blackhat®
USA 2016

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

Introduction

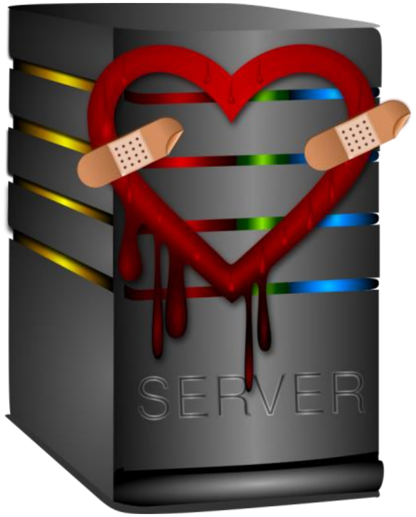
- Studied Math (Russia) & Computer Science (Germany)
- PhD in computer science (2008), Germany
  - Access control protocols for wireless sensor networks
- Researcher at FAU, Germany
  - Friedrich-Alexander University of Erlangen-Nuremberg
- Human Factors in Security & Privacy Group
  - Group leader

Agenda

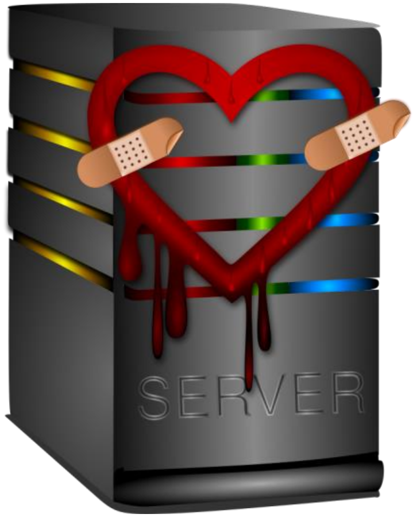
- Spear phishing studies
  - Design & ethics
  - Study 1 → pitfalls & lessons learnt
  - Study 2 → recommendations
- Role of security awareness
- Challenges in patching human vulnerabilities

Technical vs. Human Vulnerabilities

- Technical vulnerabilities
  - Found → patch / redesign / accept risk



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?
    - What can we redesign?
    - When should we accept the risk?

Spear Phishing

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

Research Questions

- Email vs. Facebook
  - Where would people click more often?
- Reasons for clicking and not clicking?
  - Would knowing this provide useful information for defenders?
  - Why can some people protect themselves better than their peers?

Study Idea

- Simulated attack
  - Send spear phishing messages to participants
- Measure clicking behavior of the participants
- 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 :-)

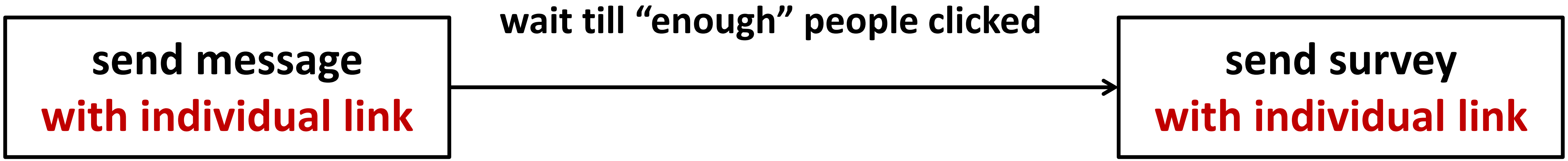
See you next time!

<firstname *of the sender>*

Ethics: Recruitment

- Participants recruited for a survey about “online behavior”
  - Don’t experiment with people without their consent!
  - Not informed beforehand about the real purpose of the study
  - Expected to receive a survey
- Incentive: win 10x10 EUR Amazon vouchers
- Time: August/September 2013

