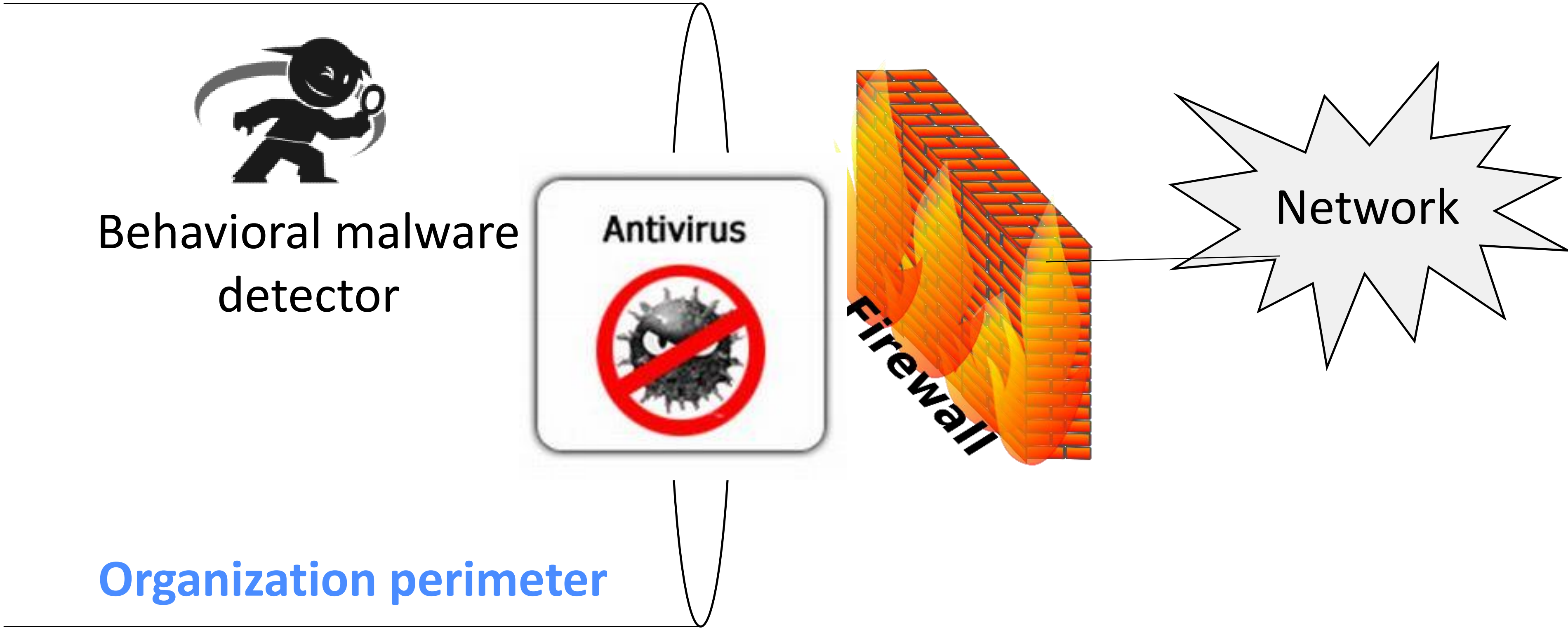
Cyber Social Engineering and Phishing: Why You and Your Organization Should Care

Daniela Oliveira
Associate Professor
Endowed IoT Term Professor
Department of Electrical and Computing Engineering
Florida Institute for Cyber Security
University of Florida

Technical Defenses



Behavioral malware detector

Organization perimeter

Network

Is the Organization’s Perimeter Safe?

Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting information and avoiding detection over time

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

Once in, the attackers stay "low and slow" to avoid detection.

They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

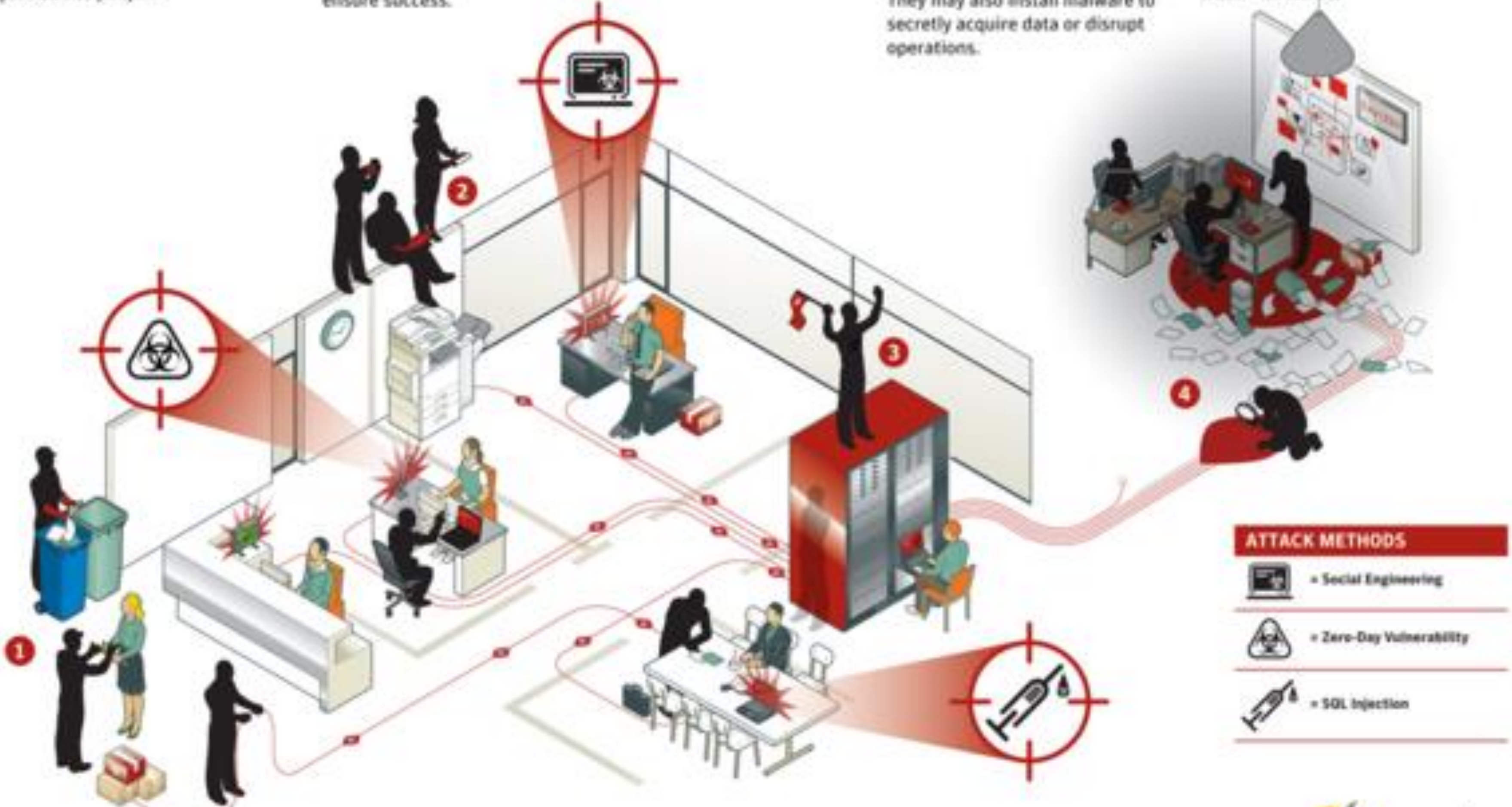
3. CAPTURE

Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



ATTACK METHODS

- = Social Engineering
- = Zero-Day Vulnerability
- = SQL Injection

Symantec.

Social Engineering

Picture credit: http://www.presidio-group.com/social-engineering-risk-real/

Influence

Social Engineering

Picture credit: http://www.presidio-group.com/social-engineering-risk-real/

Picture credit: http://www.dennisgoulet.us/2009/08/turkey-and-poults/

Picture credit: http://www.bbc.com/news/science-environment-35386042

Authority

Scarcity

Commitment

Liking

Reciprocation

Social Proof

Authority

Scarcity

Commitment/Consistency

Liking

Reciprocation

Social Proof

Influence Scenario

Lukas, 68, VP of Engineering of a large tech company

hobby: stamp collector

Wife Mia has public Facebook profile:

- disclosures family life
- mentions his hobby

Hi Lukas,

My name is Anna Freiling and I am in Mia's yoga class. She told me about your interest in stamps. My grandfather passed away recently and left me with a stamp collection from the 50s that I would like to sell. I have a website set up with pictures and prices, and if you would like to see it, please visit:

www.stampcollection.com

Thank you,
Anna

Hi Lukas,

My name is Anna Freiling and I am in Mia’s yoga class. She told me about your interest in stamps. My grandfather passed away recently and left me with a stamp collection from the 50s that I would like to sell. I have a website set up with pictures and prices, and if you would like to see it, please visit:

www.stampcollection.com

Thank you,
Anna

Scarcity

APT Incursion via Social Engineering

- Website seems legit, Lukas ends up installing malware in the organization’s computer.
- He never notices it, all technical lines of defense don’t catch it.
  - **APT in course!**

Far fetched??

