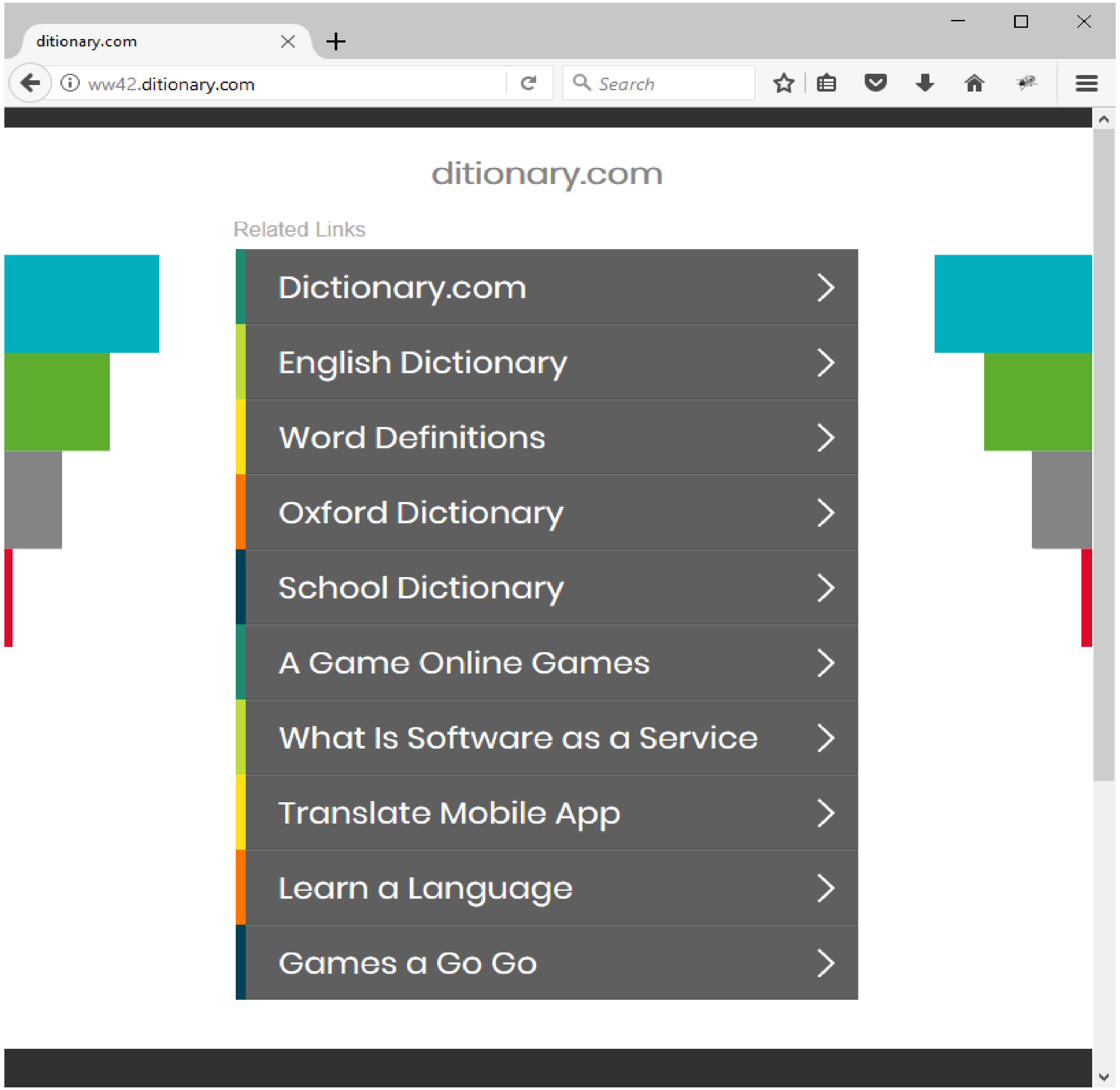
Email Typosquatting

Janos Szurdi and Nicolas Christin

Carnegie Mellon University

CyLab
Security and Privacy Institute

Di~~c~~tionary.com

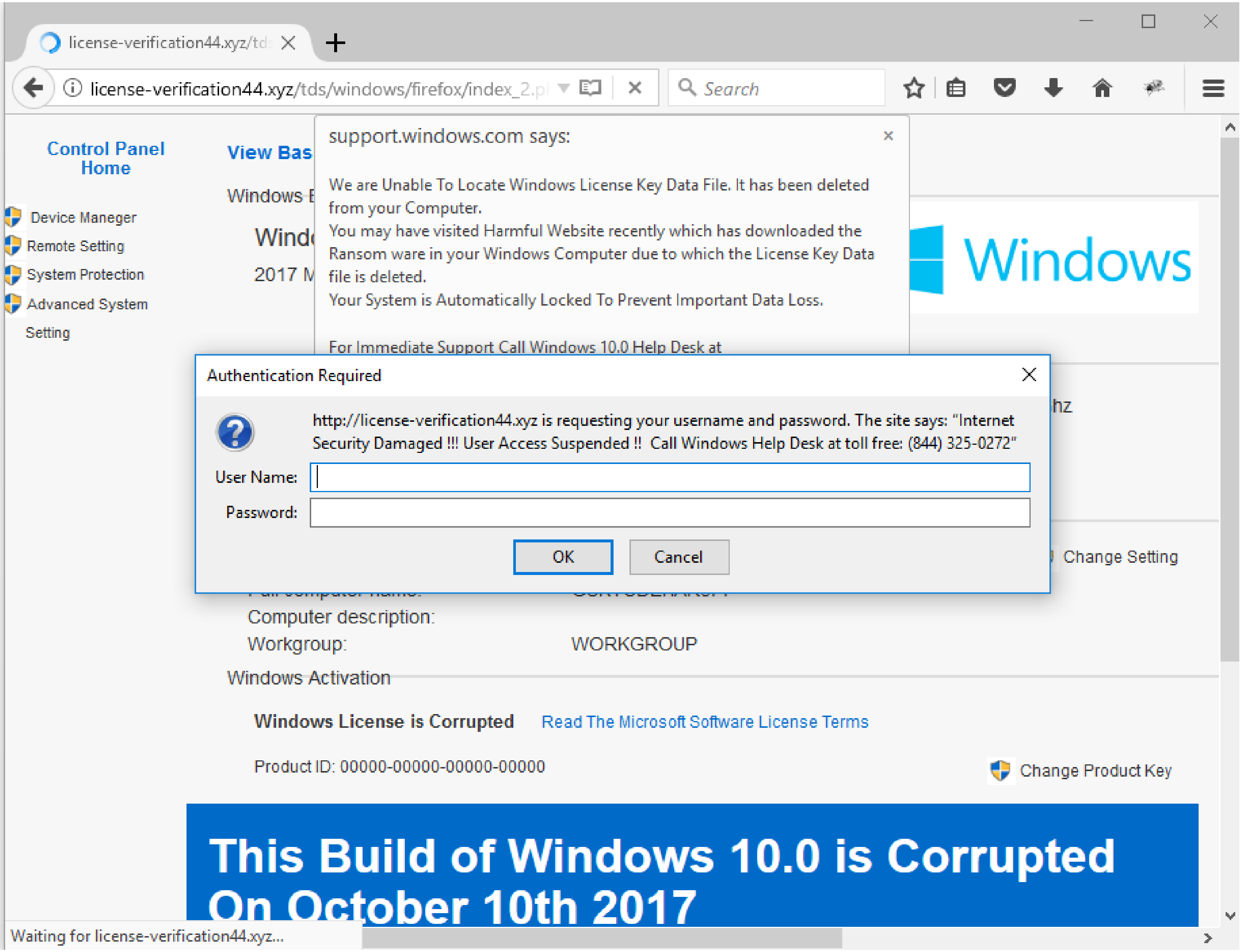


ditionary.com

Related Links

- Dictionary.com
- English Dictionary
- Word Definitions
- Oxford Dictionary
- School Dictionary
- A Game Online Games
- What Is Software as a Service
- Translate Mobile App
- Learn a Language
- Games a Go Go

~~Y~~outube.com



support.windows.com says:

We are Unable To Locate Windows License Key Data File. It has been deleted from your Computer.
You may have visited Harmful Website recently which has downloaded the Ransom ware in your Windows Computer due to which the License Key Data file is deleted.
Your System is Automatically Locked To Prevent Important Data Loss.

