

Cyber Social Engineering: Why You Should Care and Implications for Democracy

Daniela Oliveira

Associate Professor

Endowed IoT Term Professor

Department of Electrical and Computing Engineering

Florida Institute for Cyber Security

University of Florida



Social Engineering

Influence



Social Engineering





Authority

Scarcity

Commitment

Liking

Reciprocation

Social Proof

Authority





Commitment/Consistency



Liking



Reciprocation



Social Proof



Influence Scenario Compromising Democracy

Bob Harris, 68, Chairman of the 2020 Anna Smith Campaign



hobby: stamp collector

Daughter Alice has public Facebook
profile:

- disclosures family life
- mentions his hobby in a comment in
a post





Dear Mr. Harris,

My name is Eve Johnson and I am in your daughter Alice'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,
Eve*



Dear Mr. Harris,

My name is Eve Johnson and I am in your daughter Alice'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,
Eve*

Scarcity

Incursion via Social Engineering



- Bob ends up installing malware in the campaign headquarters computer.

Sensitive emails from Anna Smith and her staff leaked to the public damaging her reputation

Far fetched??

#CYBER RISK APRIL 26, 2017 / 5:53 AM / 5 MONTHS AGO

Macron campaign confirms phishing attempts, says no data stolen

Michel Rose, Eric Auchard

5 MIN READ



PARIS/FRANKFURT (Reuters) - French presidential candidate Emmanuel Macron's campaign team confirmed on Wednesday that his party had been the target of a series of attempts to steal email credentials since January but that they had failed to compromise any campaign data.



Secure
<https://www.ncsc.gov.uk/guidance/phishing-guidance-political-parties-and-their-staff>

National Cyber Security Centre
a part of GCHQ

We are using cookies to give you the best experience on our site. By continuing to use our website without changing the settings, you are agreeing to our use of cookies.

GuidanceThreatsIncident ManagementMarketplaceEducation & ResearchInsights

Published guidanceInfographicsNCSC glossary

Home > Guidance > Published guidance

Guidance

Phishing: guidance for political parties and their staff

Created: 15 May 2017
Updated: 15 May 2017

How to detect phishing attacks, and preventative measures that can reduce the likelihood of you becoming the victim of one.

The Podesta Emails

FOOTBALLSPORTTV & SHOWBIZNEWSFABLEDOOSMONEY

All NewsUK NewsUS NewsWorld NewsPoliticsOpinion

MAYBELLINE

MASTERPRECISE.inkMETALLIC LIQUID EYELINER24 HR BUDGEPROOF WEAR

Metallic Liqu...★★★★\$5.99

MPS GET HACKED All politicians are warned over cyber-security after phishing attacks target MPs

A number of MPs were sent phishing emails by hackers attempting to steal personal information

