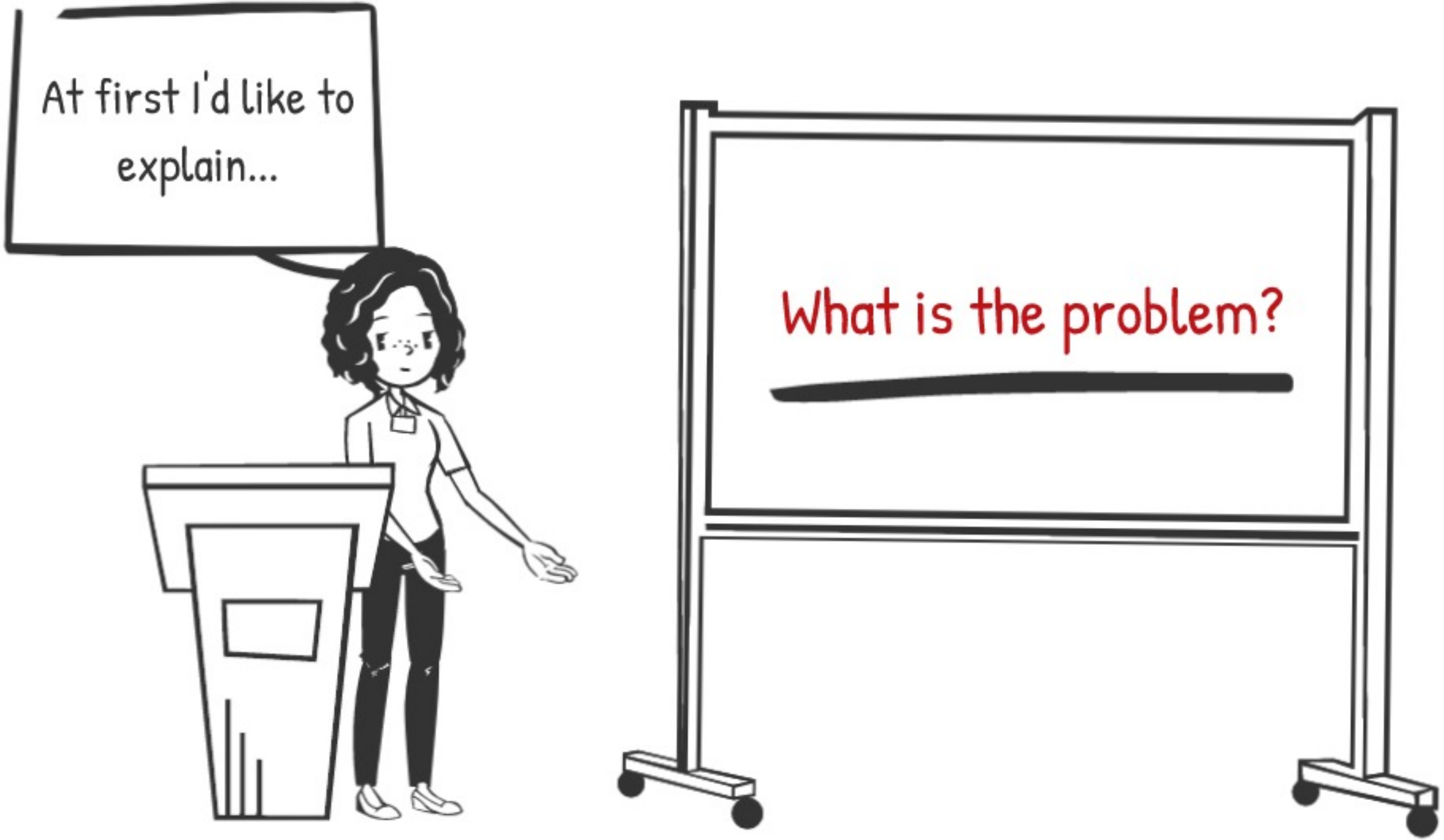
Your website has been hijacked: Raising awareness for an invisible problem

GI Sicherheit 2022 Doktorandenforum

Anne Hennig


At first I'd like to explain...
What is the problem?

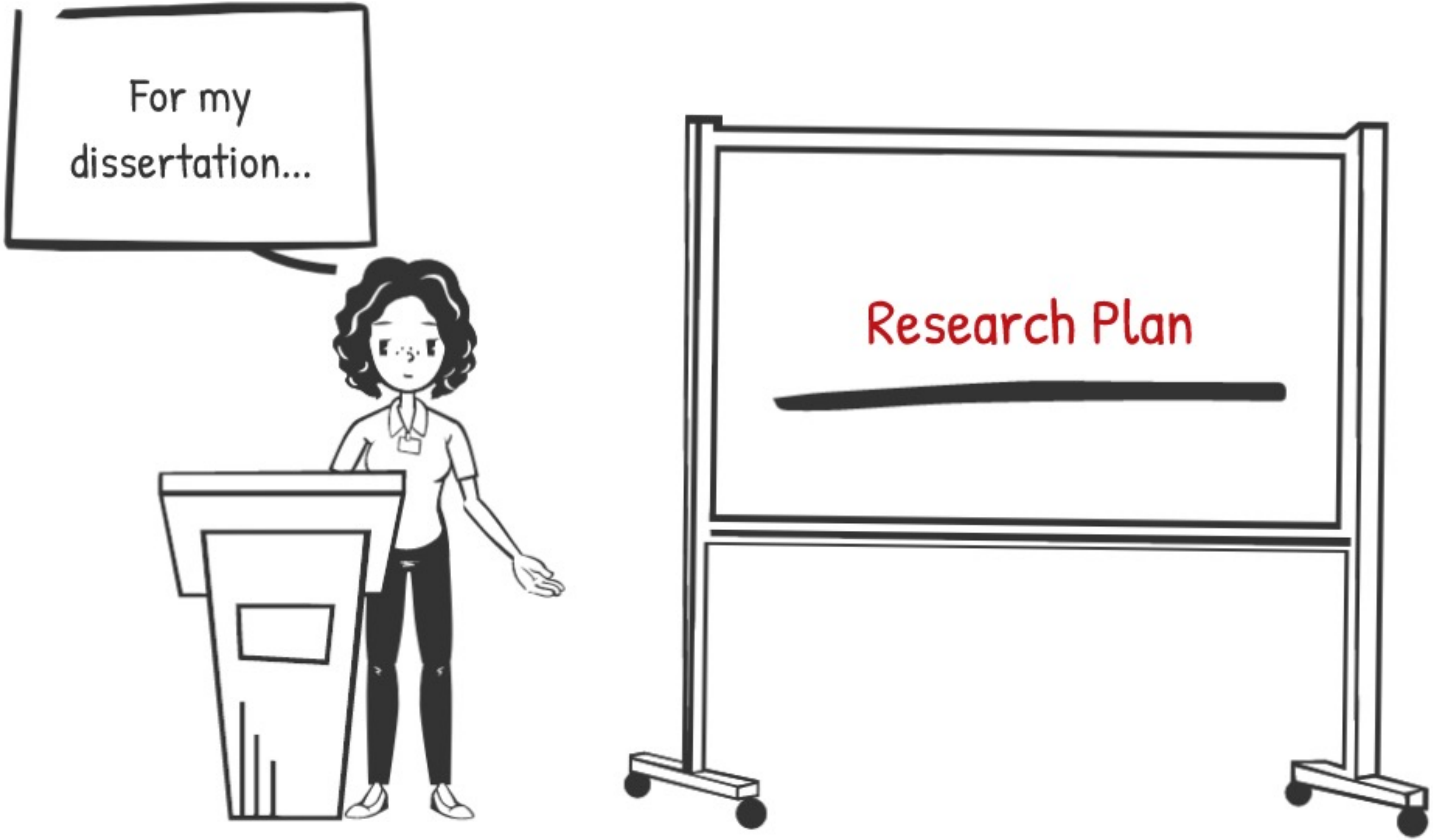
Definition “Pharma Hack”