For Immediate Support Call Windows 10.0 Help Desk at

Authentication Required

http://license-verification44.xyz is requesting your username and password. The site says: "Internet Security Damaged !!! User Access Suspended !! Call Windows Help Desk at toll free: (844) 325-0272"

User Name:

Password:

OK Cancel

Computer description:
Workgroup: WORKGROUP

Windows Activation

Windows License is Corrupted Read The Microsoft Software License Terms

Product ID: 00000-00000-00000-00000

Change Product Key

This Build of Windows 10.0 is Corrupted On October 10th 2017

Waiting for license-verification44.xyz...

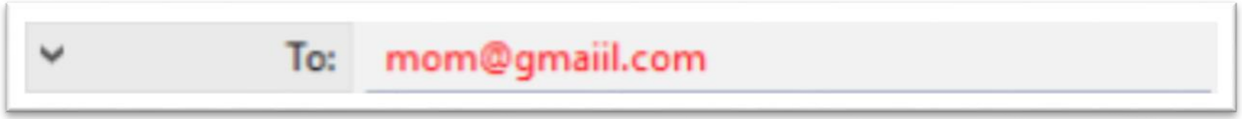
Fourteen Years of Typosquatting Research

WEB

- **2003** **Edelman**: first case study on one typosquatter
- **2006** **Wang et al.**: detection
- **2008** **Banerjee et al.**: detection
- **2009** **Chen et al.**: detection
- **2010** **Moore and Edelman**: monetization
- **2011** **Banerjee et al.**: detection
- **2014** **Szurdi et al.**: large scale study
- **2015** **Agten et al.**: longitudinal study and **Khan et al.**: quantifying harm to users
- **2017** **Miramirkhani et al.**: technical support scam

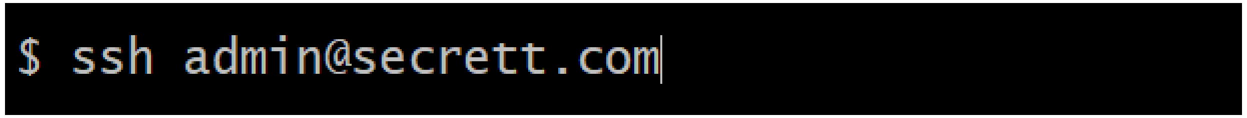
Other Applications Using DNS

- Email:



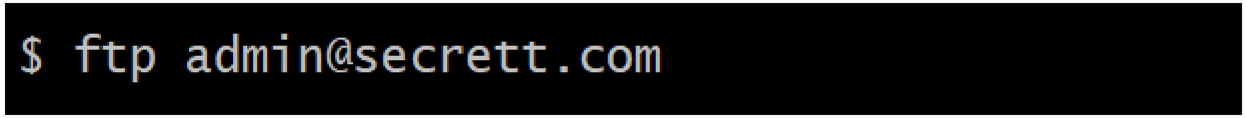
To: mom@gmaiil.com

- SSH:



```
$ ssh admin@secrett.com
```

- FTP:



```
$ ftp admin@secrett.com
```

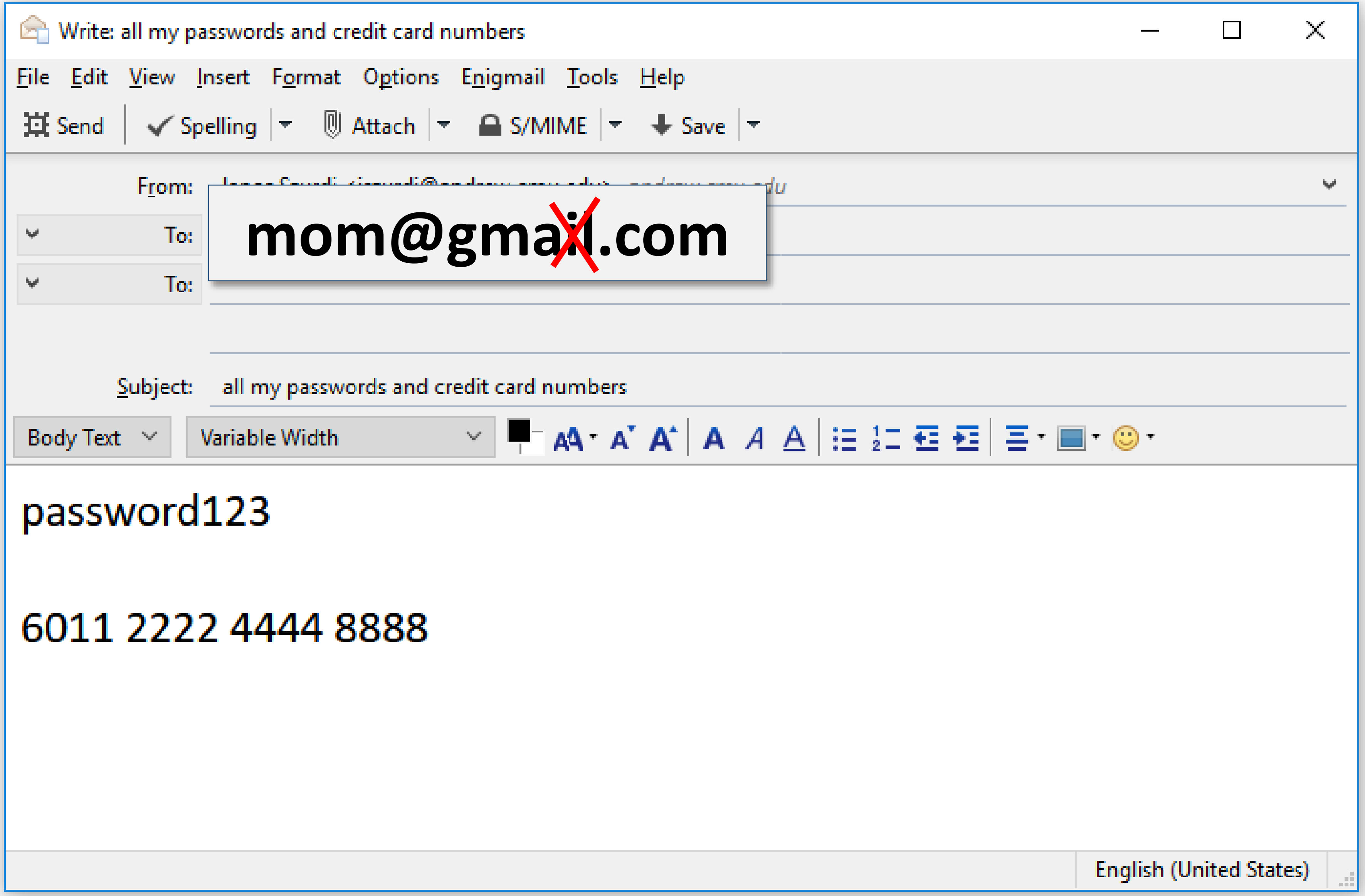
- Godai group 2011: white paper on email typosquatting
- Vissers et al. 2017: name server typosquatting

Agenda

1. **Email Typo Mistakes**
   - What are the email typo mistakes users can make?
2. **In the shoes of typosquatters**
   - Do users make email typo mistakes frequently?
3. **Typosquatting in the wild**
   - Can typosquatters collect emails on a large scale?
   - How much emails typosquatting domains in the wild receive?
4. **In the shoes of the victims**
   - Do typosquatters actually collect emails?

