Exploiting Curiosity and Context

How to make people click on a dangerous link despite their security awareness

Zinaida Benenson

zinaida.benenson@fau.de

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

- Joint work with
  - Freya Gassmann, University of Saarland, Germany
  - Robert Landwirth, FAU of Erlangen-Nuremberg, Germany
- Acknowledgments for data gathering and analysis
  - Nadina Hintz, Andreas Luder, Anna Girard, Gaston Pugliese

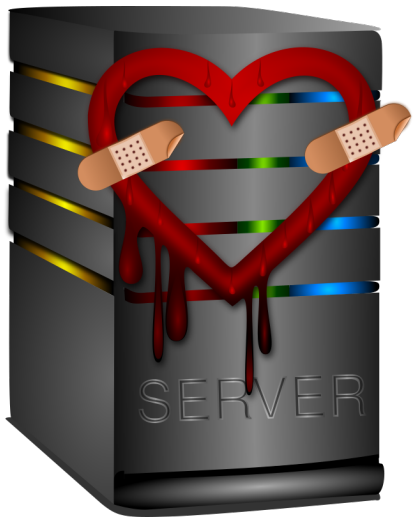
Introduction

- Studied math (Russia) & computer science (Germany)
- PhD in computer science (2008), Germany
  - Access control protocols for wireless sensor networks
- Researcher at FAU, Germany
  - Friedrich-Alexander-Universität Erlangen-Nürnberg
- Human Factors in Security & Privacy Group
  - Group leader

Agenda

- Spear phishing studies
  - Design & ethics
  - Study 1 → pitfalls & lessons learnt
  - Study 2 → recommendations
- Role of security awareness
- Challenges in patching human vulnerabilities

Technical vs. Human Vulnerabilities



- Technical vulnerabilities
  - Found → patch / redesign / accept risk
- Human vulnerabilities
  - Know how to exploit
  - Do we know how to patch?
    - Is security awareness THE solution?

Spear Phishing

- Academic research: > 1000 papers since 2004
- Phishing as a service (PhaaS)
  - KnowBe4, PhishMe, Wombat Security, many others
  - Pentesting the humans

What don’t we know yet?

Research Questions

- **Email vs. Facebook**
  - Difference in clicking rates?
- **Reasons** for clicking and not clicking?
  - Why can some people protect themselves better than their peers?
  - Would knowing this provide useful information for defenders?

Study Idea

- Simulated attack
  - Send spear phishing messages with a link
  - Senders: non-existing persons
  - Recruit university students for participating in the study
    - Email / Facebook
- Measure clicking behavior
- Ask them in a follow-up survey why they clicked / did not click

Message

Hey <receiver's *first name*>,

here are the pictures from the last week:

http://*<IP address>*/photocloud/page.php?h=*<USER ID>*

access denied

Please do not share them with people who have not been there :-)

See you next time!

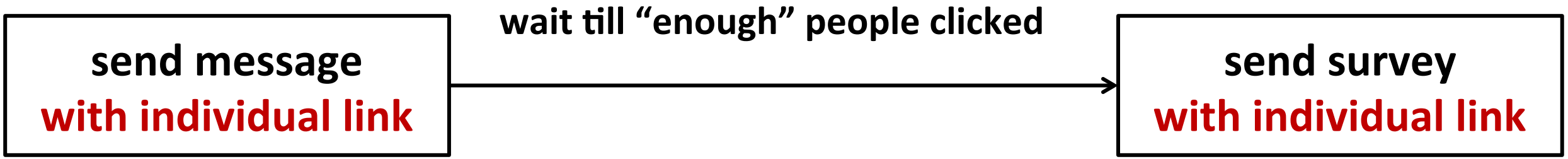
<firstname *of the sender*>

Ethics: Recruitment

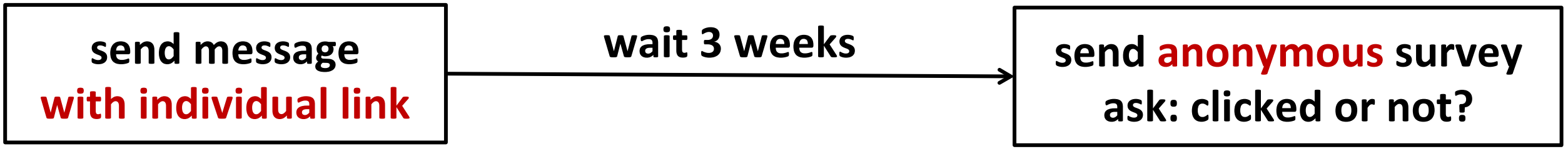
- Don't experiment with people without their consent!
- Participants recruited for a survey about "online behavior"
  - Not informed beforehand about the real purpose of the study
- Incentive: win 10x10 EUR online shopping voucher
- Time: August/September 2013

