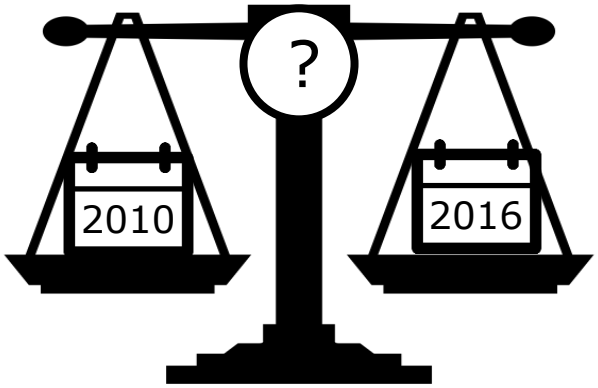
A Second Look at Password Composition Policies in the Wild: Comparing Samples from 2010 and 2016

Peter Mayer, Jan Kirchner, Melanie Volkamer



Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag
IT-Sicherheit IN DER WIRTSCHAFT
KMU AWARE
SECUSO SECURITY · USABILITY · SOCIETY
TECHNISCHE UNIVERSITÄT DARMSTADT

This talk

What it is about

- Password Composition Policies (PCP)
- Replication of study by Florêncio & Herley (SOUPS'10)

Outline

1. Description of original study
2. Description of our replication study
3. Conclusions

Original study – Overview

Motivation

- Unknown what influences PCP strength

Goal

- Identify website features' influence on PCP strength

Original study – Method Investigated Features

Website feature
Observation and evidence
Size of the service
User name public
Value of the resources protected
Extractable value of the resources protected
Who lives with the consequences of a breach
Advertising accepted
Site advertises
User has choice

Original study – Method Investigated Features

Website feature	Hypothesized effect
Observation and evidence	↑
Size of the service	
User name public	
Value of the resources protected	
Extractable value of the resources protected	
Who lives with the consequences of a breach	
Advertising accepted	↓
Site advertises	
User has choice	

Original study – Method
Investigated Features

Website feature	Hypothesized effect	Actual effect on PCP strength
Observation and evidence	↑	?
Size of the service		
User name public		
Value of the resources protected		
Extractable value of the resources protected		
Who lives with the consequences of a breach		
Advertising accepted	↓	
Site advertises		
User has choice		

Original study – Method Website Sampling

- Quantcast traffic rank
  - Top (rank 1 – 20)
  - High (rank 101 - 110)
  - Medium (rank 1001 - 1010)
- Website type
  - Largest Banks
  - Biggest Universities
  - Top computer science departments
  - Government

Original study – Method Identification of PCPs

- Searched websites for policy
- Created account whenever possible
- If no PCP could be found: Internet search
- First PCP found used in study

Original study – Method Determining strength and features

Measuring PCP strength

$$N_{min} * log_2(C_{min})$$

(N_{min}: minimum length, C_{min}: minimum character set)

Evaluation of website features

- Some based on analyses
- Some based on argumentation

Original study – Results

Website feature	Hypothesised effect	Actual effect on PCP strength
Observation and evidence	↑	-
Size of the service		-
User name public		-
Value of the resources protected		-
Extractable value of the resources protected		-
Who lives with the consequences of a breach		-
Advertising accepted	↓	↓
Site advertises		↓
User has choice		↓

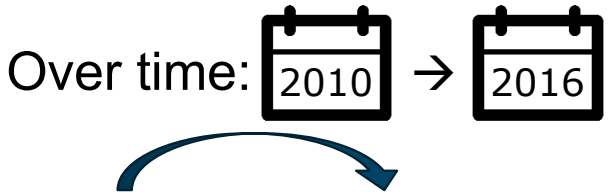
Replication study – Overview

Motivation

- Several years since original study
- Only websites from the USA

Goal

- Replication of study



Website feature	Hypothesized effect	Actual effect on PCP strength		
		USA 2010	USA 2016	Germany 2016

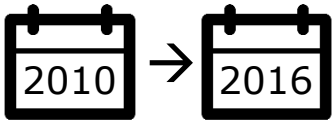
Replication study – Method Website sampling

- USA 2010 (original sample)
- USA 2016
  - Same websites as USA 2010 sample (minus 5 websites)
  - Updated PCP strength values
- Germany 2016
  - Sampled from the same categories
  - German traffic ranks, banks, universities

Replication study – Method Deviations

- Use of Alexa ranks instead of Quantcast ranks
- Manual check whether websites accept advertising

Replication study – Research Questions

Over time: 

RQ1: Has the average PCP strength in the USA sample changed since the original study?