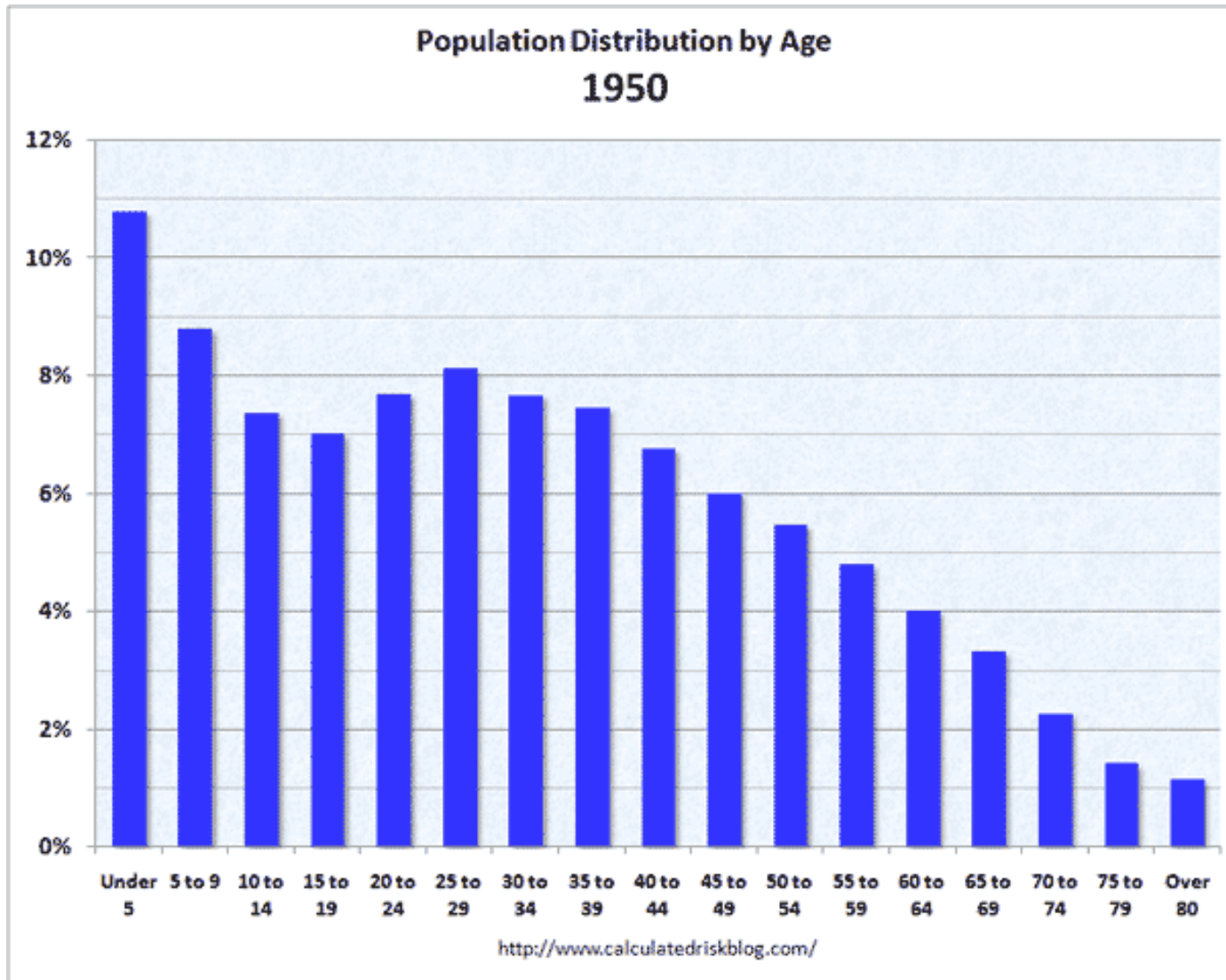
By Huao Gve



How susceptible are people?

