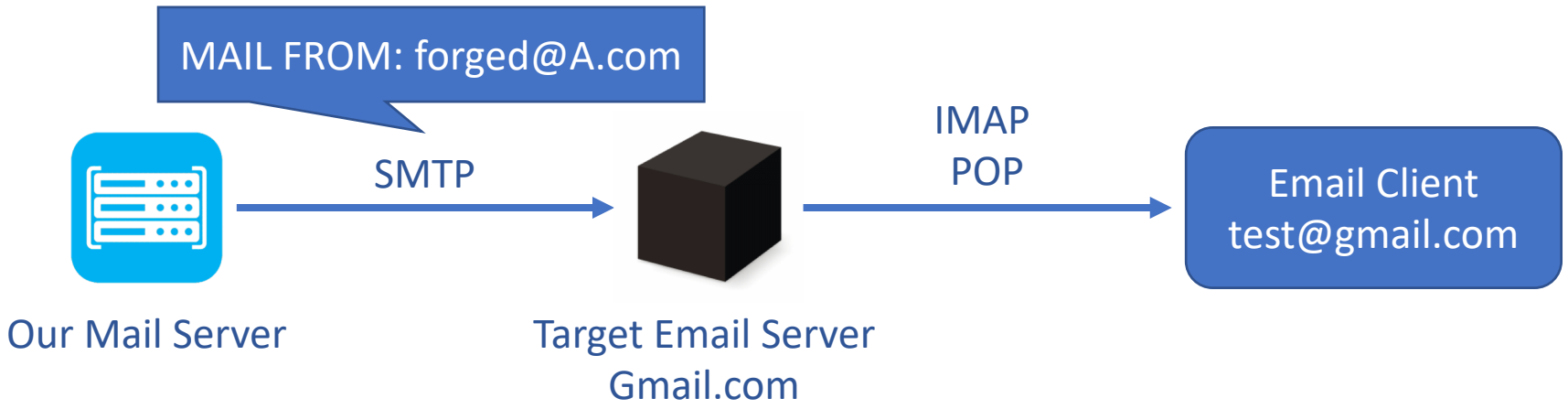
- Measurement + user study
  - 35 popular email providers' reaction to spoofing emails
  - A user study (N=488) to examine users' reaction to warnings

Outline

- ~~Introduction~~
- End-to-end Spoofing Experiments
- User Study

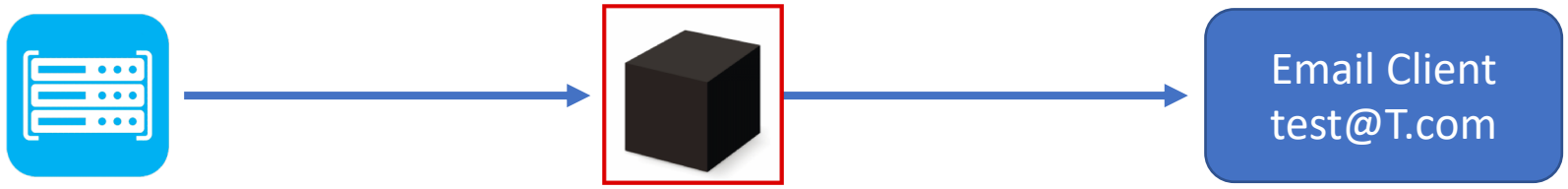
End-to-end Spoofing Experiments

- Goal: Understand how email providers handle spoofing emails
- Method:
  - Black-box testing
  - Control input and observe output
- Register our own accounts as email receivers
- Change input email



Target Email Providers

- 35 Email providers



Our Mail Server

Target Email Server

Full Authentication Check (16)

Gmail, Inbox by Gmail, YAHOO!, iCloud, Hotmail | Outlook, Aol., @mail.ru, NAVER, 網易 NETEASE www.163.com, 126 网易免费邮, yeah.net 网易免费邮, inbox.lv, Tutanota, ProtonMail, FastMail, SEZNAM.CZ

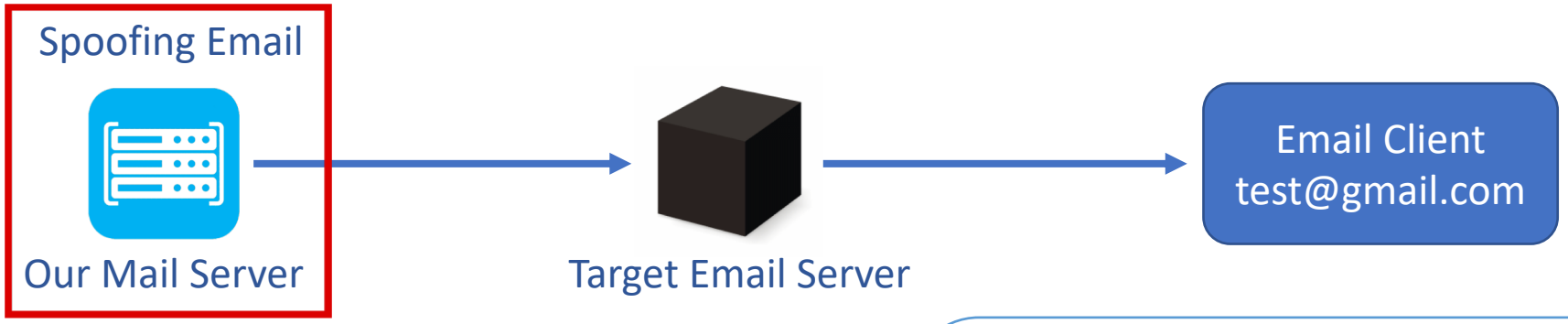
Partial Authentication (15)

ZOHO, mail.com, JUNO, mynet, GMX, POCZTA, DaUm, Mail QQ邮箱 mail.qq.com, interia, WP.PL, SAPO, runbox professional email services, sina 新浪网, 搜狐 SOHU.com, onet

No Authentication (4)

rediff, T Online, [freemail], excite

Controlled Parameters for Spoofing Emails



Spoofed Sender x 30

SPF/DKIM, strict policy (x10)

SPF/DKIM, relaxed policy (x10)