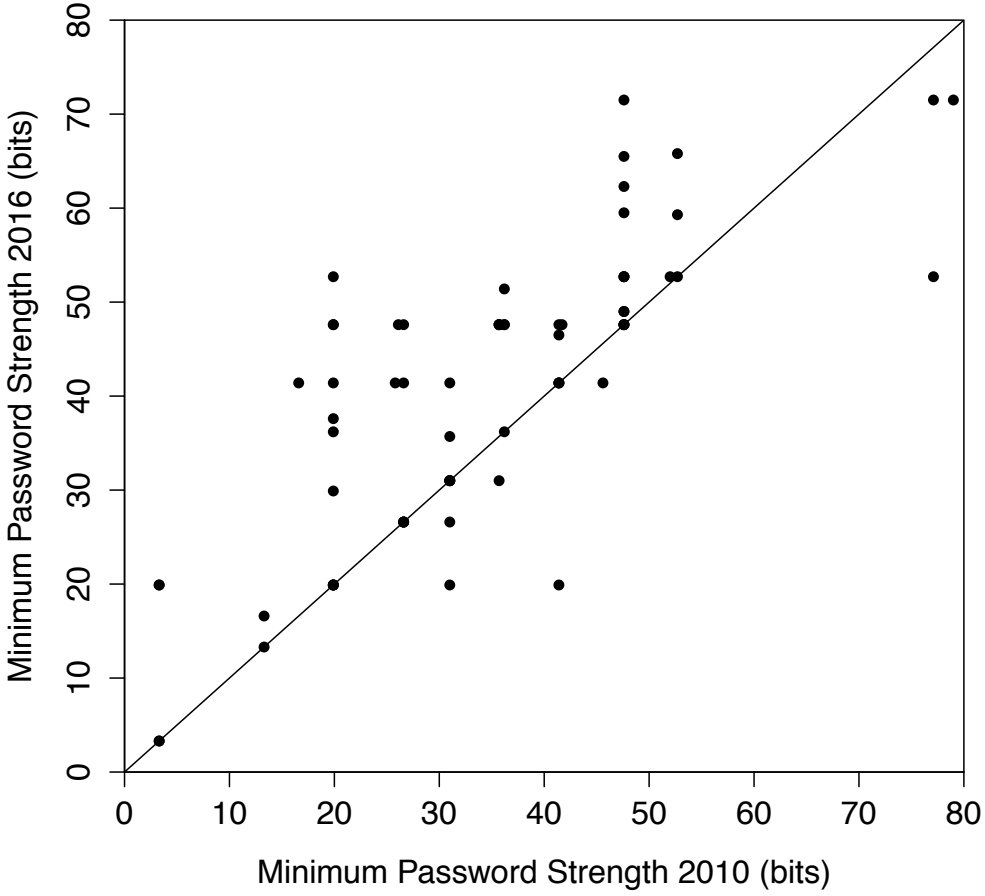
RQ2: Do the effects of the website features on the PCP strength from the original study still apply to the USA 2016 sample?

Across countries: 

RQ3: How do the German and USA samples compare in terms of PCP strength?