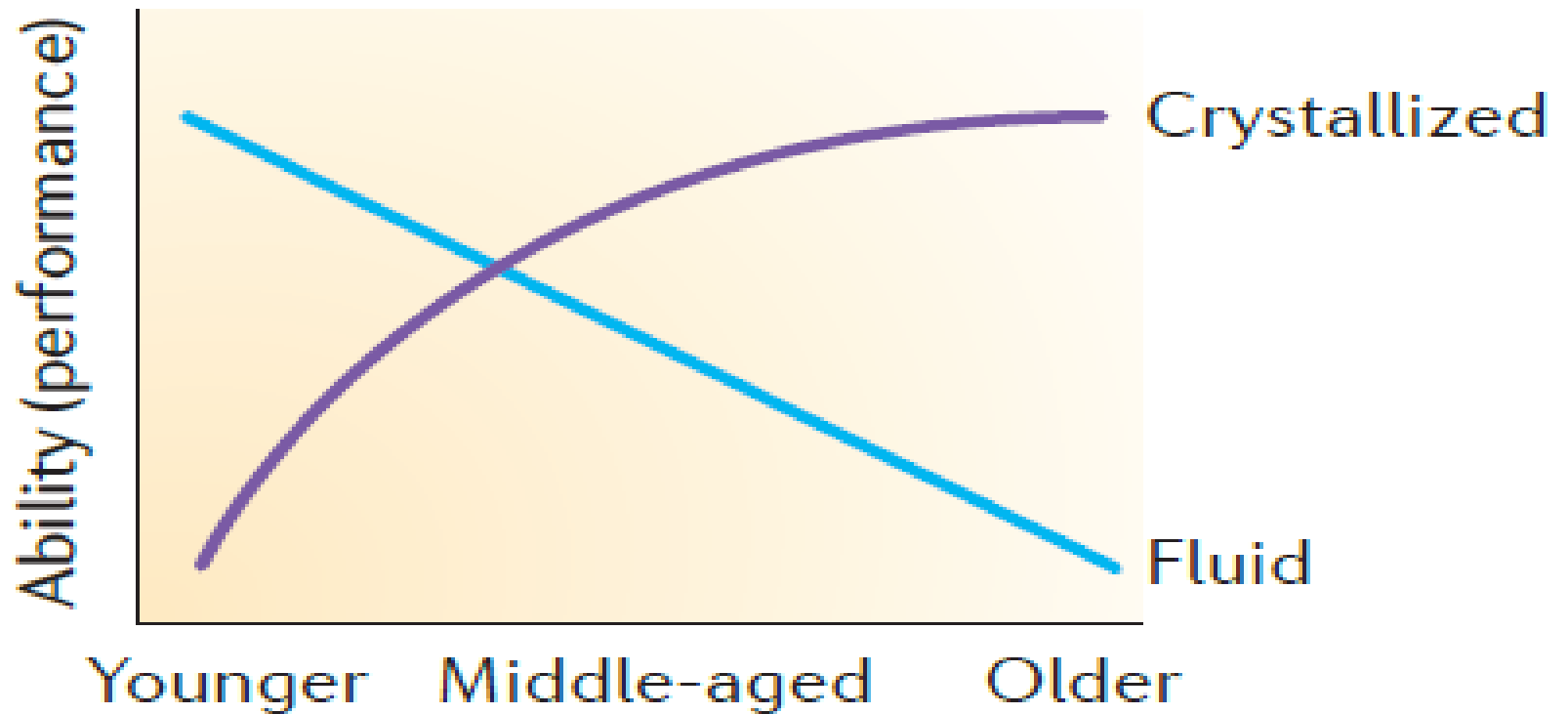
An analysis of phishing susceptibility

Case Study: Older vs Younger Adults

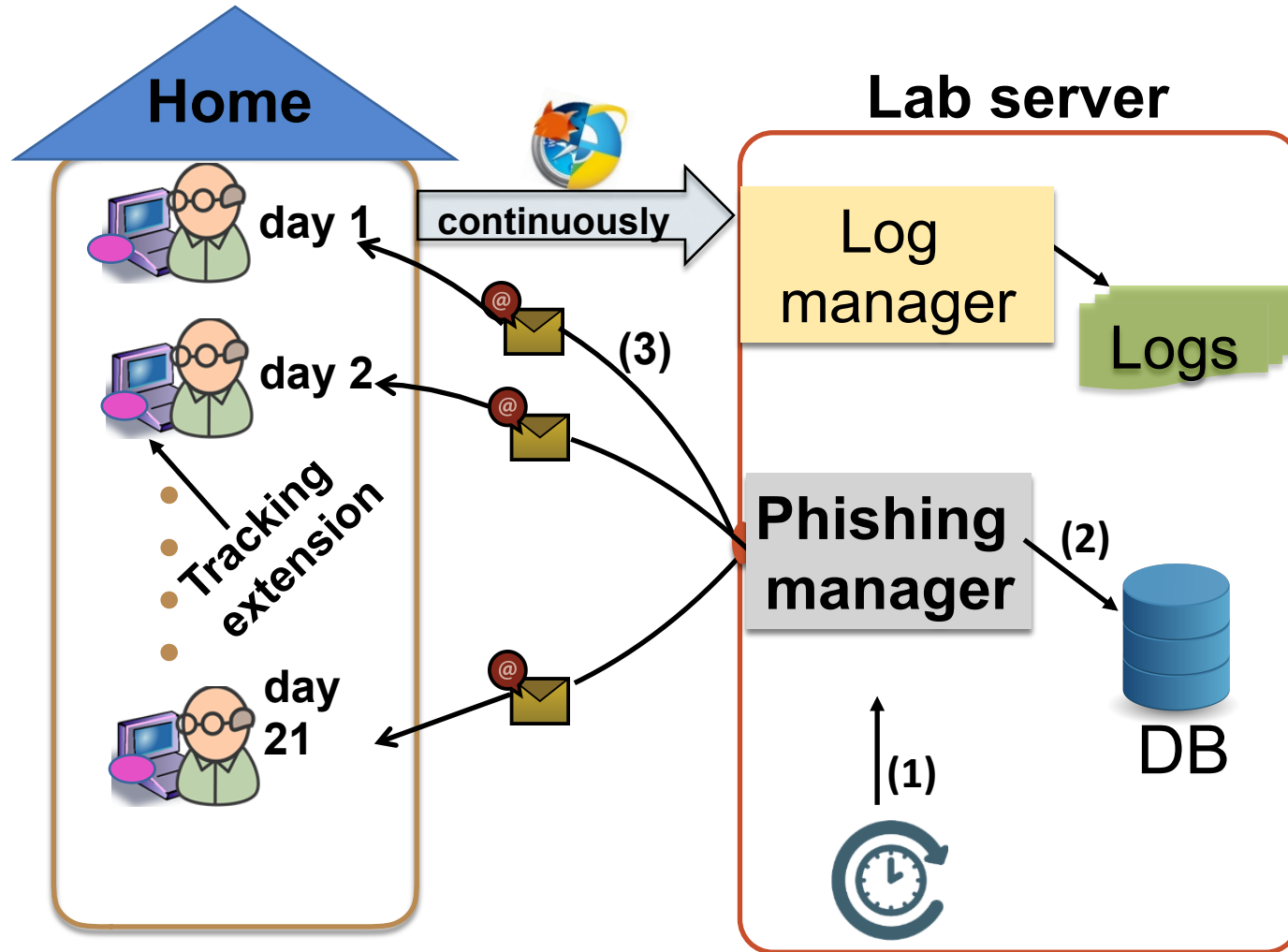




Cognitive change across adulthood



Behavioral Study on Phishing Susceptibility



Participants & Demographics

