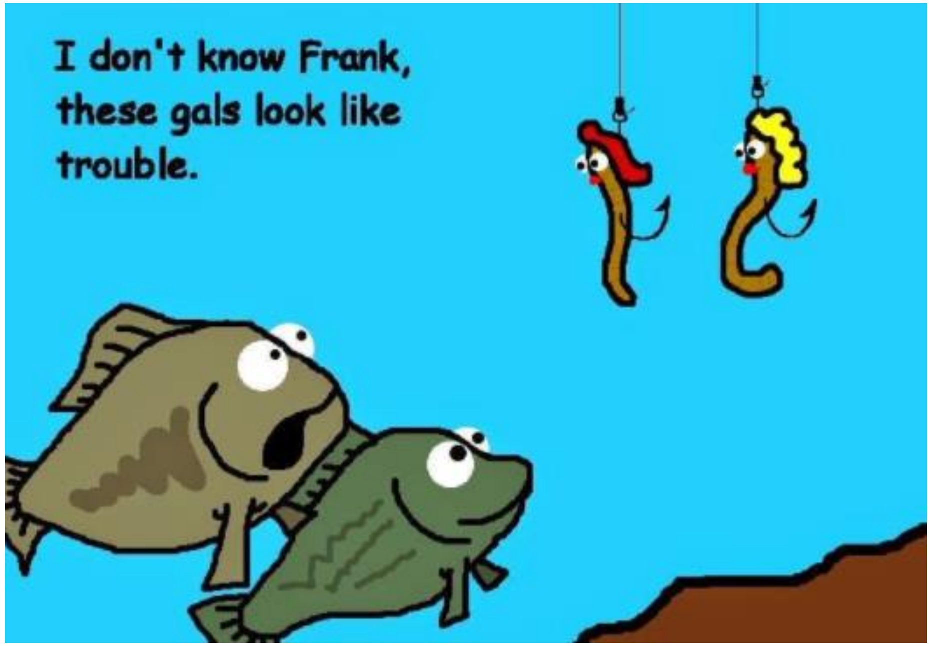
Still Plenty of Phish in the Sea - A Taxonomy of User-Oriented Phishing Interventions and Avenues for Future Research

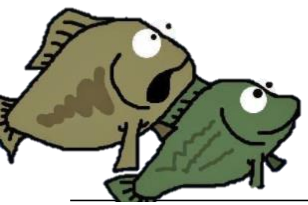
Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig,

Christian Reuter, Alexander Benlian and Joachim Vogt

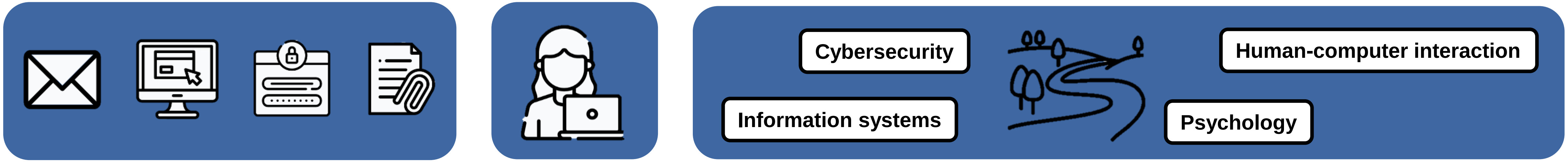


Twitter @FishingHumor

TECHNISCHE UNIVERSITÄT DARMSTADT



Frank’s friend is right!



Research goal: Systematization of knowledge

RQ1: How does current research on user-oriented phishing interventions tackle the aim of guiding users towards secure online behavior?

RQ2: Which avenues for future research emerge from the existing phishing intervention literature?