Some stats or … Confessions of a Social Engineer (SE)

- 66% of attacks (especially in organizations) start with SE (online and offline)
- Personal and company social media are SE toolbox
- Professional SE can hack a company in less than 30 min after info gathering

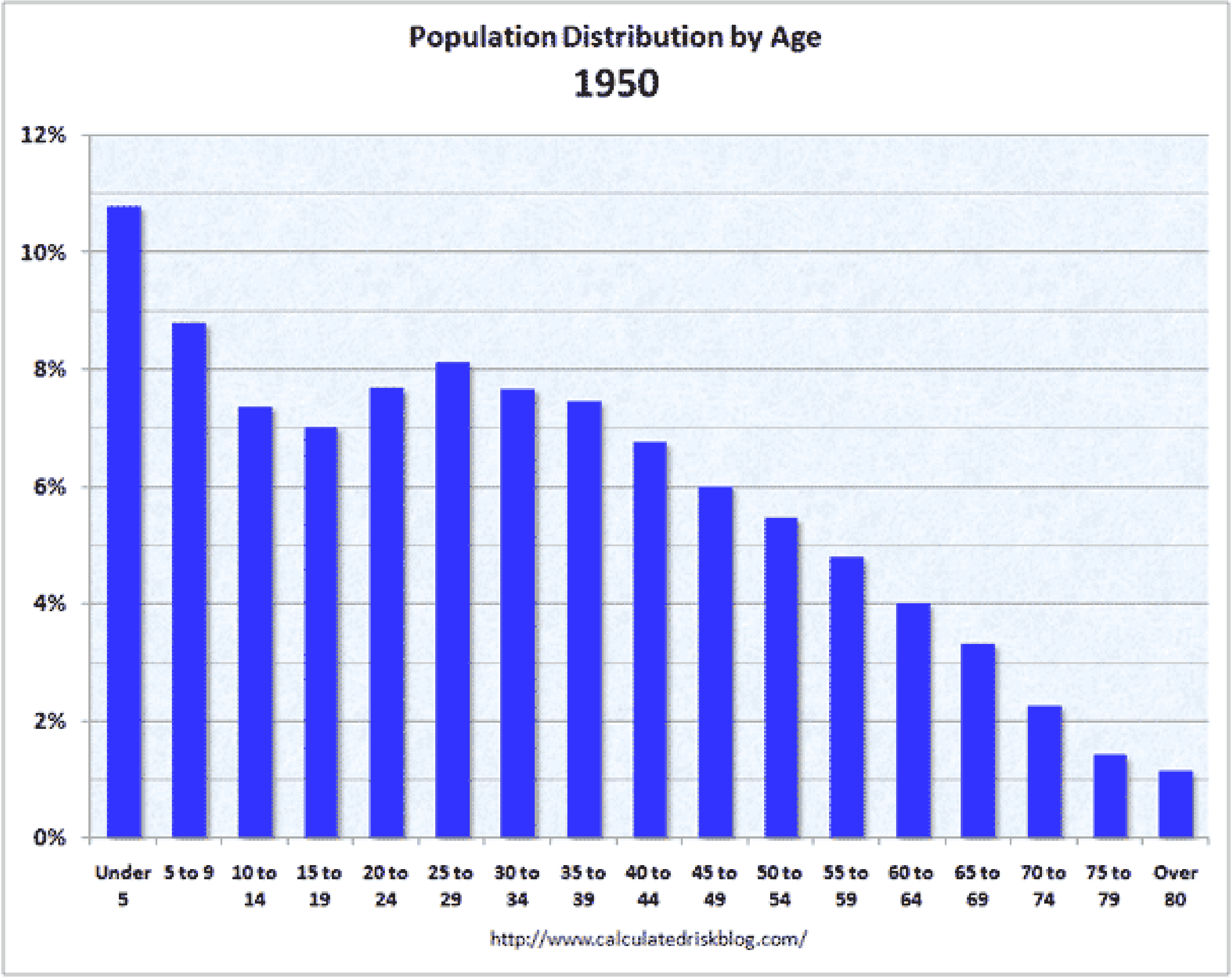
Rachel Tobac, social engineering contest DefcCon 2016 (2nd Place)

Source: Rachel Tobac. Hacking the Wetware: How a Noob Compromised 2 Companies with Social Engineering. Grace Hopper Celebration of Women in Computing 2017.

How susceptible are people?