Ethics: Connecting Behavior with Survey



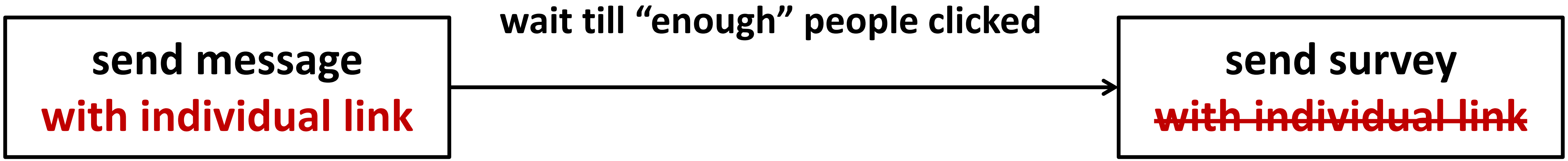
send message
with individual link

wait till “enough” people clicked

send survey
with individual link

Ethics: Connecting Behavior with Survey

Survey should be anonymous → validity of the answers vs. lying to participants

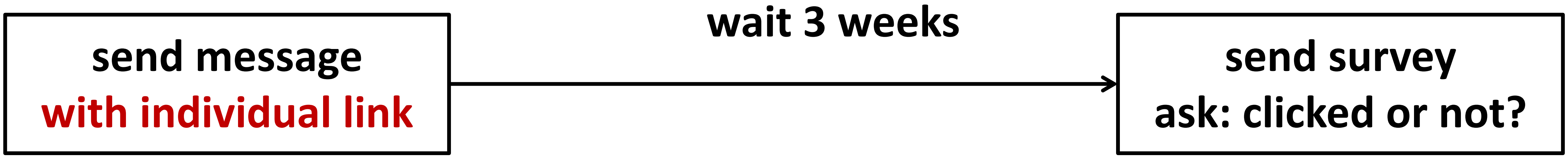


send message
with individual link