Ethics: Connecting Behavior with Survey

Survey should be anonymous → validity of the answers

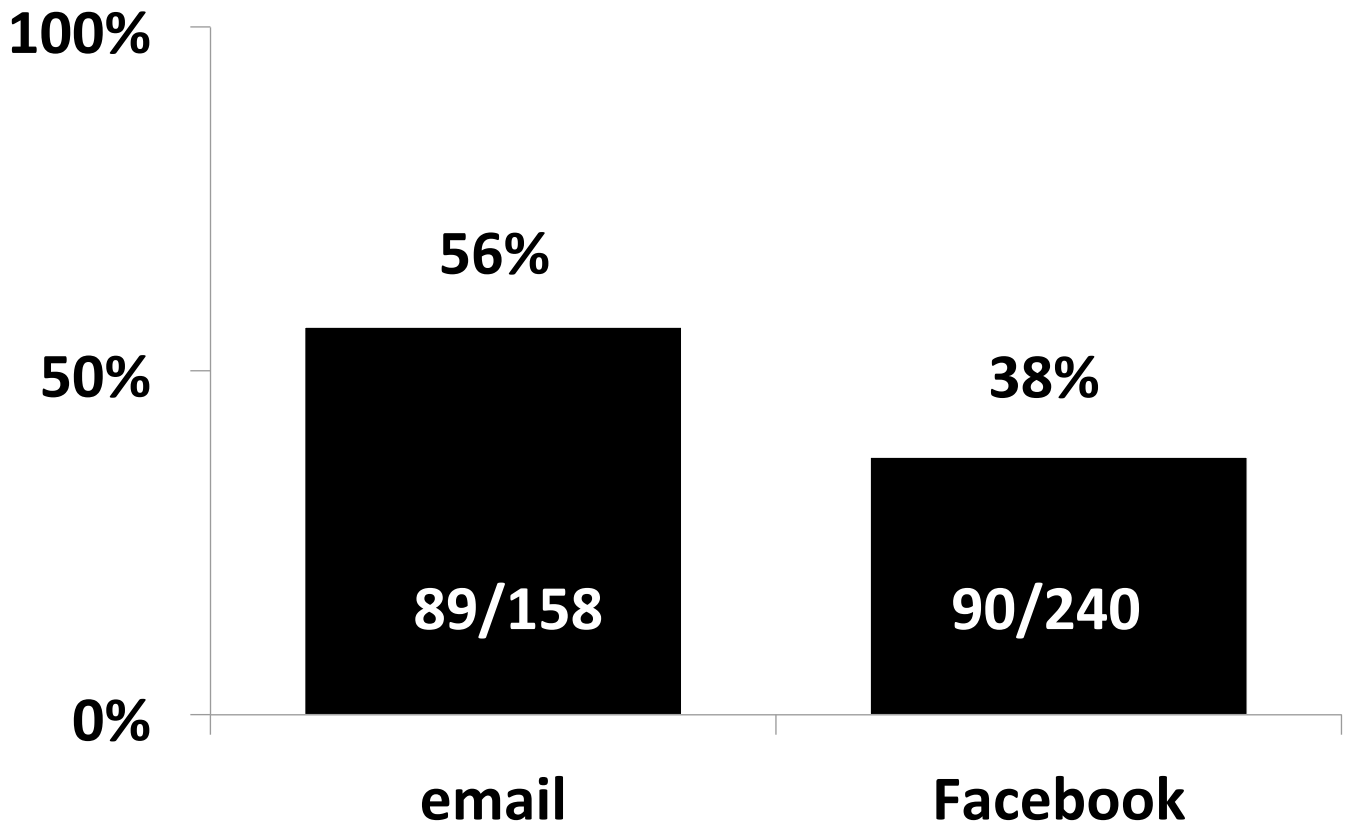


Final Design



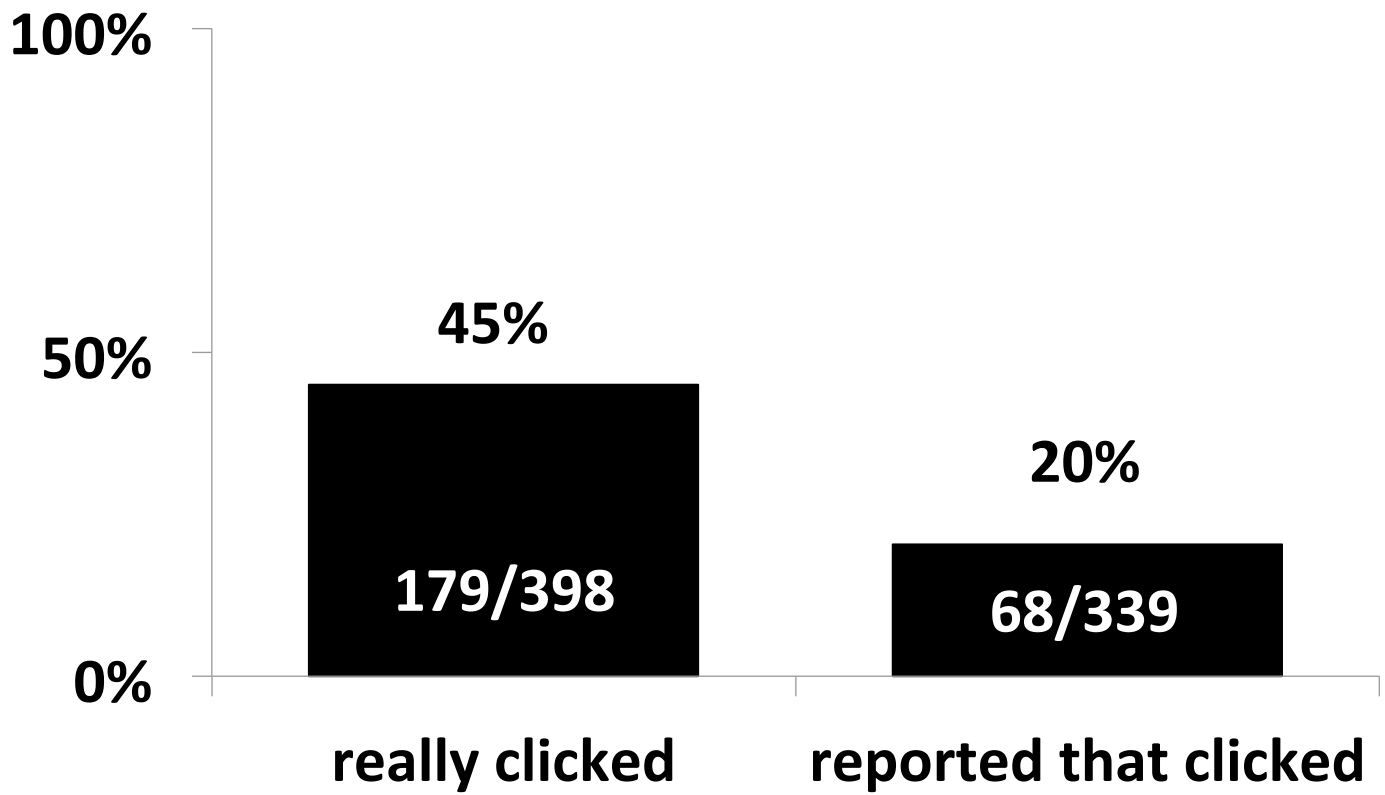
Study 1:Clicked

Statistically significant difference



Study 1: Survey

Answered survey: 85% (339 out of 398)