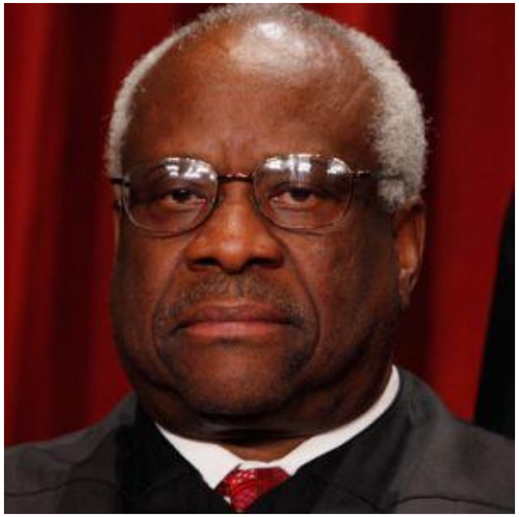
An analysis of phishing susceptibility

Case Study: Older vs Younger Adults

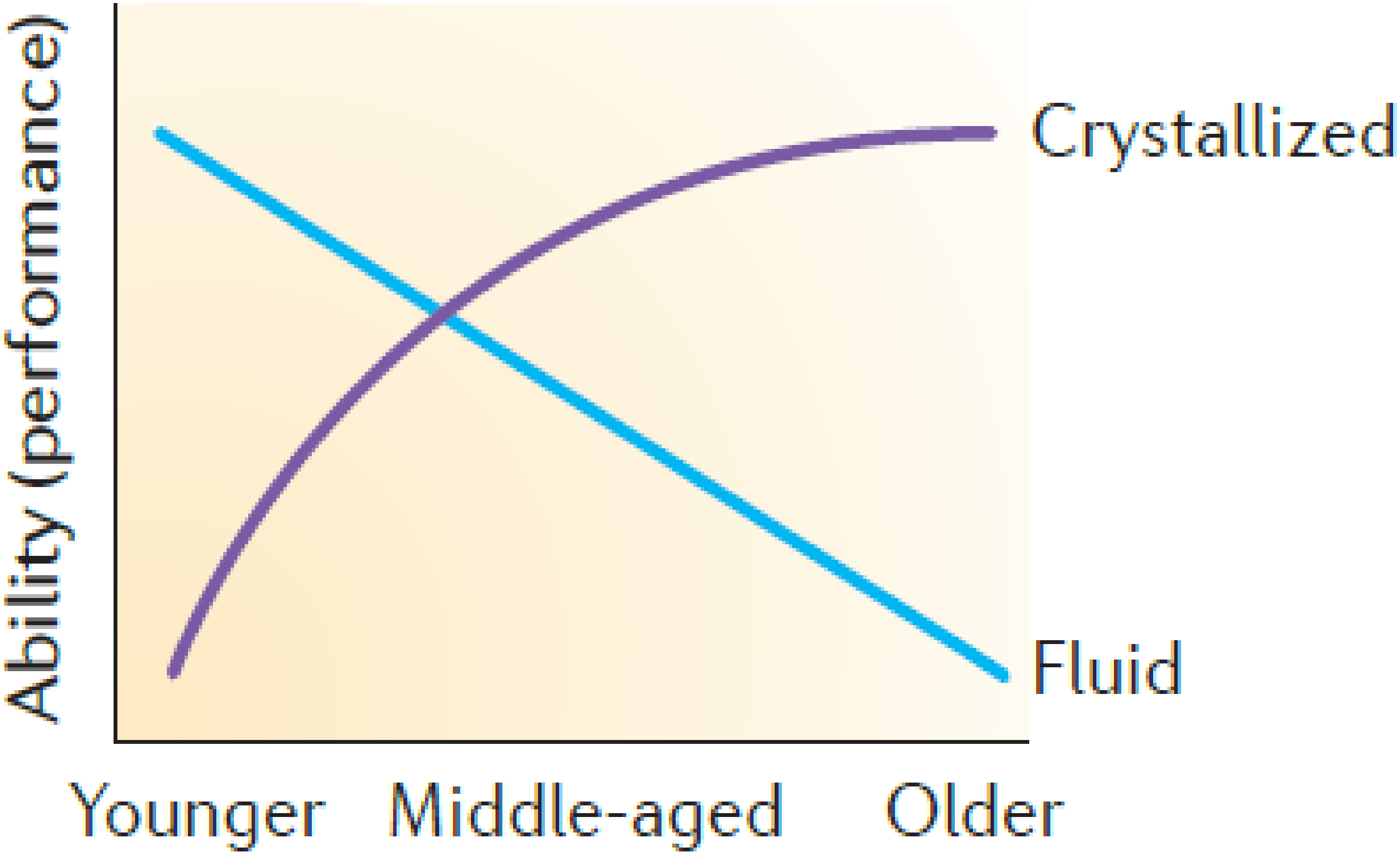


http://www.calculatedriskblog.com/

Census Bureau actual through 2010; projections through 2050



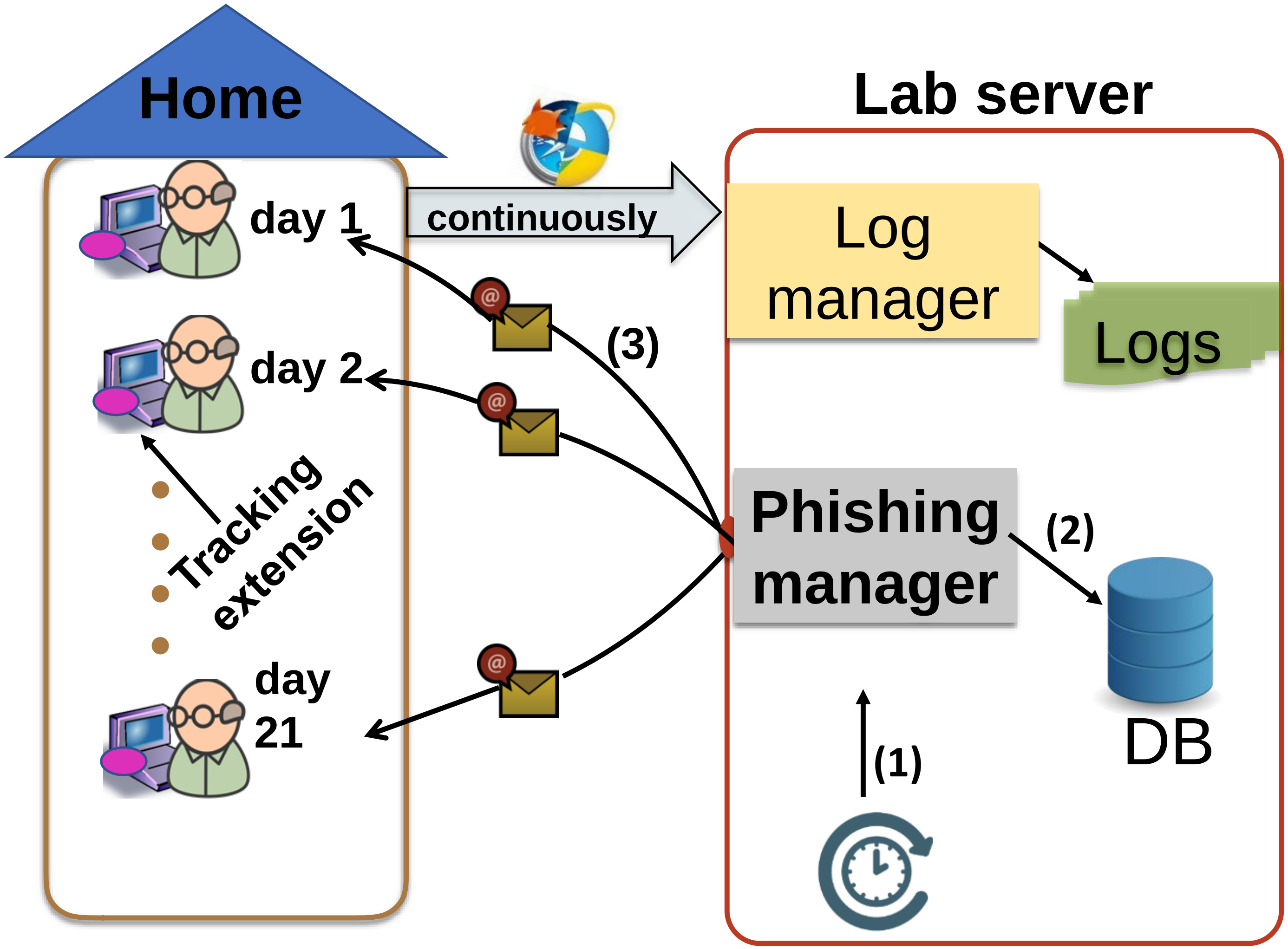
Cognitive change across adulthood



Agarwal et al., 2009; Samanez-Larkin & Knutson, 2015

The
Podesta
Emails

Behavioral Study on Phishing Susceptibility



Oliveira et. al. On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. ACM CHI'17

Study approved by UF IRB

Participants & Demographics

158 participants, North Central Florida, USA

	Younger Participants	Older Participants
N	99	59
% female	55.6	44.1
Age	**21.57 (3.80)**	**70.98 (8.30)**
Years of Education	**14.24 (3.57)**	**16.30 (2.79)**
Hrs of Exercise per week	5.40 (3.43)	8.84 (10.50)
Physical Health	7.72 (1.54)	7.53 (1.97)
Mental Health	**8.00 (1.52)**	**8.57 (1.50)**
Hrs on Internet per week	7.35 (2.90)	7.09 (2.98)

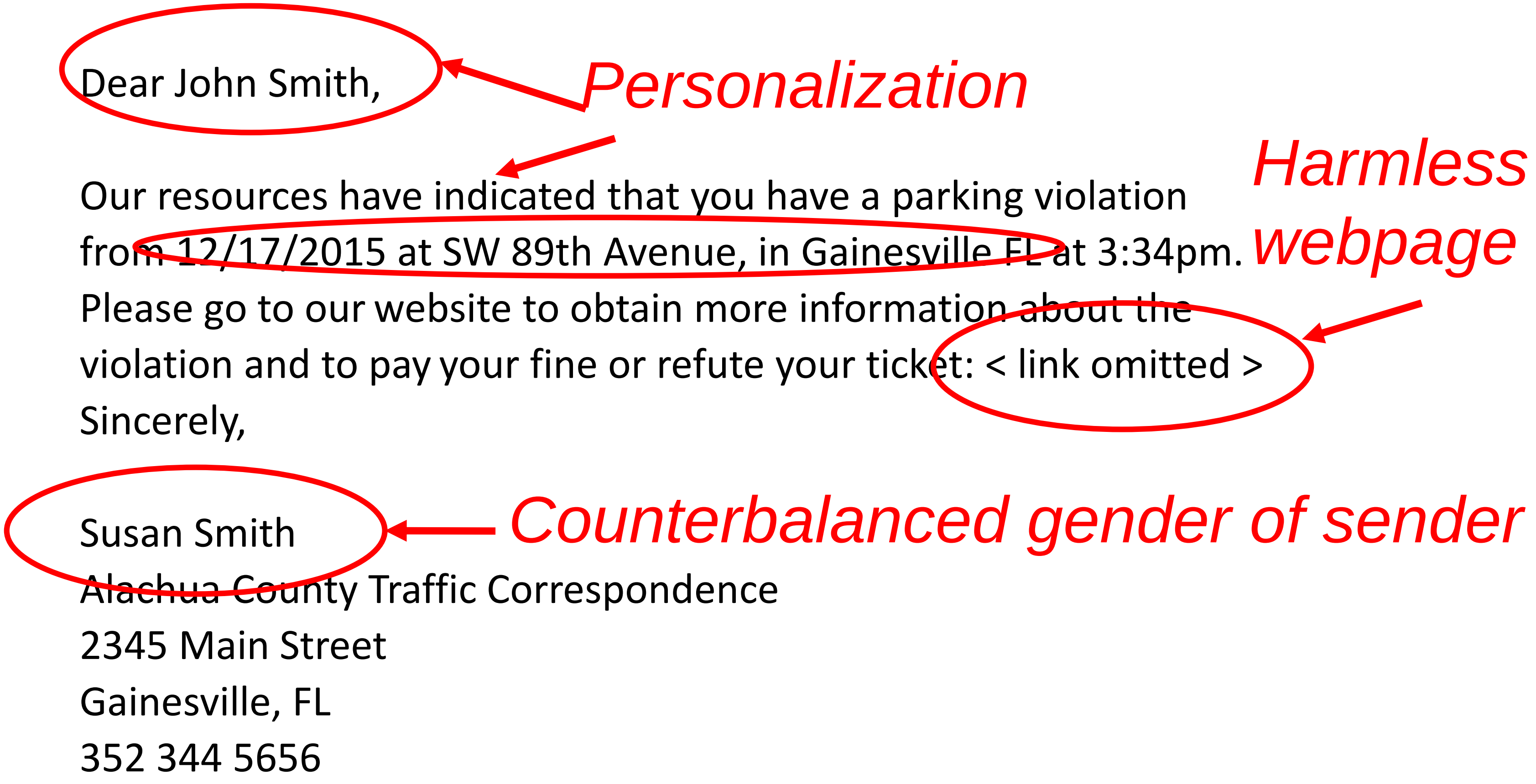
Note. **Bold** indicates significant age differences at *p* < .05.