No SPF/DKIM/DMARC (x10)

facebook

ebay

The Pirate Bay

Content x 5

Phishing, Benign

Blank, Blank w/ URL, Blank w/ attachment

IP x 2

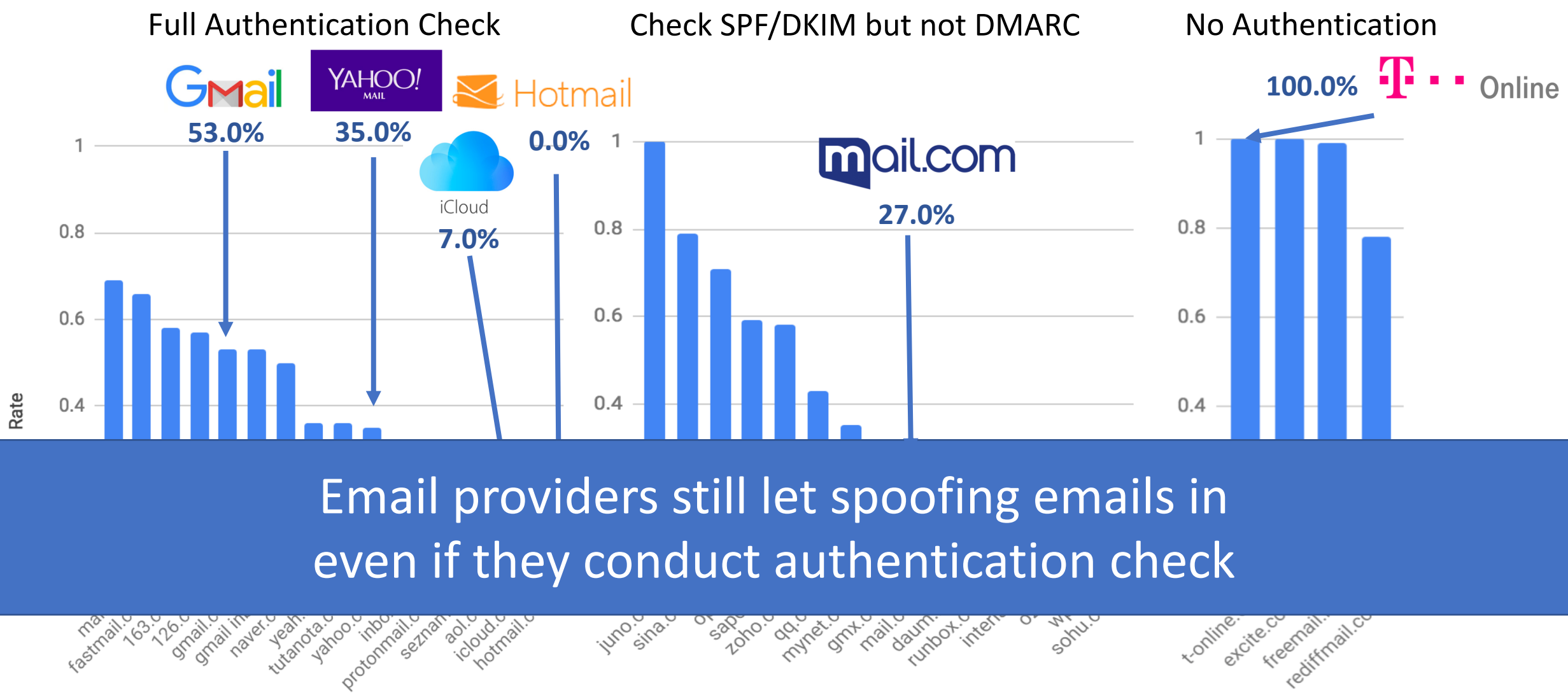
Static, Dynamic

Experiment Setup

IRB Approved

- Repeat 5 times
- Randomized sending order
- 30 x 5 x 2 x 5 = 1500 emails per service
- 1500 x 35 = 52500 emails in total
- Carefully controlled sending rate

Penetration Rate



Email providers still let spoofing emails in even if they conduct authentication check

Impacting Factors

Sender strict policy
Receiver full authentication
The penetration rate is lowest but still 13%

Receiver	Spoofed Sender Address Profile: Strict	Relaxed	None
Full Authentication	0.13	0.45	0.6
Partial Authentication	0.28	0.37	0.5

Penetration Rate

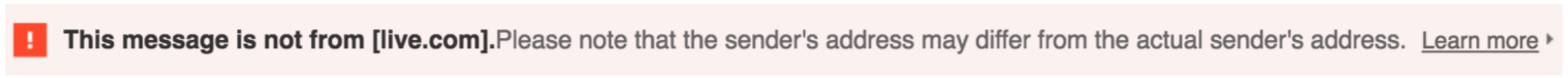
- 0 - 0.25
- 0.25 - 0.5
- 0.5 - 0.75

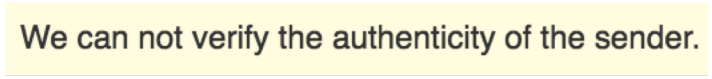
1. It takes both senders and receivers to configure correctly
2. Even so there are 13% penetration rate

How Do Email Providers Give Warning

29/35 web clients and 24/28 mobile clients didn't give any warnings

	Web	Mobile
Gmail	✓	✓
Naver	✓	✓
Protonmail	✓	✓
163.com 126.com	✓	✗
Mail.ru	✓	✗





Outline

- ~~Introduction~~
- ~~End-to-end Spoofing Experiments~~
- User Study

How Effective are These Security Indicators

- Research Questions
  - How do users react to spoofing emails?
  - How effective are warnings?
- Challenge
  - How to capture the realistic user reactions?
  - Lab experiment has limited ability to reflect reality [3]
- Method **IRB Approved**
  - Try to make users not aware they are in an experiment to capture realistic reaction
  - Inform users after experiment
  - Users can withdraw data anytime with payment