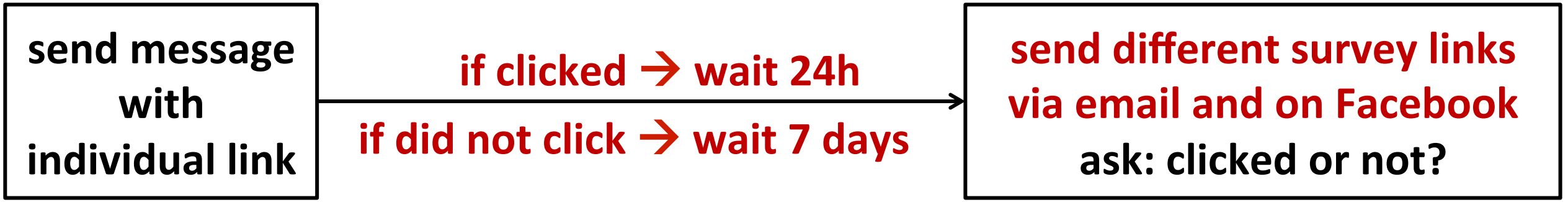
Study 2: Design Changes

On January 7th, 2014:

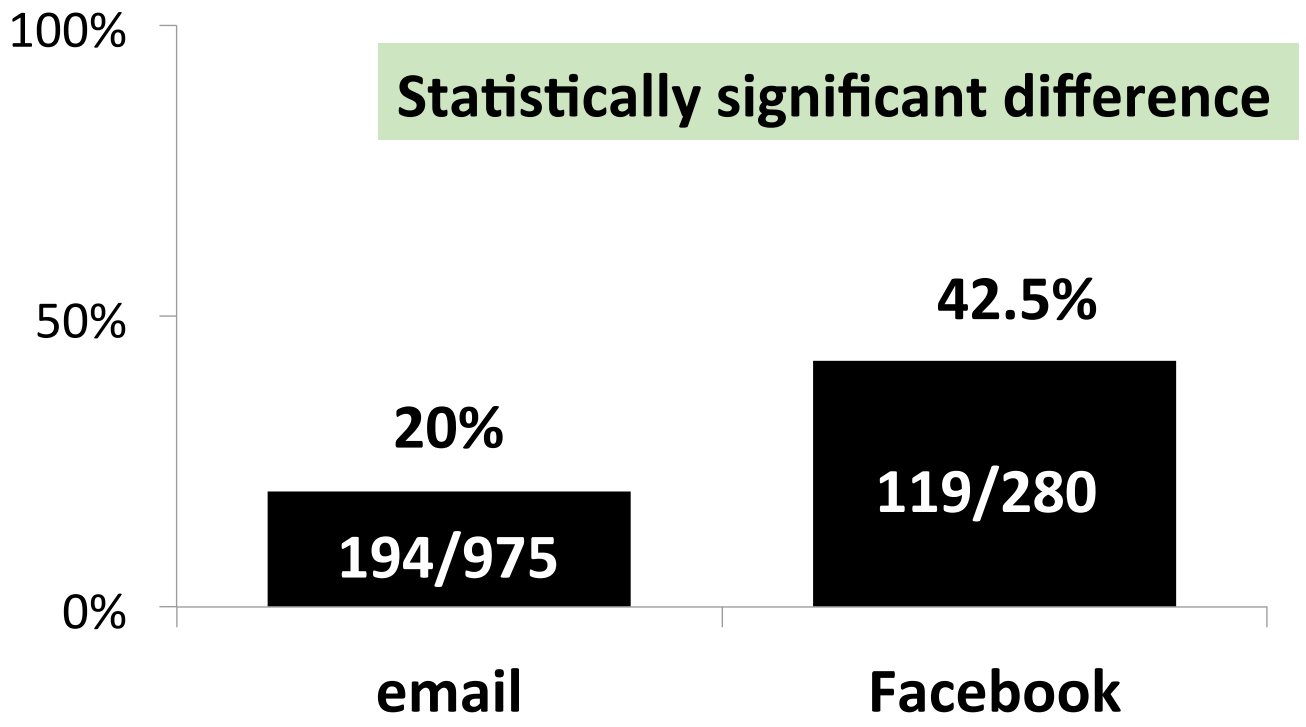
Hey,

the New Year party was great! here are the pictures:

http://*<IP address>*/photocloud/page.php?h=*<USER ID>*



Study 2: Clicked

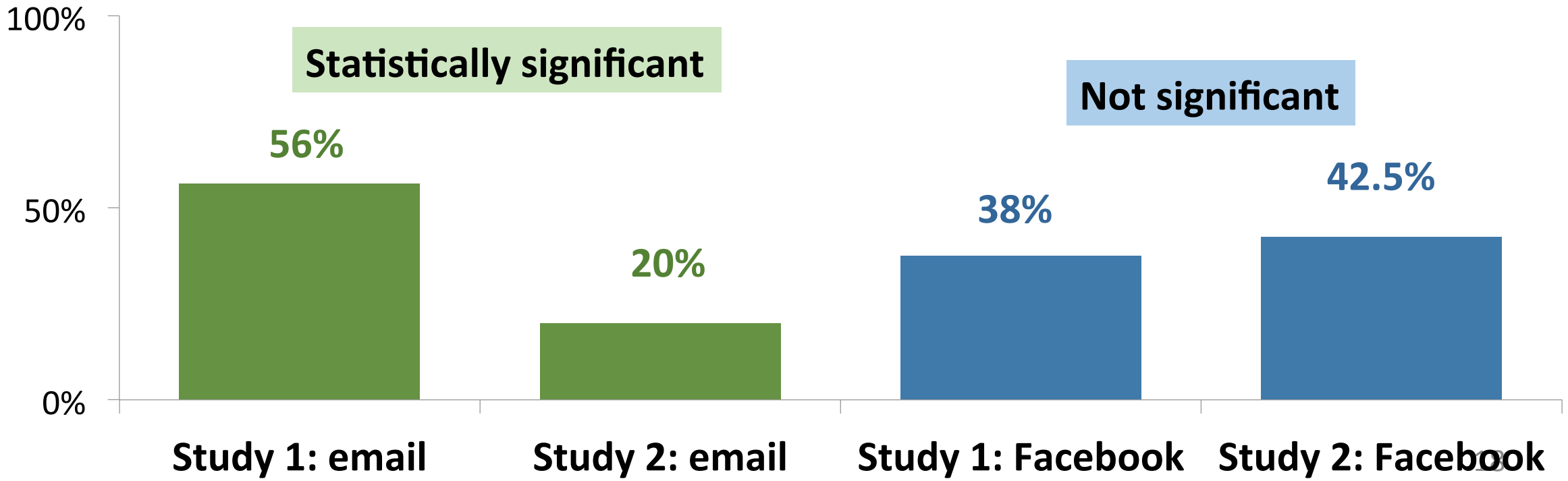


Addressing by Name

Important via email, but not on Facebook?