Methodology: Systematic literature review

- ACM Digital Library
- IEEE Explore
- Web of Science
- A* and A CORE-ranked security conferences and journals

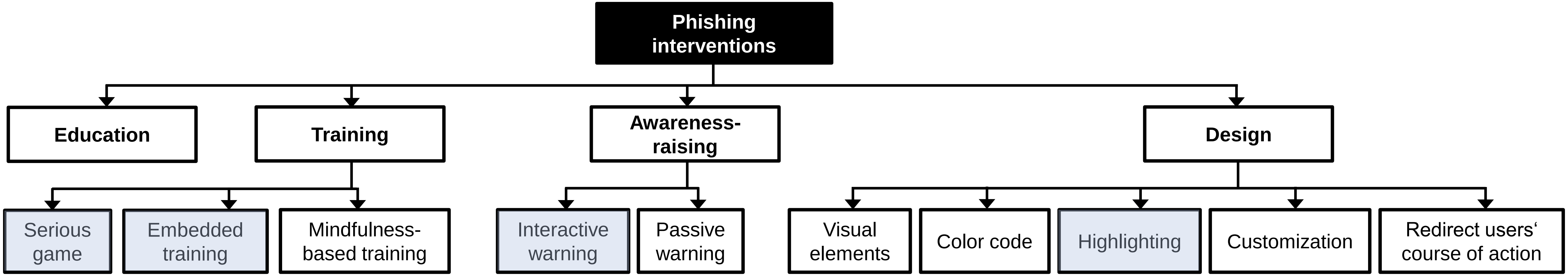
Peer-reviewed studies in English available as of June 2020

phish* AND (interven* OR prevent* OR educat* OR detect* OR train* OR nudg* OR appeal)

2,124 articles

Final literature sample: **64 articles**

How can phishing interventions be taxonomized?



Phishing interventions

Education

Training

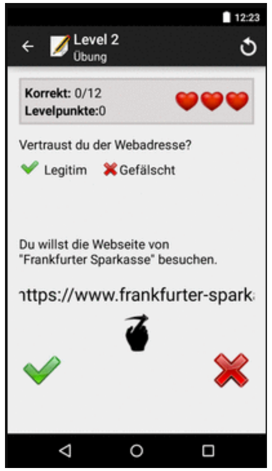
- Serious game
- Embedded training
- Mindfulness-based training

Awareness-raising

- Interactive warning
- Passive warning

Design

- Visual elements
- Color code
- Highlighting
- Customization
- Redirect users' course of action



12:23

Level 2
Übung

Korrekt: 0/12
Levelpunkte:0

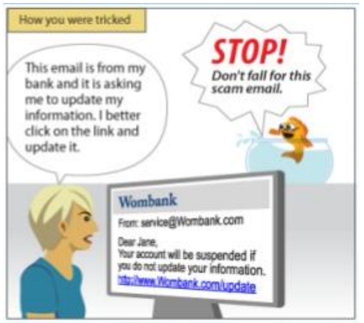
Vertraust du der Webadresse?

✓ Legitim ✗ Gefälscht

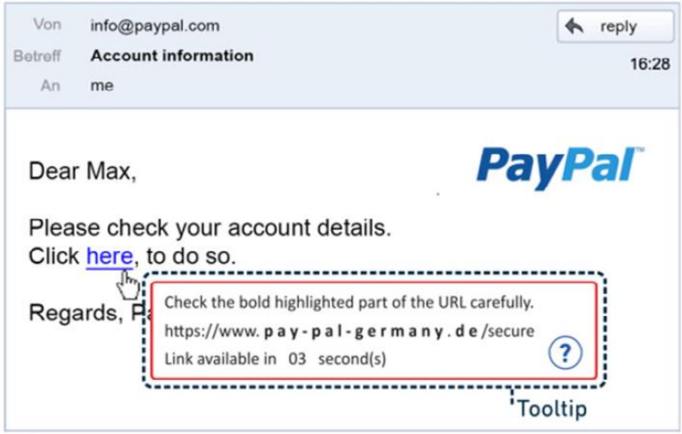
Du willst die Webseite von "Frankfurter Sparkasse" besuchen.