158 participants – North Central Florida

	Young 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,

Personalization

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,

*Harmless
webpage*

Susan Smith

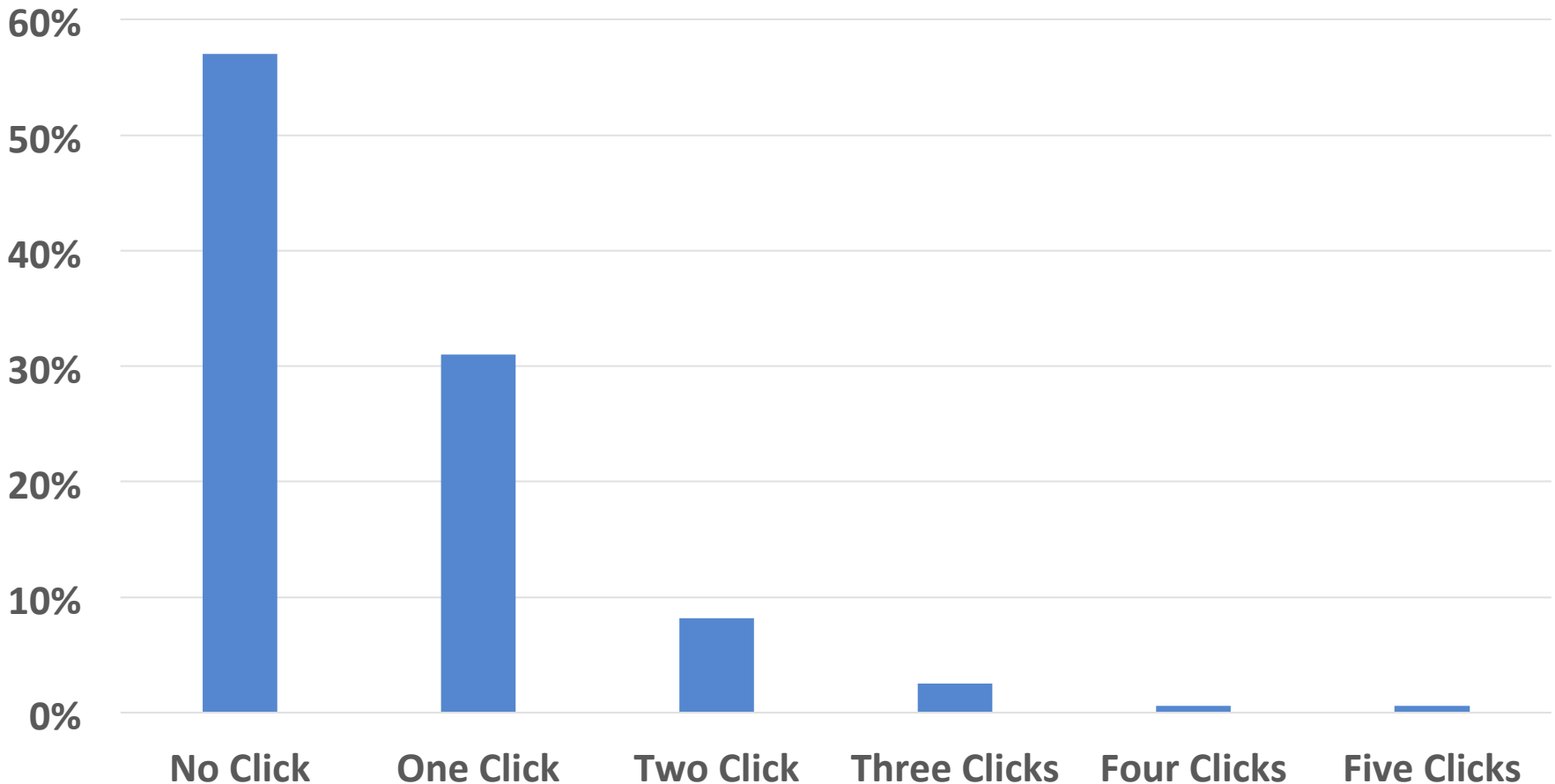