Email Typo Mistakes

Receiver Typo



From:

To: mom@gma~~i~~l.com

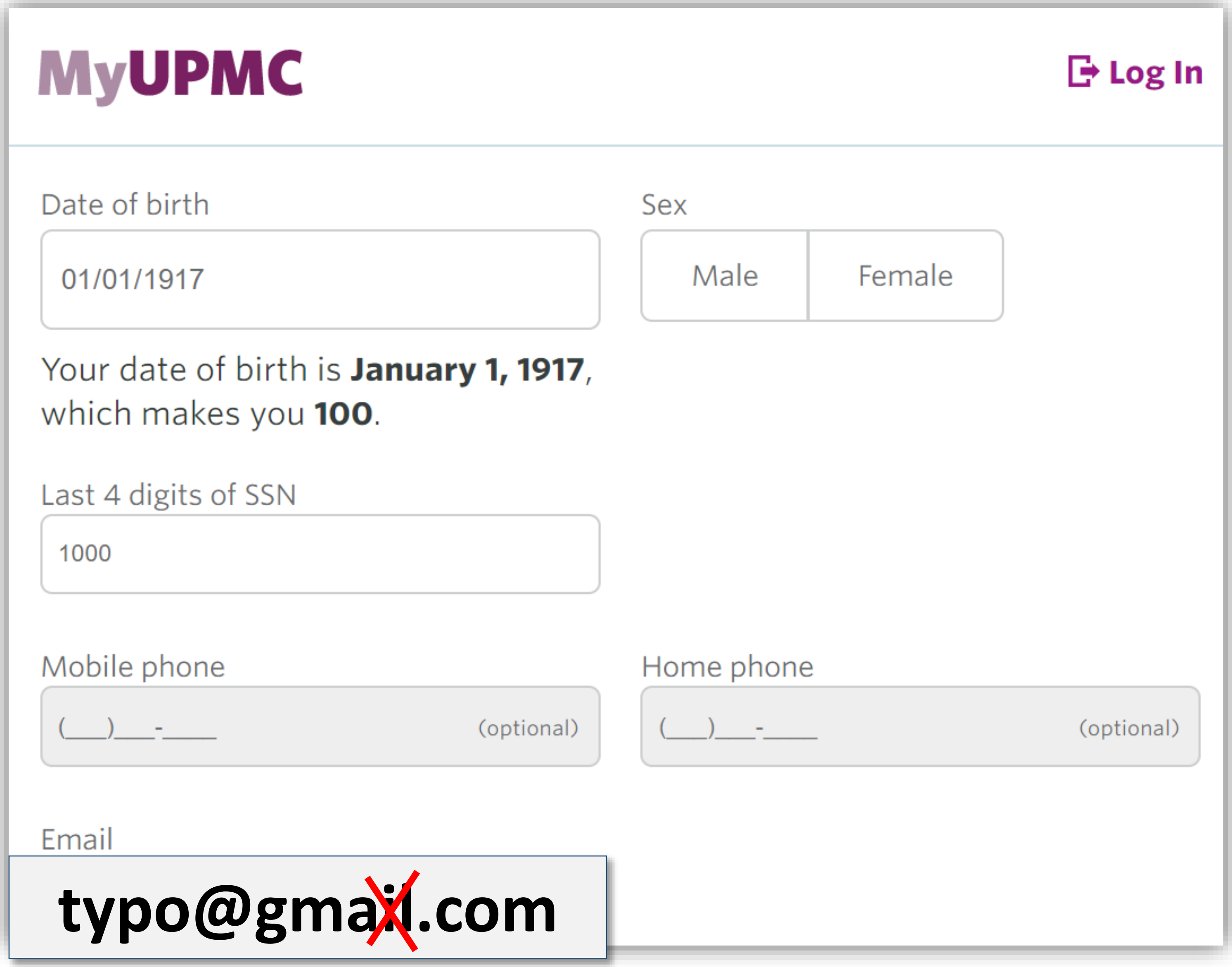
To:

Subject: all my passwords and credit card numbers

password123

6011 2222 4444 8888

Reflection Typo



Date of birth

01/01/1917

Sex

Male | Female

Your date of birth is **January 1, 1917**, which makes you **100**.

Last 4 digits of SSN

1000

Mobile phone

(___)___-____ (optional)

Home phone

(___)___-____ (optional)

Email

typo@gma~~il~~.com

When Reflection Typos Are Really Bad

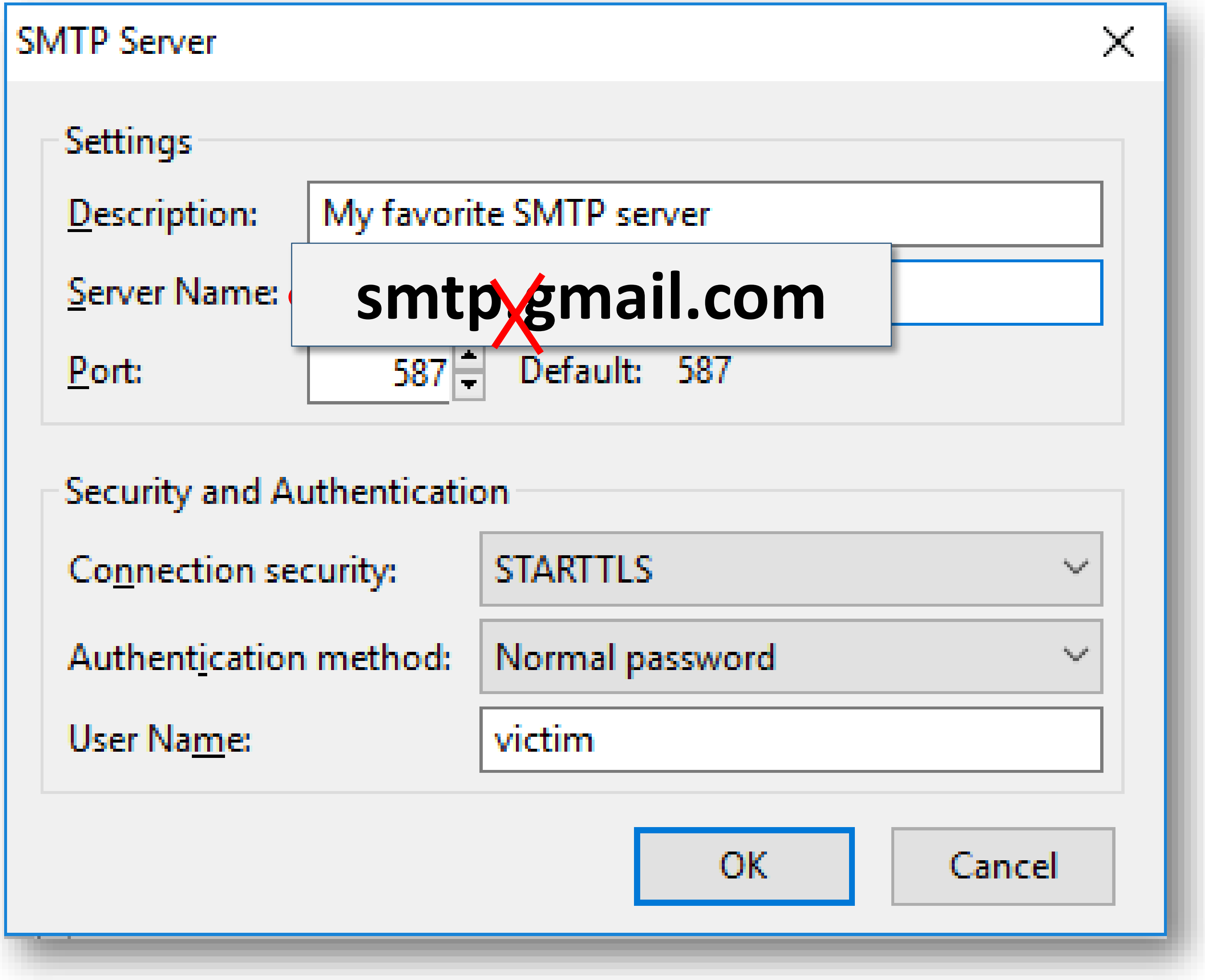
When mistake affects other users!