Attacker deploys code on vulnerable website

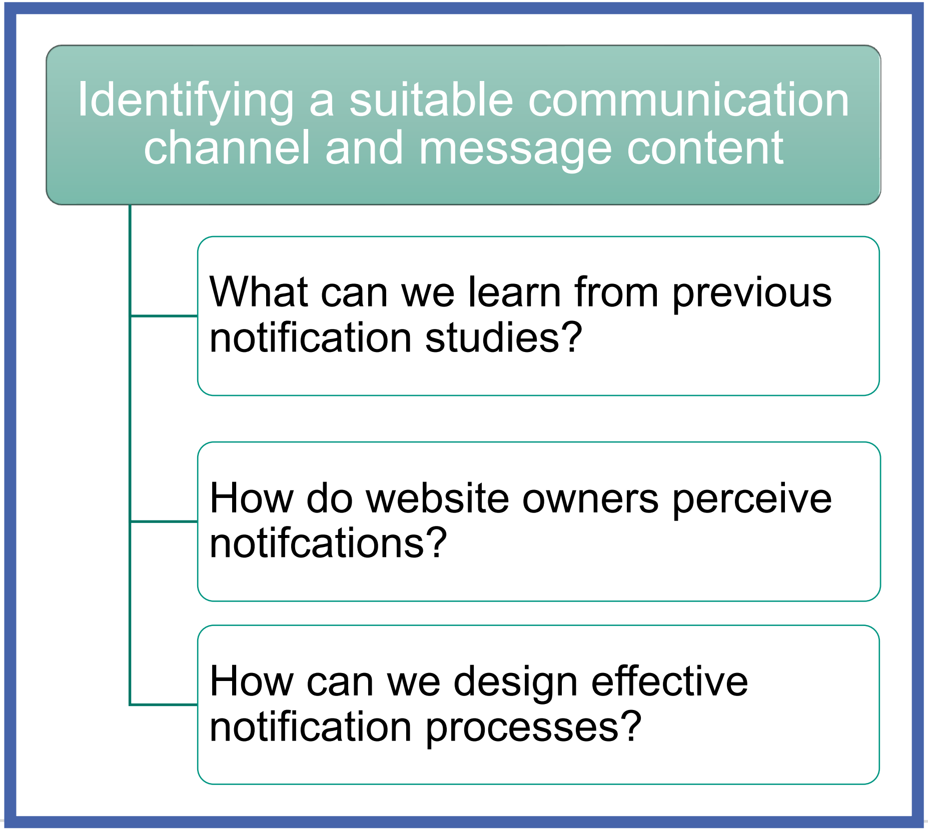
Search results of hacked website redirect to a fake shop (e.g. fake pharmacy)

Manipulation is not visible on the genuine website, only in the search engine results

Website owners (mainly) have to rely on the security community to be informed about the security issue

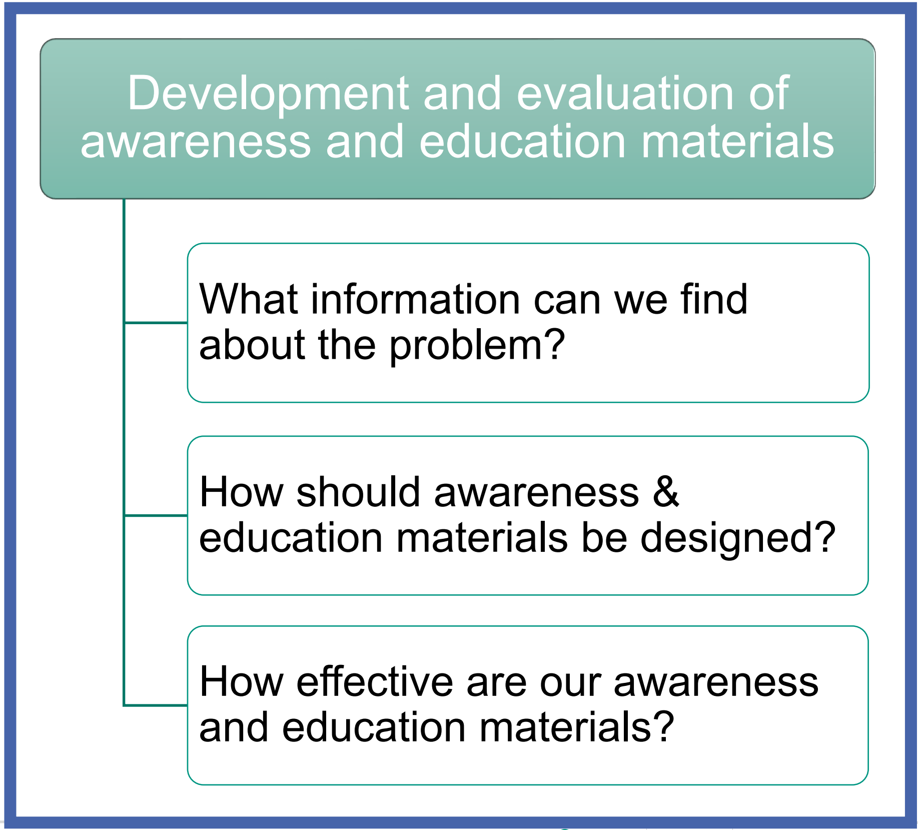

For my dissertation...
Research Plan

Research Plan



Identifying a suitable communication channel and message content

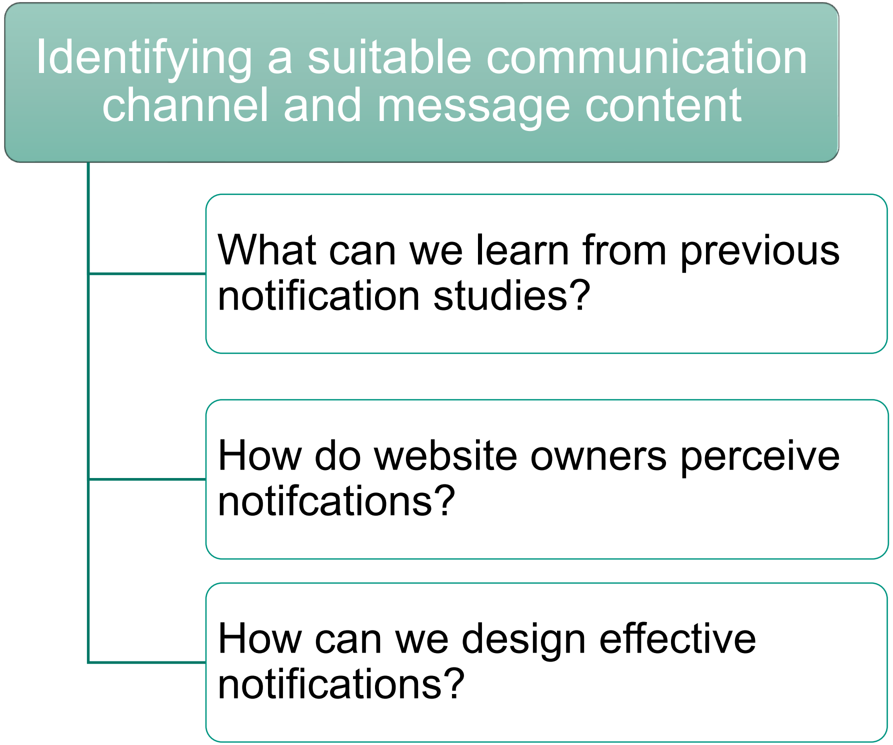
- What can we learn from previous notification studies?
- How do website owners perceive notifcations?
- How can we design effective notification processes?