Counterbalanced gender of sender

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

Authority Weapon + Legal Life Domain

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

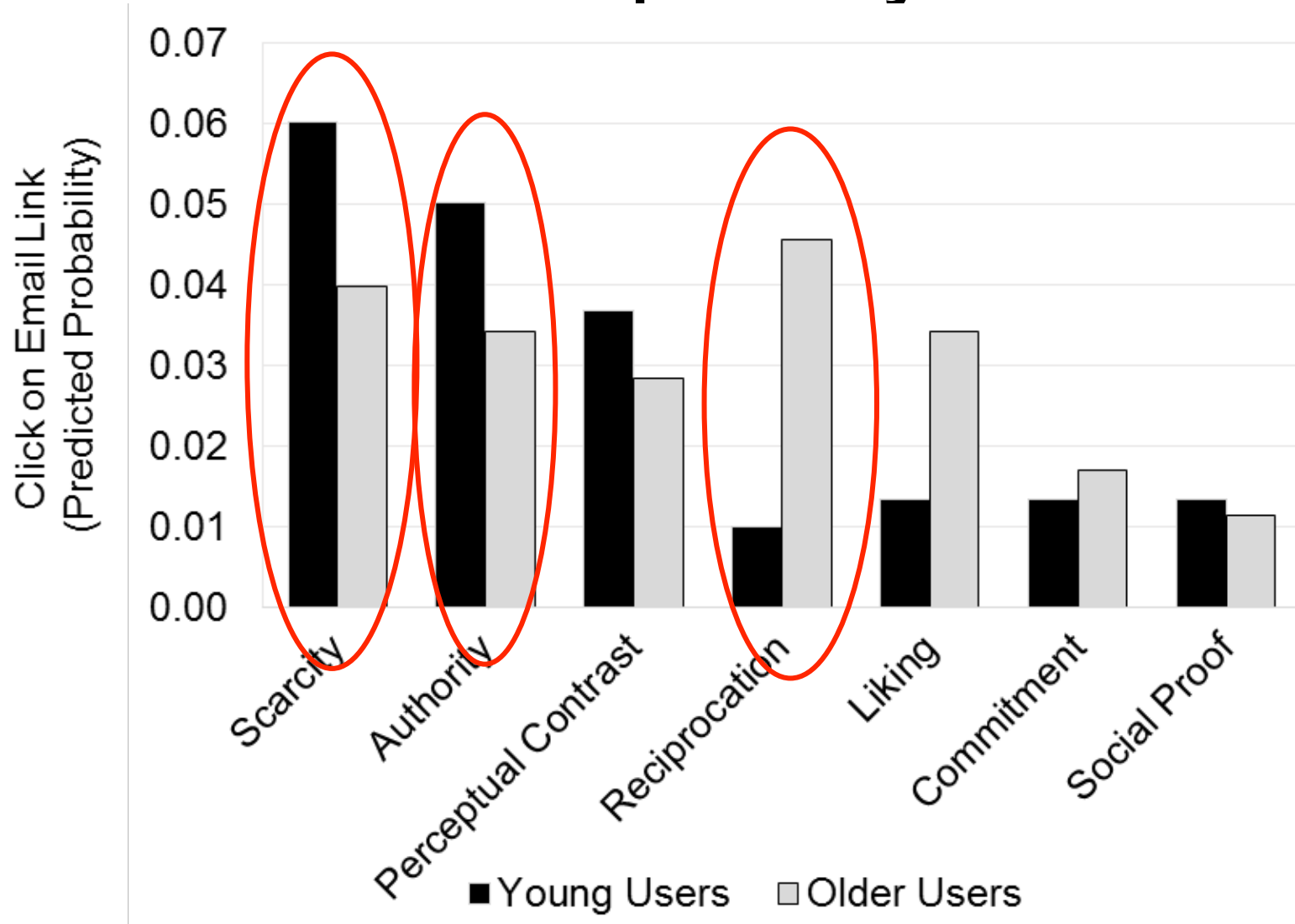
Probability of clicking in emails: 3.2% vs 2.9%