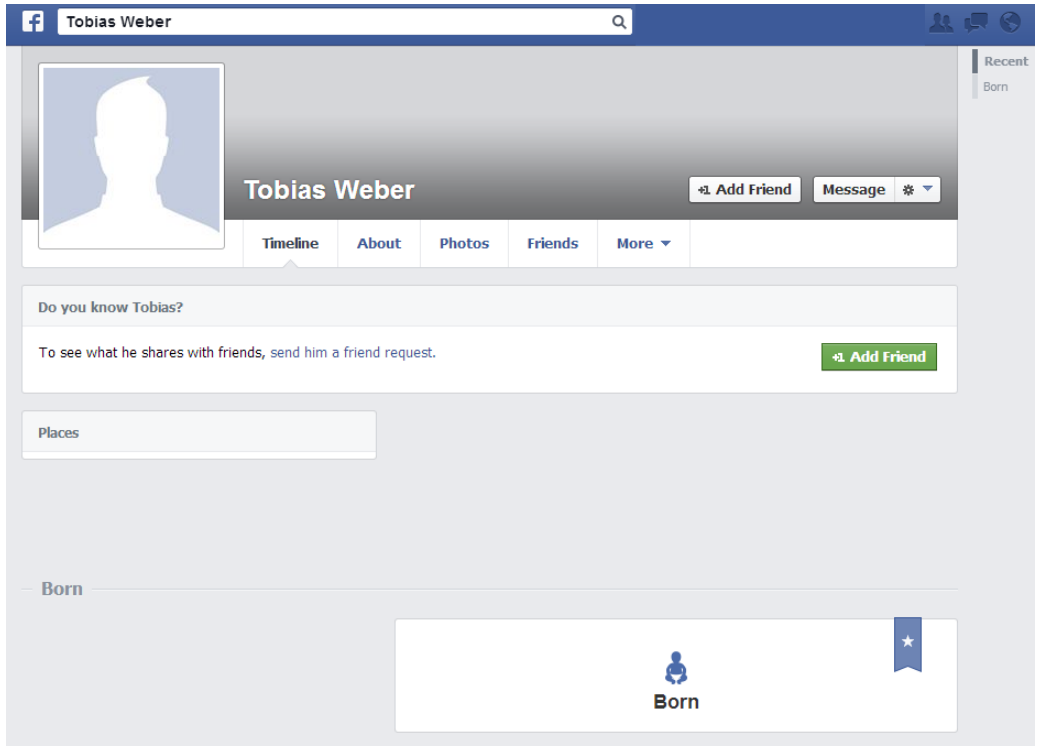
Disclaimer: Study 1 ≠ Study 2!!!