Dear John Smith,

Our resources have indicated that you have a parking violation from 12/17/2015 at SW 89th Avenue, in Gainesville FL at 3:34pm. Please go to our website to obtain more information about the violation and to pay your fine or refute your ticket: < link omitted >
Sincerely,

Susan Smith
Alachua County Traffic Correspondence
2345 Main Street
Gainesville, FL
352 344 5656

Authority Weapon + Legal Life Domain



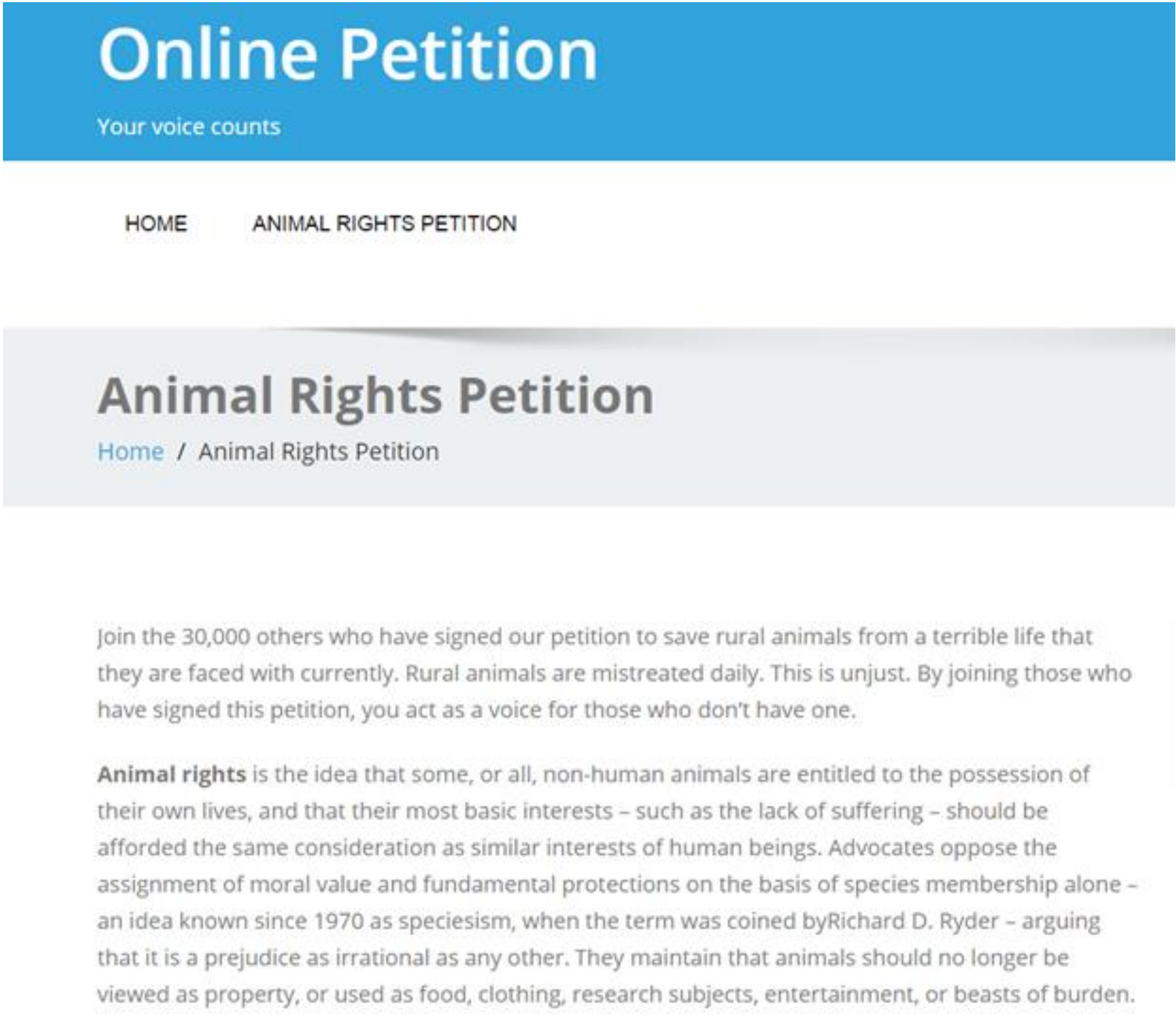
Dear John Smith,

Our resources have indicated that you have a parking violation from 12/17/2015 at SW 89th Avenue, in Gainesville FL at 3:34pm. Please go to our website to obtain more information about the violation and to pay your fine or refute your ticket: < link omitted >

Sincerely,

Susan Smith
Alachua County Traffic Correspondence
2345 Main Street
Gainesville, FL
352 344 5656