someone@zohomil.com: we received several

- job applications
- with CVs containing personal information

Several job advertisement copy pasted with the same mistyped address

SMTP Typo



SMTP Server

Settings

Description: My favorite SMTP server

Server Name:

smtp✗gmail.com

Port: 587 Default: 587

Security and Authentication

Connection security: STARTTLS

Authentication method: Normal password

User Name: victim

In The Shoes of Typosquatters

Collection Ethics

IRB approved

- Took measures beyond IRB requirement

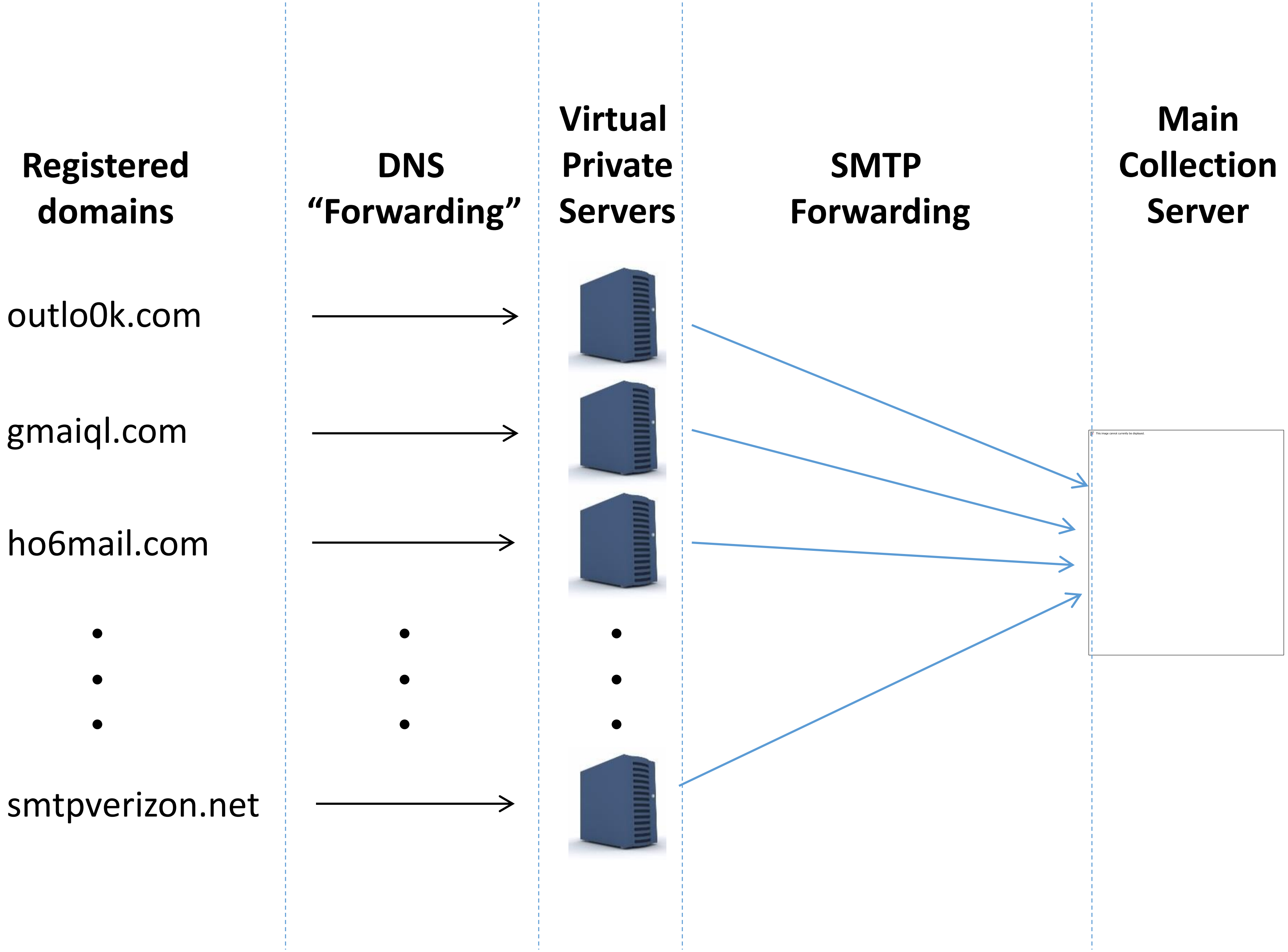
Registering typosquatting domains

- Potential trademark infringement
- On request surrender domains

Collecting personal emails

- Protect personal information
  - Keep on secure server
  - Encrypt emails
- Protect privacy
  - Remove sensitive data
  - Minimize the number of emails viewed

Collection Infrastructure



Registered domains

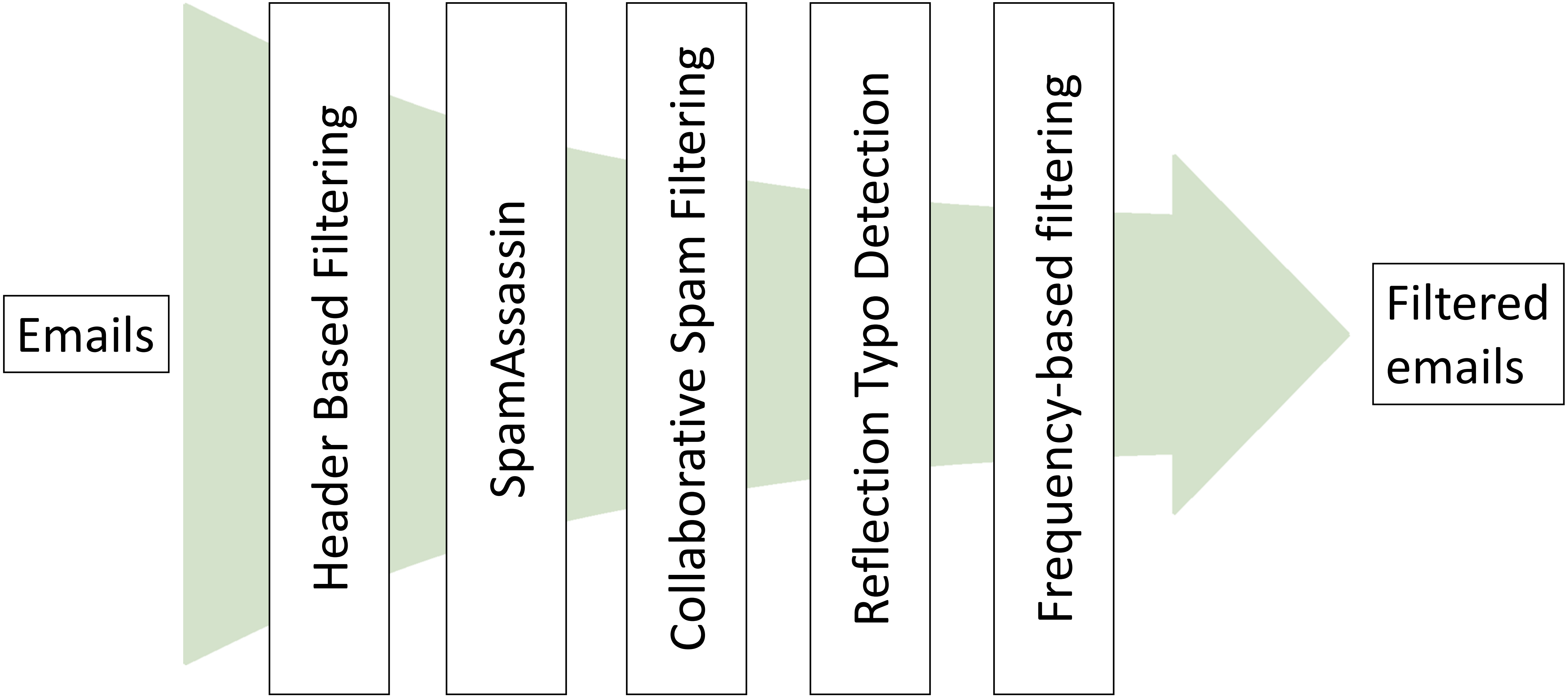
DNS "Forwarding"