Development and evaluation of awareness and education materials

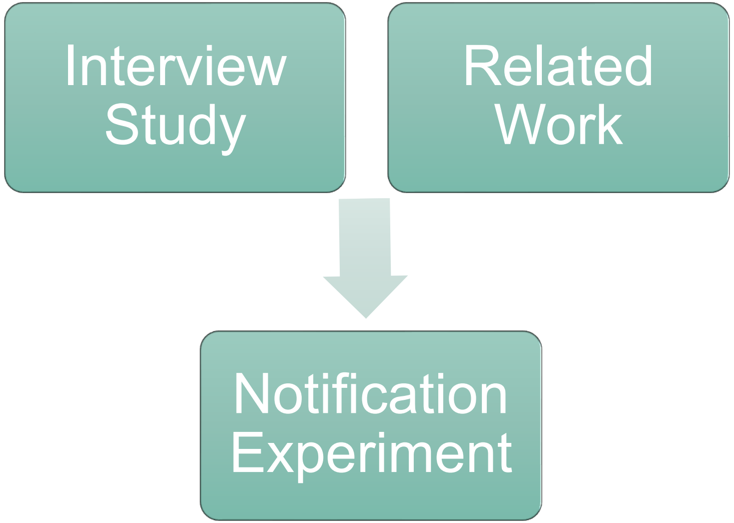
- What information can we find about the problem?
- How should awareness & education materials be designed?
- How effective are our awareness and education materials?

Research Plan - Notification



Identifying a suitable communication channel and message content

- What can we learn from previous notification studies?
- How do website owners perceive notifcations?
- How can we design effective notifications?



Interview Study

Related Work

Notification Experiment

Related Work

Related Work

~~Links~~

~~S/MIME~~ Social Media?

Google Search Console? Tool! Media Coverage! Mediators?

Links? Sender! Mailbot Phone? Letter! ~~Translation~~

~~Private Person~~ ~~Sender~~ ~~Generic email addresses~~

Sender?

~~Email~~

Webmaster?

Detailed Information! Reminder?

~~Tool~~

Uni Law Group

Webhoster

Email!

~~Reminder~~

~~Detailed Information~~

Non-Profit Organization!

Karlsruhe Institute of Technology

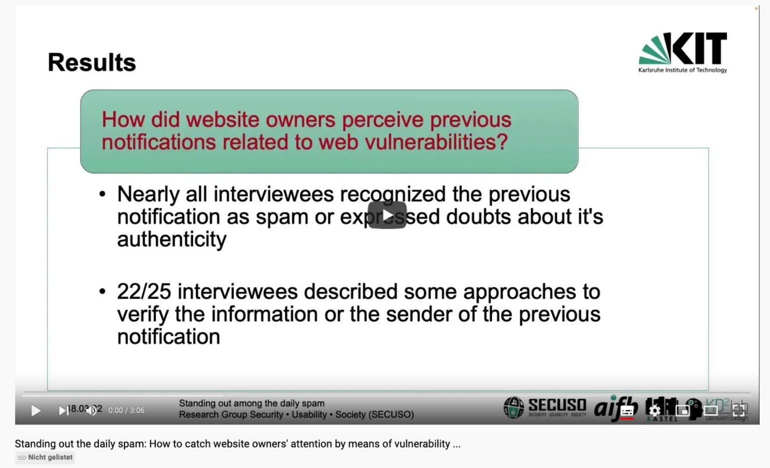
Interview Study

We asked ourselves...

How do website owners perceive (web) vulnerability notifcations?

„Standing out among the daily spam: How to catch website owners attention by means of vulnerability notifications“

Hennig, A, Neusser, F., Pawelek, A., Herrmann, D., Mayer, P.



Results

How did website owners perceive previous notifications related to web vulnerabilities?

- Nearly all interviewees recognized the previous notification as spam or expressed doubts about it's authenticity
- 22/25 interviewees described some approaches to verify the information or the sender of the previous notification

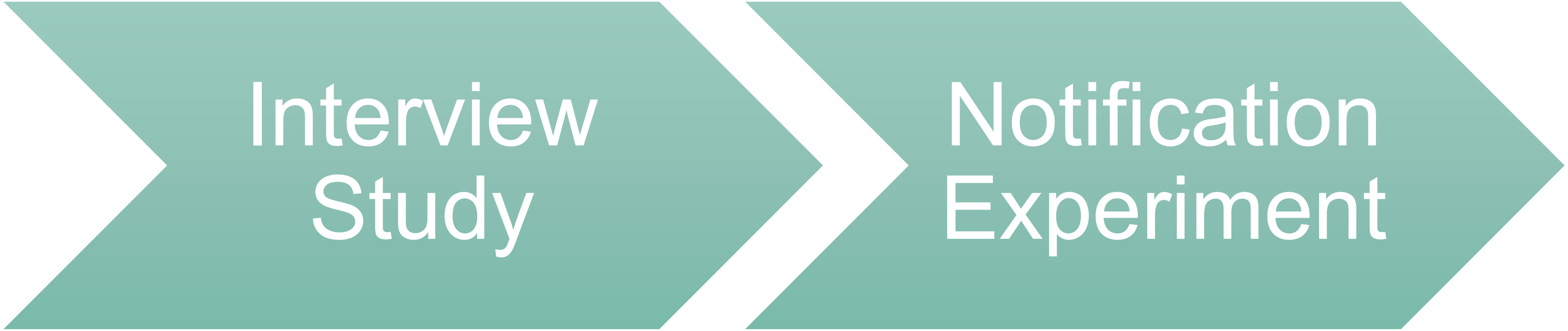
18.03.22
0:00 / 3:06
Standing out among the daily spam
Research Group Security • Usability • Society (SECUSO)

Standing out the daily spam: How to catch website owners' attention by means of vulnerability ...

Nicht gelistet

https://www.youtube.com/watch?v=X1DMHW2T7Y4

https://doi.org/10.1145/3491101.3519847



Interview Study

Notification Experiment

The main question...
Which notifications are most effective?