Authority Weapon + Legal Life Domain



Online Petition

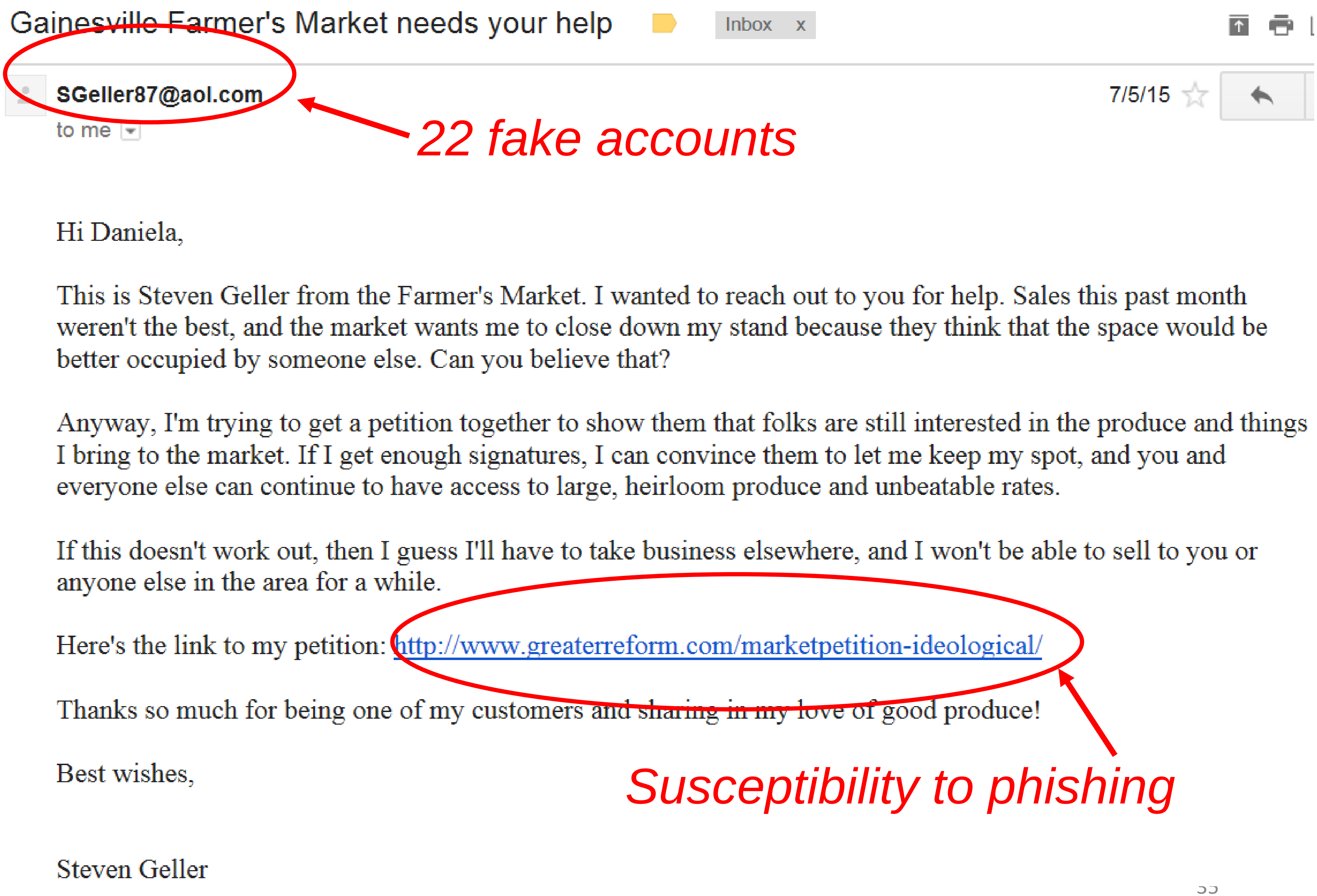
Your voice counts

Animal Rights Petition

Home / Animal Rights Petition

Join the 30,000 others who have signed our petition to save rural animals from a terrible life that they are faced with currently. Rural animals are mistreated daily. This is unjust. By joining those who have signed this petition, you act as a voice for those who don't have one.

Animal rights is the idea that some, or all, non-human animals are entitled to the possession of their own lives, and that their most basic interests – such as the lack of suffering – should be afforded the same consideration as similar interests of human beings. Advocates oppose the assignment of moral value and fundamental protections on the basis of species membership alone – an idea known since 1970 as speciesism, when the term was coined byRichard D. Ryder – arguing that it is a prejudice as irrational as any other. They maintain that animals should no longer be viewed as property, or used as food, clothing, research subjects, entertainment, or beasts of burden.



Gainesville Farmer's Market needs your help

SGeller87@aol.com

to me

7/5/15

22 fake accounts

Hi Daniela,

This is Steven Geller from the Farmer's Market. I wanted to reach out to you for help. Sales this past month weren't the best, and the market wants me to close down my stand because they think that the space would be better occupied by someone else. Can you believe that?

Anyway, I'm trying to get a petition together to show them that folks are still interested in the produce and things I bring to the market. If I get enough signatures, I can convince them to let me keep my spot, and you and everyone else can continue to have access to large, heirloom produce and unbeatable rates.

If this doesn't work out, then I guess I'll have to take business elsewhere, and I won't be able to sell to you or anyone else in the area for a while.

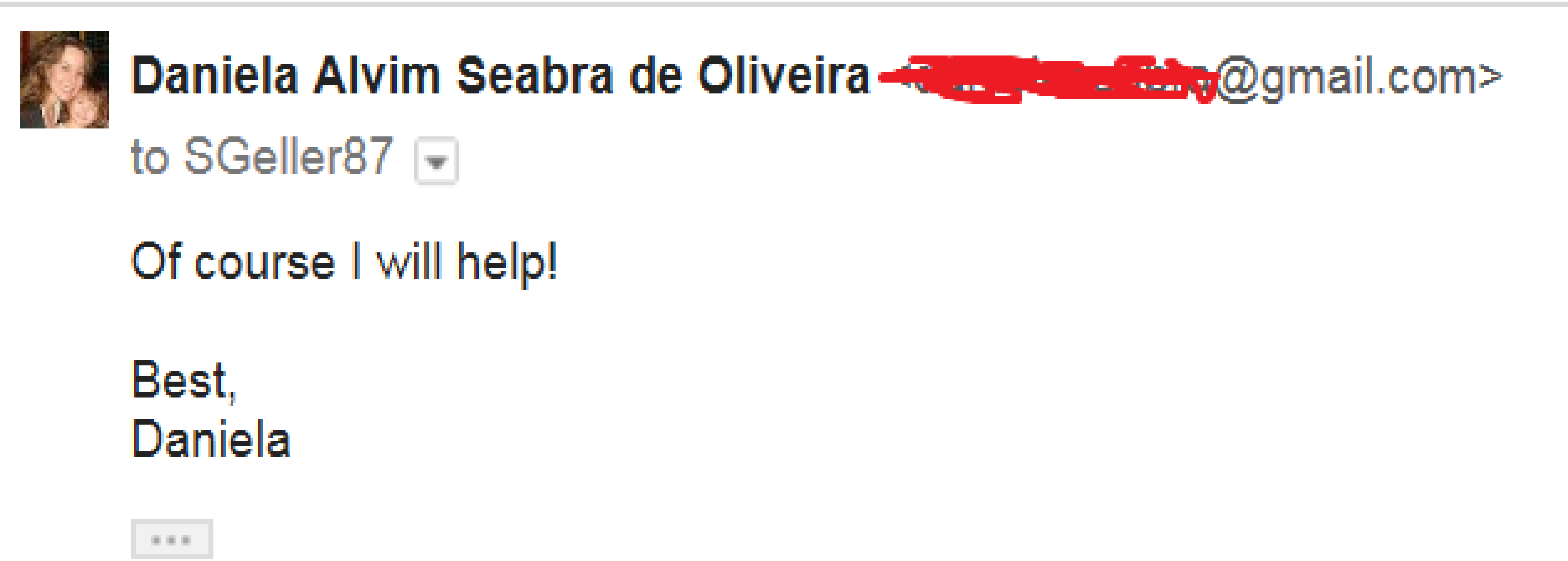
Here's the link to my petition: http://www.greaterreform.com/marketpetition-ideological/

Thanks so much for being one of my customers and sharing in my love of good produce!