wait till “enough” people clicked

send survey
~~with individual link~~

Final Design



send message

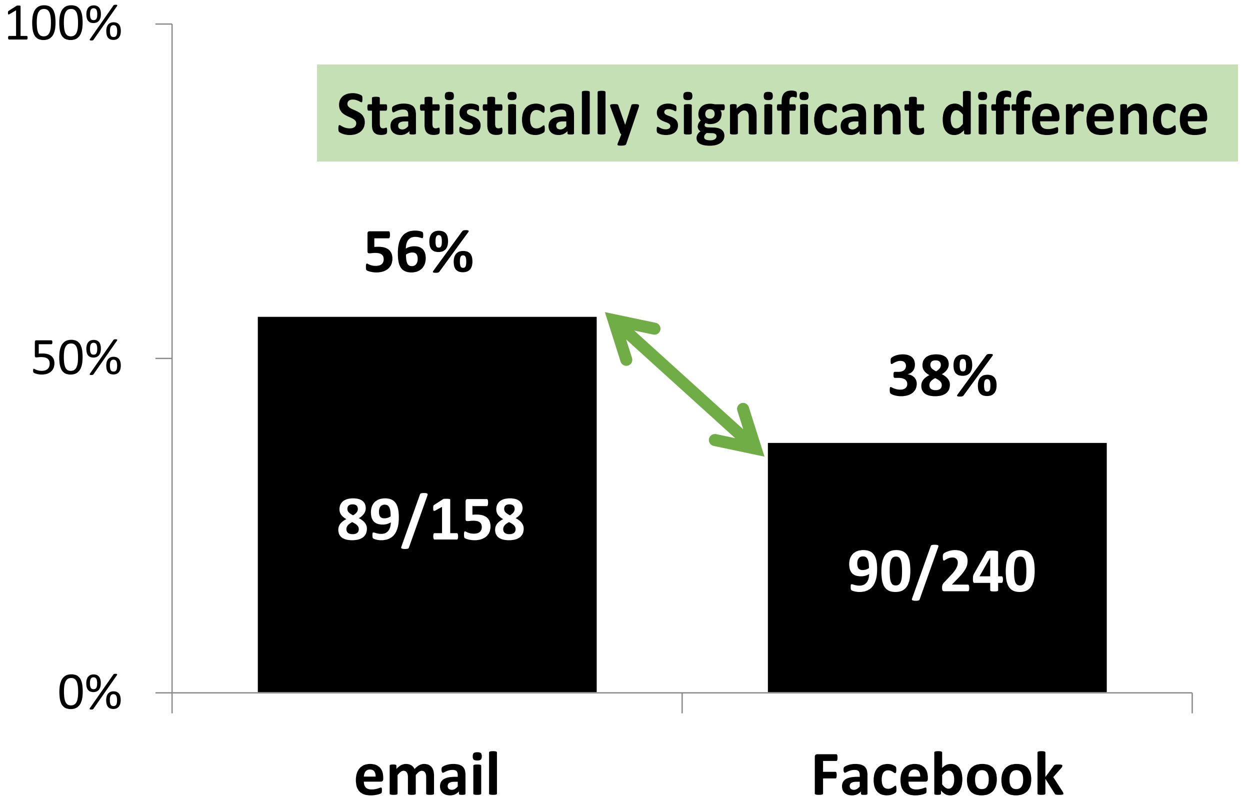
with individual link

wait 3 weeks

send survey

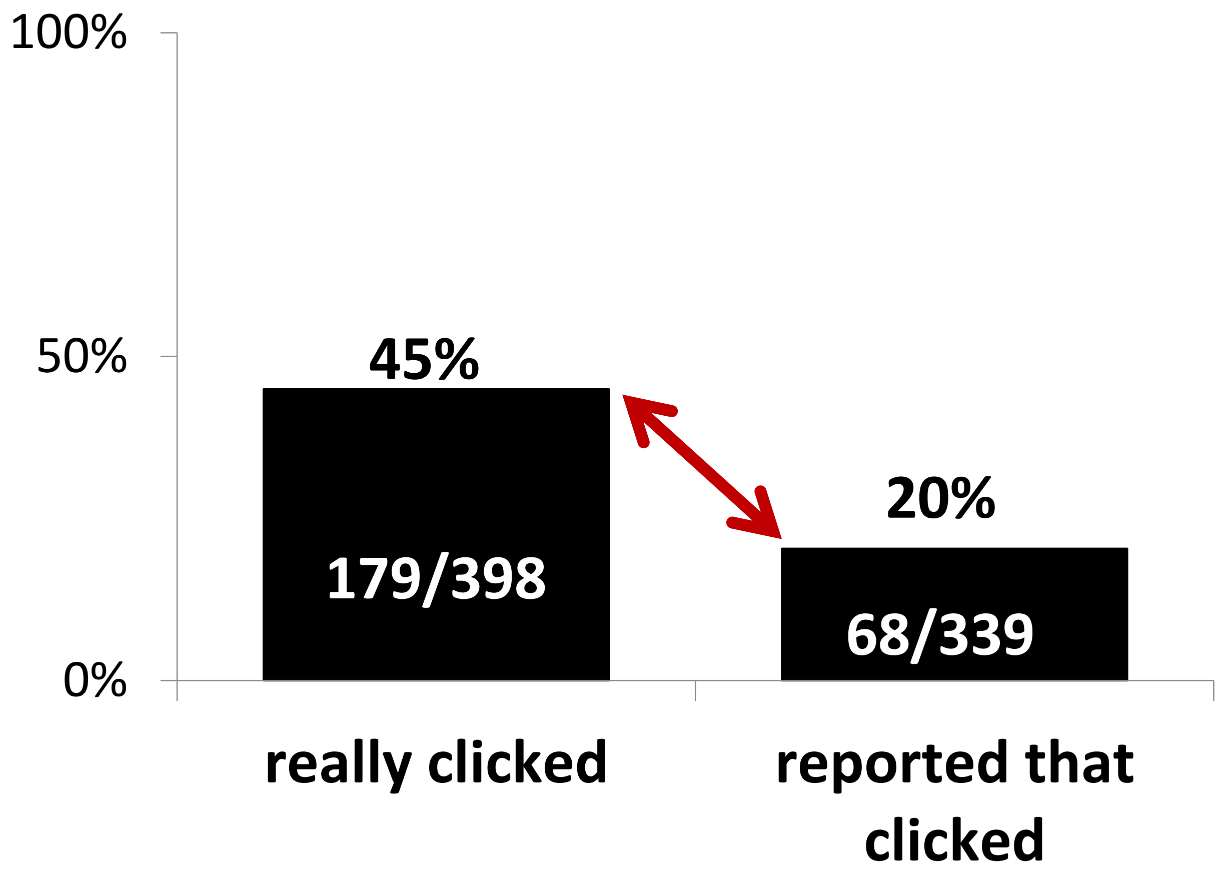
ask: clicked or not?

Study 1:Clicked



Study 1: Survey

Answered survey: 85% (339 out of 398)



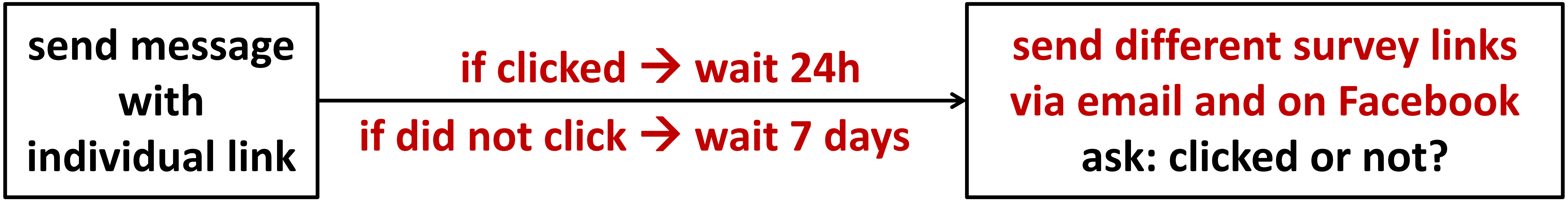
Study 2: Design Changes

On January 7th, 2014:

