Zurich University
of Applied Sciences
School of
Engineering
InIT Institute of Applied
Information Technology

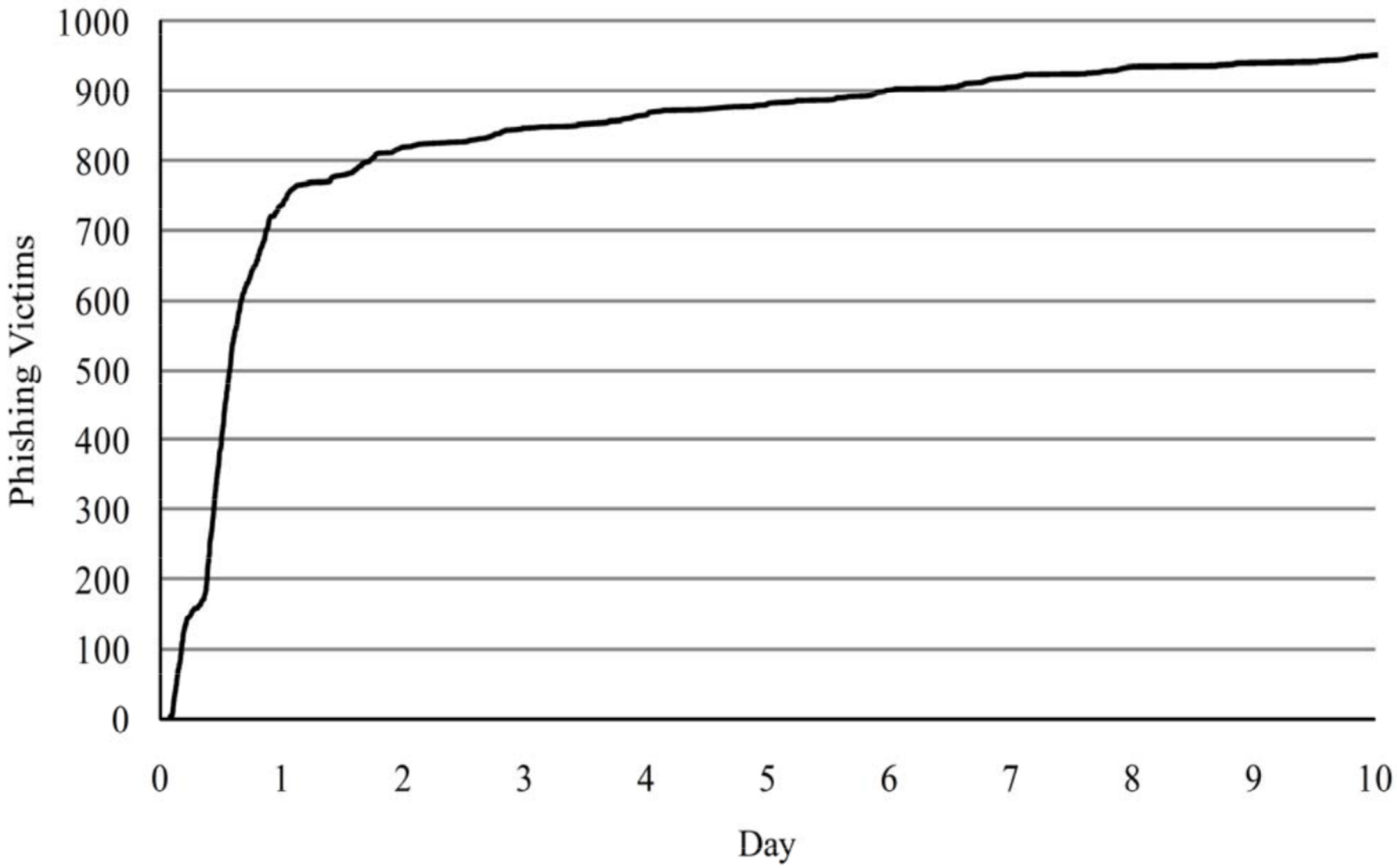
How to Phish – How does the perfect embedded training look like?

Prof. Dr. Bernhard Tellenbach
Daniel Jampen

Starting Point

- ZHAW wanted to do phishing awareness training
- We got the task to:
  - Check out the tooling situation for launching phishing campaigns
  - Check out the scientific body of knowledge - How to do a an effective training?
    - Frequency, difficulty level etc.
- Well, if you ask this a researcher…
  - Analyzed roughly 150 scientific papers about phishing
  - What training and with what parameters works best?