Best wishes,

Susceptibility to phishing

Steven Geller



Daniela Alvim Seabra de Oliveira [redacted]@gmail.com>

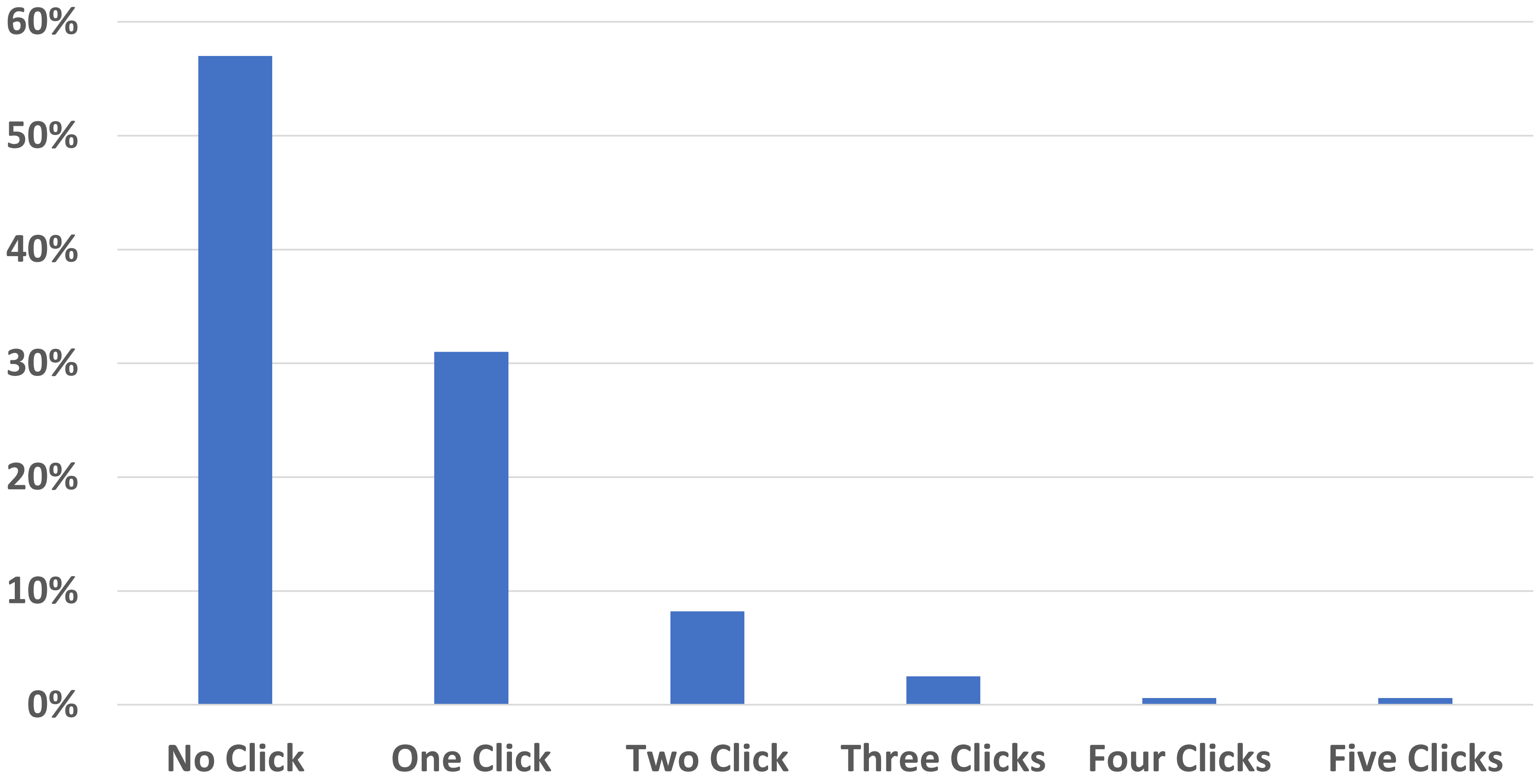
to SGeller87

Of course I will help!

Best,
Daniela

Overall Susceptibility

43% of participants fell for the emails at least once



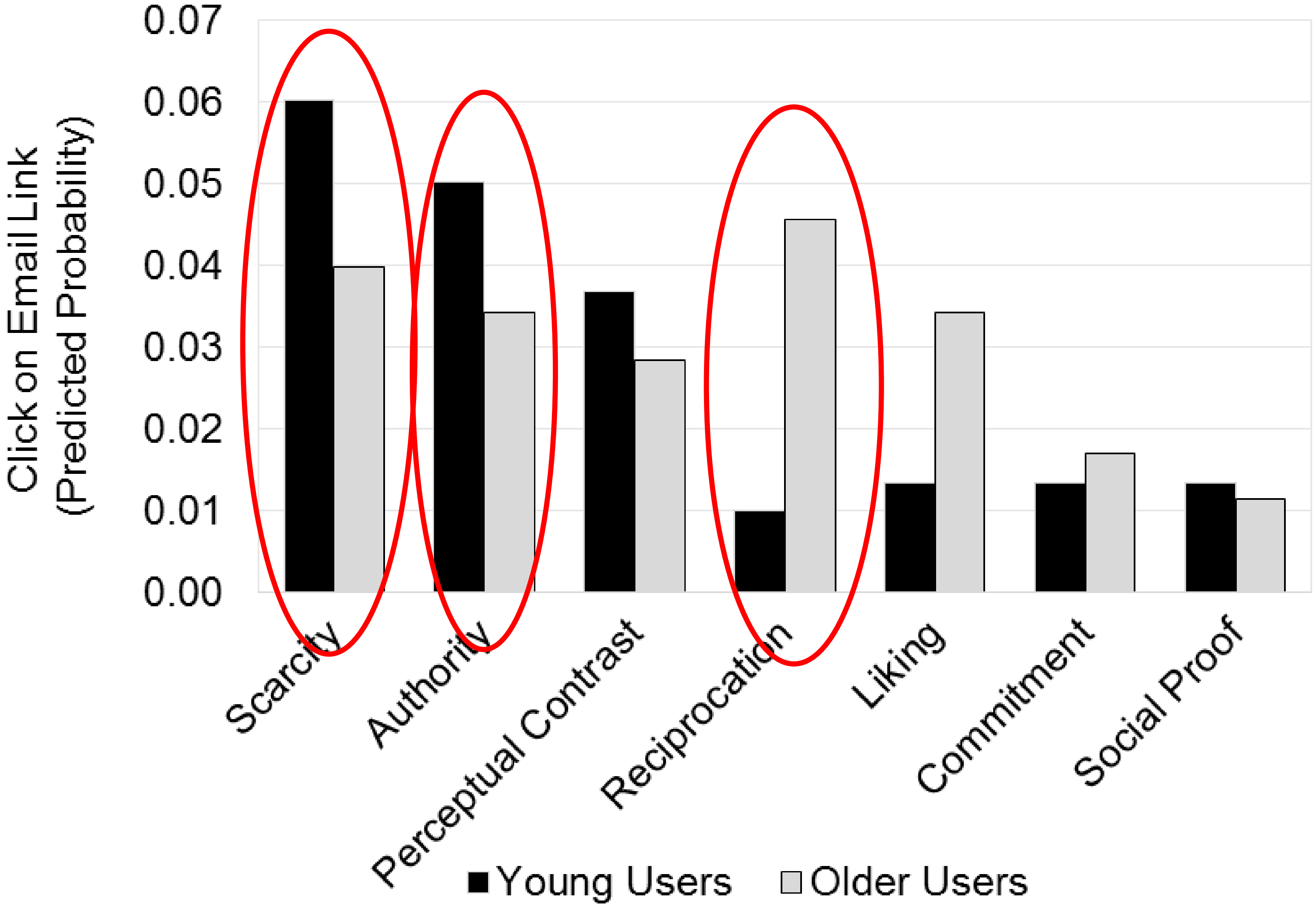
Older adults more susceptible than younger adults into falling for a phishing email

Probability of clicking in emails: 3.2% vs 2.9%

Huge effect for older women: the most susceptible group

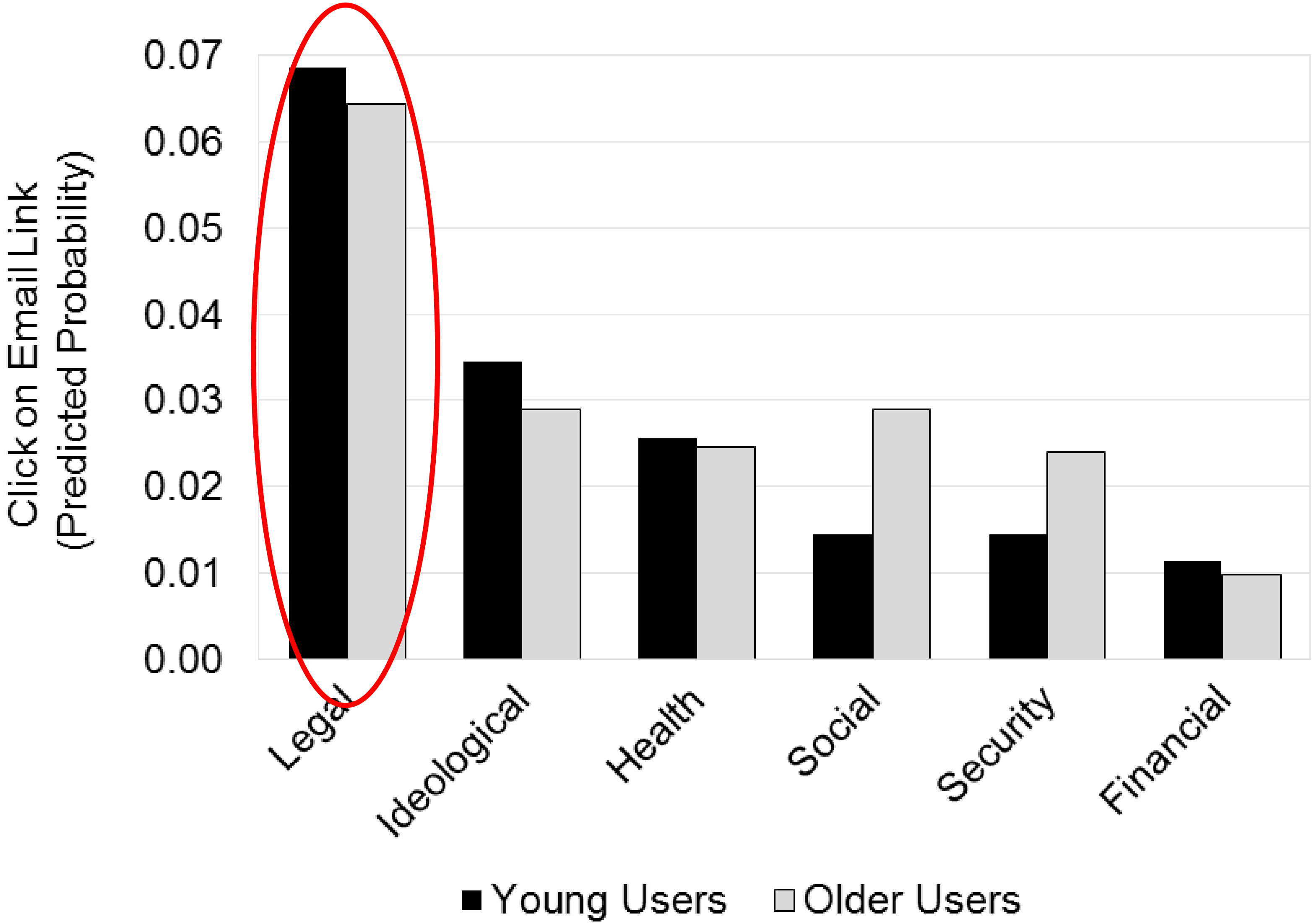
Multilevel logistic regression
(B = .98, z = 2.02, p = .04)