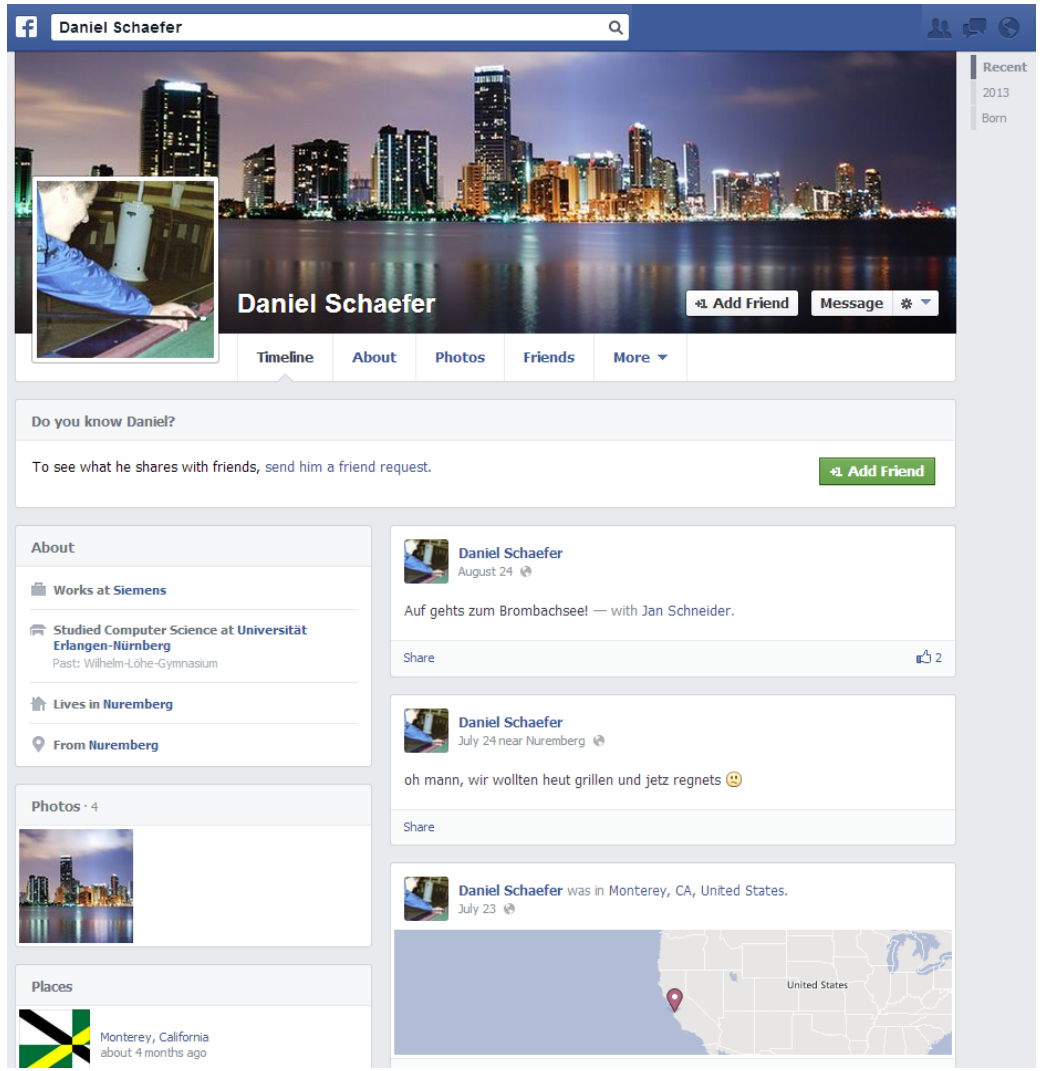
→ Different messages



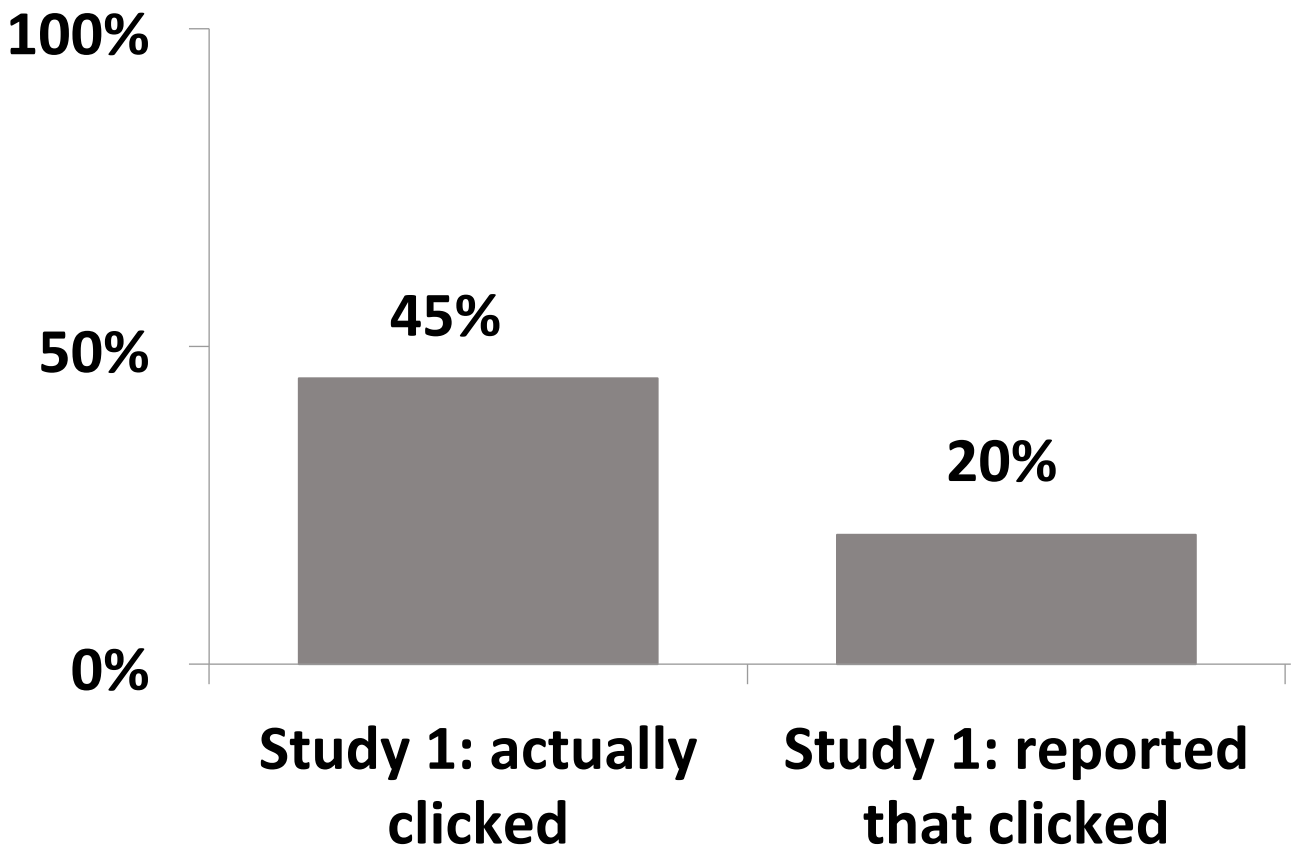
Both Studies: Factors Not Statistically Correlated to Clicking

- Gender of sender
- Gender of receiver
- Friend request on Facebook
- Amount of information on sender's Facebook profile

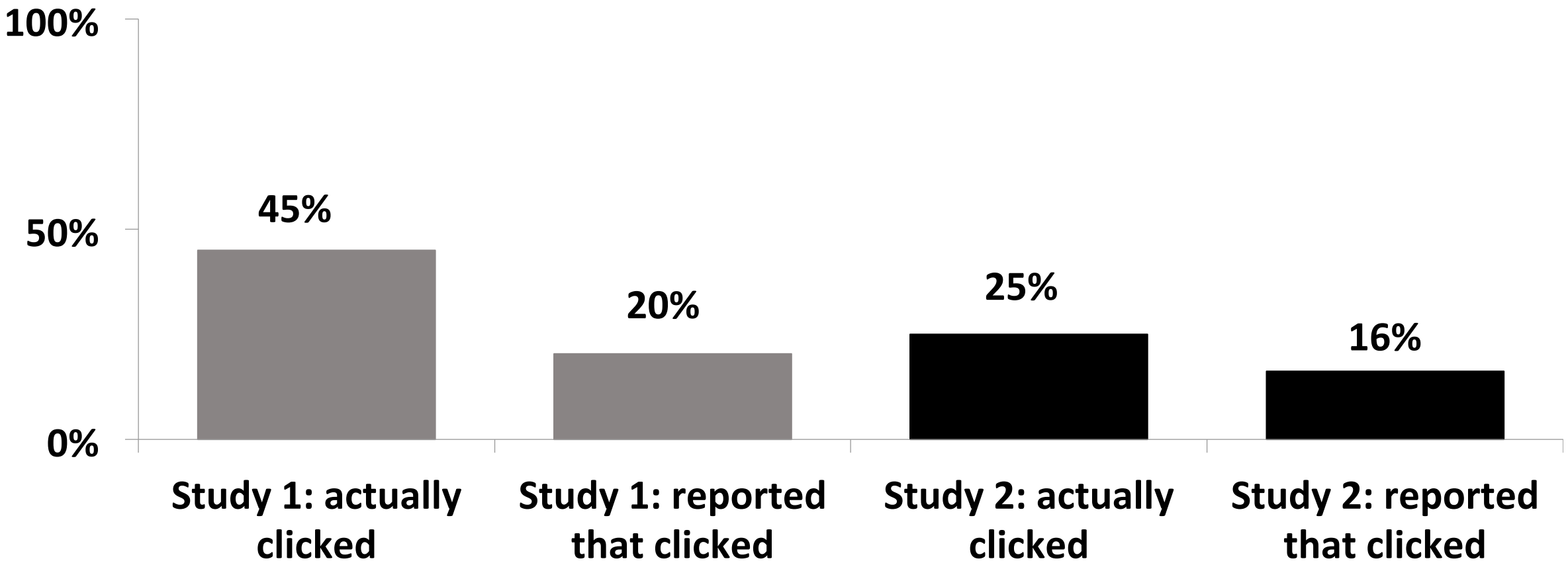

Tobias Weber
Recent
Born
Tobias Weber
Add Friend
Message
Timeline
About
Photos
Friends
More
Do you know Tobias?
To see what he shares with friends, send him a friend request.
Add Friend
Places
Born
Born