Hey,

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

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



send message with individual link

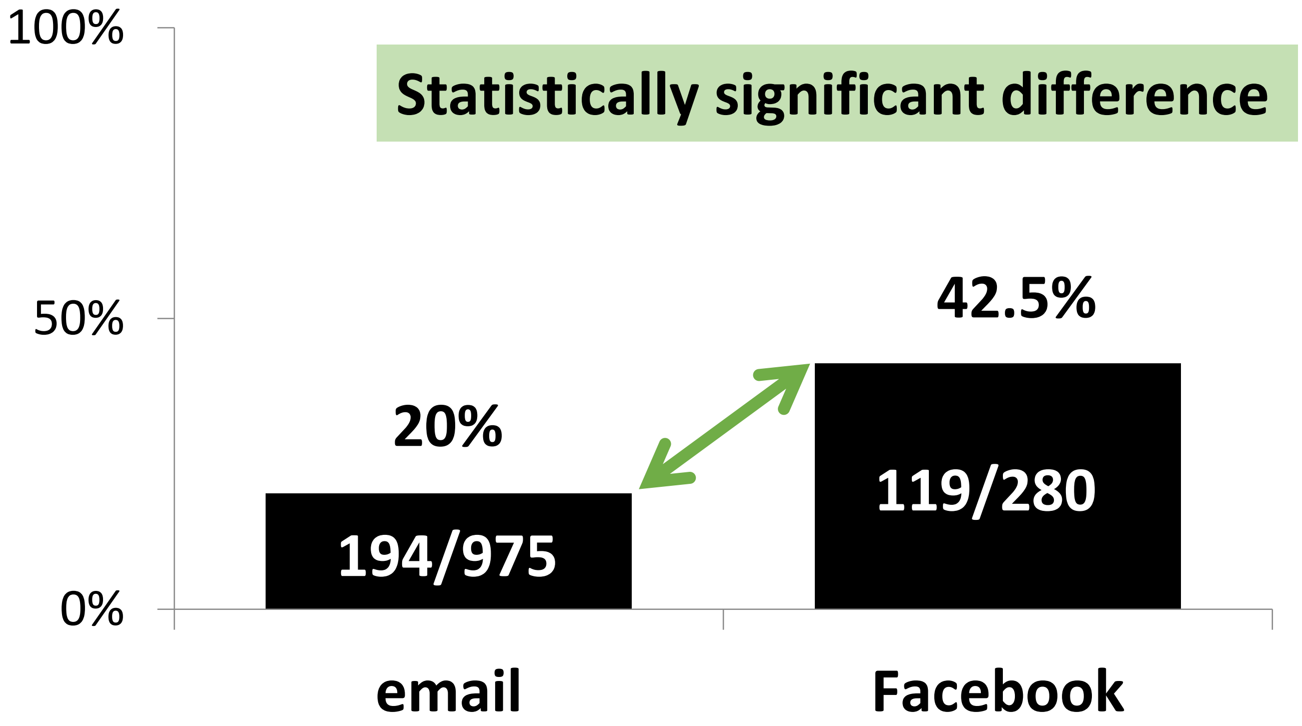
if clicked → wait 24h

if did not click → wait 7 days

send different survey links via email and on Facebook

ask: clicked or not?