Phase 1/2: Set Up Deception

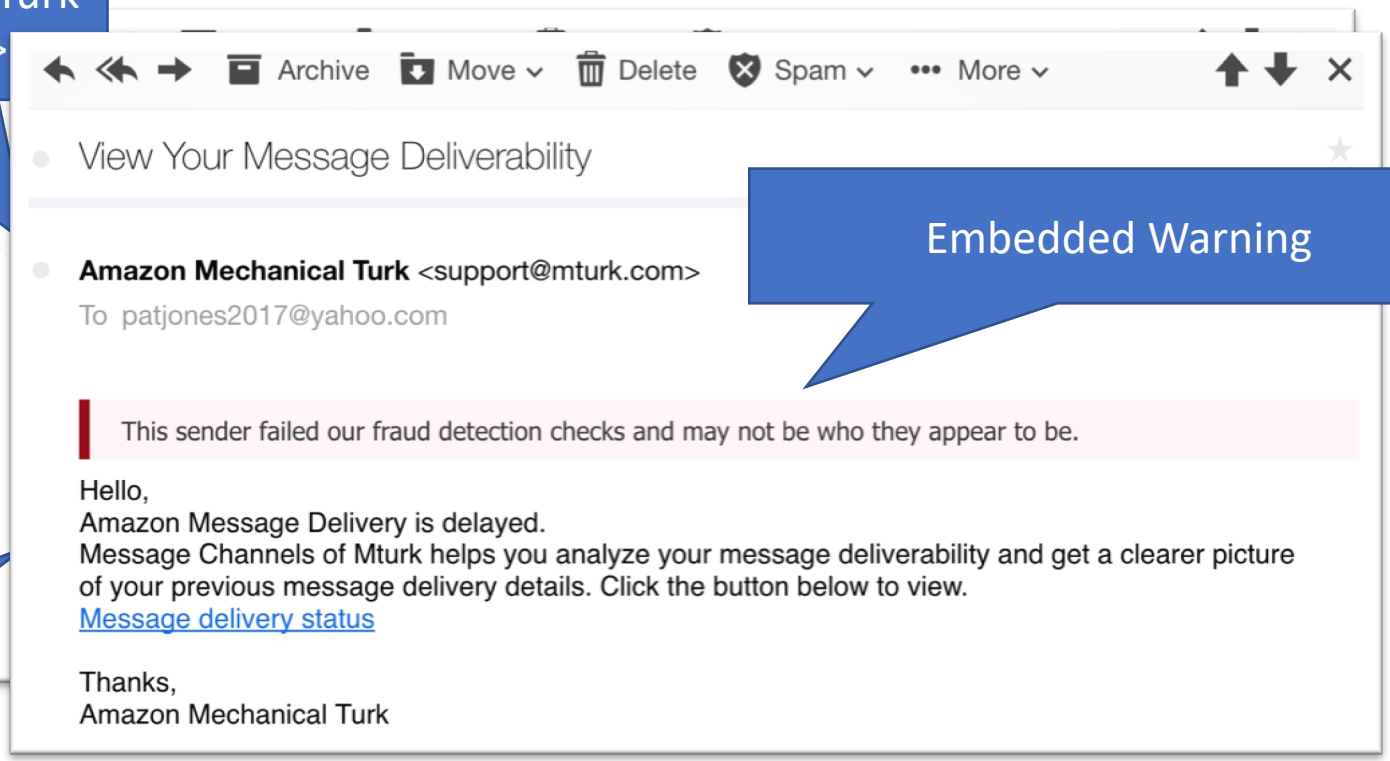
- Frame the study as a survey to understand email using habits
  - Ask for users' email address
  - Send the participant an email with 1x1 tracking pixel
  - Ask questions about the email using habits and other distraction questions
  - Pay users and make users believe the survey is over

- Purpose:
  - Collect and validate users' email addresses
  - Test if the tracking pixel works

Phase 2/2: Sending Actual Spoofing Emails

- Wait for 10 days and send users spoofing emails
- Wait for another 20 days and send debriefing emails

From Amazon Mechanical Turk <support@mturk.com>

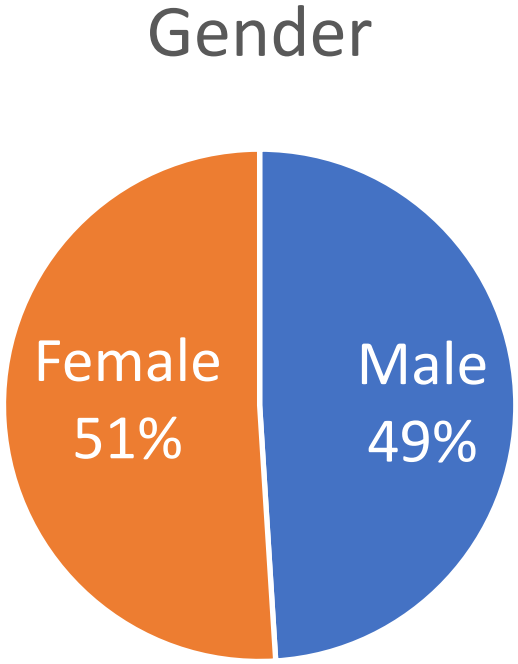


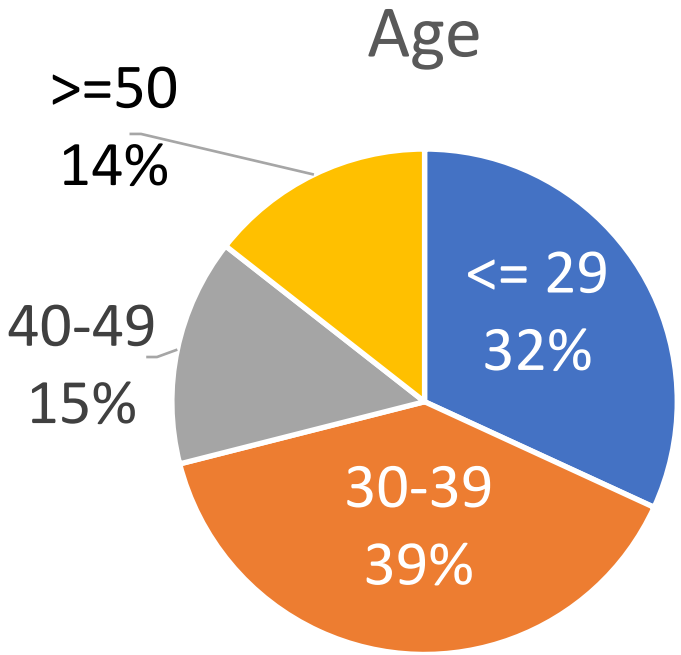
Embedded Warning

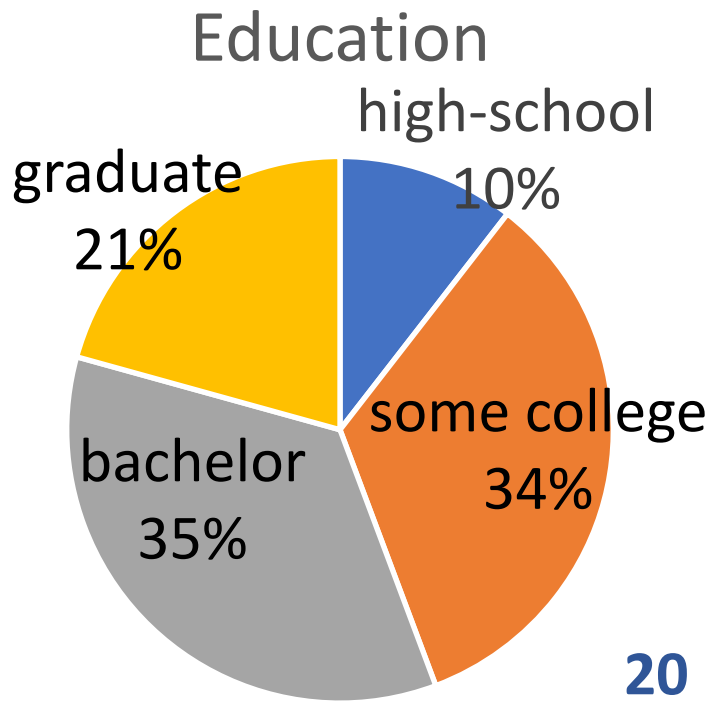
A link points to our server

Deception User Study: Recruiting Participants

- Amazon Mechanical Turk
- Recruited 488 users
  - 243 in no warning group
  - 245 in warning group