Huge effect for older women: the most susceptible group

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

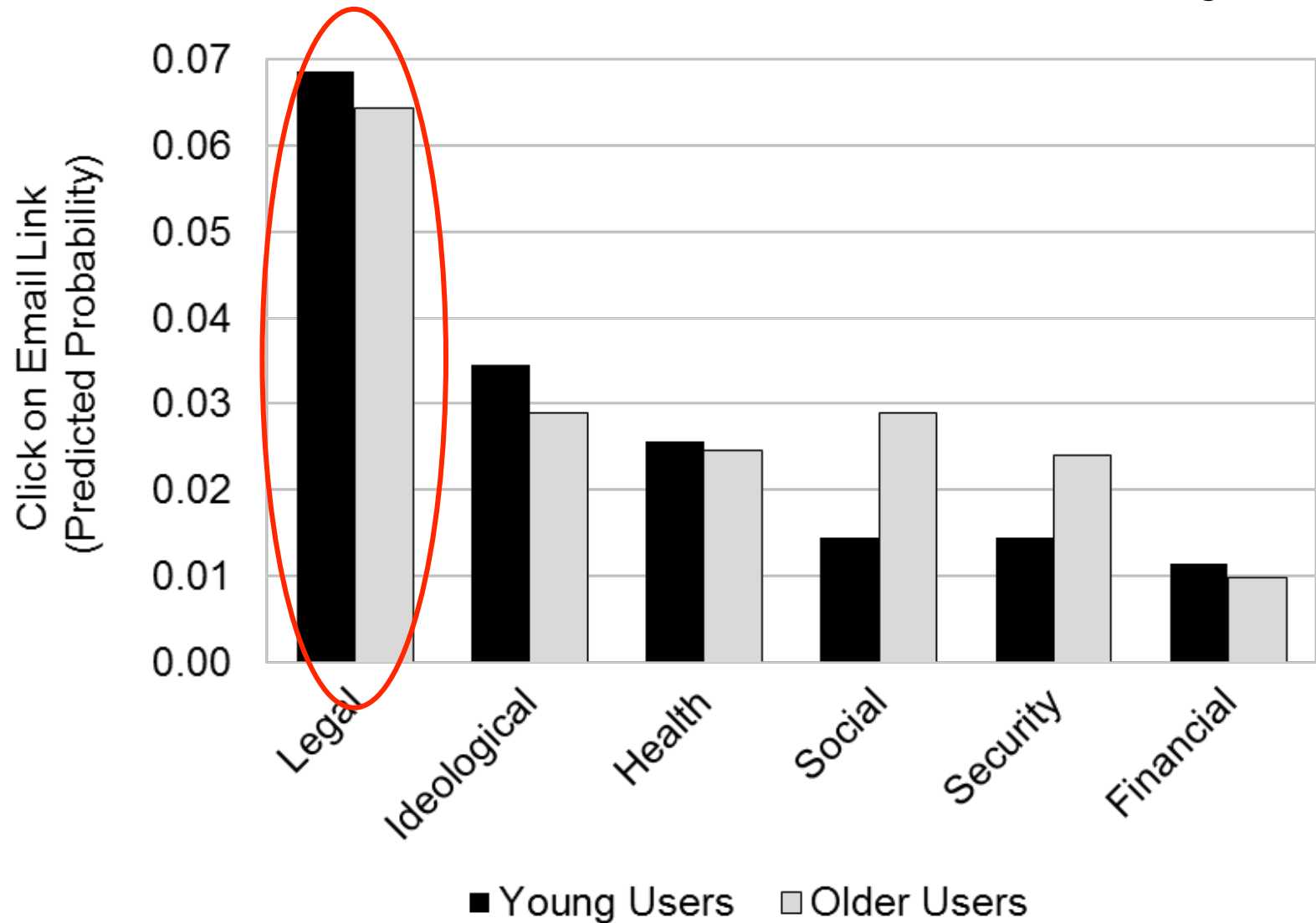


Weapons of Influence x Susceptibility



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

Life Domains x Susceptibility



Interventions

Anti-
Phishing
Training

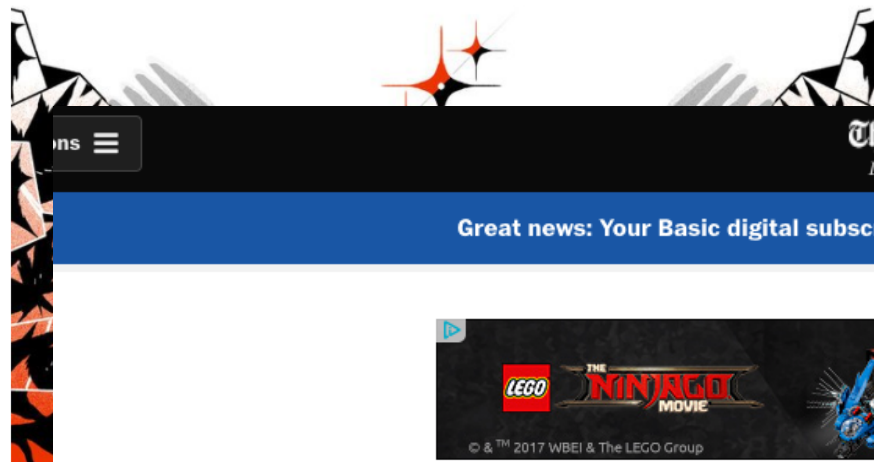


Anti-Phishing
Guidelines

The new frontier: Influencing voter's opinion

FRANK BRUNI
To Serve Is to Sl

By NINA JANKOWICZ SEPT. 25, 2017

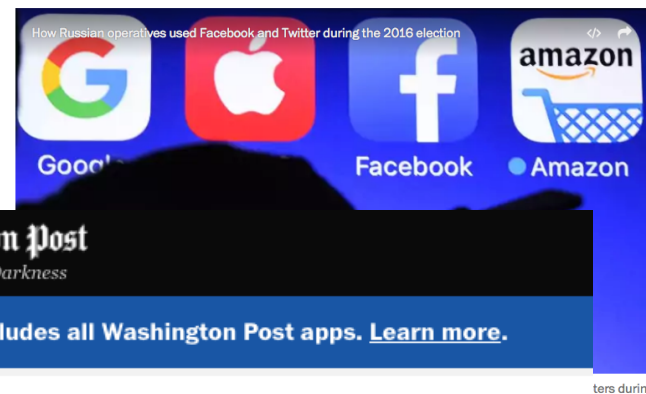


Nick Ily

Obama tried to give Zuckerberg a wake-up call over fake news on Facebook

1.20% ANNUAL PERCENTAGE YIELD
ON ALL BALANCE TIERS

ally. DO IT RIGHT.
LEARN MORE
ALLY BANK, MEMBER FDIC



ters during

Do You
Speed

Russian operatives used Facebook ads to exploit America's racial and religious divisions

Thank you!

daniela@ece.ufl.edu

Backup Slides

Gainesville Farmer's Market needs your help

Inbox x



SGeller87@aol.com

7/5/15 ☆



to me ▾

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 ~~XXXXXXXXXX@gmail.com~~@gmail.com>