Virtual Private Servers

SMTP Forwarding

Main Collection Server

Spam Filtering



Emails

Header Based Filtering

SpamAssassin

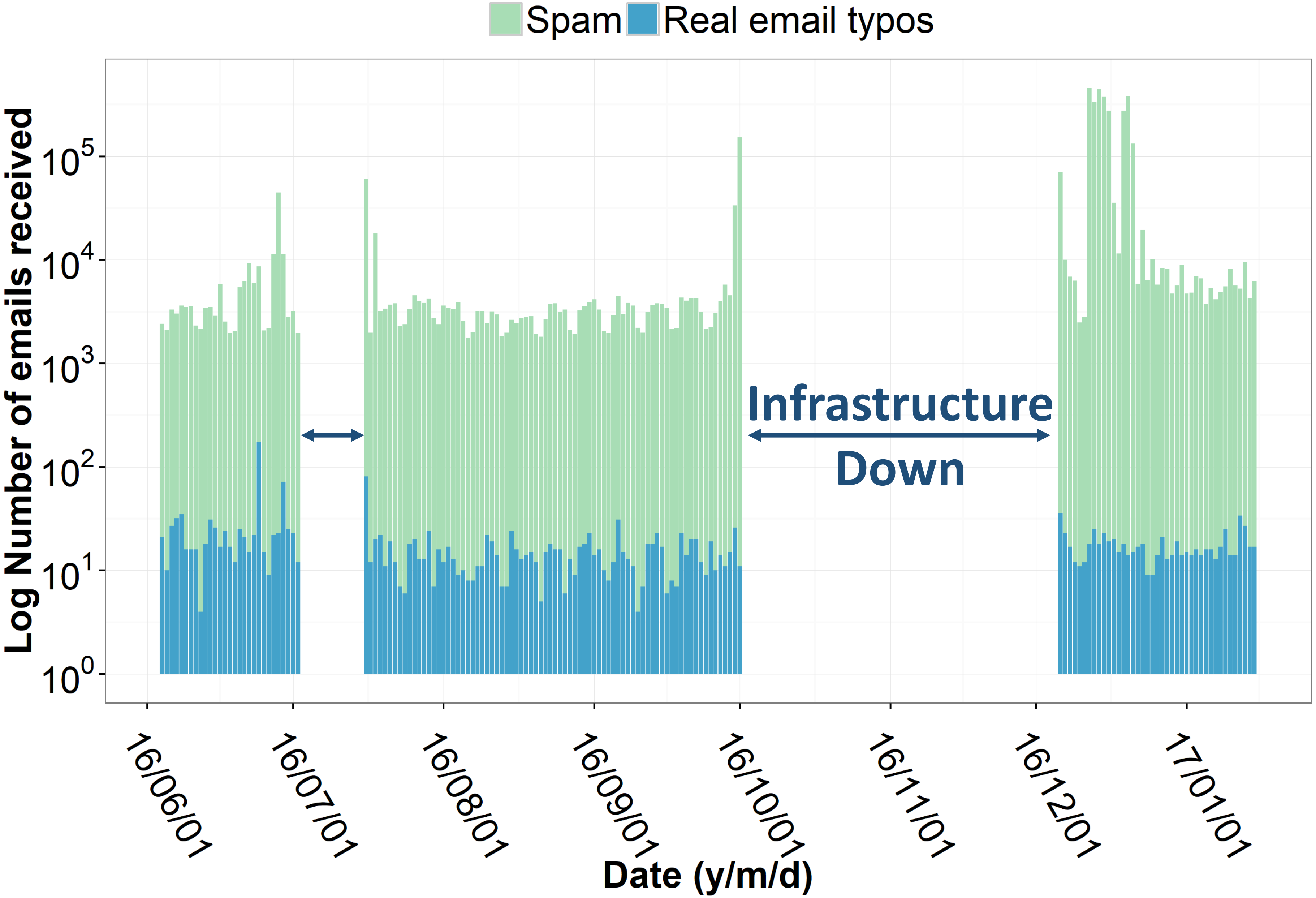
Collaborative Spam Filtering

Reflection Typo Detection

Frequency-based filtering

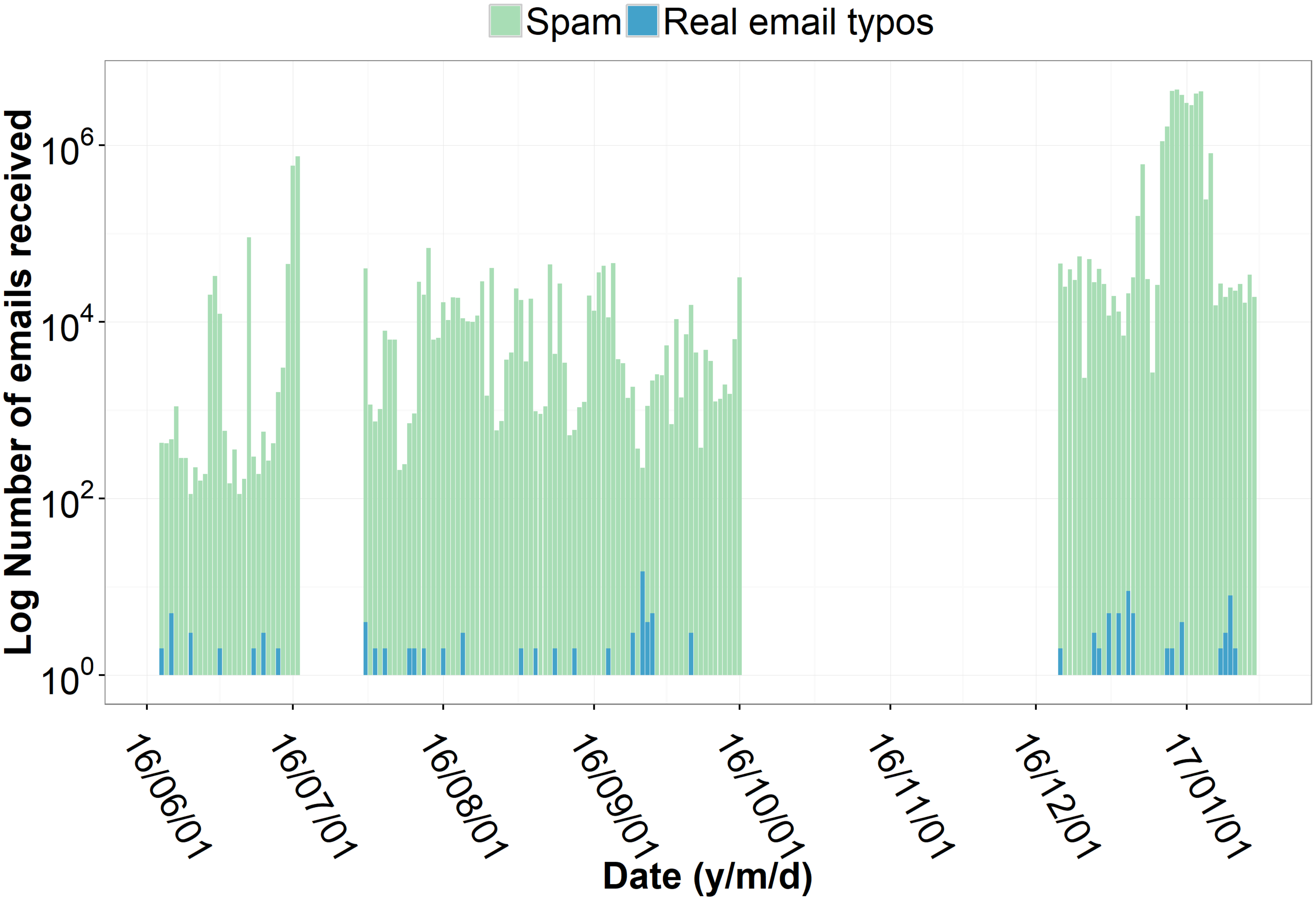
Filtered emails

Receiver Typo Emails Collected

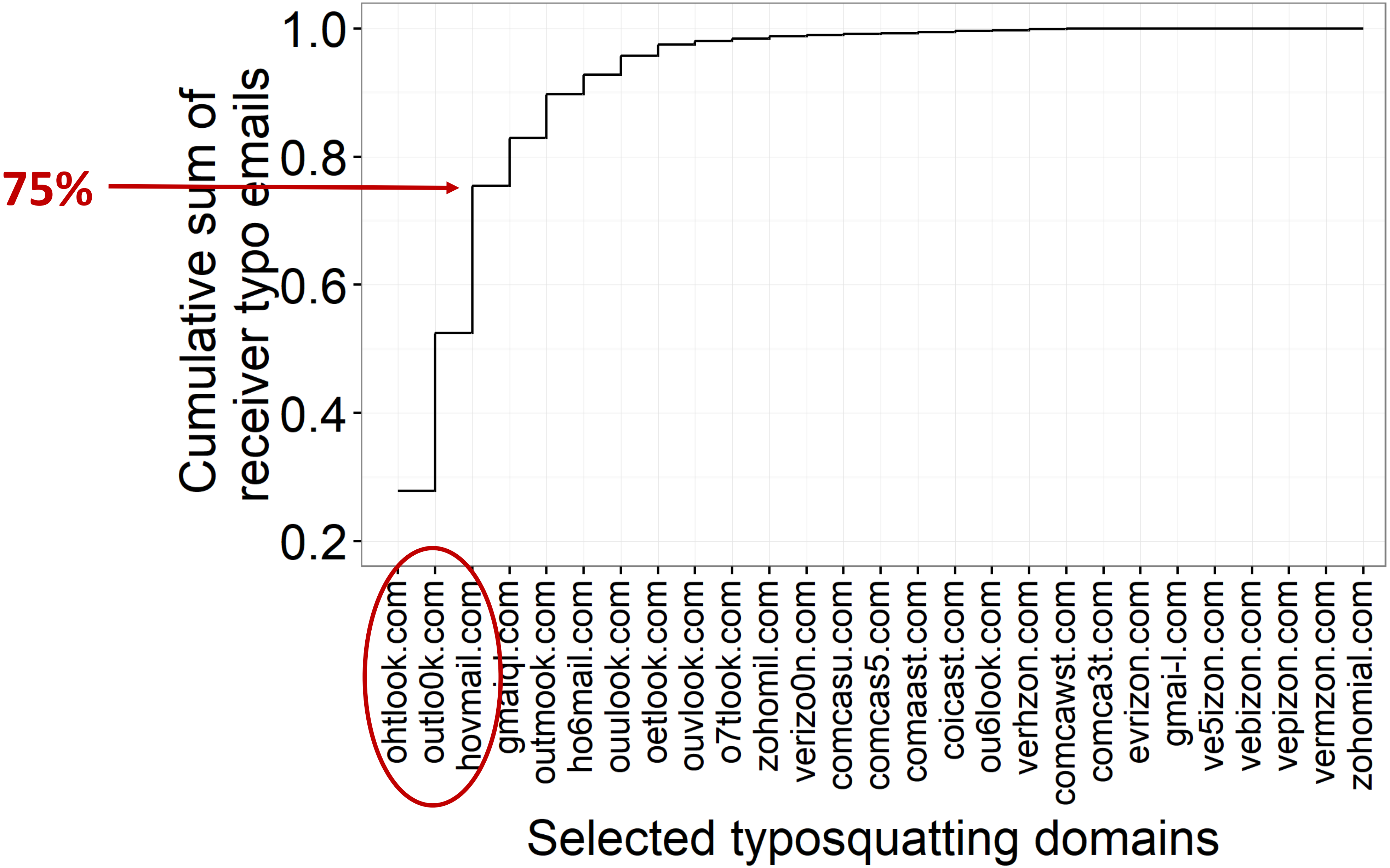


Infrastructure Down