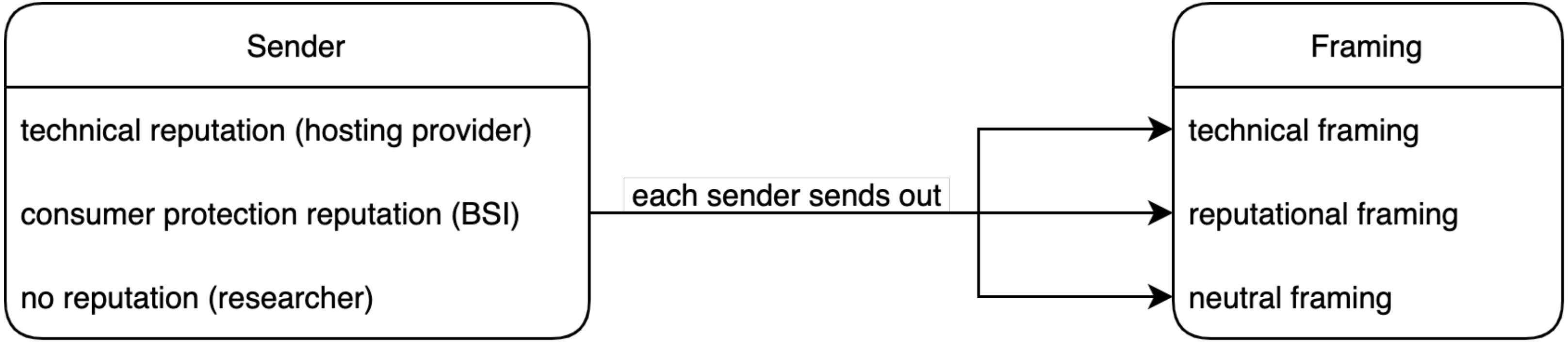
Research Questions

RQ_ES1 Which sender has which impact on the remediation rate?

RQ_ES2 Which framing has which impact on the remediation rate?

RQ_ES3 Do sender and framing of a message correlate with respect to the remediation rate?

Study Design Notification Experiment



Sender

technical reputation (hosting provider)

consumer protection reputation (BSI)

no reputation (researcher)

each sender sends out

Framing

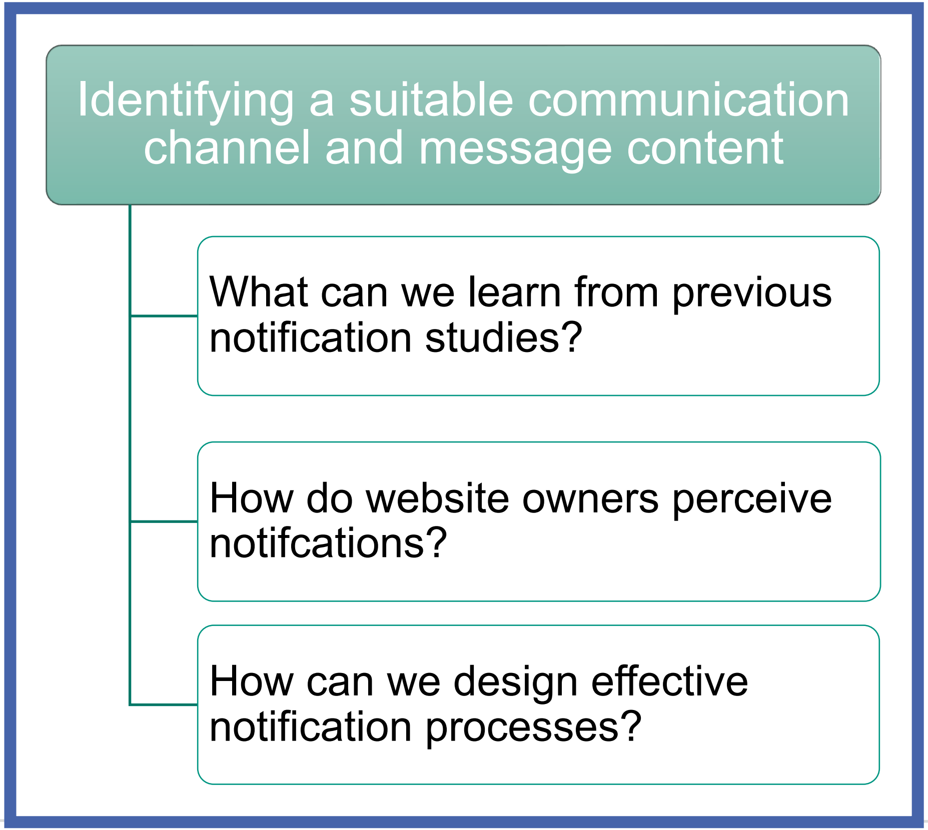
technical framing

reputational framing

neutral framing

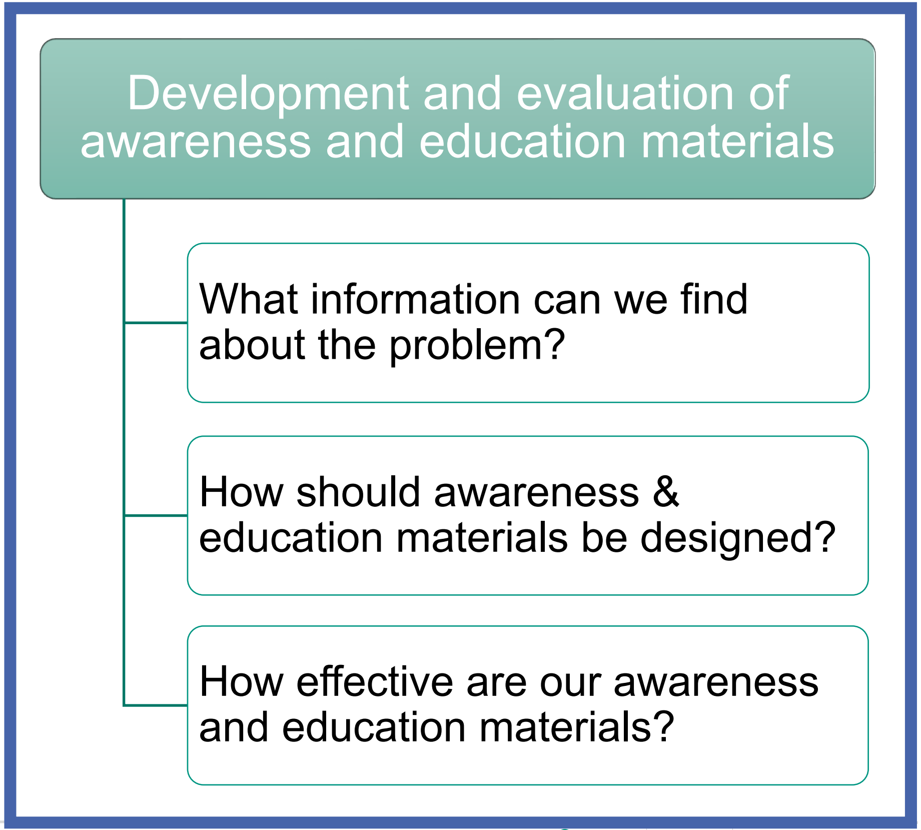
We also suggest...
Raising awareness for the problem is important!