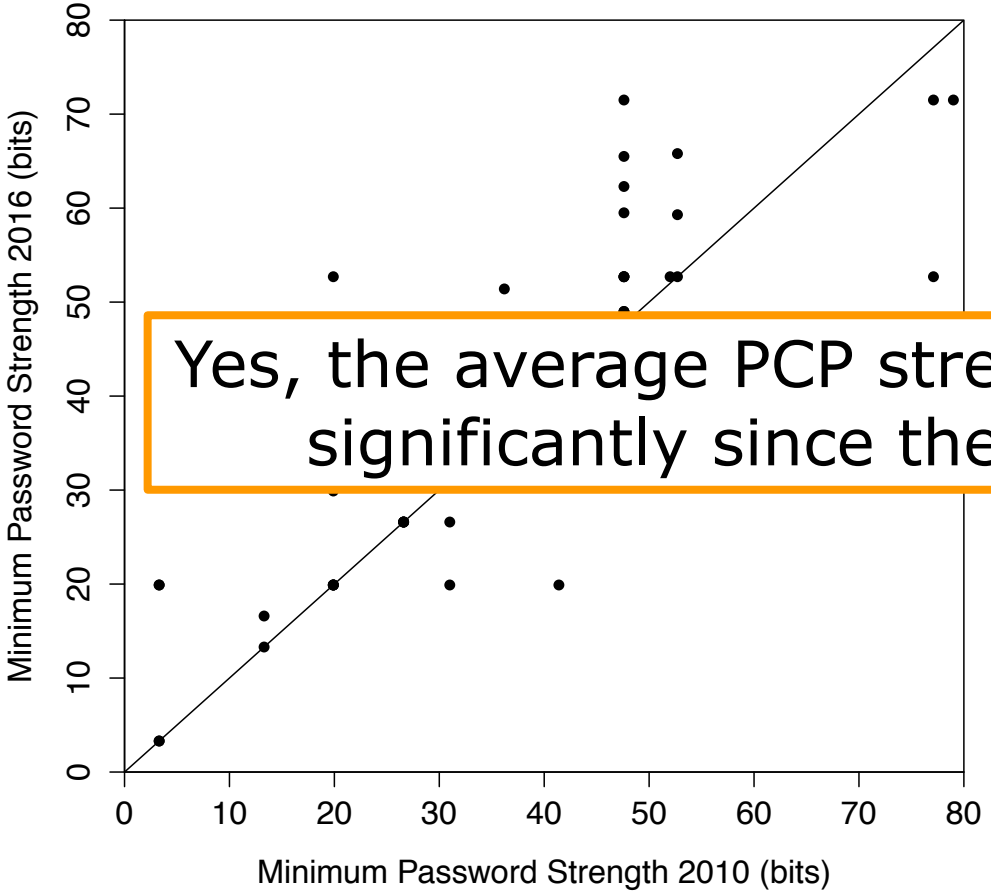
RQ4: Do the effects of the website features on the PCP strength from the original study translate to the German sample?

Replication study – Results
RQ1: Strength over time



	Category	USA 2010	USA 2016
Traffic	Top traffic	19.9	26.6
	High traffic	19.9	41.5
	Medium traffic	36.2	46.5
Website type	Bank	31.0	35.7
	Education	41.7	47.6
	Government	47.6	52.7
	Others	19.9	29.9
Overall		**35.7**	**41.4**

Replication study – Results
RQ1: Strength over time



Yes, the average PCP strength has increased significantly since the original study.

	Category	USA 2010	USA 2016
Website traffic	Top traffic	19.9	26.6
	High traffic	19.9	41.5
			46.5
			35.7
	Education	41.7	47.6
	Government	47.6	52.7
	Others	19.9	29.9
Overall		**35.7**	**41.4**

Replication study – Results
RQ2: Features over time

Website feature	Hypothesised effect	Actual effect on PCP strength	
		USA 2010	USA 2016
Observation and evidence	↑	-	-
Size of the service		-	-
User name public		-	-
Value of the resources protected		-	-
Extractable value of the resources protected		-	-
Who lives with the consequences of a breach		-	-
Advertising accepted	↓	↓	↓
Site advertises		↓	-
User has choice		↓	↓

Replication study – Results
RQ2: Features over time

Website feature	Hypothesised effect	Actual effect on PCP strength	
		USA 2010	USA 2016
Observation and evidence		-	-
Size of the service		-	-
User name public			-
Value of th			-
Extractabl protected			-
Who lives with the consequences of a breach		-	-
Advertising accepted	↓	↓	↓
Site advertises		↓	-
User has choice		↓	↓

Only one website feature seems to have changed.