ıttps://www.frankfurter-spark

NoPhish, Canova et al. 2015


How you were tricked
This email is from my bank and it is asking me to update my information. I better click on the link and update it.
STOP! Don't fall for this scam email.
Wombank
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update

PhishGuru,
Kumaraguru et al. 2007



Von info@paypal.com
Betreff **Account information**
An me

reply

16:28

PayPal

Dear Max,

Please check your account details.
Click here, to do so.

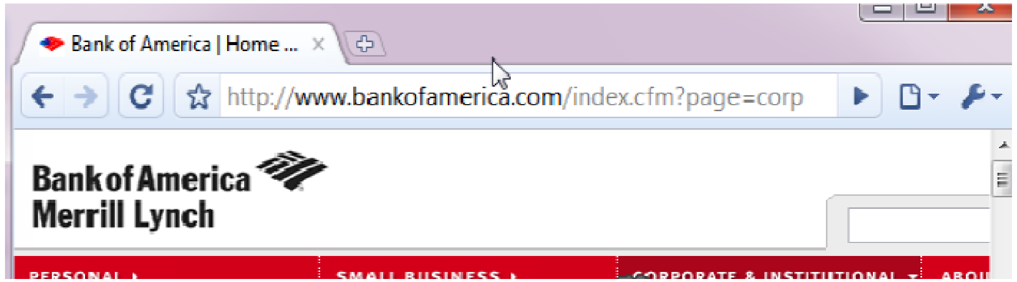
Regards, P

Check the bold highlighted part of the URL carefully.
https://www.**pay-pal-germany.de**/secure
Link available in 03 second(s)

?