Study 2: Clicked

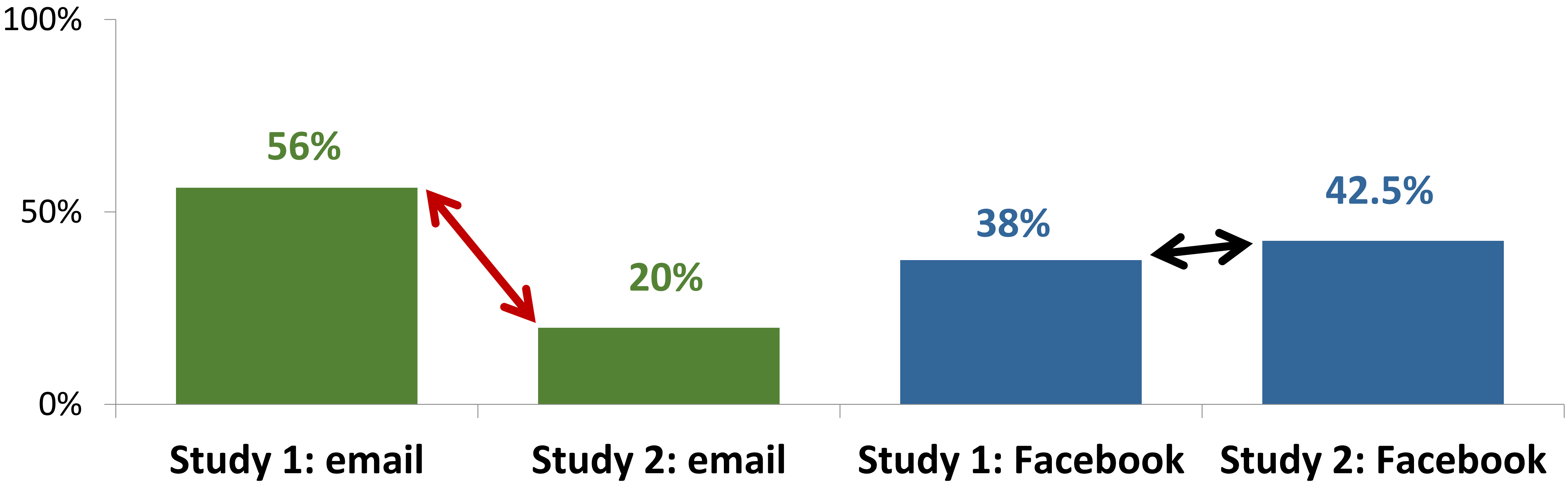


Addressing by Name

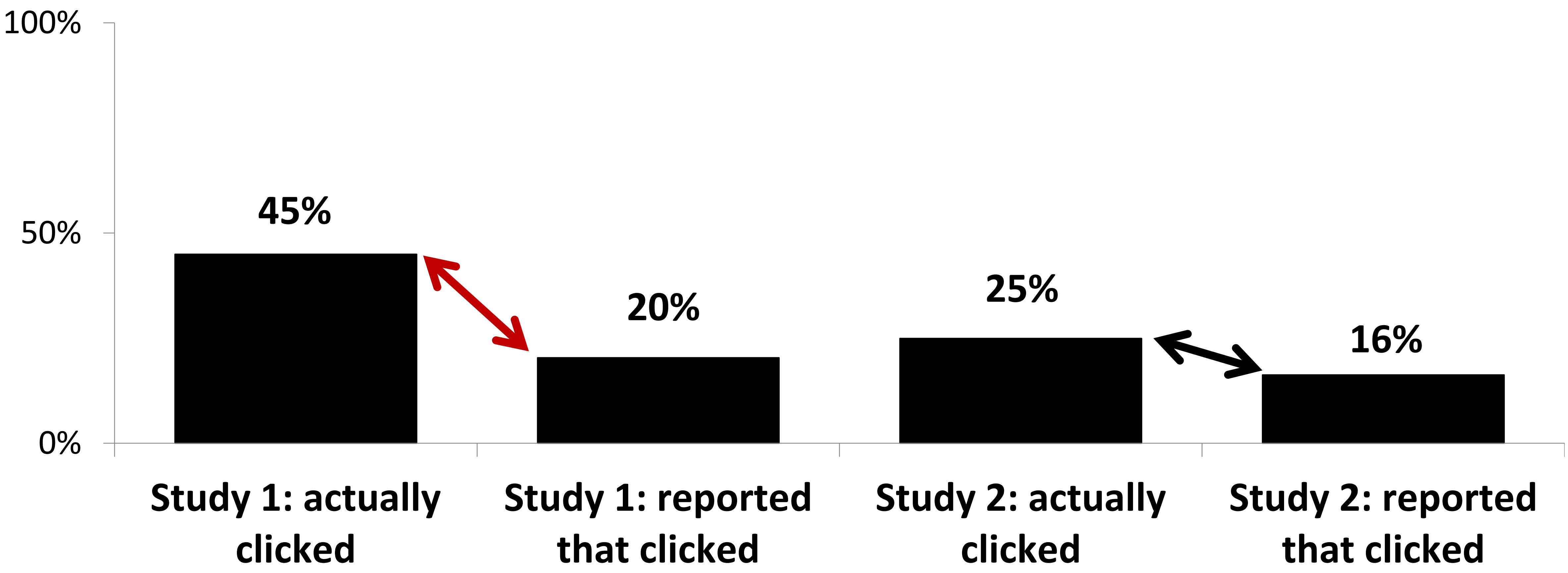
Important via email, but not on Facebook?

Disclaimer: Study 1 ≠ Study 2!!!