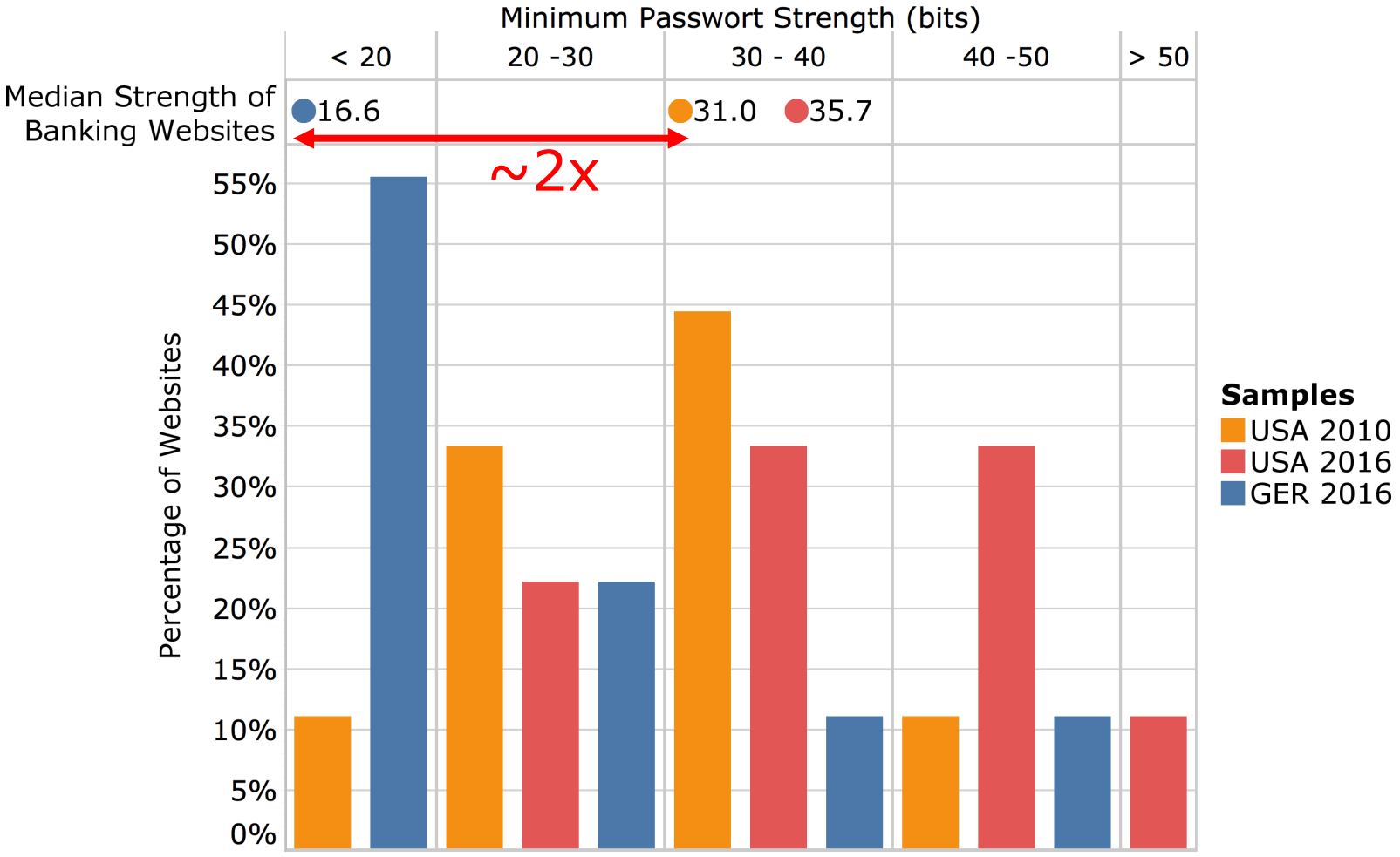
Replication study – Results
RQ3: Strength across countries

	Category	USA 2010	USA 2016	Germany 2016
Traffic	Top traffic	19.9	26.6	26.6
	High traffic	19.9	41.5	26.6
	Medium traffic	36.2	46.5	19.9
Website type	Bank	31.0	35.7	16.6
	Education	41.7	47.6	30.8
	Government	47.6	52.7	47.6
	Others	19.9	29.9	26.6
Overall		**35.7**	**41.4**	**26.6**