Deception User Study: Results

Phase	Users	Without Warning	With Warning
Phase 1	All Participants	243	245

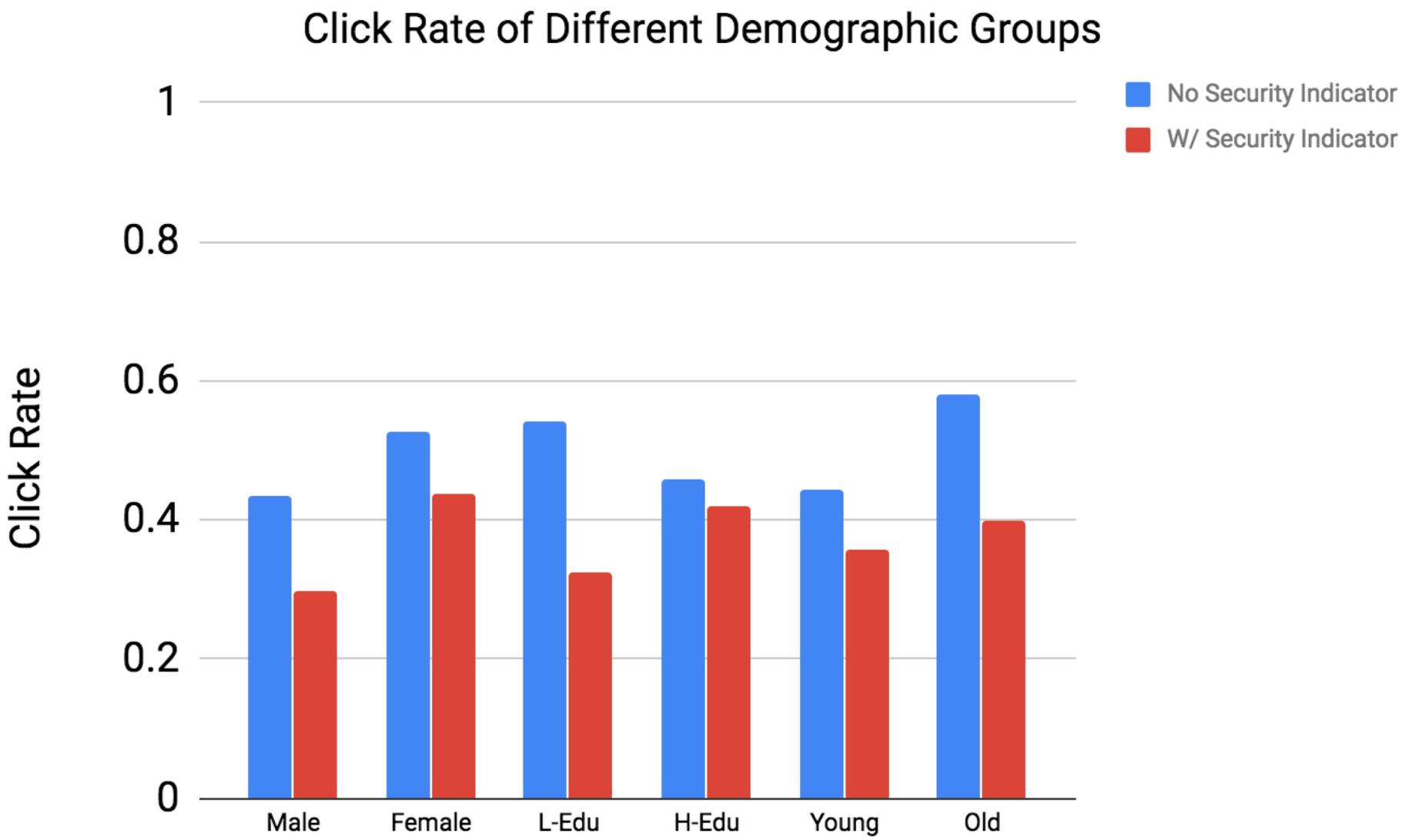
1. Warning only slightly lowers the click rate
2. The absolute click rate is still high

Discussion

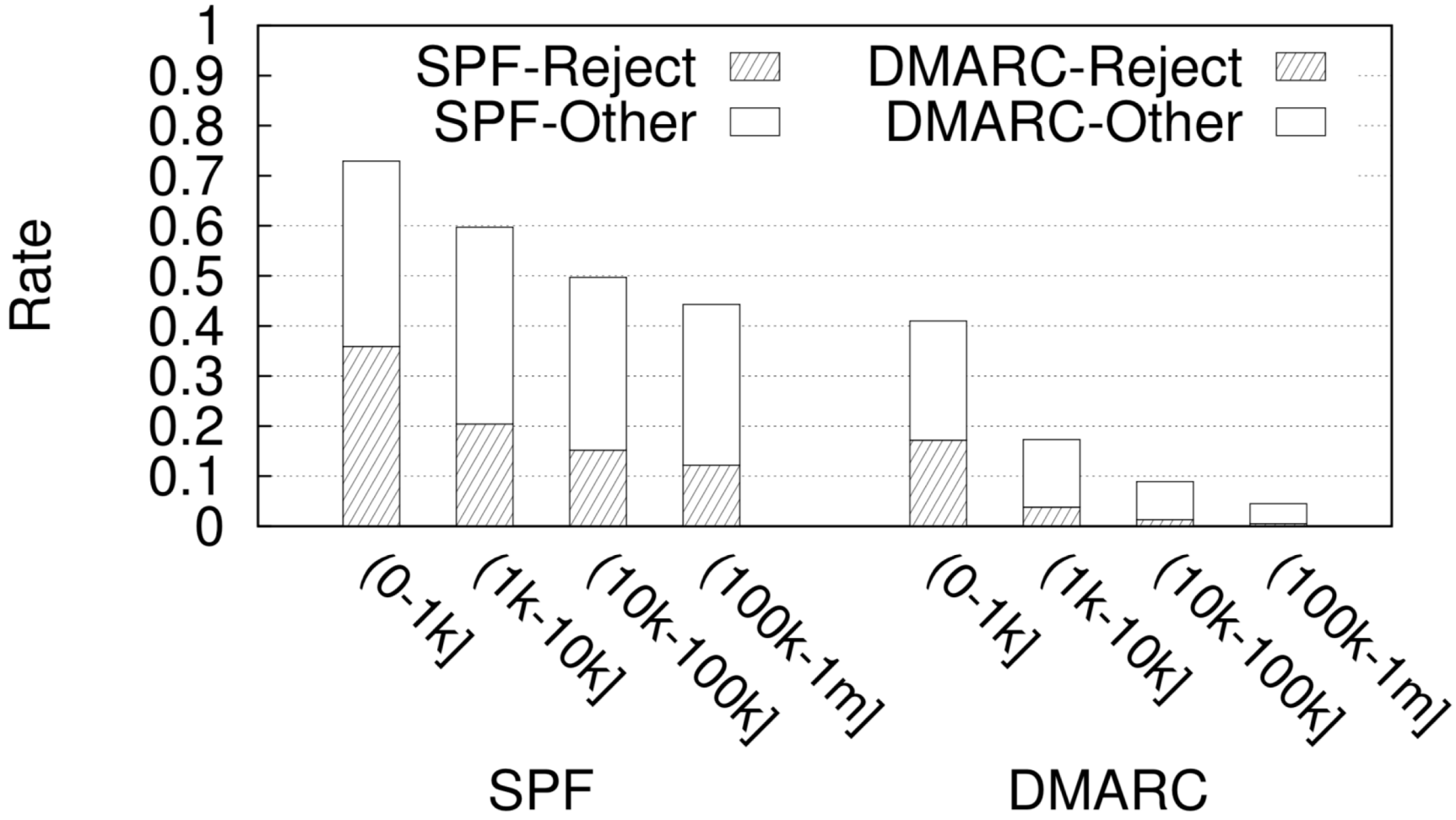
- A big gap between server detection and user protection
  - Most email providers let spoofing emails reach inbox
  - Most email providers lack necessary warnings
  - Warnings can’t fully eliminate the risk
- Countermeasures
  - Promote SPF, DKIM and DMARC
  - Place warning consistently across web and mobile clients
- Future work
  - Design more effective warnings
  - Defeat warning fatigue
  - User training and education