Research Plan



Identifying a suitable communication channel and message content

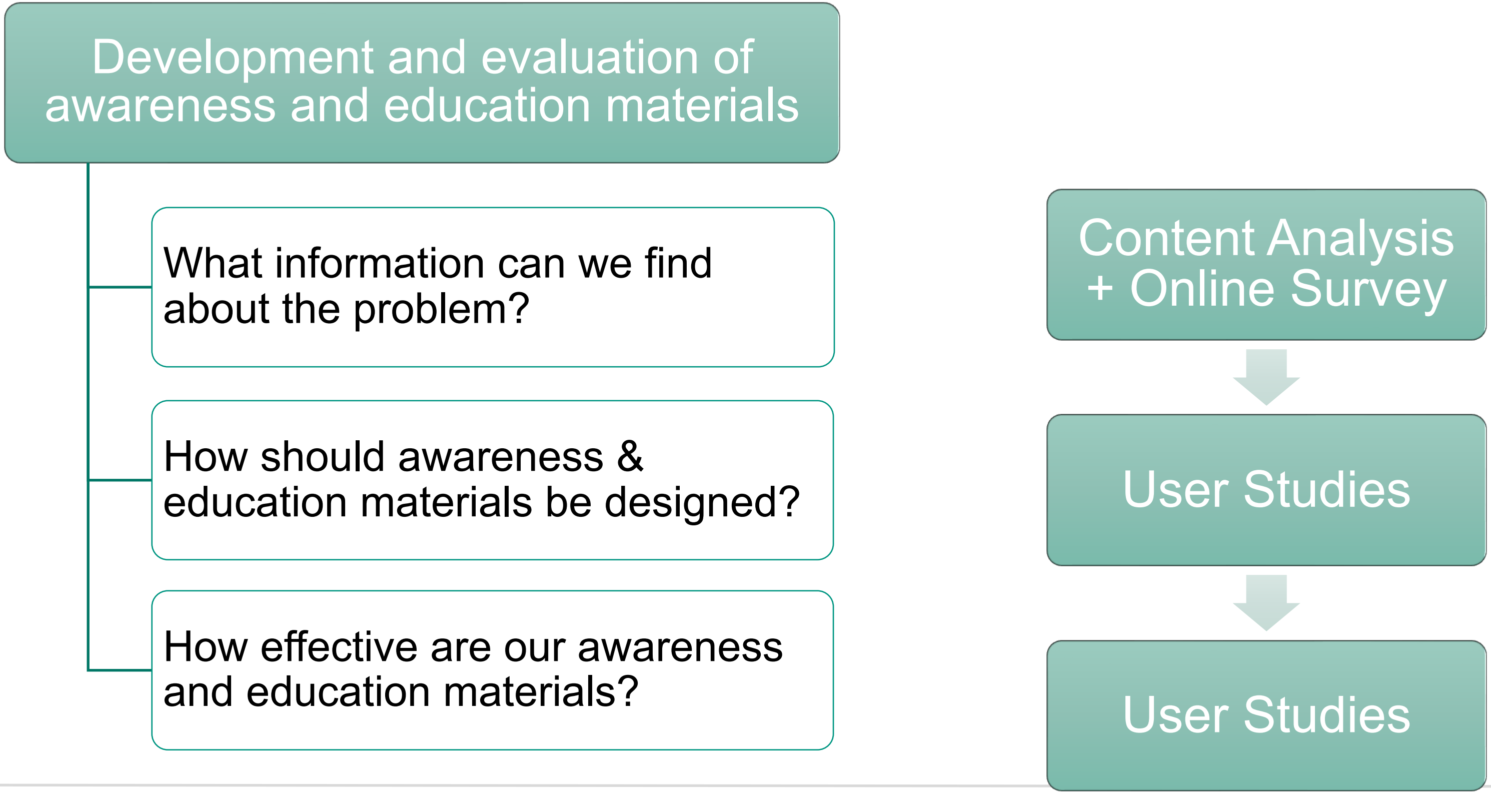
- What can we learn from previous notification studies?
- How do website owners perceive notifcations?
- How can we design effective notification processes?



Development and evaluation of awareness and education materials

- What information can we find about the problem?
- How should awareness & education materials be designed?
- How effective are our awareness and education materials?

Research Plan - Awareness



Development and evaluation of awareness and education materials

What information can we find about the problem?

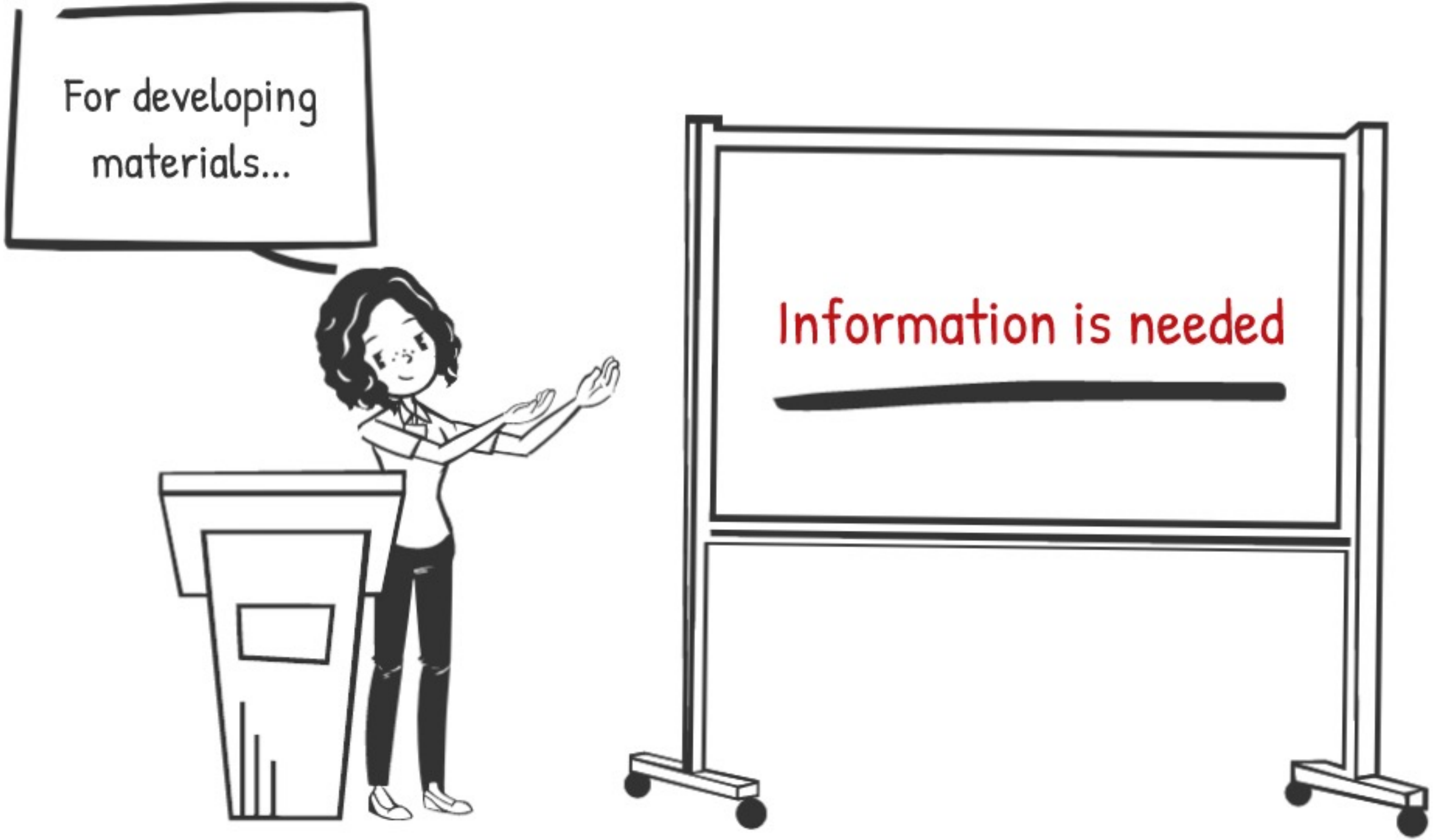
How should awareness & education materials be designed?

How effective are our awareness and education materials?

Content Analysis + Online Survey

User Studies

User Studies


For developing materials...
Information is needed

Research Questions

RQ_CA1 What information and materials about the problem can we find in often used information channels?