Replication study – Results
RQ3: Strength across countries

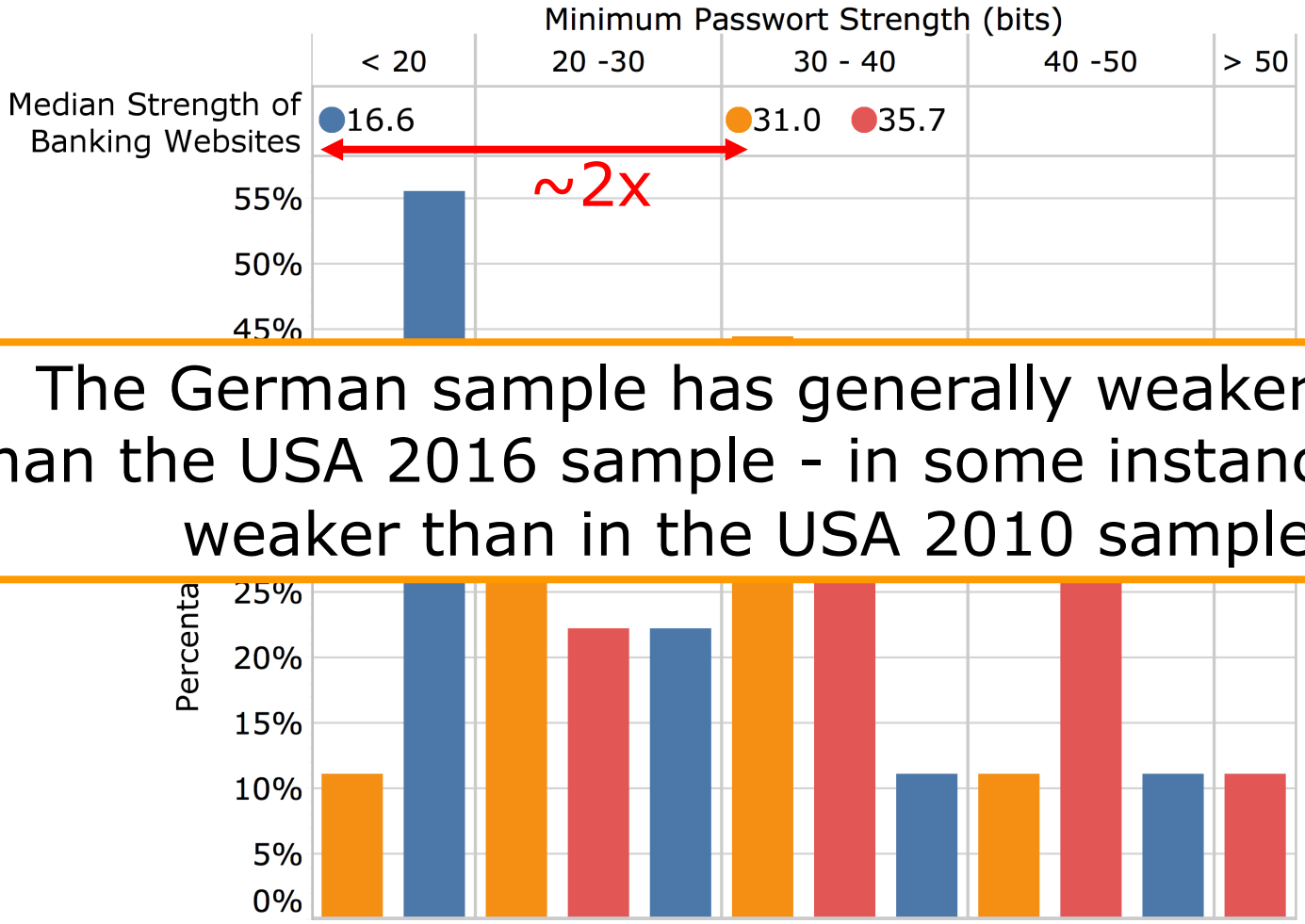
	Category	USA 2010	USA 2016	Germany 2016
Traffic	Top traffic	19.9	26.6	26.6
	High traffic	19.9	41.5	26.6
	Medium traffic	36.2	46.5	19.9
Website type	Bank	31.0	35.7	16.6
	Education	41.7	47.6	30.8
	Government	47.6	52.7	47.6
	Others	19.9	29.9	26.6
Overall		**35.7**	**41.4**	**26.6**