Daniel Schaefer
Recent
2013
Born
Daniel Schaefer
Add Friend
Message
Timeline
About
Photos
Friends
More
Do you know Daniel?
To see what he shares with friends, send him a friend request.
Add Friend
About
Works at Siemens
Studied Computer Science at Universität Erlangen-Nürnberg
Past: Wilhelm-Löhe-Gymnasium
Lives in Nuremberg
From Nuremberg
Photos · 4
Places
Monterey, California
about 4 months ago
Daniel Schaefer
August 24
Auf gehts zum Brombachsee! — with Jan Schneider.
Share
2
Daniel Schaefer
July 24 near Nuremberg
oh mann, wir wollten heut grillen und jetz regnets
Share
Daniel Schaefer was in Monterey, CA, United States.
July 23
United States

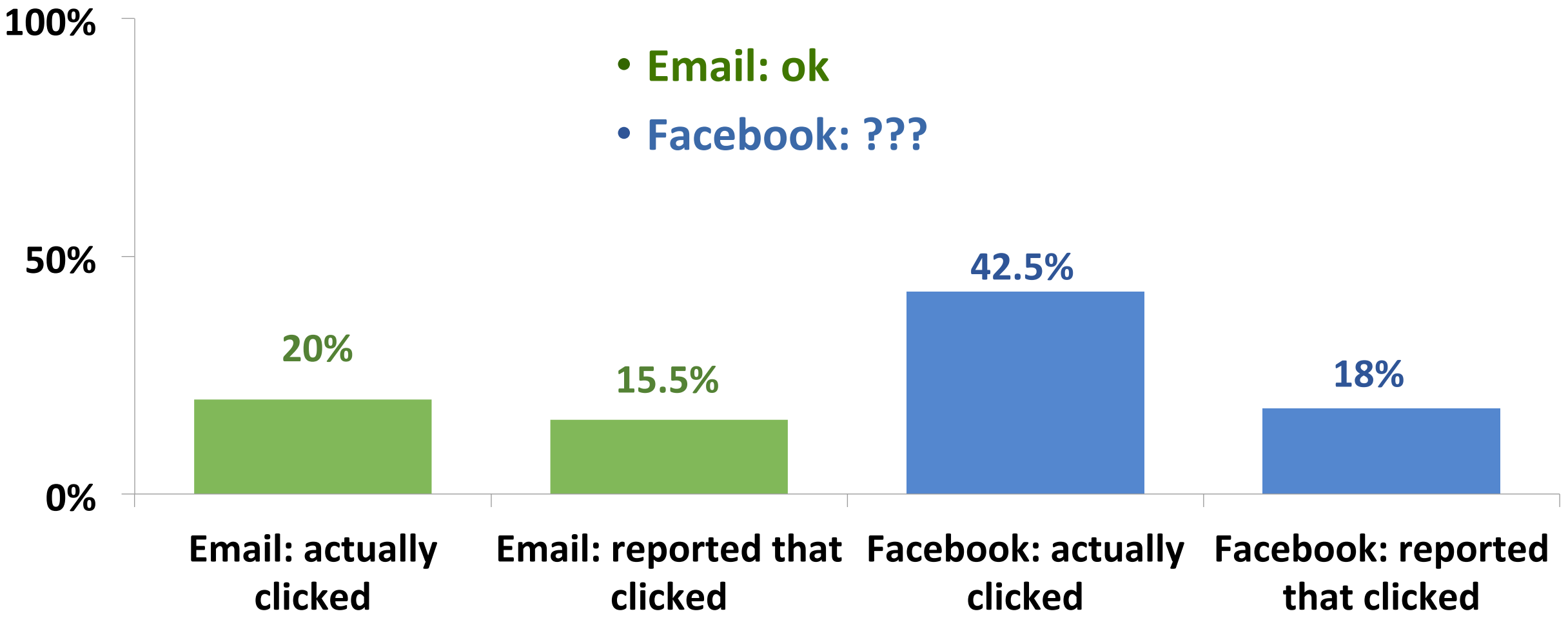
Study 1 vs. Study 2: Survey Reliability



Study 1 vs. Study 2: Survey Reliability



Study 2: Email vs. Facebook Survey Reliability



Reasons for Clicking: Results

- **Curiosity: 34%**

“Curiosity”

- *“I was curious”*
- *“I wanted to see what is there”*
- *“Out of interest”*
- *“I wanted to find out more about the pictures”*
- *“I did not know the sender, but wanted to see who is on the pictures”*

Reasons for Clicking: Results

(some people reported multiple reasons)

- **Curiosity: 34%**
- **Fits my New Year party: 27%**
- **Investigation: 17%**
- **Known sender: 16%**
- **Trust into technical context: 11%**

"Trust Into Technical Context"

- *"My computer blocks access if there is a virus problem"*
- *"I knew, if this was something dangerous, my Kaspersky would protect me"*
- *"I use Firefox and MacOS, so I'm not afraid of the viruses"*
- *"I used Tor Bundle"*
- *"After I googled, photocloud seemed to be a clean website"*
- *"I googled the email address […] I found nothing"*
- *"IP came from the university"*
- *"I consider the webmail of the university to be safe"*

Reasons for Clicking: Results

(some people reported multiple reasons)

- Curiosity: 34%
- Fits my New Year party: 27%
- Investigation: 17%
- Known sender: 16%
- Trust into system: 11%
- Really pictures of me? 7%

Reasons for Non-Clicking
(some people reported multiple reasons)

- Unknown sender: 51%
- Virus / Spam / Phishing / Scam / Fake: 44%
- Does not fit my New Year celebration: 36%
- Does not fit my way of life: 12%
- Investigation: 6%
  - FB profile: 2%

Did Not Click Because Of Privacy (6%)