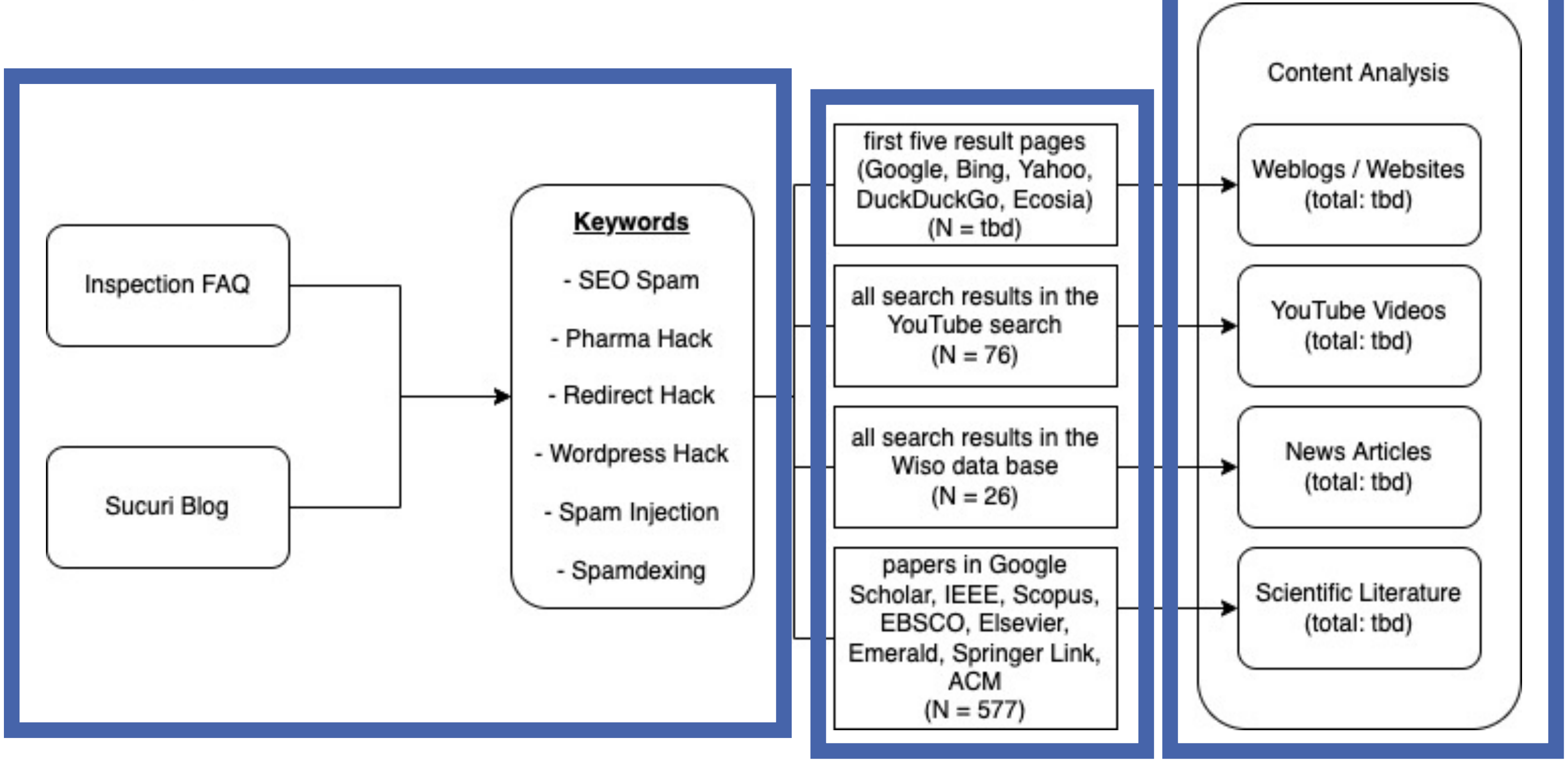
RQ_CA2 What are the characteristics of these information and materials (language? length? design?)?

RQ_CA3 How is the problem described in these information and materials (terms? which information?)?

RQ_CA4 What additional elements (e.g. graphical materials or recommendation of specific tools) are provided in these information and materials?