SMTP Typo Emails Collected



Not All Typosquatting Domains Are Equal



Typosquatting Domain Quality

Domain	# Emails	Is Fat Finger?
ohtlook.com	1320	TRUE
outlo0k.com	1170	TRUE
outmook.com	324	FALSE
ouulook.com	137	FALSE
oetlook.com	84	FALSE
ouvlook.com	25	FALSE
o7tlook.com	20	TRUE
ou6look.com	7	TRUE

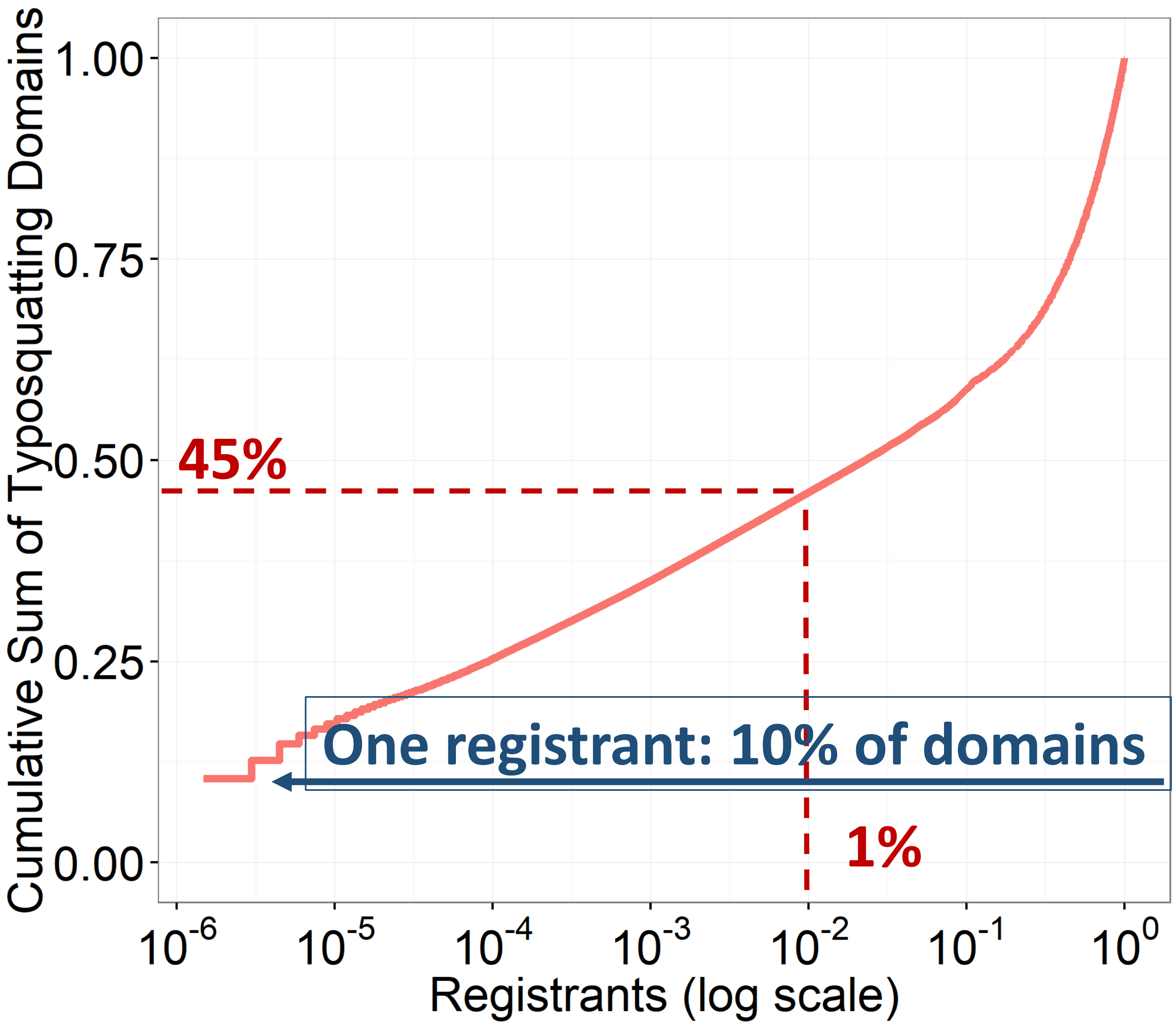
hovmail.com	1095	FALSE
ho6mail.com	147	TRUE

