Black Hat Webcast, January 19, 2017

# This Could Happen to You: Reasons for Clicking on Ransomware-Infected Links and Attachments

**Zinaida Benenson**

zinaida.benenson@fau.de

Friedrich-Alexander-Universität Erlangen-Nürnberg

**What makes people click?**
**What can we do about this?**

# Personalization: Known Sender

- Research by Jagatic et al.
  - Social phishing. *Communications of the ACM*, 2007
- Email to students from a spoofed social network friend
  - Message: “check this out!” + link
  - 72% clicked (and entered login credentials)
- Same email from a non-existing person
  - 16% clicked

# Personalization: Sender Knows Me

- Our research: two studies
- Emails or Facebook messages to students
- From non-existing persons
- More details: Black Hat USA 2016
  https://www.youtube.com/watch?v=ThOQ63CyQR4

**Study 1**

**Hey <receiver's *first name*>,**

**here are the pictures from the last week:**

**http://<*IP address*>/photocloud/<*USER ID*>**

**Study 2**

**Hey,**

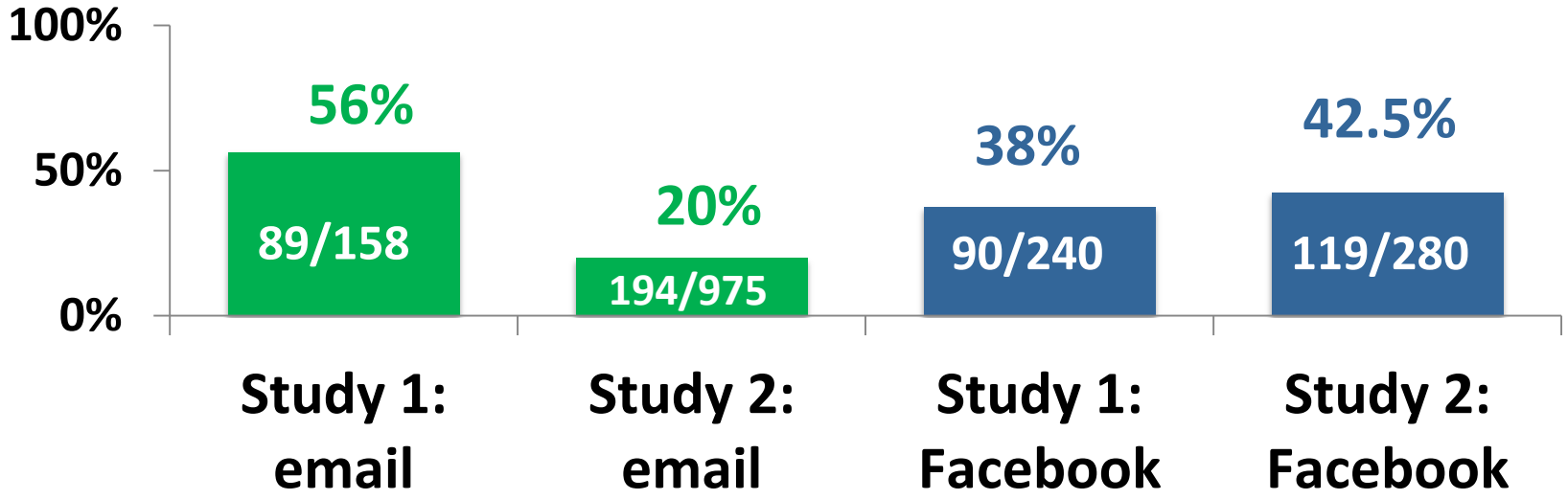
**the New Year's Eve party was great! here are the pictures:**

**access denied**

# Personalization: Addressing by Name

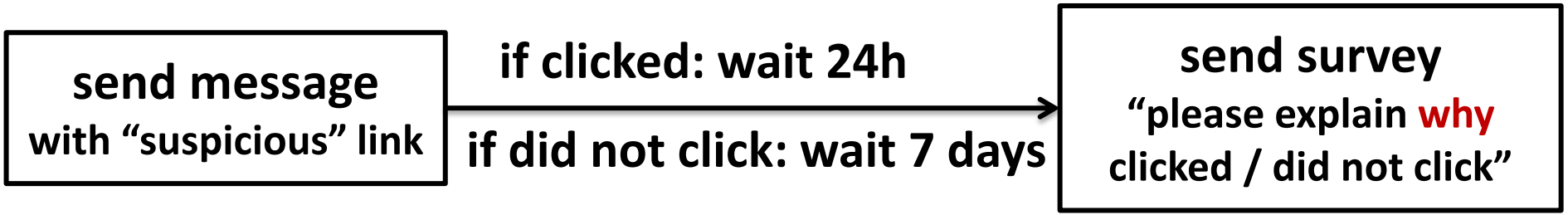
## Important via email, but not on Facebook?