Thank You

Deception User Study: Results



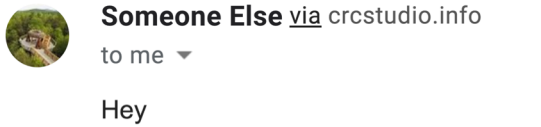
Things are Worse with Less Popular Domains



Misleading UI Elements

When spoofing existing contacts or conducting same-domain spoofing

Profile Picture



Web & Mobile

Gmail

Inbox by Gmail

ZOHO

Web

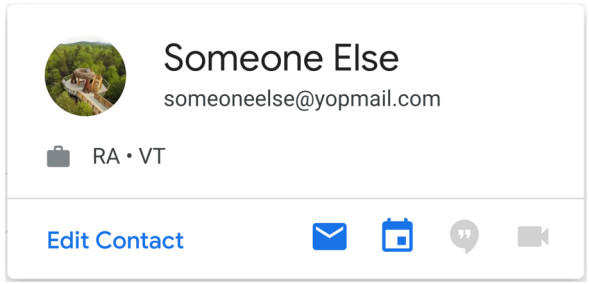
iCloud

Mobile

GMX

mail.com

Name Card



Web & Mobile

YAHOO!

GMX

Hotmail | Outlook

mail.com

SEZNAM.CZ

FastMail

Tutanota

Web

Aol.

JUNO

Gmail

sina 新浪网

Mobile

NAVER

126 网易免费邮

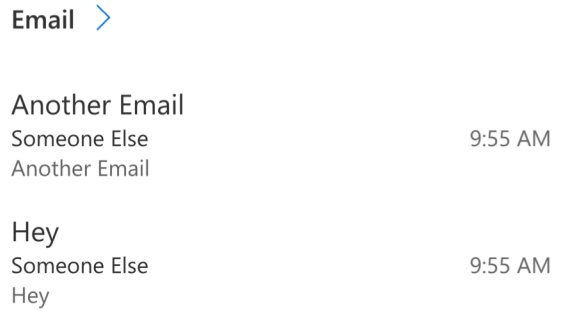
yeah .net

網易 NETEASE www.163.com

搜狐 SOHU.com

ZOHO

Email History



Web & Mobile

Hotmail | Outlook

@mail.ru

126 网易免费邮

yeah .net

網易 NETEASE www.163.com

ZOHO

Mail QQ邮箱

Web

GMX

YAHOO!