Factors of profitability

- **Popularity** of target domain is the most important
- **Keyboard distance**
- **Conspicuousness**

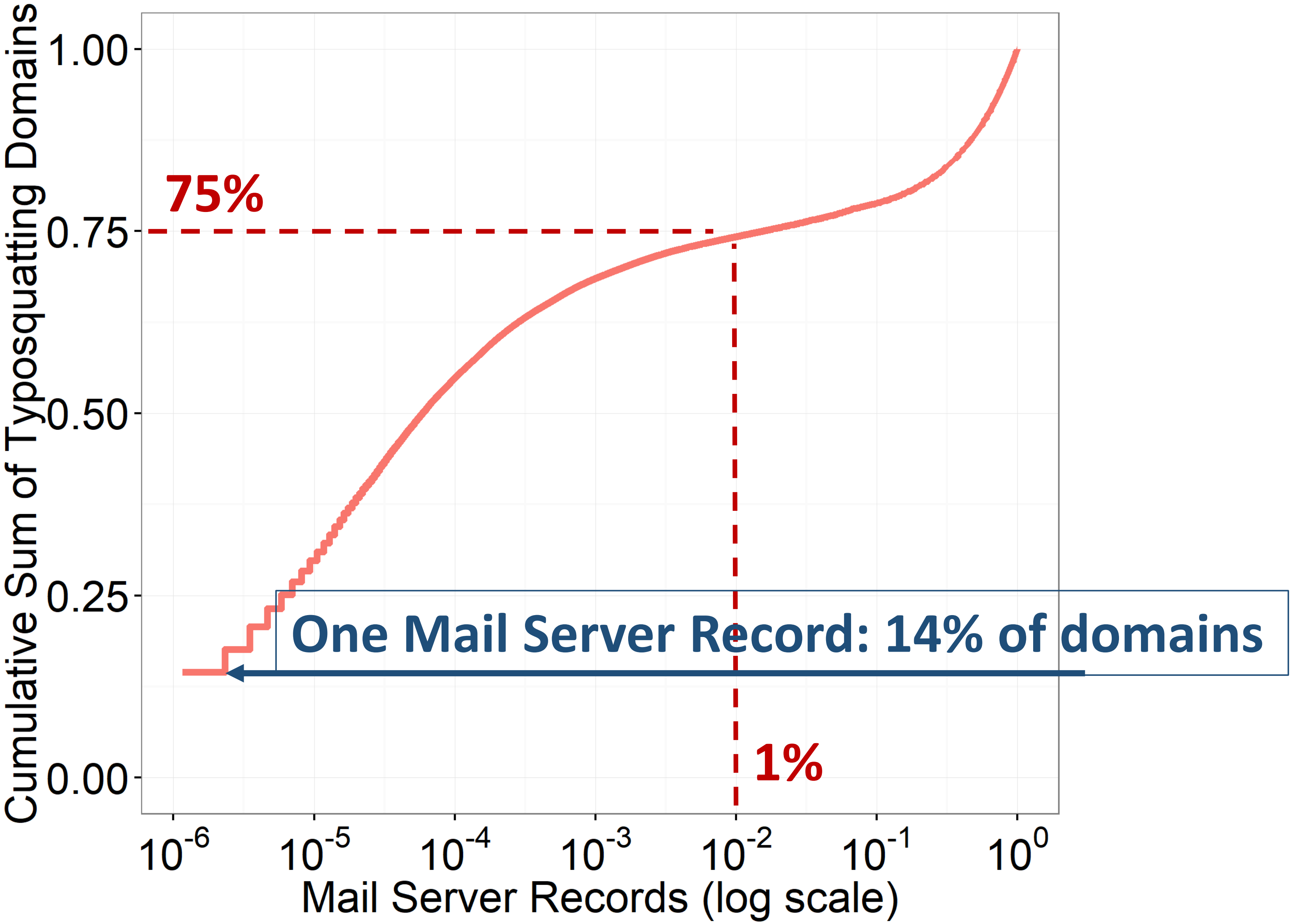
Typosquatting In The Wild

Infrastructure Concentration: Registrants



One registrant: 10% of domains

Infrastructure Concentration: Mail Server Records



75%

1%

One Mail Server Record: 14% of domains

Email Typosquatting Eco-system

High SMTP support

- Millions of typosquatting domains
- 2/3 of typo domains can receive emails

Infrastructure serving typosquatting

- Average name servers: 4% typosquatting
- Bad name servers: up to 89% typosquatting

Targeting email protocols

- 41 SMTP typos of Alexa top 10k
- smtpgmail.com
- smtphotmail.com

Both privacy protected and typosquatting

Extrapolation

Model

- Based on our previous observations
- Features: Popularity, conspicuousness and keyboard distance

Extrapolate to

- 1211 typosquatting domains
- Targeting: gmail.com, hotmail.com, outlook.com, comcast.com, verizon.com

Estimate:

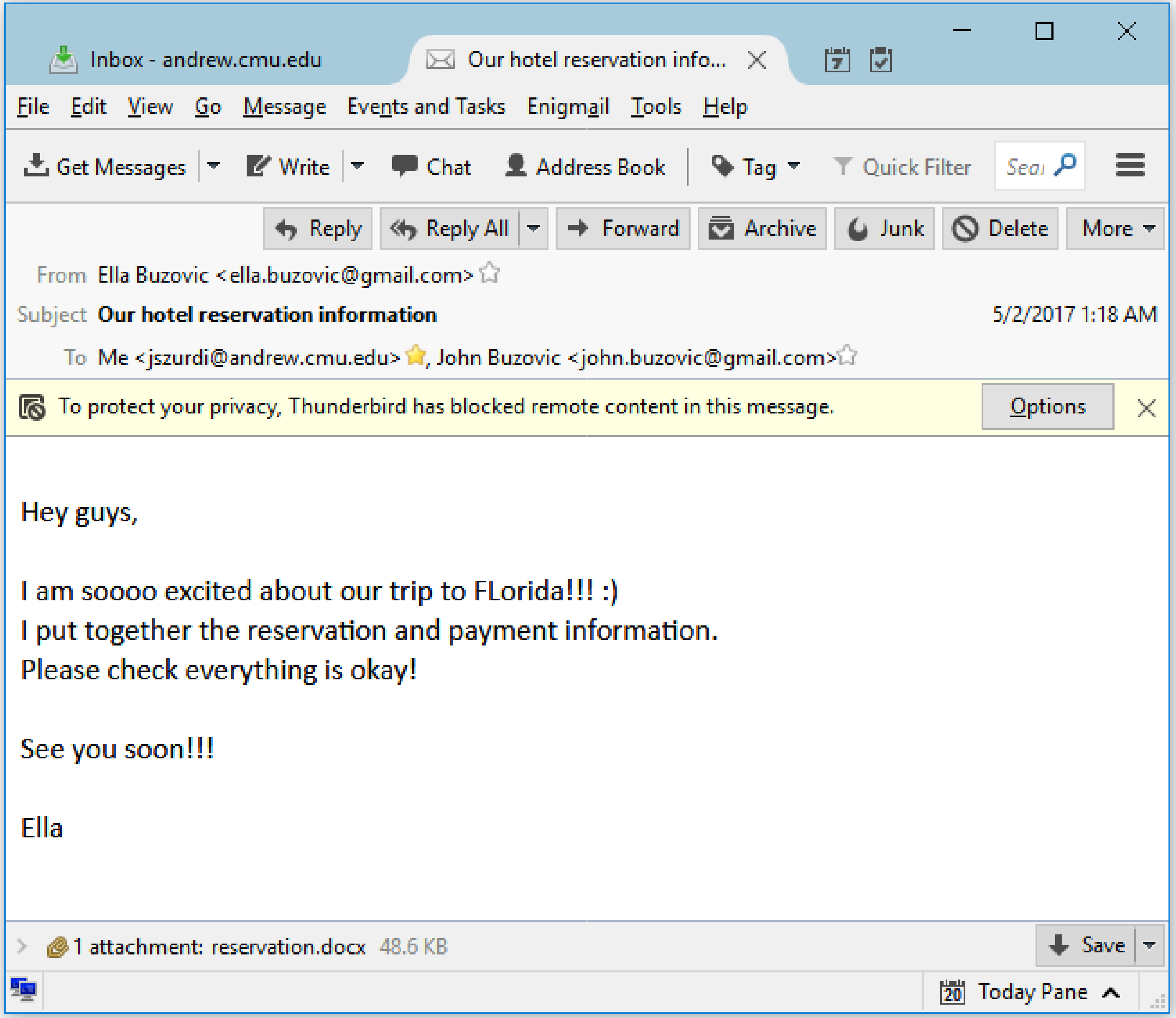
- 850,000 emails/year received

One email costs one penny to collect

- Ideal for spear phishing or scam campaigns

In The Shoes of The Victims

Honey Email with Honey Token



From Ella Buzovic <ella.buzovic@gmail.com>

Subject **Our hotel reservation information** 5/2/2017 1:18 AM

To Me <jszurdi@andrew.cmu.edu>, John Buzovic <john.buzovic@gmail.com>

To protect your privacy, Thunderbird has blocked remote content in this message.

Hey guys,

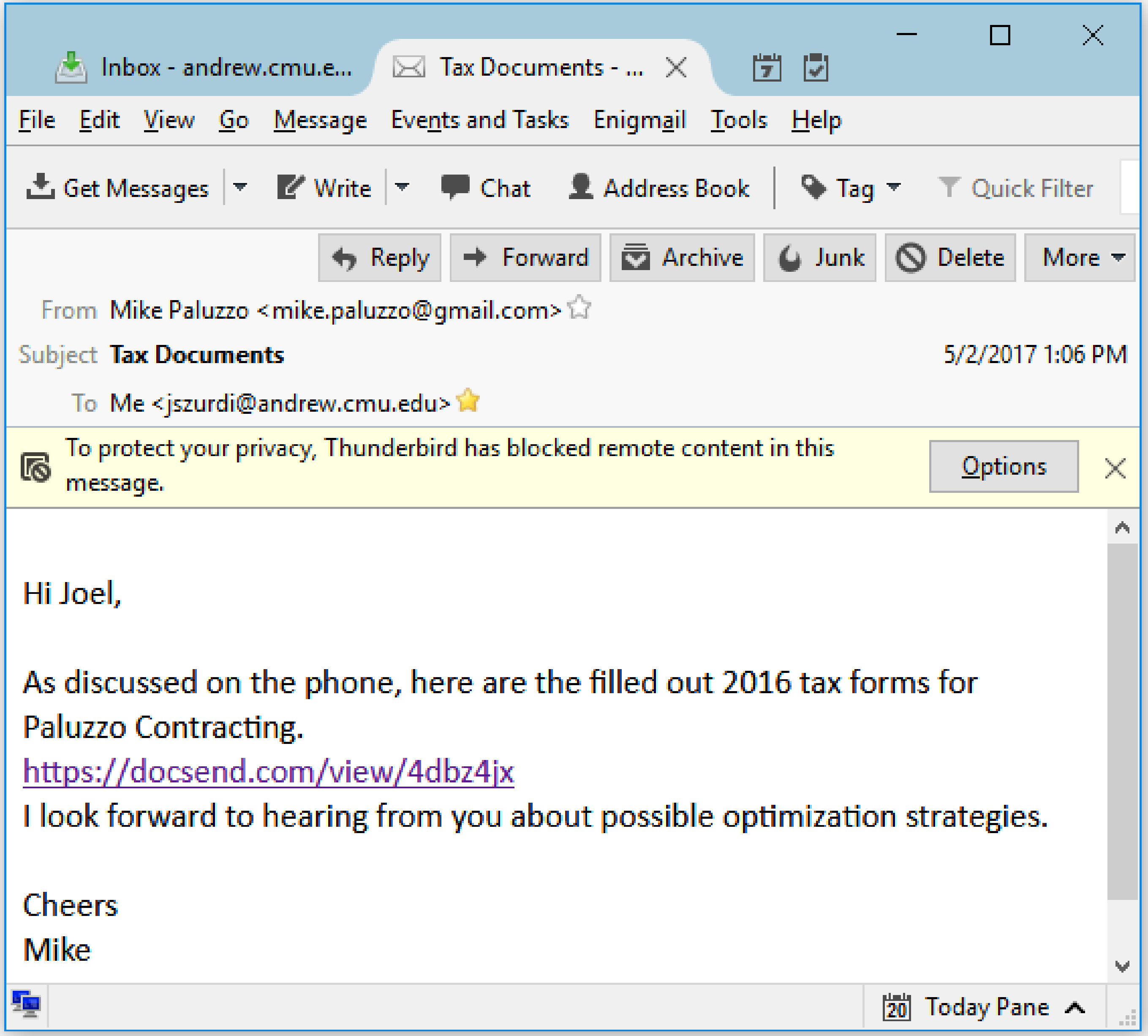
I am soooo excited about our trip to FLorida!!! :)
I put together the reservation and payment information.
Please check everything is okay!

See you soon!!!

Ella

1 attachment: reservation.docx 48.6 KB

Honey Email with Honey Account



From Mike Paluzzo <mike.paluzzo@gmail.com>

Subject **Tax Documents** 5/2/2017 1:06 PM

To Me <jszurdi@andrew.cmu.edu>

To protect your privacy, Thunderbird has blocked remote content in this message.

Hi Joel,

As discussed on the phone, here are the filled out 2016 tax forms for Paluzzo Contracting.
https://docsend.com/view/4dbz4jx
I look forward to hearing from you about possible optimization strategies.

Cheers
Mike

Large Scale Test

Tested

- 50,000 typosquatting domains

Domains accepting our emails

Domain registration type	Percent accepted our emails
All	14 %
Public registration	4 %
Private registration	27 %

Sensitive targets

- disvover.com, bankofamericqa.com, nuaghtyamerica.com and comcacst.com

Emails read

- 19 based on our logs

Sensitive Information Test

Tested

- 7269 domains
- previously accepted our email

Emails read

- 15 based on our logs

Sensitive information accessed

- Tax document accessed from Caracas Venezuela
- Shell account access attempt from Poland

Summary

- Users sent us emails with sensitive data
- Typosquatting domains' profitability depends on
  - Popularity
  - Conspicuousness
  - Keyboard distance
- Typosquatters have infrastructure in place to collect emails
- One email costs one penny to collect
- Exploitation of email typosquatting is not confirmed

jszurdi@andrew.cmu.edu