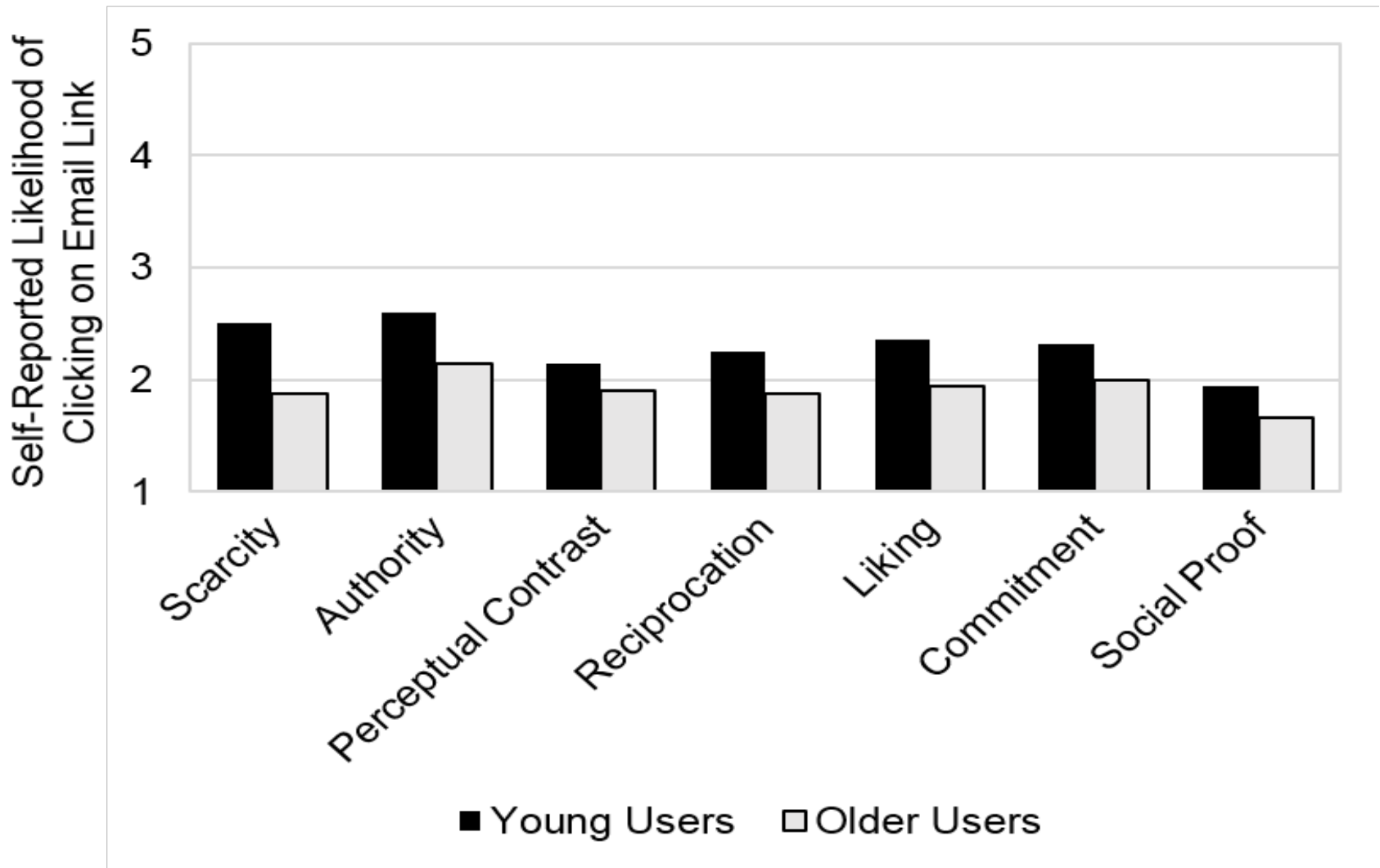
to SGeller87 

Of course I will help!