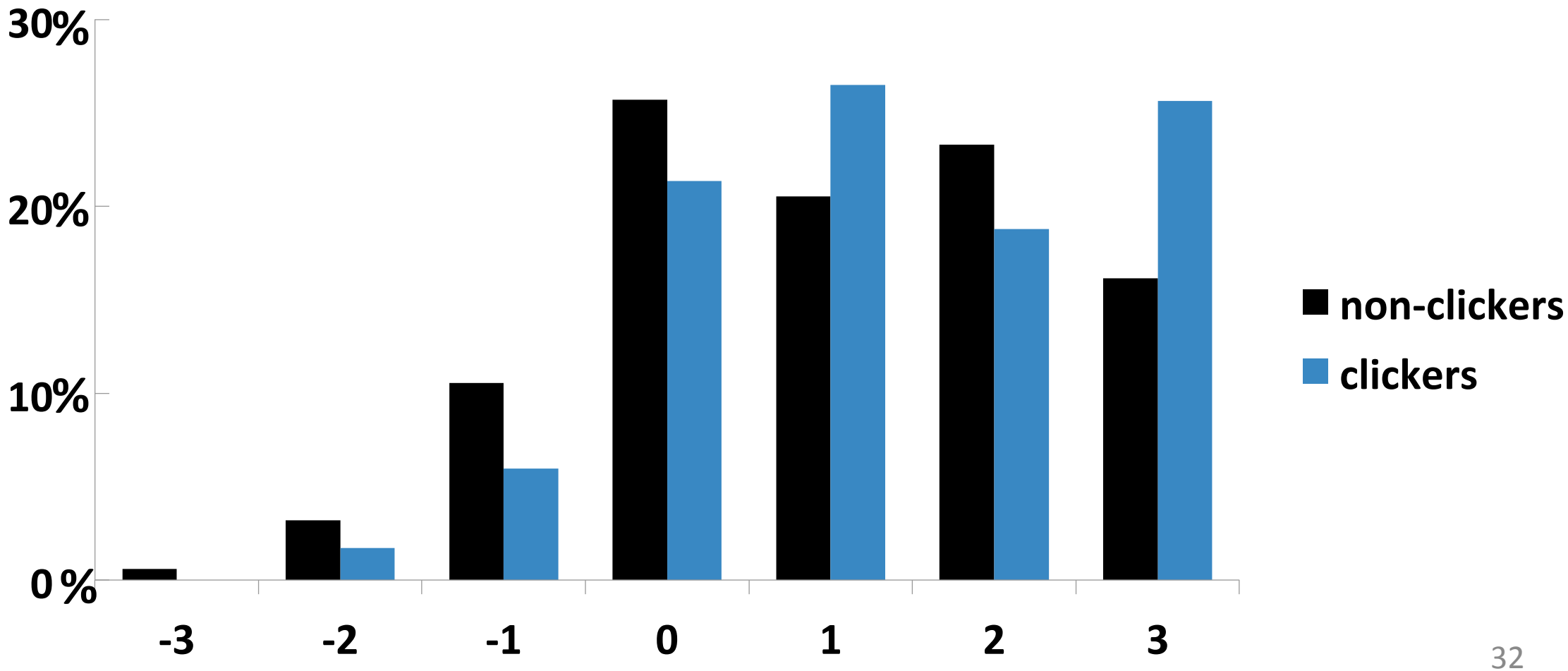
- *"It (the message) seemed to be private"*
- *"I though the message was genuine and wanted protect privacy"*
- *"It said: please don't click if you don't know me"*
- *"The message was not for me"*
- *"I did not see any reason to look up private pictures of a stranger who obviously made a mistake"*

Factors Not Statistically Correlated with Reported Clicking

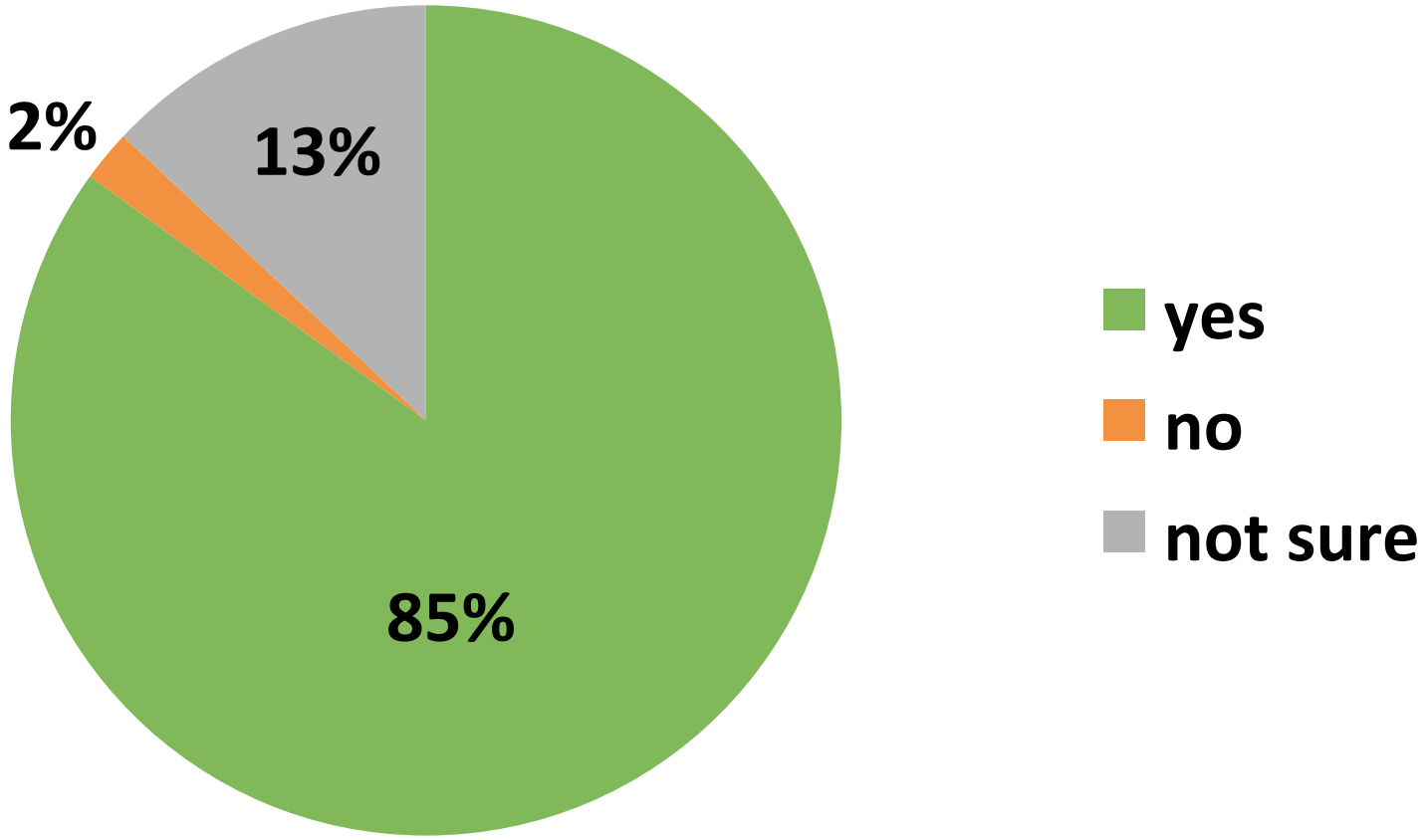
- IT security knowledge (self-assessed)
- Knowledge that email sender can be spoofed
- Knowledge that links can be dangerous

Attitude towards Participation in the Study

(-3=very negative, 3=very positive)



Should Such Studies be Conducted in The Future?