**Disclaimer: Study 1 ≠ Study 2!!!**
**(different user groups, different messages)**



# How Do People Explain Their Clicking?

**Additionally in Study 2**



# Reasons for Clicking: Results

## (107 answers, some people reported multiple reasons)

- Curiosity / interest: 34%
- Plausible content, fits expectations: 27%
  - Fits users' New Year's Eve party
- Investigation: 17%
  - What happened? Can I help?
- Known sender: 16%
  - We used top 10 German names for fake senders

# Trust Into Technology / Organization: 11%

- *"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"*

# Fear: 7%

- **Really pictures of me?**
  - ***"Although I felt unsafe, my fear that a stranger might have my pictures was very strong. There are so many possibilities nowadays to make photos that one never knows who might have made them, and under which circumstances."***

- **Clicking not the sign of low security awareness**

# Automatic reaction: 3%

- *"I clicked automatically"*
- *"I first clicked on the link and then it came to me that no person with this name was actually present*

# First Click, Then React: 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.”***

# What Makes People Click

- Emotions
  - Positive: curiosity, interest
  - Negative: fear
- Plausible content, fits expectations
- Investigation (what is going on?), helpfulness
- Personalization
  - Known sender
  - Addressing by name
- Trust into technology / organizational protection
- Automatic reaction

# Could This Happen to YOU?

- Security experts are seldom targeted
  - Because targeting other users is easier
- Security experts are human
  - Right targeting *might* work on them, too

# Personal Example:
# Targeting a Security Expert
## (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**

**Luckily, this message was genuine**
**But it could have been spear phishing**
***All targeting information was available online***

# Awareness 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

# aka

# Security Mindset

# 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

# Can Employees Be Aware of Targeted Attacks?

**Should they go into the 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**

# False negatives versus False positives

- False negatives
  - Dangerous messages not detected
  - Security experts usually worry most about these
- But false positives are a problem, too!
  - Benign messages classified as dangerous
    - Deleted, no action taken
  - Lost opportunities
  - Business / personal conflicts

# Personal Example: A False Positive

**(anonymized)**

**From:** setup@company-I'm-dealing-with.com
**To:** zinaida.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: CMPVDM240620161577890202297**

**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.**

# If a security awareness program is not effective, what could be the reasons?

- Security aware behavior is difficult to maintain
  - Constant vigilance is tiring
  - Emotions and automatisms
- Business cases and work practices clash with expected security behavior
  - If people receive a lot of email attachments, how can they distinguish legitimate ones?
  - If people receive a lot of links, how much delay would be introduced if they check all of them?
- Social norms clash with expected security behavior
  - Trust, expected normal behavior
    - Should I really ask my colleague / my boss if they really sent me this file?
  - They might think I'm wasting their time or I'm incompetent

# Can we make users security aware by catching them on insecure behavior?

- **Is Phishing as a Service a good idea?**

# Phishing as a Service: Example

- December 12th 2015, 1:30pm, a Police Division in Berlin
- Email: store all your work and private passwords in the secure password storage of the Berlin police
  - Corporate design
  - Signature: Central Division, from non-existing person
- Sent to 466 police officers
  - 252 of them clicked, 35 gave their credentials
- This was a Phishing as a Service email
- Speaker 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”

# Pentesting the Humans

- What can we learn from this test?
  - Police officers are human
- What are the officers supposed to do?!
  - Check every internal email that gives orders?
  - Are they supposed to distrust such emails?
- Technical solution?
  - Example: visually distinguish internal & external emails
  - Help the users, save effort, avoid mistakes

# User-Centric Protection

- **User-centric thinking: how would protection measures affect**
  - **Business cases, overall productivity**
  - **Social norms, trust relationships**
- **Technical stuff**
  - **Backups, patches, updates, network segmentation, … (add more)**
  - **Globally disable macros and scripts?**
- **Processes from users' perspective**
  - **For victims: attack reporting procedures**
  - **How to inform users about an ongoing attack?**
  - **What do you want them to do in case of an attack?**

# Feasible User Involvement?

- **Report** suspicious messages
  - Be prepared that people will report a lot of benign stuff
  - Ensure **quick** responses
- **Reliable** indicators for switching into "James Bond mode"
  - Example: internal versus external emails
  - False positives **destroy trust** into the indicator
- **Stop** sending "phishy" legitimate messages
  - And communicate this to the users
- **Expect** mistakes and be prepared

# Evidence needed

- If you run “phishing as a service” or other awareness measures in your organization
- Then please contact me for a research interview
  - Confidentiality guaranteed
  - Help security community to understand pros and cons of anti-phishing measures
  - Help establish evidence-based security
    - As opposed to snake-oil-based

# Key Takeaways

- What makes people click
  - Personalization
  - Plausibility of content & context
  - Emotions (positive and negative)
  - Automatic reactions
- Think and act user-centric
  - Stop treating users as “the main problem” or “the weakest link”
- Design of countermeasures
  - What do you want people to do? Will they be able to do this?
  - Feasibility of business cases? False positives?
  - Effect on productivity? Well-being? Trust relationships?