Best,
Daniela



Low Susceptibility Awareness, Particularly Among Older Users



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

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

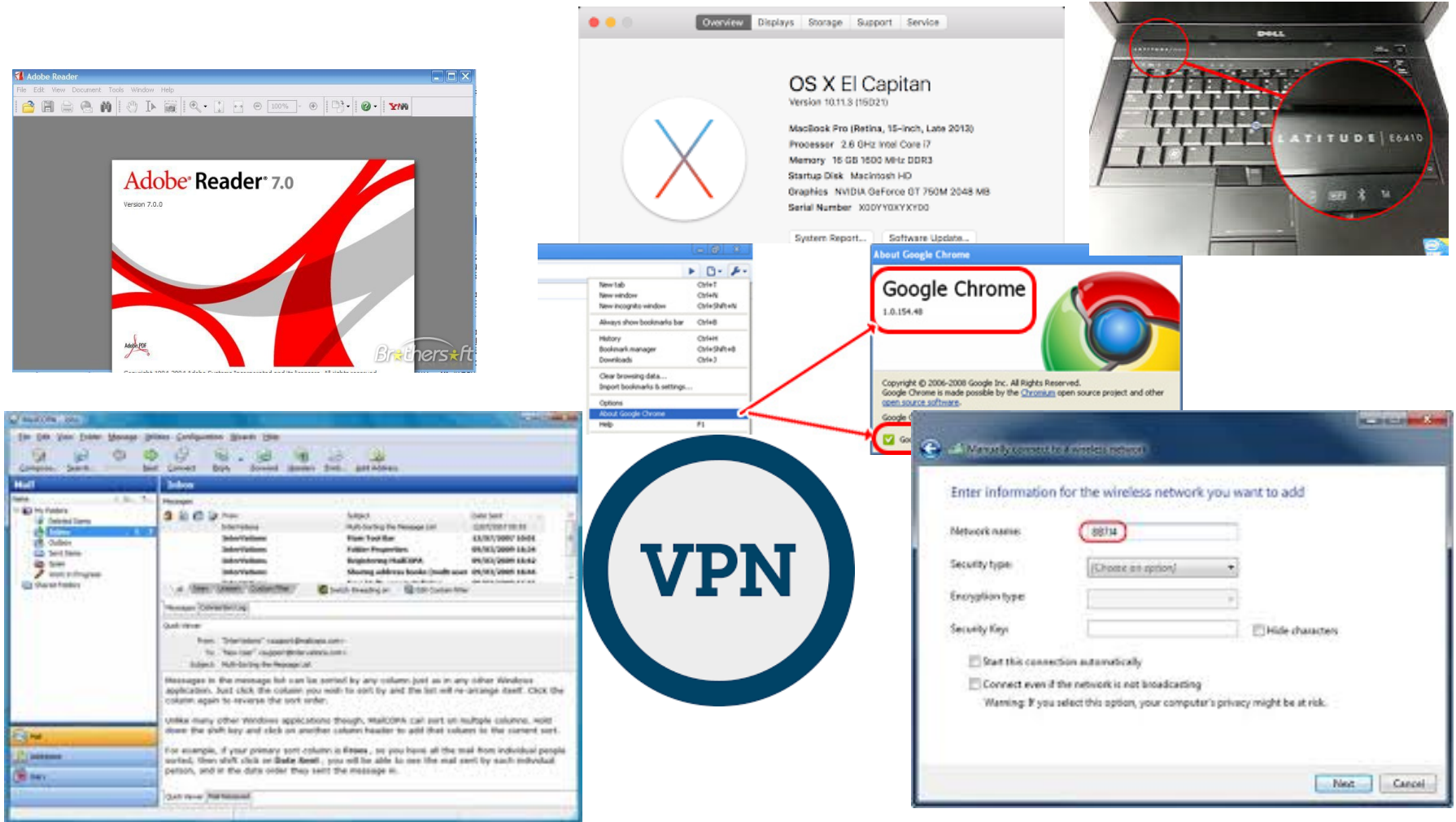
Rachel Tobac, social engineering contest DefcCon 2016 (2nd Place)



How do SE Find What They Need in Social Media?

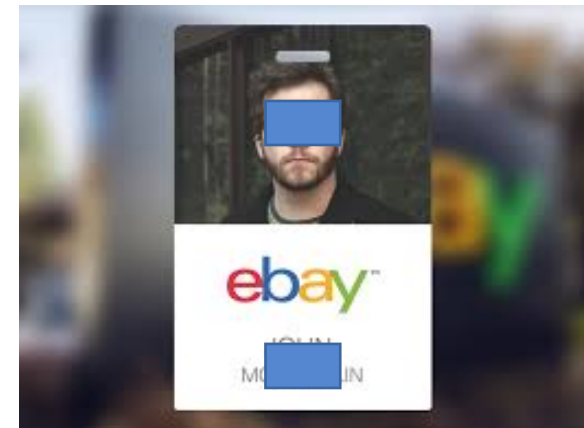
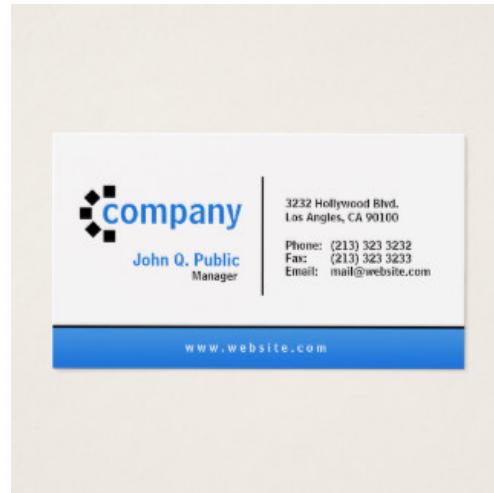
- Instagram: geotag searching, hashtag searching
- Facebook: <https://searchisback.com> - Facebook Dorking
- Twitter: hashtag and picture searching
- LinkedIn: tags and photos
- Request by “females” : high success rate

What Information SE Target?



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



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

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

Female SE – High success rates

- [https://youtu.be/ isu6fx3Qwl](https://youtu.be/isu6fx3Qwl)

ONE SIZE DOES NOT FIT ALL

Non lavare in lavatrice
resistente agli strappi

Phishing Warnings

Anti-Phishing Training

Anti-Phishing Guidelines

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