Limitations

- Study 1 ≠ Study 2
  - Only tentative comparisons across two studies!
- Validity of the reasons
  - Cannot look into people's heads at the moment of clicking
- "reported clickers" ≠ "real clickers"

Lesson 1: Targeting

- Curiosity / Interest
  - 78% knew that links can be dangerous
- Context
  - Known sender
    - 82% knew that sender can be spoofed
  - Plausibility: situation & expectations
- Facebook: do people notice that they clicked?

Lesson 2: Requirements on Users

- Be suspicious:
  - Even if you know the sender
  - Even if the message fits your current situation
  - Even if the message fits your work and life practices
- Be suspicious of everything!

Deception Mode

Let me introduce…

- Highly trained special agent
- A lot of people want to kill him
- (Almost) any person in his life can be a traitor
- Has to be in deception mode in every life situation
- Does his job excellently
- Does not exist ☹

Want Your Employees Be Aware of Spear Phishing?

- Want themto be in James Bond mode every time they read a message?


accounting


sales


public relations


human resources


customer support

- Add this to job descriptions
- Make sure to pay them adequately

Being Security Aware: Personal Adventures

Personal Example 1: Curiosity / Interest
(anonymized)

From: john.smith@turner.com

To: zinaida.benenson@fau.de

Subject: CNN request -- about your upcoming Black Hat talk

Zinaida,

John at CNN here. I'm the news network's cybersecurity reporter. Here's a link to my work, in case you're not familiar with it.

I saw the description of your upcoming Black Hat talk. Your topic looks fantastic!

Can we get an exclusive look at your research and write the first news story about it?

Cheers,

John Smith

john.smith@CNN.com

Personal Example 2: Context
(anonymized)

From: Journal of Experiments (EXPE) exp@editorial-expe.com

To: zinaida.benenson@fau.de

Subject: Invitation to Peer Review EXPE-M-35-00737

Dear Dr. Benenson, In view of your expertise […]

[…]

If you would like to review this paper, please click this link:

http://expe.editorial-expe.com/l.asp?i=35189&l=GKXKMQK

If you do not wish to review this paper, please click this link:

http://expe.editorial-expe.com/l.asp?i=87665&l=6HN7KK

Best regards,

Editor

<name I've never heard of>

From: Journal of Experiments (EXPE) exp@editorial-expe.com

To: zinaida.benenson@fau.de

Subject: Invitation to Peer Review EXPE-M-35-00737

Dear Dr. Benenson, In view of your expertise […]

[…]

If you would like to review this paper, please click this link:

http://expe.editorial-expe.com/l.asp?i=35189&l=GKXKMQ

If you do not wish to review this paper, please click this link:

http://expe.editorial-expe.com/l.asp?i=87665&l=6HN7KK

Best regards,

Editor

<name I've never heard of>

First Click, Then Notice: Messages to Helpdesk

D. Caputo et al. "Going spear phishing: Exploring embedded training and awareness."
IEEE Security & Privacy Magazine, 2014

- *"I clicked on it inadvertently without thinking and exited Explorer without reading the link."*
- *"I just opened this. Then followed link like an idiot. Then killed the process using Task Manager. Please advise as what to do."*
- *"I can't believe I actually clicked on the link! Let me know if there's something I need to do to ensure my laptop isn't infected, or if this is just a prank."*

Personal Example 3: An Attachment
(anonymized)

From: setup@company-I'm-dealing-with.com

To: zinaid.benenson@fau.de

Subject: Message ID:23519-0297:FRT-92362. Workitem Number: CMPVDM24062016157789020297

Attachment: attach/15072016/29375.docx

Hi, Please see request details below. Please provide the required information by replying to this email.

Query Reason: Banking details

Workitem Number: CMPVDM240620161577890202 97

Created Date: 15-Jul-2016

Name: Zinaida Benenson

Comments: Dear Sir/Madam In order for us to complete the set up of your account within our system, we need your bank account details to which settlement of your invoices should be made. Please complete the attached form in full and return to us, ensuring it has been signed by an authorized signatory.

Lesson 3: Pentesting & Patching Humans

- What are the reasons for ineffectiveness of an awareness training?
  - Curiosity / interest → natural & creative human traits
  - "This message fits my current situation" / "I know the sender" → useful decisional heuristics
- What price users pay for an effective awareness training?
  - James Bond mode
  - False positives? Work slowdown?
  - Breakdown of social relationships? Atmosphere of distrust?
  - Embarrassment? Shame? Anger?

Feasible User Involvement?

- Report suspicious messages?
  - Be prepared to get "amateur security"!

  (Bruce Schneier about "If you see something, say something")
- Reliable indicators for switching into "James Bond mode"
  - False positives destroy trust into the indicator
  - Digitally sign messages
    - Non-experts misinterpret meaning / don't notice
    - Can be social engineered into accepting an invalid signature
- Stop sending "phishy" legitimate messages
- Expect mistakes

Key Takeaways

- Spear phishing: what defense is feasible and beneficial for humans?
  - People won't and can't abstain from decisional heuristics
  - Don't require permanent James Bond mode
- Pentesting and patching humans is tricky
  - What do you want people to do?
  - Think about consequences for people & for company
  - Always ask consent
- Talk to the users
  - Automated observation and measurement are not enough
  - Ask directly about their experiences, opinions, work practices

Research & evidence needed!
If your company is interested, please talk to me

Zinaida Benenson

zinaida.benenson@fau.de

Thank you! Questions?

Please complete the Speaker Feedback Surveys