→ Different timing, different messages

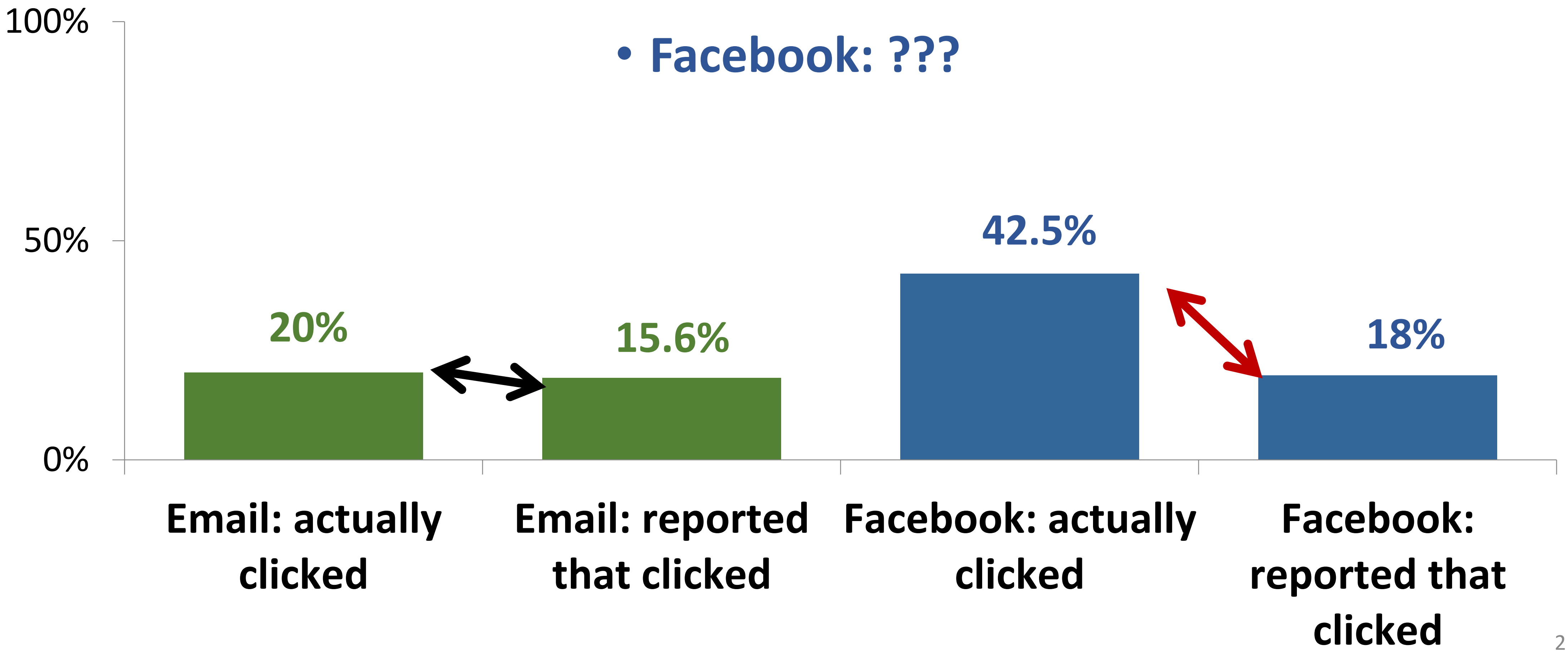


Study 1 vs. Study 2: Survey Reliability



Study 2: Email vs. Facebook Survey Reliability

- Email: ok
- Facebook: ???



Reasons for Clicking: Results

- **Curiosity: 34%**
- **Fits my New Year party: 27%**
- **Investigation: 17%**
- **Known sender: 16%**
- **(My) system is secure: 11%**
- **Really pictures of me? 7%**
- **Automatically 3% (4 people)**
- **Some people gave more than one reason**

Reasons for Clicking: Method

- Content analysis, 2 coders
- Codebook
  - Codes: “curiosity”
  - Description: in which cases are these codes assigned
  - Examples
    - *“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”*
- Coders’ agreement: Cohen’s Kappa > 0.7 (substantial agreement)
  - Statistical measure for agreement

Reasons for Non-Clicking

- Unknown sender: 51%
  - Behavioral rule: 9%
- Virus / Spam / Phishing / Scam / Fake: 44%
- Does not fit my New Year's Eve celebration: 36%
- Does not fit my way of life: 12%
- Investigation: 6%
  - FB profile: 2%
- I'm not the intended receiver: 6% → privacy

Factors Not Correlating with Reported Clicking

- Age, gender
- IT security knowledge (-3=very low, 3=very high)
- Knowledge that email sender can be spoofed (yes/no/don’t know)
- Knowledge that links can be dangerous (yes/no/don’t know)