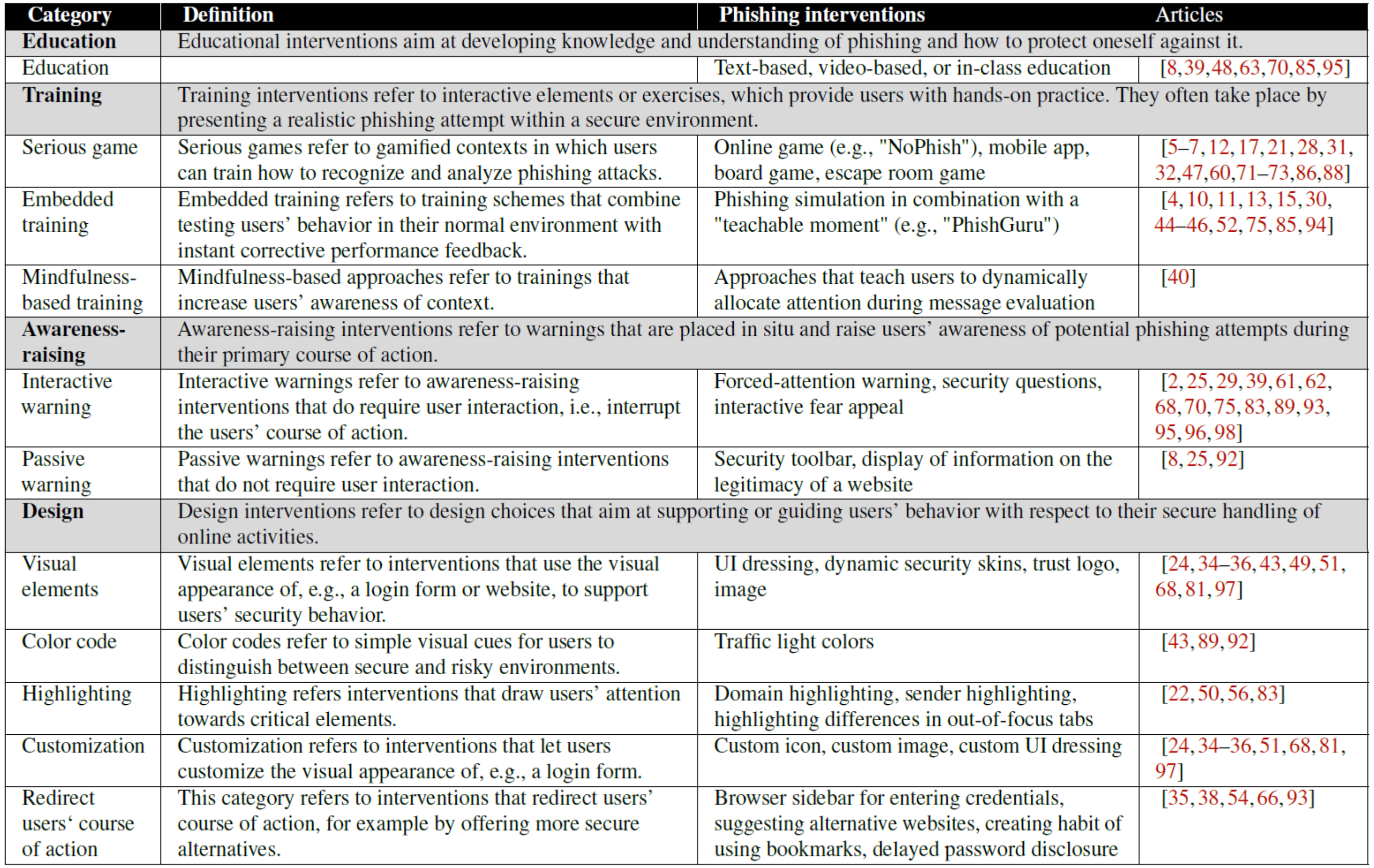
Tooltip

Torpedo, Volkamer et al. 2017


Bank of America | Home ...
http://www.bankofamerica.com/index.cfm?page=corp
Bank of America
Merrill Lynch
PERSONAL
SMALL BUSINESS
CORPORATE & INSTITUTIONAL
ABOU