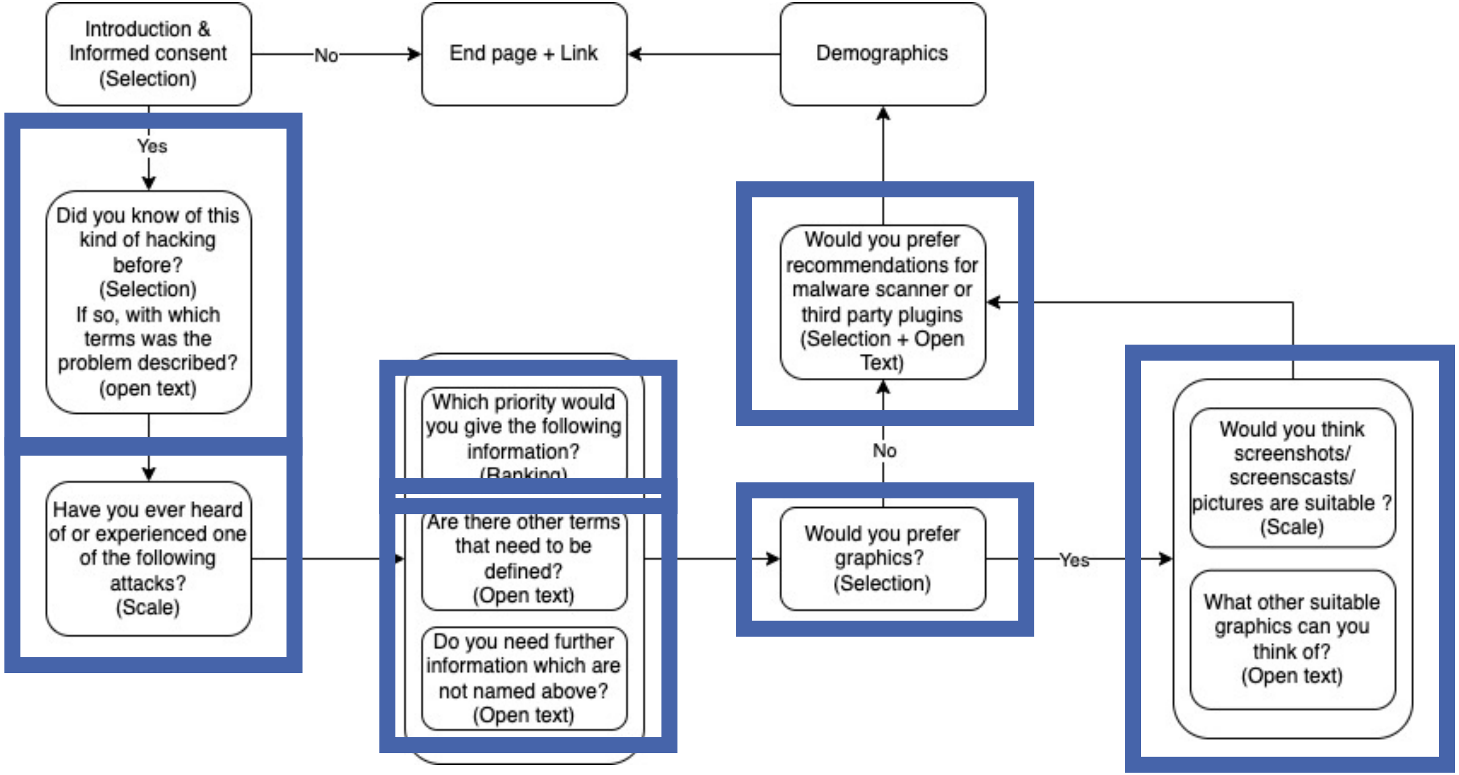
Content Analysis

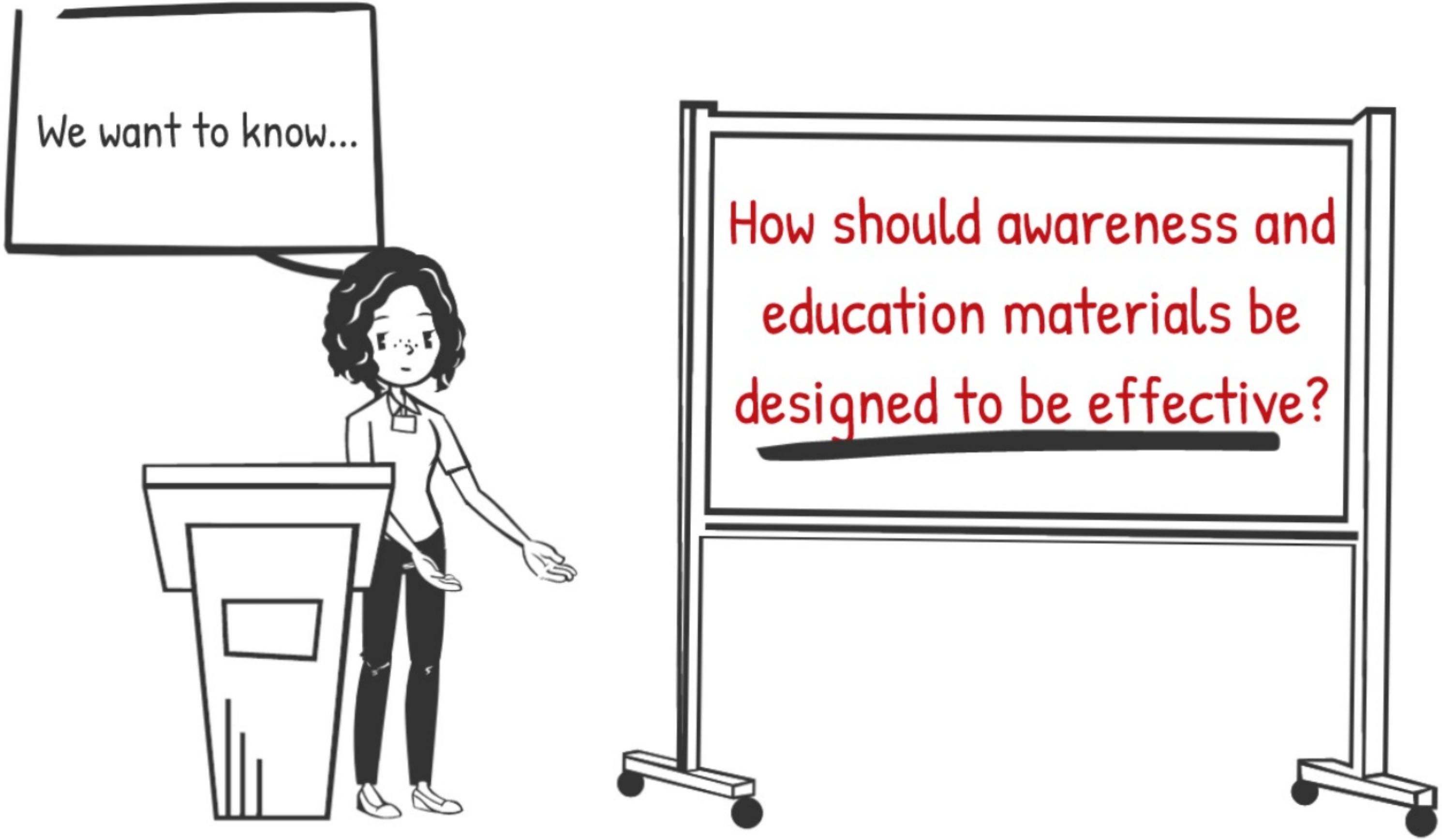
Study Design Content Analysis


Inspection FAQ
Sucuri Blog
Keywords
- SEO Spam
- Pharma Hack
- Redirect Hack
- Wordpress Hack
- Spam Injection
- Spamdexing
first five result pages (Google, Bing, Yahoo, DuckDuckGo, Ecosia) (N = tbd)
all search results in the YouTube search (N = 76)
all search results in the Wiso data base (N = 26)
papers in Google Scholar, IEEE, Scopus, EBSCO, Elsevier, Emerald, Springer Link, ACM (N = 577)
Content Analysis
Weblogs / Websites (total: tbd)
YouTube Videos (total: tbd)
News Articles (total: tbd)
Scientific Literature (total: tbd)

Online Survey

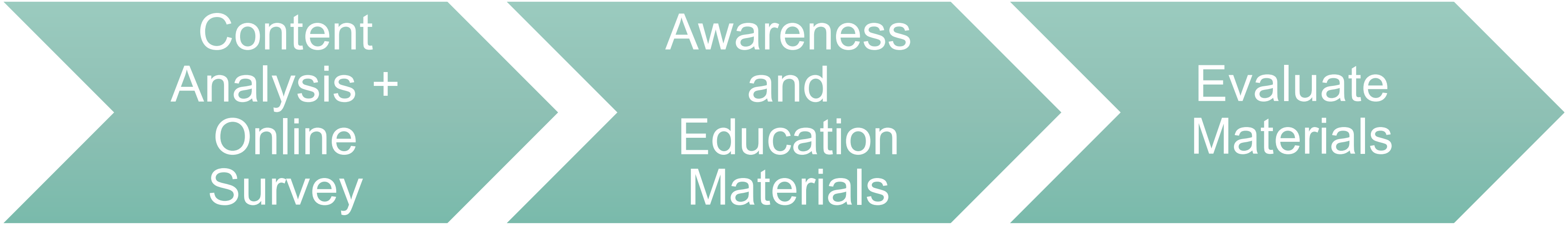
Study Design Online Survey


Introduction & Informed consent (Selection)
No
End page + Link
Demographics
Yes
Did you know of this kind of hacking before? (Selection) If so, with which terms was the problem described? (open text)
Have you ever heard of or experienced one of the following attacks? (Scale)
Which priority would you give the following information? (Ranking)
Are there other terms that need to be defined? (Open text)
Do you need further information which are not named above? (Open text)
Would you prefer recommendations for malware scanner or third party plugins (Selection + Open Text)
No
Would you prefer graphics? (Selection)
Yes
Would you think screenshots/ screenscasts/ pictures are suitable ? (Scale)
What other suitable graphics can you think of? (Open text)



We want to know...

How should awareness and education materials be designed to be effective?