NAVER

DaUm

Gmail

inbox.lv

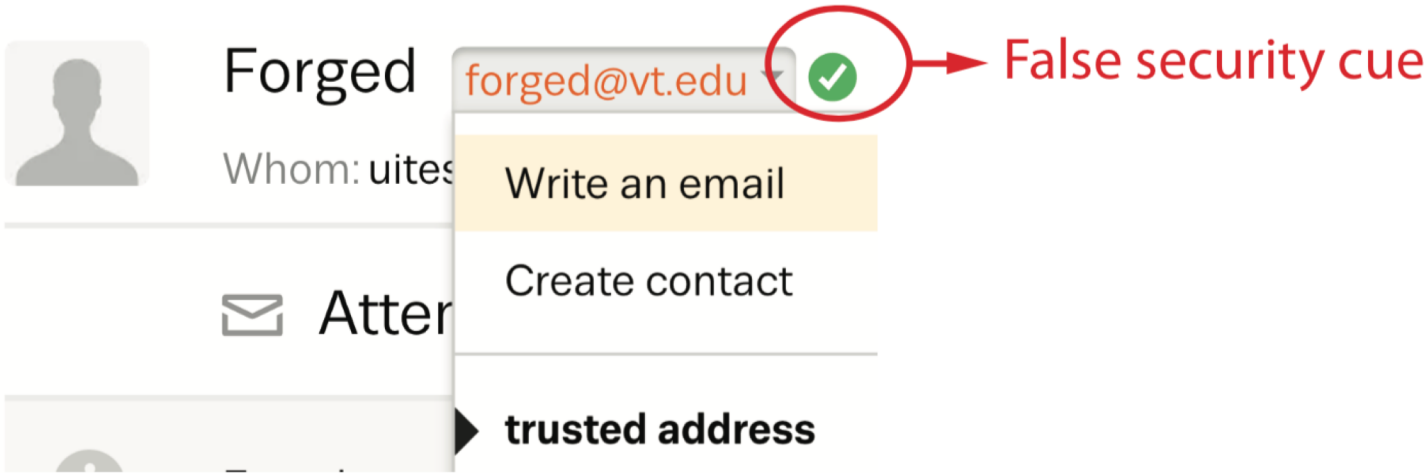
interia

SAPO

sina 新浪网

mail.com

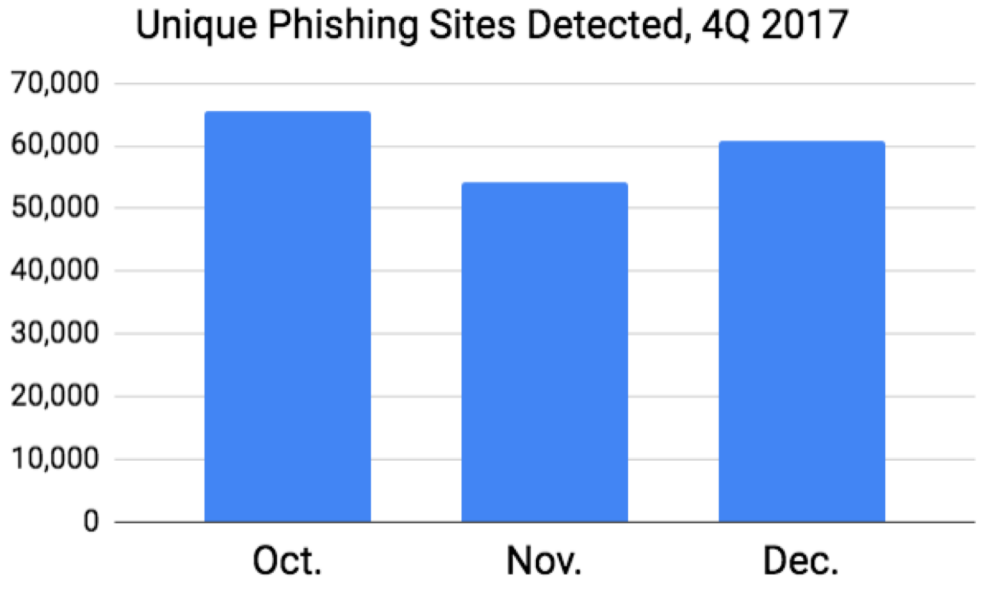
Misleading UI Elements



Seznam.cz

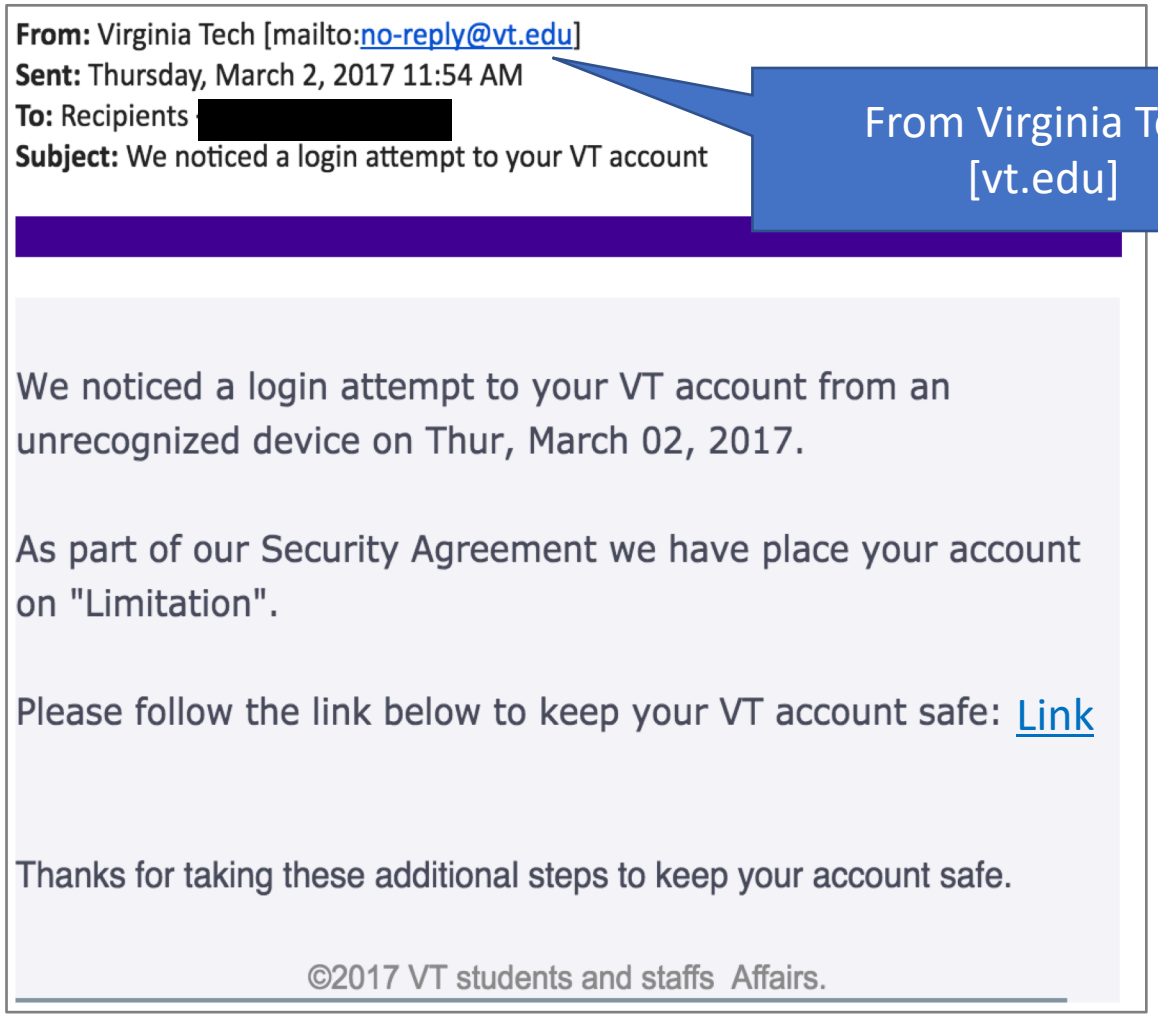
Spoofing is a Critical Step in Spear Phishing

- Email spoofing is widely used in spear phishing attacks
  - "Business email compromise" (BEC) scams became a major problem in 2015[3]
  - Use similar domain names or spoofed domain names[3]