Factors Correlating with Reported Clicking

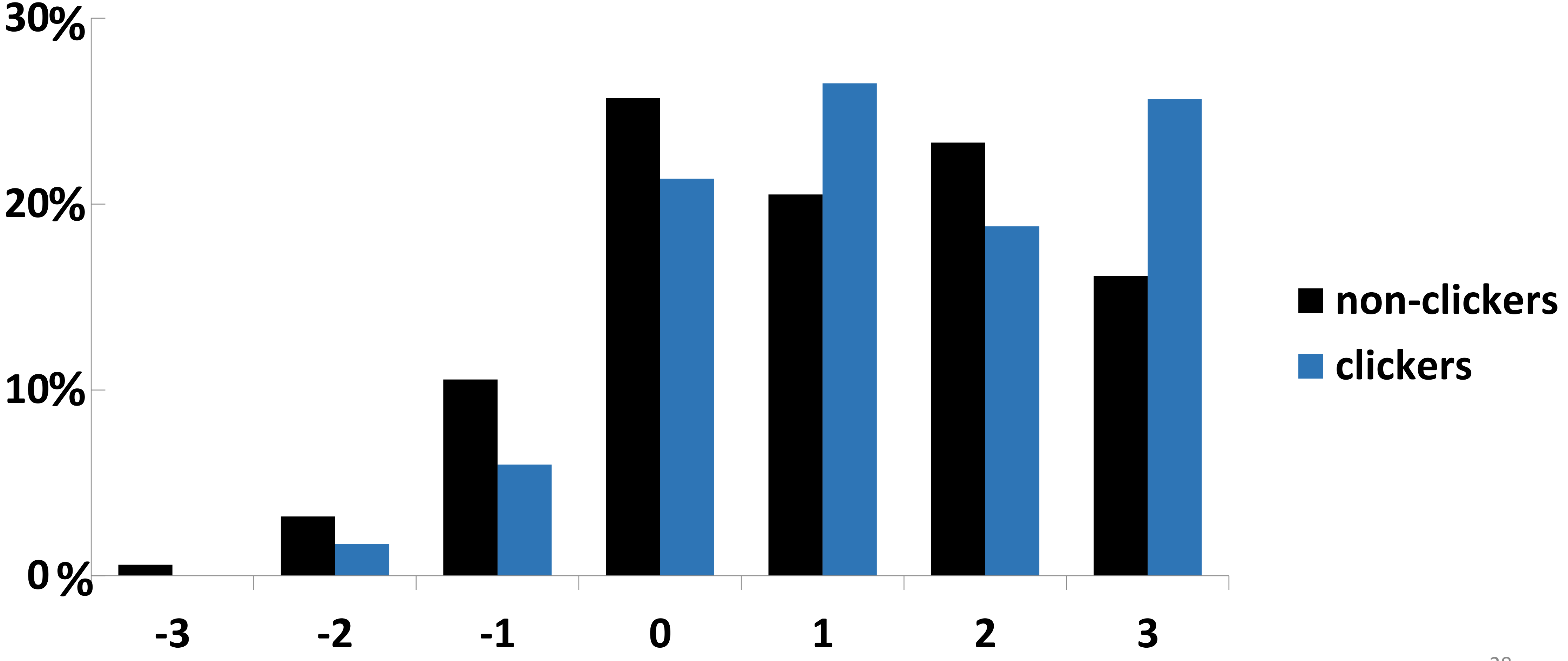
- Ability to recognize messages from criminal senders (-3=very low, 3=very high)
  - Higher reported ability ↔ lower clicking rate → consistent representation of self?
- Attention paid to the message (-3=very low, 3=very high)
  - More attention ↔ higher clicking rate
- Mood at the moment of message reception (psychometric scale)
  - More positive mood ↔ higher clicking rate → “cognitive ease”?
- → This is only correlation, not causation!
- Reported clicking, not real behavior!

Reported Impact

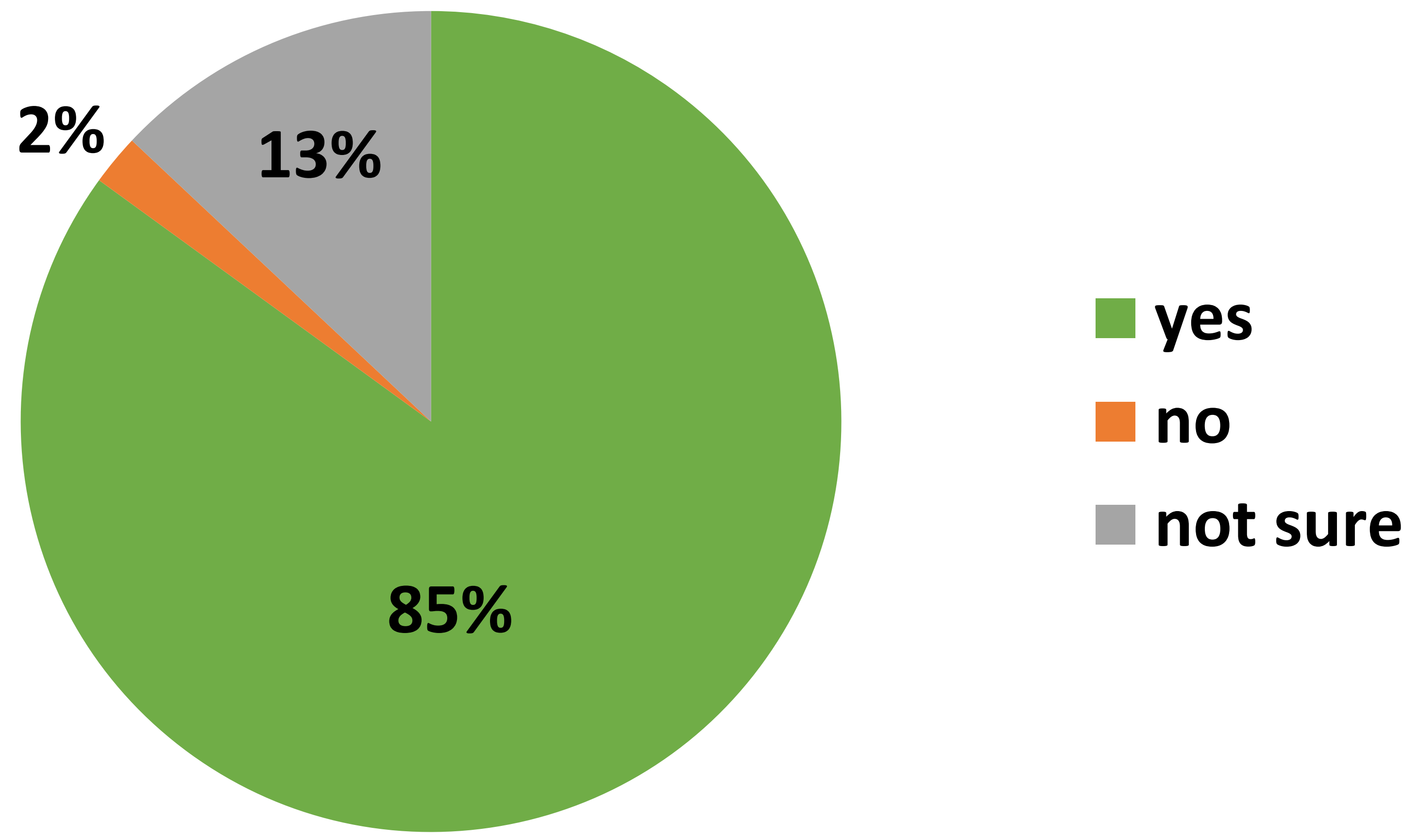
- Be more careful in the future (no further explanations): 31%
- Be careful with messages / links from unknown senders: 28%
- Think more about risks of Internet usage: 26%

