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

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/
Authority
Scarcity
Commitment
Liking
Reciprocation
Social Proof
Authority
Scarcity
Commitment/Consistency

A Global Petition By Animal Lovers
STOP ANIMAL ABUSE
PETFINDER.MY
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
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??
Macron campaign confirms phishing attempts, says no data stolen

Michel Rose, Eric Auchard

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.
How susceptible are people?

An analysis of phishing susceptibility
Case Study: Older vs Younger Adults

Population Distribution by Age
1950

[Bar chart showing population distribution by age in 1950]

Census Bureau actual through 2010; projections through 2050
Cognitive change across adulthood

Ability (performance)

Crystallized

Fluid

Younger  Middle-aged  Older

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

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

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
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 ($B = -.41$, $z = -4.91$, $p \leq .001$)
Interventions

- Anti-Phishing Training
- 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/
The new frontier: Influencing voter’s opinion
The Only Way to Defend Against Russia’s Information War

By NINA JANKOWICZ  |  SEPTEMBER 25, 2017

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

Russian operatives used Facebook ads to exploit America’s racial and religious divisions
Thank you!

daniela@ece.ufl.edu
Backup Slides
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,

Steven Geller
Daniela Alvim Seabra de Oliveira <daniela.sav@gmail.com> to SGeller87

Of course I will help!

Best,
Daniela
Low Susceptibility Awareness, Particularly Among Older Users

\[(B = -0.78, z = -2.11, p = 0.035)\]
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 DefCon 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?

How Social Media is Used to Target Companies

How do SE Find What They Need in Social Media?

- Instagram: geotag searching, hashtag searching
- Facebook: [https://searchisback.com](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
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