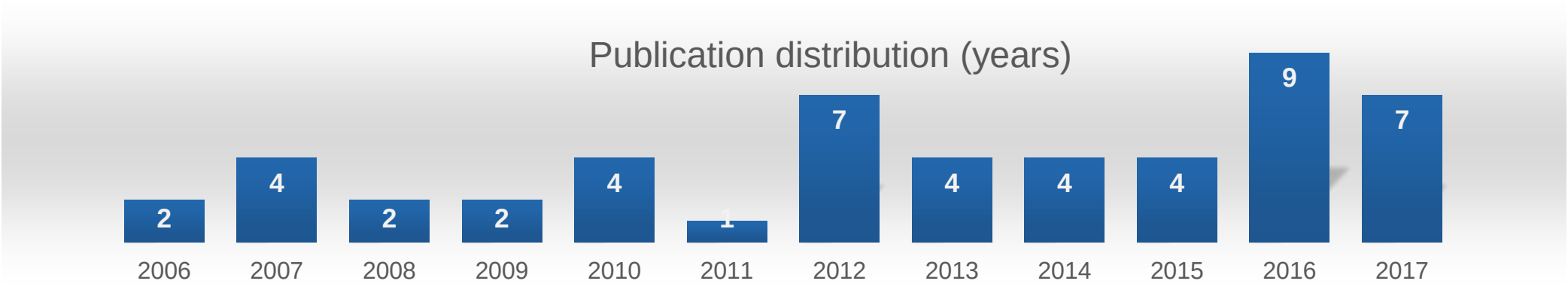
When can we evaluate the results?



Phishing in a university community: Two large scale phishing experiments
Jamshaid G. Mohebzada ; Ahmed El Zarka ; Arsalan H. Bhojani ; Ali Darwish

Research – Categories & Publications

Category	Amount of included publications
Impact of the Target Group	21
Email Content and Structure	11
Feedback	21
Knowledge Retention	11
Training Impact	22
Total	**50**
Total publications checked	138



Impact of Target Group

Parameter	Has impact	No impact
Age	[13], [25]	[12], [16]
Gender	[14], [24], [25]	[12], [16], [17], [26]
Scientific degree	[12], [13]	-
High use of online activities	-	[27]
Email experience	[28], [29]	-
Increased submissiveness	[28]	-
Awareness level	[12]	-
Known sender address	[31]	-
Job technicalness	-	[15], [30]

Email Content and Structure

Parameter	Has impact	No impact
Content	persuasive [32], scarcity [25], authority [25], trust symbols [34], [35]	spelling errors [37]
Topic	shipping [32], order [32], received fax [32], complaint [32],legal emails [25], banks [21], government institutions [21]	Other gain [19], other loss [19], individual gain [19], individual loss [19], financial topics [25]
Link URL	category 5, 6 [33], [49], same protocol [18], contains secure or similar terms [49]	category 1,2,7 [33]
Design	clone of original [18], [36]	-

Email Content and Structure – Link Categories

URL Spoofing Tricks	Level
a) IP address, no brand (e.g. http://130.82.162.6/)	Level 2
b) Random/unrelated/trustworthy domain, no brand (e.g. https://marketchippy.com/ or http://www.account.com/login)	Level 3
c) Random/unrelated/trustworthy domain, brand in subdomain (e.g. http://paypal.kjdhsbc.com/signin)	Level 4
d) Random/unrelated/trustworthy/IP domain, brand in path (e.g. http://online-payment.com/www.paypal.com/)	Level 5
e) Derivated domains (e.g. https://www.facebook-login.com/)	Level 6
f) Introducing typos (e.g. http://www.twittter.com/)	Level 7
g) Replacing Character(s) (e.g. http://www.arnazon.com/)	Level 8

Feedback – Training Types

Parameter	More impact	Less/no impact
Short term train-ing	in-class [26], [45]	-
Long term train-ing	recurring [38] embedded train-ing [16], [38], [43], [45]	-
Warning messages	effective [46] if interrupting user [23]	toolbar [41]

Knowledge Retention

Parameter	Value
Approach	recurring [38] training [13], [16], [19], [38], [47] individualized per user [38]
Minimum interval	7 days [15], [39], 16 days [48], 28 days [13]
Maximum interval	set by management [38], less than 5 months [49]

Science – Conclusions from studing research

Category	Parameter(s)	Value
Impact of the Target Group	Target demographics	non-conclusive results
	Identify targets	train everyone or use CRI
Email Content and Structure	Best email topics	Shipping, Orders, received fax
	Email persuasiveness	more = better
	Email design	1:1 clone of legitimate mail
	Level design	**increasing difficulty**
Training Impact	Education form	Initial course, then ongoing training
Feedback	Feedback	embedded training, imminent
	Education progression	**level system, per user**
Knowledge Retention	Training interval(s)	adjusted to levels, min. 4x/year

Now What?

- We have results from our study of the scientific body of knowledge
- Tools: We have found that there are a lot of phishing training tools and program for embedded training

- Important finding: Existing tools …
  - … have limited automation capabilities
  - … are often «single email» campaign products
  - … are usually not considering the skills of the targets
  - … are **not using research results** on how to do «high impact» training
  - … do not have ways to share the workload in a community

Goal/Vision – The «perfect» tool

- High impact - Training backed and further optimized by science
- Community functions - Share the workload
- Fire-and-forget - Fully automated training
- Privacy by design – Reporting & data sharing

- Let’s do it!

… but not alone!

THANK YOU!