Replication study – Results
RQ3: Strength across countries



SECUSO SECURITY · USABILITY · SOCIETY
TECHNISCHE UNIVERSITÄT DARMSTADT

Replication study – Results
RQ3: Strength across countries



The German sample has generally weaker PCPs than the USA 2016 sample - in some instances even weaker than in the USA 2010 sample.

Replication study – Results
RQ4: Features across countries

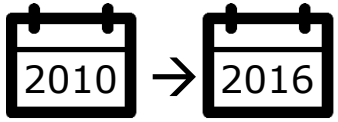
Website feature	Hyp. effect	Actual effect on PCP strength		
		USA 2010	USA 2016	Germany 2016
Observation and evidence	↑	-	-	-
Size of the service		-	-	-
User name public		-	-	-
Value of the resources protected		-	-	-
Extractable value of the resources protected		-	-	-
Who lives with the consequences of a breach		-	-	-
Advertising accepted	↓	↓	↓	-
Site advertises		↓	-	-
User has choice		↓	↓	↓

Replication study – Results
RQ4: Features across countries

Website feature	Hyp. effect	Actual effect on PCP strength		
		USA 2010	USA 2016	Germany 2016
Observation and evidence		-	-	-
Size of the service		-	-	-
User name public				
V				
Extractable value of the resources protected		-	-	-
Who lives with the consequences of a breach		-	-	-
Advertising accepted		↓	↓	-
Site advertises	↓	↓	-	-
User has choice		↓	↓	↓

Only one feature translates to the German sample.

Conclusions

RQ1 & RQ2 - Over time: 

- PCP strength in the USA has risen
- Not all features translate over time
- No effect of features hyp. to increase PCP strength

➜ Open questions

- Which features actually increase PCP strength?

Conclusions

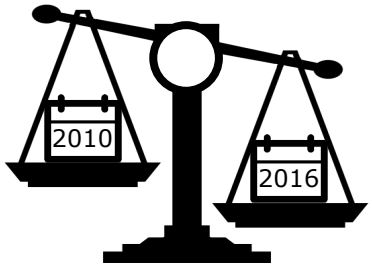
RQ3 & RQ4 - Across countries:  → 

- PCPs in the German sample are generally weaker
- In particular German banks stand out
  - On average weak PCPs, some very restrictive e.g.
    - Exactly 6-digit PINs
    - Exactly 5 characters, must have letter and numbers, no symbols allowed
  - Tight lock out policies (3 strikes)
  - Mandated usage of two factor authorisation (of transactions)

➜ Open questions

- Do users find this trade-off appropriate in the banking context?
- Would they like to make this trade-off elsewhere?

Questions?



Over time
- Rise in PCP strength
- One feature has lost effect
- Others remain unchanged

Across Countries
- PCPs in German sample weaker
- German banking websites stand out

Limitations
- Strength measure is rough
- Only investigated website features not technologies on user side
- Some analyses use approximations
- Same websites in USA sample for 2010 and 2016

Website feature	Hypothesised effect	Actual effect on PCP strength		
		USA 2010	USA 2016	Germany 2016
Advertising accepted	↓	↓	↓	-
Site advertises		↓	-	-
User has choice		↓	↓	↓

SECUSO SECURITY · USABILITY · SOCIETY
TECHNISCHE UNIVERSITÄT DARMSTADT
KARLSTADS UNIVERSITET

KMU AWARE

- Part of the initiative „IT-Sicherheit in der Wirtschaft“

www.it-sicherheit-in-der-wirtschaft.de

- **Goal:** Development of IS awareness and education materials for inclusion in web-based training platform

SECUSO SECURITY · USABILITY · SOCIETY
TECHNISCHE UNIVERSITÄT DARMSTADT

Icons

All icons from https://thenounproject.com/ and licensed under a Creative Commons Attribution 3.0 United States License or in the public domain.

Artists: Iconika, logan