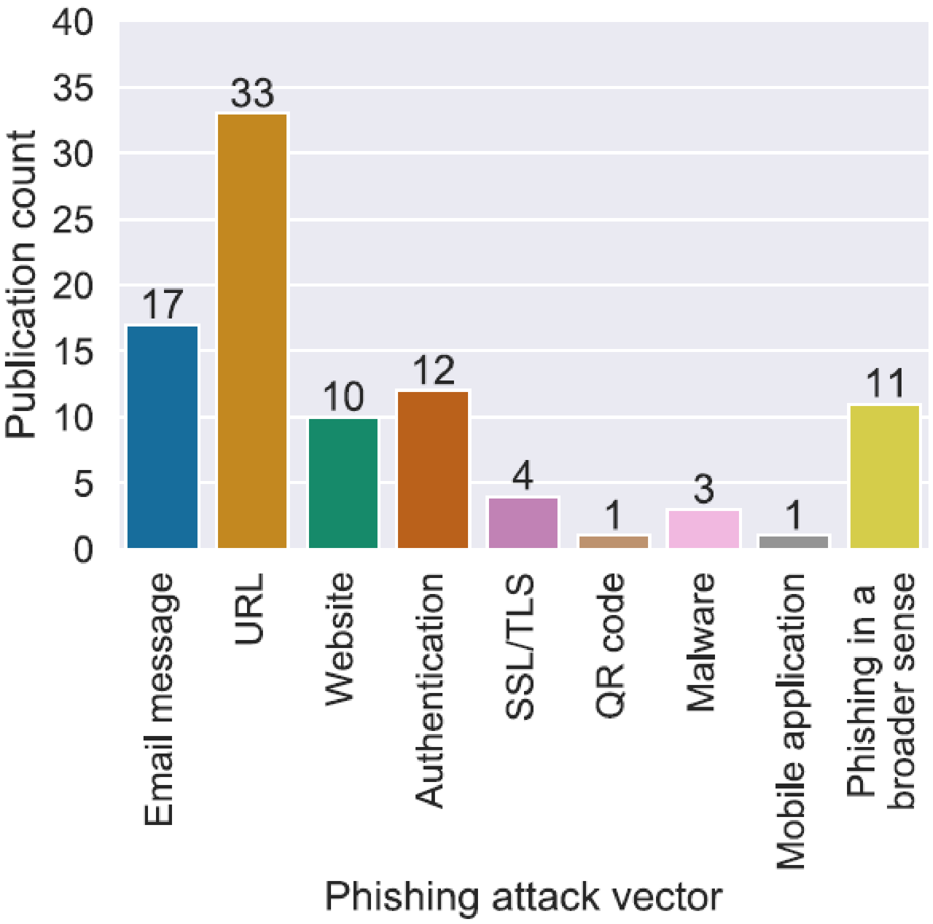
Domain highlighting, Lin et al. 2019

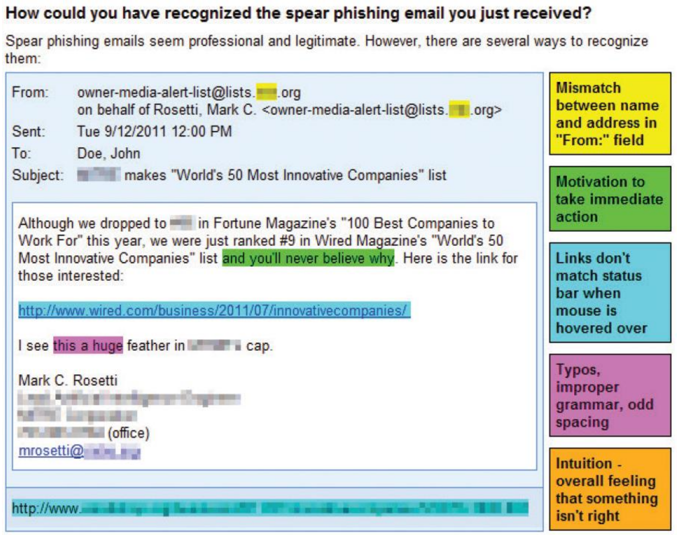
How can phishing interventions be taxonomized?



Category	Definition	Phishing interventions	Articles
Education	Educational interventions aim at developing knowledge and understanding of phishing and how to protect oneself against it.		
Education		Text-based, video-based, or in-class education	[8,39,48,63,70,85,95]
Training	Training interventions refer to interactive elements or exercises, which provide users with hands-on practice. They often take place by presenting a realistic phishing attempt within a secure environment.		
Serious game	Serious games refer to gamified contexts in which users can train how to recognize and analyze phishing attacks.	Online game (e.g., "NoPhish"), mobile app, board game, escape room game	[5–7,12,17,21,28,31,32,47,60,71–73,86,88]
Embedded training	Embedded training refers to training schemes that combine testing users' behavior in their normal environment with instant corrective performance feedback.	Phishing simulation in combination with a "teachable moment" (e.g., "PhishGuru")	[4,10,11,13,15,30,44–46,52,75,85,94]
Mindfulness-based training	Mindfulness-based approaches refer to trainings that increase users' awareness of context.	Approaches that teach users to dynamically allocate attention during message evaluation	[40]
Awareness-raising	Awareness-raising interventions refer to warnings that are placed in situ and raise users' awareness of potential phishing attempts during their primary course of action.		
Interactive warning	Interactive warnings refer to awareness-raising interventions that do require user interaction, i.e., interrupt the users' course of action.	Forced-attention warning, security questions, interactive fear appeal	[2,25,29,39,61,62,68,70,75,83,89,93,95,96,98]
Passive warning	Passive warnings refer to awareness-raising interventions that do not require user interaction.	Security toolbar, display of information on the legitimacy of a website	[8,25,92]
Design	Design interventions refer to design choices that aim at supporting or guiding users' behavior with respect to their secure handling of online activities.		
Visual elements	Visual elements refer to interventions that use the visual appearance of, e.g., a login form or website, to support users' security behavior.	UI dressing, dynamic security skins, trust logo, image	[24,34–36,43,49,51,68,81,97]
Color code	Color codes refer to simple visual cues for users to distinguish between secure and risky environments.	Traffic light colors	[43,89,92]
Highlighting	Highlighting refers interventions that draw users' attention towards critical elements.	Domain highlighting, sender highlighting, highlighting differences in out-of-focus tabs	[22,50,56,83]
Customization	Customization refers to interventions that let users customize the visual appearance of, e.g., a login form.	Custom icon, custom image, custom UI dressing	[24,34–36,51,68,81,97]
Redirect users' course of action	This category refers to interventions that redirect users' course of action, for example by offering more secure alternatives.	Browser sidebar for entering credentials, suggesting alternative websites, creating habit of using bookmarks, delayed password disclosure	[35,38,54,66,93]