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
- Context
  - Known sender
  - Plausibility: situation & expectations
- Strong emotions
- Facebook vs. email difference
  - Facebook: do people notice that they clicked?
  - Addressing by name more important for email → tentative result

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

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!

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!
- → Be in James Bond mode!

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!
- → Be in the James Bond mode!
- Normal people cannot function well in this mode
- What externalities are likely to arise?

Personal Example 1: Curiosity / Interest

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

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>

Personal Example 2: Context

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: A False Positive

From: setup@company-I’m-dealing-with.com
To: zinaid.benenson@fau.de

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

Hi, Please see request details below. Please provide the required information by replying to this email.
Query Reason: Banking details
Workitem Number: CMPVDM24062016157789020297
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.

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: CMPVDM24062016157789020297

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.

Phishing as a Service: Example

- **December 2015, several Local Divisions of Police Berlin**
- **Email: store all your work and private passwords in the secure password storage of the Berlin police**
  - **Signature: Central Services Division (ZSE), from non-existing person**
- **Sent to 466 police officers, 252 of them clicked, and 35 gave their credentials**
- **Website blocked after 40 min**
- **Management board member of the Police Union:**
  - **Officers receive so many official emails, cannot be expected to pay attention to every detail**
  - **Police is "the mirror image of our society"**

Sources (in German):
http://www.morgenpost.de/berlin/article206570827/Aufregung-um-Mail-Attacke-auf-Berliner-Polizei.html
http://www.tagesspiegel.de/berlin/telefonstreich-bei-der-berliner-polizei-attacke-noch-nicht-aufgeklaert/12659326.html

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 and reliable decisional heuristics
- What price users pay for an effective awareness training?
  - Being suspicious of everything? → James Bond mode
  - False positives? Work slowdown?
  - Breakdown of social relationships? Atmosphere of distrust?
  - Embarrassment? Shame? Anger?

Feasible User Involvement?

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

  (Bruce Schneier about "If you see something, say something")
- Reliable indicators for switching into the "James Bond mode"?
  - No false positives!!! → immediately destroy trust into the indicator forever
  - Digital signatures? → Non-experts misinterpret their meaning or don't notice

Research & evidence needed!

If your company is interested, please talk to me

Key Takeaways

- **Spear phishing: what defense is feasible and beneficial for humans?**
  - **Curiosity → natural and indispensable human characteristics**
  - **Context → very useful and time-saving heuristics**
  - **Don’t require the permanent James Bond mode**
- **Pentesting and patching humans**
  - **What is your purpose? What do you want to achieve?**
  - **Does your pentesting method fit your purpose?**
  - **Think about consequences for people & for company**
  - **Always ask consent**
- **Talk to the users**
  - **Observing and measuring is not enough**
  - **Ask directly about their experiences, opinions, work practices**

Thank you! Questions?

Please complete the Speaker Feedback Surveys

Zinaida Benenson

zinaida.benenson@fau.de