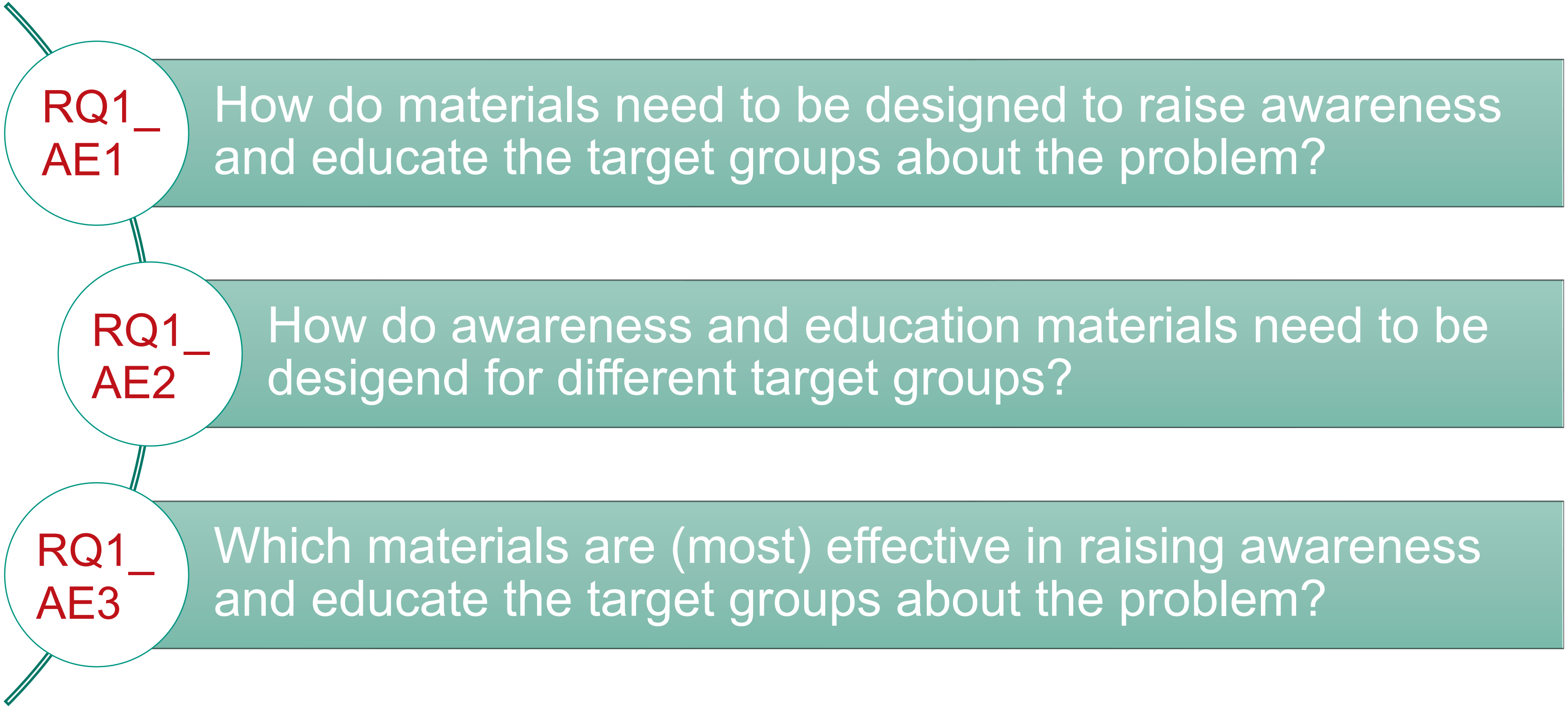


Content Analysis + Online Survey

Awareness and Education Materials

Evaluate Materials

(Possible) Research Questions



RQ1_ AE1 How do materials need to be designed to raise awareness and educate the target groups about the problem?

RQ1_ AE2 How do awareness and education materials need to be desigend for different target groups?

RQ1_ AE3 Which materials are (most) effective in raising awareness and educate the target groups about the problem?

Study Design Ideas

Expert Interviews (Hosting Provider? Mediators?)

Focus Group Interviews (Website Owners?)

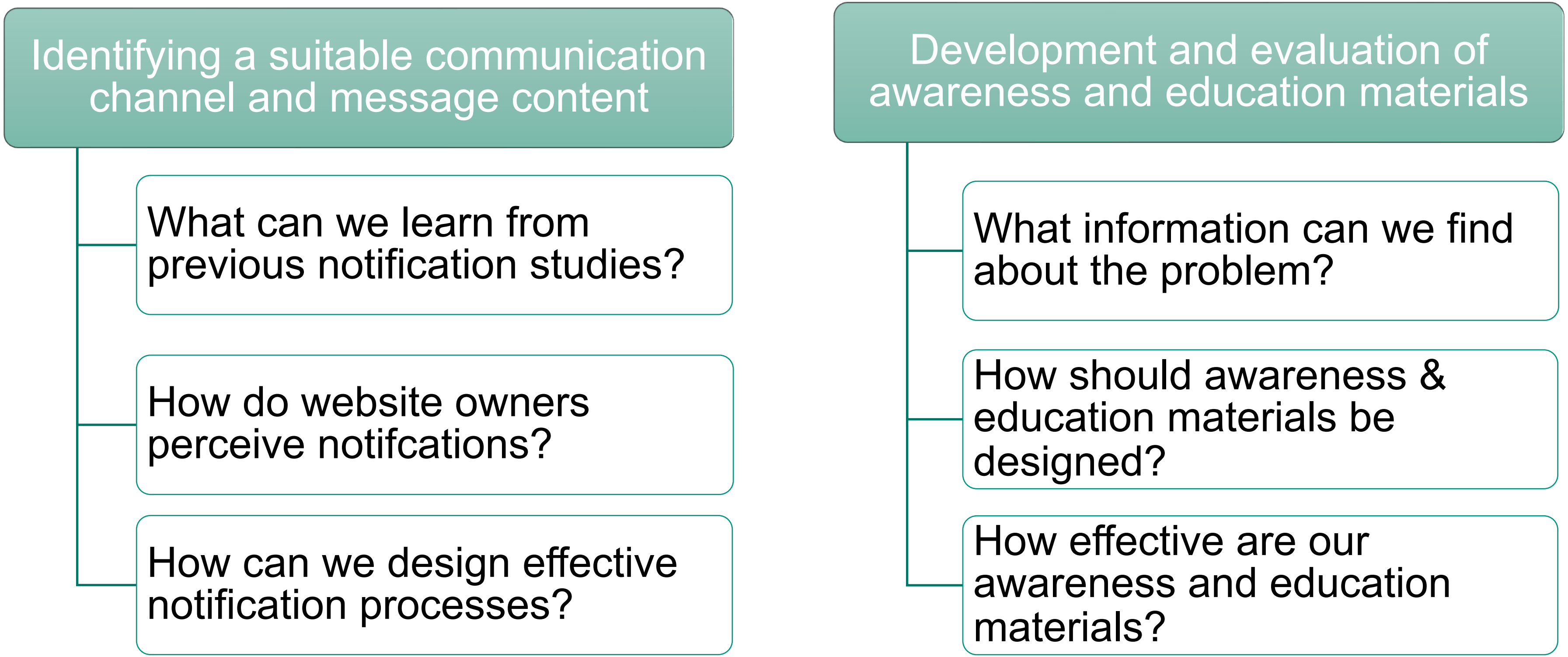
Surveys (Atendees of Information Events?)

Online Surveys (Users in General?)

Observational Studies (Users in General?)

To conclude...
Research Plan

Research Plan



Identifying a suitable communication channel and message content

- What can we learn from previous notification studies?
- How do website owners perceive notifcations?
- How can we design effective notification processes?

Development and evaluation of awareness and education materials

- What information can we find about the problem?
- How should awareness & education materials be designed?
- How effective are our awareness and education materials?

Thank you for your attention!

Any Questions?