Which phishing attack vector is addressed?





How could you have recognized the spear phishing email you just received?

Spear phishing emails seem professional and legitimate. However, there are several ways to recognize them:

From: owner-media-alert-list@lists.[redacted].org
on behalf of Rosetti, Mark C. <owner-media-alert-list@lists.[redacted].org>
Sent: Tue 9/12/2011 12:00 PM
To: Doe, John
Subject: [redacted] makes "World's 50 Most Innovative Companies" list

Although we dropped to [redacted] in Fortune Magazine's "100 Best Companies to Work For" this year, we were just ranked #9 in Wired Magazine's "World's 50 Most Innovative Companies" list and you'll never believe why. Here is the link for those interested:

http://www.wired.com/business/2011/07/innovativecompanies/

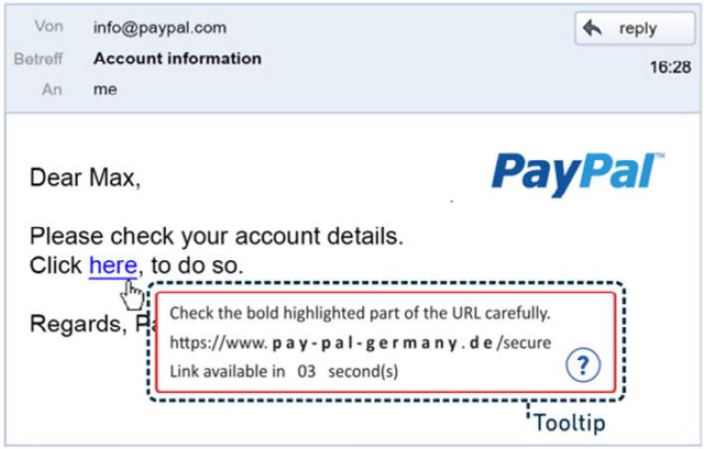
I see this a huge feather in [redacted] cap.

Mark C. Rosetti
[redacted]
[redacted] (office)
mrosetti@[redacted]

http://www.[redacted]

Mismatch between name and address in "From:" field
Motivation to take immediate action
Links don't match status bar when mouse is hovered over
Typos, improper grammar, odd spacing
Intuition - overall feeling that something isn't right