Weapons of Influence x Susceptibility



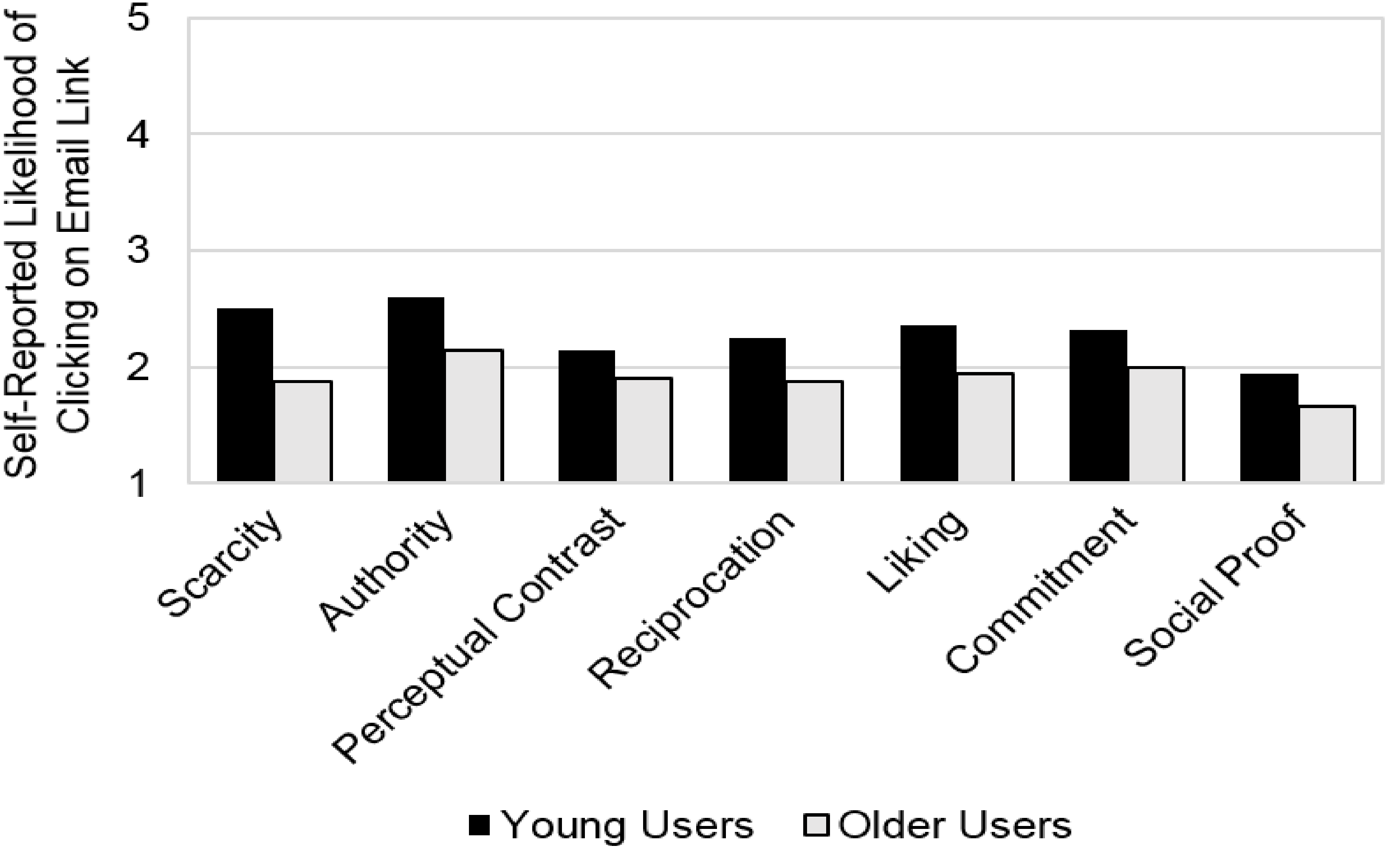
Multilevel logistic regression (B = .20, z = 2.03, p = .04)

Life Domains x Susceptibility



Multilevel logistic regression (B = -.41, z = -4.91, p <= .001)

Low Susceptibility Awareness, Particularly Among Older Users

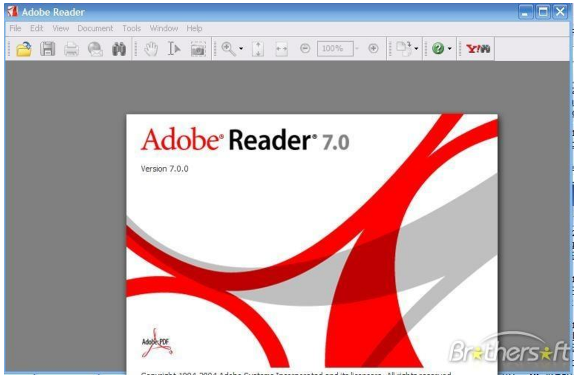


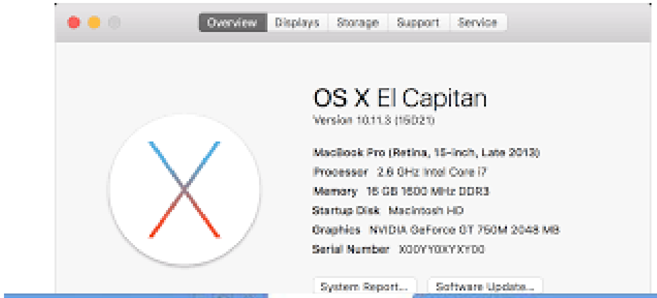
(B = -.78, z = -2.11, p = .035)

Concluding Remarks

What companies should know to protect themselves?

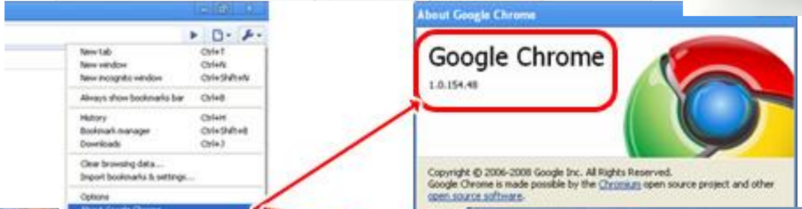
What Information SE Target?





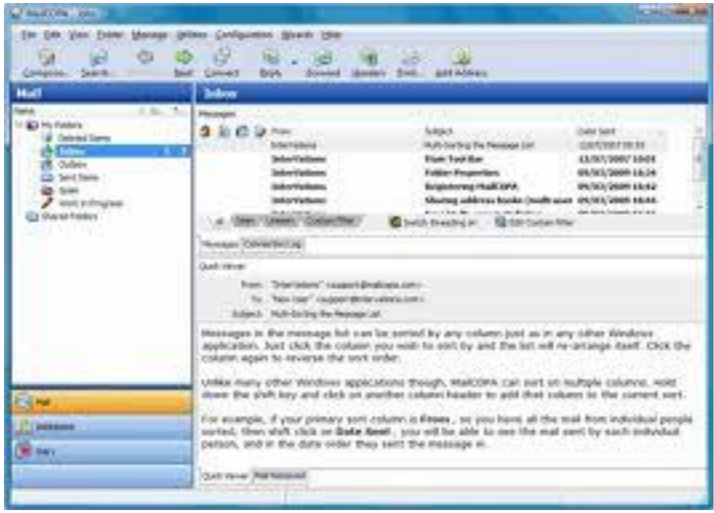
OS X El Capitan
Version 10.11.3 (15D21)

MacBook Pro (Retina, 15-inch, Late 2013)
Processor 2.6 GHz Intel Core i7
Memory 16 GB 1600 MHz DDR3
Startup Disk Macintosh HD
Graphics NVIDIA GeForce GT 750M 2048 MB
Serial Number X00YY0XYXYD0



Google Chrome
1.0.154.48

Copyright © 2006-2008 Google Inc. All Rights Reserved.
Google Chrome is made possible by the Chromium open source project and other open source software.