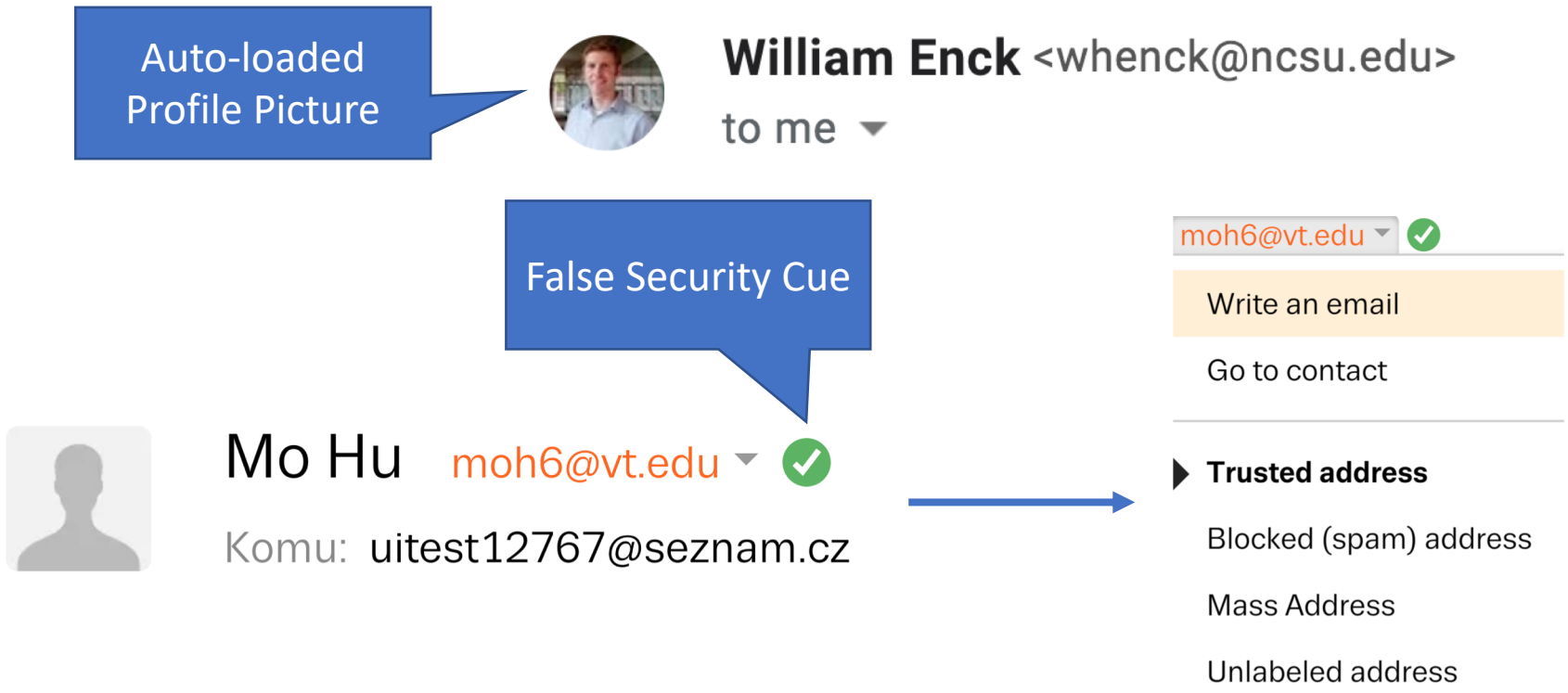


2. Figure from Phishing Activity Trends Report 4th quarter 2017, APWG.
3. Phishing Activity Trends Report, 1st-3rd quarters 2015, APWG.

Virginia Tech 2017



Misleading UI Elements



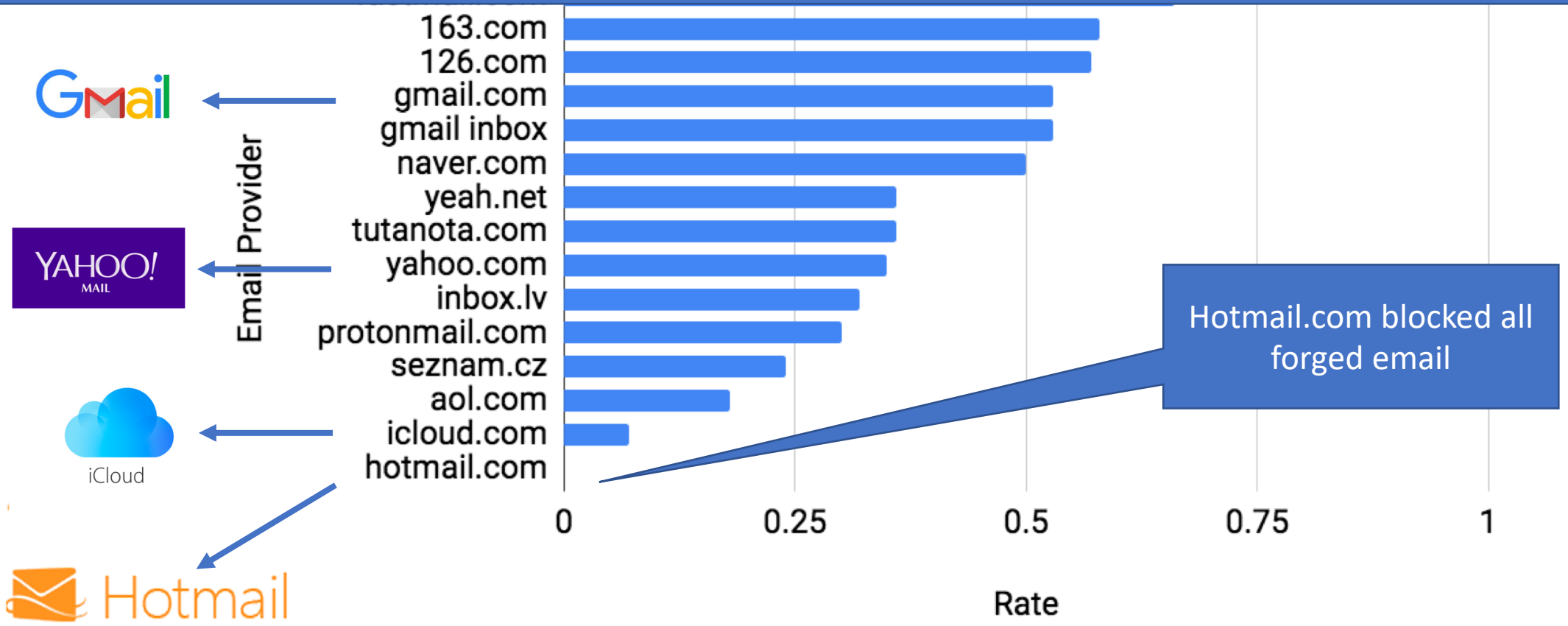
- Auto-loaded name card and email history