Caputo et al. 2014



Von info@paypal.com
Betreff Account information
An me

Dear Max,

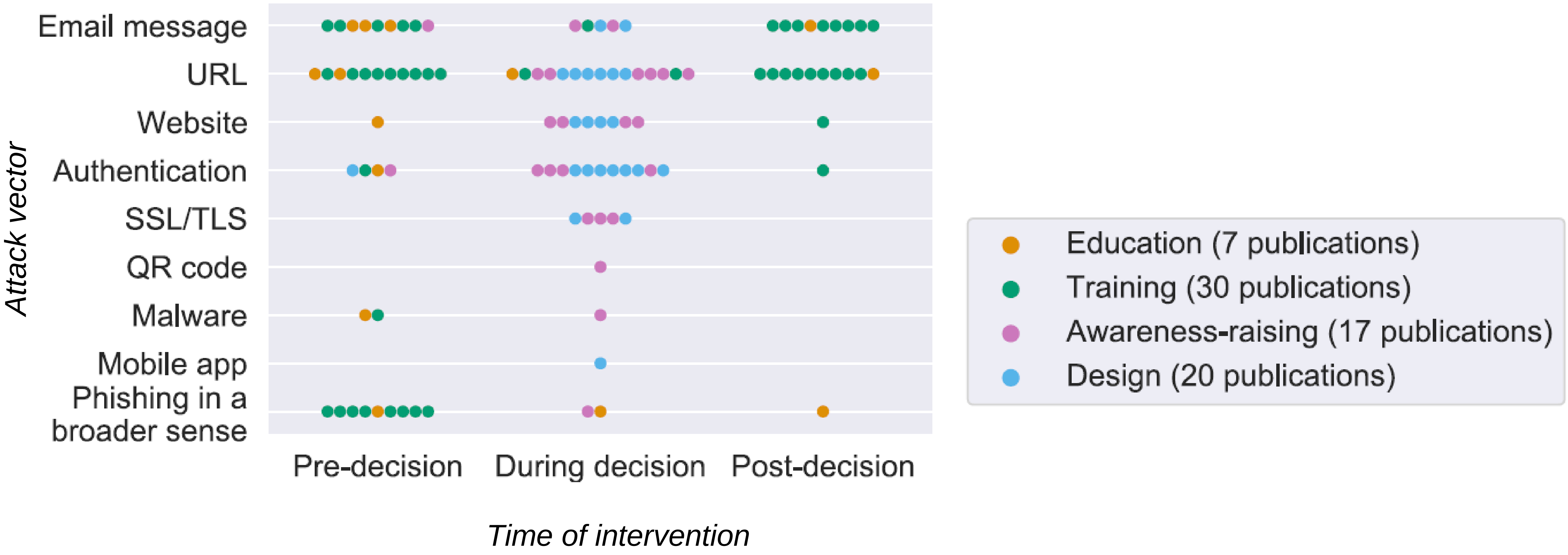
Please check your account details.
Click here, to do so.

Regards, P

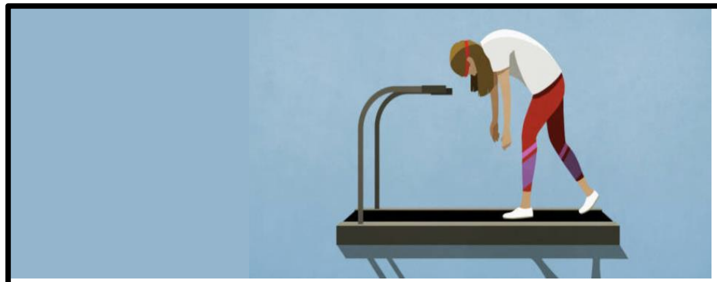
Check the bold highlighted part of the URL carefully.
https://www.**pay-pal-germany.de**/secure
Link available in 03 second(s)

Torpedo, Volkamer et al. 2017

When does which intervention take place?



Avenues for future research



Minimize user effort and intrusiveness

Help users shift their cognitive frame

Explore the potential of (enriched) digital nudging, e.g., facilitate / reinforce / fear

Protect users from malware attacks

Thank you!

Anjuli Franz
Technical University of Darmstadt, Germany
Chair of Information Systems & E-Services

franz@ise.tu-darmstadt.de
https://www.linkedin.com/in/anjuli-franz/

TECHNISCHE UNIVERSITÄT DARMSTADT

ATHENE
National Research Center for Applied Cybersecurity