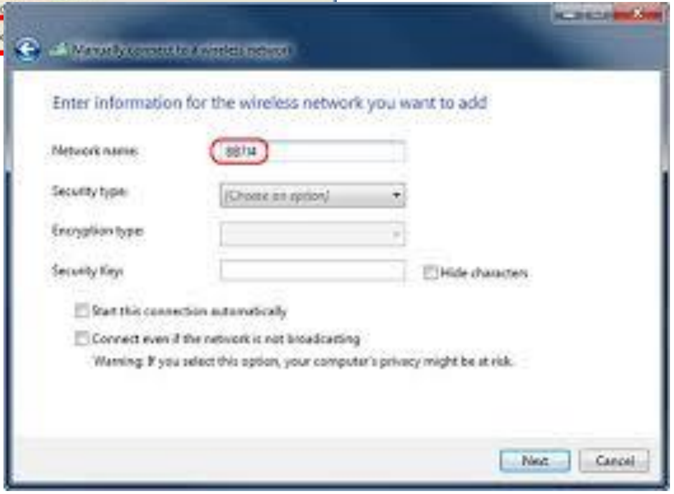


From: "InterVations" <support@mailcopa.com>
To: "New User" <support@intervations.com>
Subject: Multi-Sorting the Message List

Messages in the message list can be sorted by any column just as in any other Windows application. Just click the column you wish to sort by and the list will re-arrange itself. Click the column again to reverse the sort order.

Unlike many other Windows applications though, MailCOPA can sort on multiple columns. Hold down the shift key and click on another column header to add that column to the current sort.

For example, if your primary sort column is **From**, so you have all the mail from individual people sorted, then shift click on **Date Sent**, you will be able to see the mail sent by each individual person, and in the date order they sent the message in.



Enter information for the wireless network you want to add

Network name: 88714

Security type: [Choose an option]

Encryption type:

Security Key: ☐ Hide characters

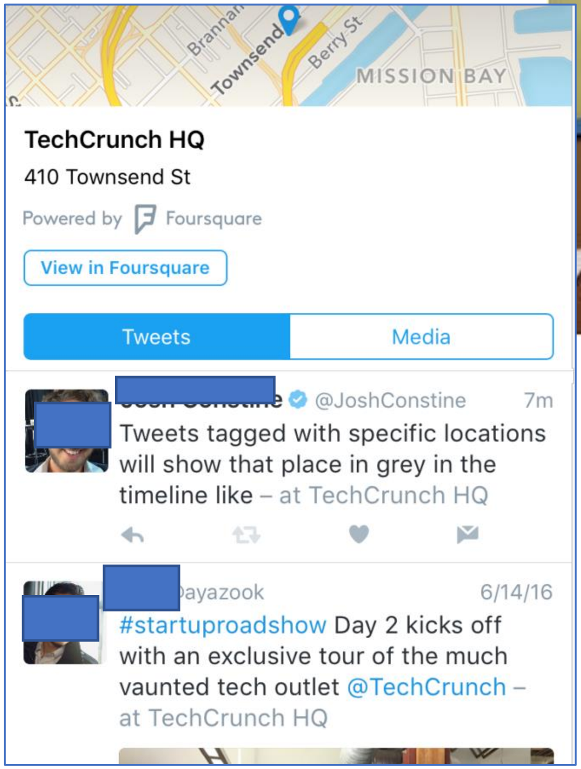
☐ Start this connection automatically

☐ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Source: Rachel Tobac. Hacking the Wetware: How a Noob Compromised 2 Companies with Social Engineering. Grace Hopper Celebration of Women in Computing 2017.

How Social Media is Used to Target Companies



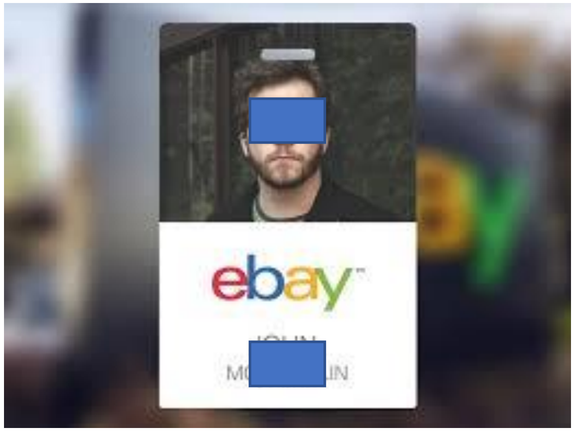
TechCrunch HQ
410 Townsend St

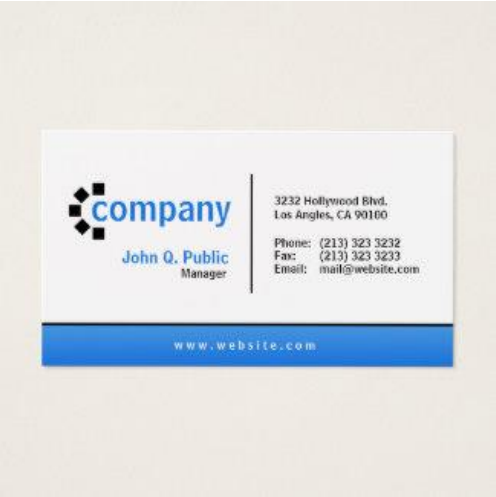
Powered by Foursquare

View in Foursquare

[redacted] @JoshConstine 7m
Tweets tagged with specific locations will show that place in grey in the timeline like – at TechCrunch HQ

[redacted]ayazook 6/14/16
#startuproadshow Day 2 kicks off with an exclusive tour of the much vaunted tech outlet @TechCrunch – at TechCrunch HQ





company
John Q. Public
Manager

3232 Hollywood Blvd.
Los Angeles, CA 90100

Phone: (213) 323 3232
Fax: (213) 323 3233
Email: mail@website.com

www.website.com

AXA
BARCLAYS CAPITAL
bhpbilliton
CHARTIS
CLEARCHANNEL
COMMERZBANK
COVIDIEN
DIAGEO
GLENCORE
groupm
ICAP
inova
JWT
Landor
lenovo
Linklaters
NORTON ROSE
QANTAS
REUTERS
RioTinto
SITA
Standard Chartered
TAG Heuer
Tenaris
TRAFIGURA
WPP

Source: Rachel Tobac. Hacking the Wetware: How a Noob Compromised 2 Companies with Social Engineering. Grace Hopper Celebration of Women in Computing 2017.

How do SE Find What They Need in Social Media?

- Instagram: geotag searching, hashtag searching
- Facebook: https://searchisback.com - Facebook Dorking
- Twitter: hashtag and picture searching
- Linkedin: vendor tags and photos
- Indeed/Glassdoor: reviews and photos
- Quora/Reddit: tell all

Source: Rachel Tobac. Hacking the Wetware: How a Noob Compromised 2 Companies with Social Engineering. Grace Hopper Celebration of Women in Computing 2017.

How do SE Pick Their Targets?

- Collect any phone numbers they can find
- 3rd party vendors posting and tagging your company and your employees
- C-level management: You are a target!
- Employees posting on social media about your company

Source: Rachel Tobac. Hacking the Wetware: How a Noob Compromised 2 Companies with Social Engineering. Grace Hopper Celebration of Women in Computing 2017.

Female SE – High success rates

- https://youtu.be/_isu6fx3QwI

Interventions

Anti-Phishing Training

Phishing Warnings

Anti-Phishing Guidelines

Credit: http://www.kaptest.com/blog/bar-exam-insider/2016/05/31/one-size-does-not-fit-all-when-it-comes-to-studying-for-the-bar-exam/

Our Group’s Future Work

Natural Language Processing to detect influence in emails

Warnings about cues to deception in email in an age-targeted fashion

Acknowledgements

- Dr. Natalie Ebner (Associate Professor of Psychology, UF - Collaborator, co-PI)
- Tian Lin (Postdoc, Dept. of Psychology, UF)
- Research Assistants (ECE and Psychology Depts.):
  - Donovan Ellis
  - Sandeep Dommaraju
  - Harold Rocha
  - Huizi Yang
  - Melis Muroglodu
  - Devon Weir
  - Adam Soliman

Vielen Dank!

daniela@ece.ufl.edu