Deception User Study: Results

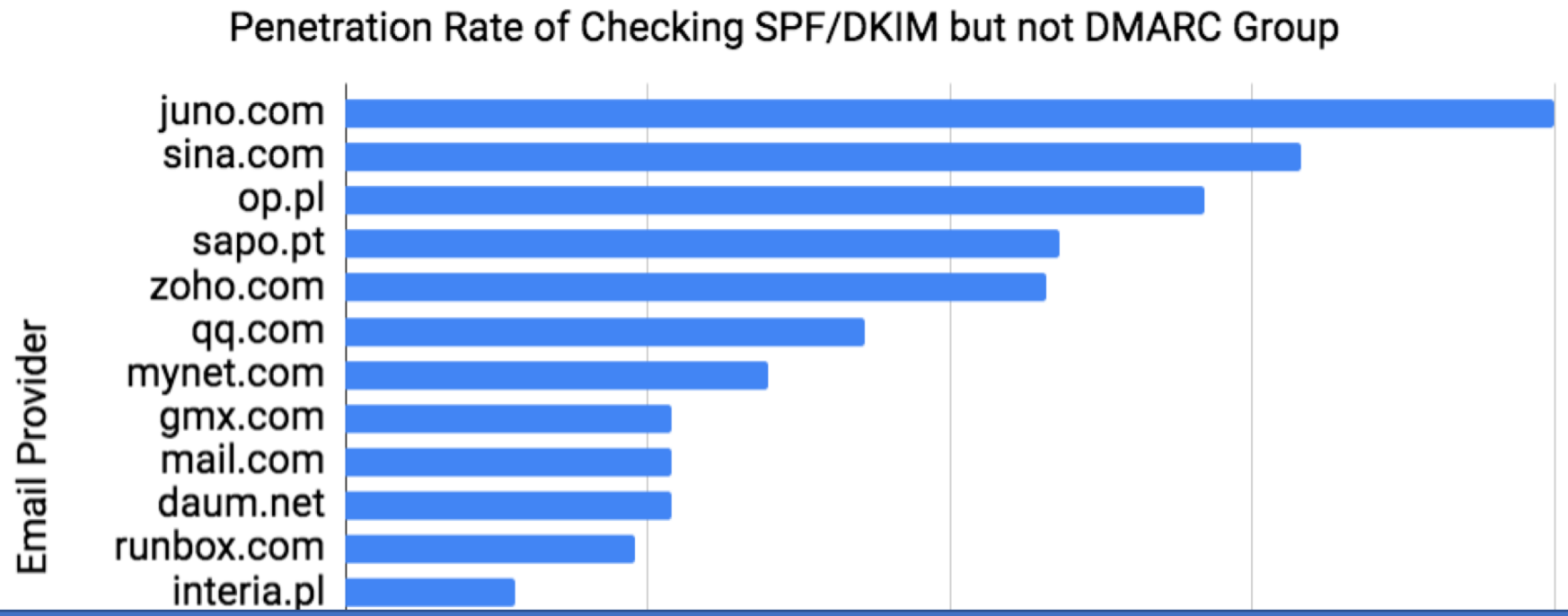
Users	Without Indicator		With Indicator	
	Desktop	Mobile	Desktop	Mobile
Opened Email	45	49	41	45
Clicked URL	21	25	15	17
Click Rate	46.7%	51.0%	36.6%	37.8%

End-to-end Spoofing Experiments: Results

Email providers still let forged emails in even if they conduct authentication check

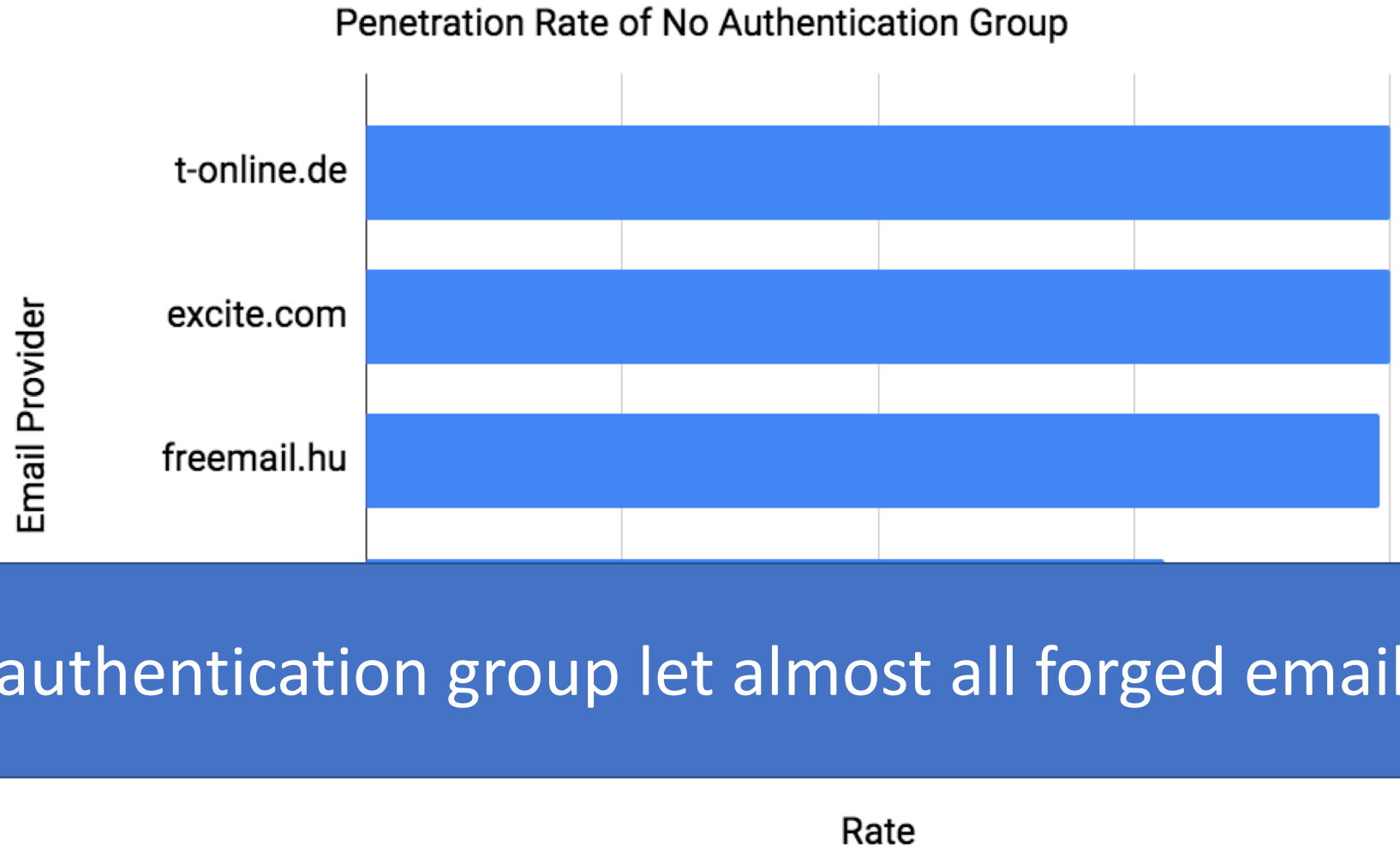


End-to-end Spoofing Experiments: Results



Email providers still let forged emails in
even if they conduct authentication check

End-to-end Spoofing Experiments: Results



No authentication group let almost all forged emails in

End-to-end Spoofing Experiments: Results

	IP	
Authentication	Static	Dynamic
Full Authentication	0.57	0.27
Check SPF DKIM But not DMARC	0.53	0.26
No authentication	0.95	0.94

1. It’s easier for static IP to conduct spoofing