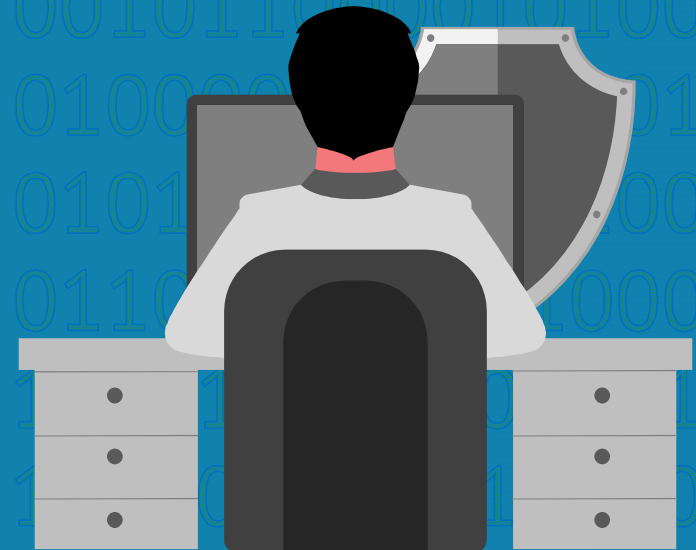


Humans in Information Security: Neglect, Compliance, and Incentives

Eran Toch, Tel Aviv University
IBM Security Seminar – December 2016



Eran Toch

Department of Industrial
Engineering

Faculty of Engineering

Tel Aviv University

<http://toch.tau.ac.il/>

Twitter: @erant

erant@post.tau.ac.il



Thesis by Lena Petrykina

Funded by the ICRC – Blavatnik
Interdisciplinary Cyber Research
Center

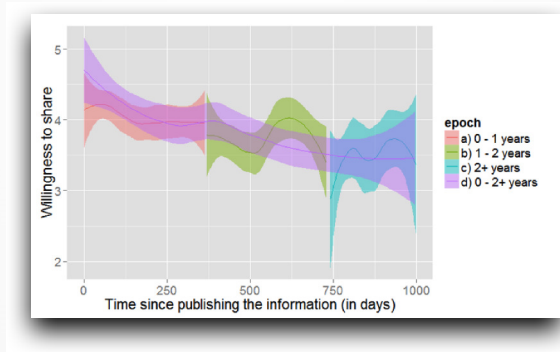
Usable Privacy and Security (more at <http://toch.tau.ac.il>)

Crowdsourcing Privacy Preferences



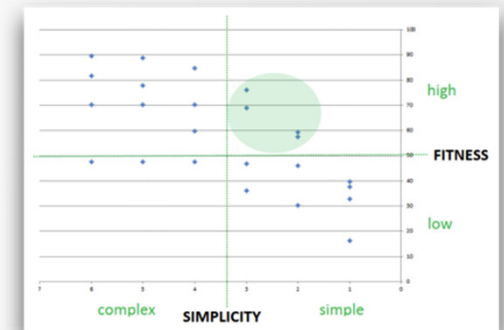
(Barak, Cohen, Gazit, and Eran Toch; 2013; Toch, 2015)

Longitudinal Privacy Behaviors



(Rave-Ayalon & Toch ,2015; Rave-Ayalon & Toch ,2016)

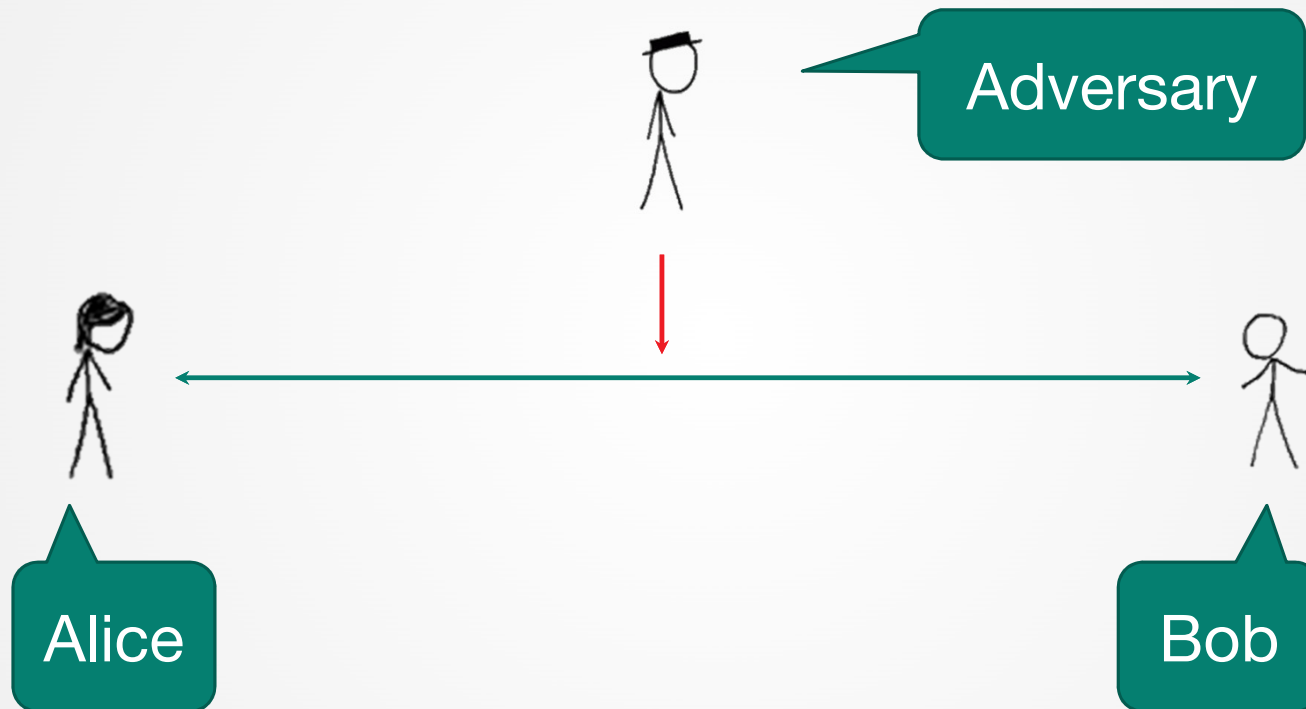
Analyzing Privacy & Security Defaults



(Toch, 2010; Hirschprung, Maimon & Toch, 2013; Hirschprung, Toch, Bolton, and Maimon; 2016)

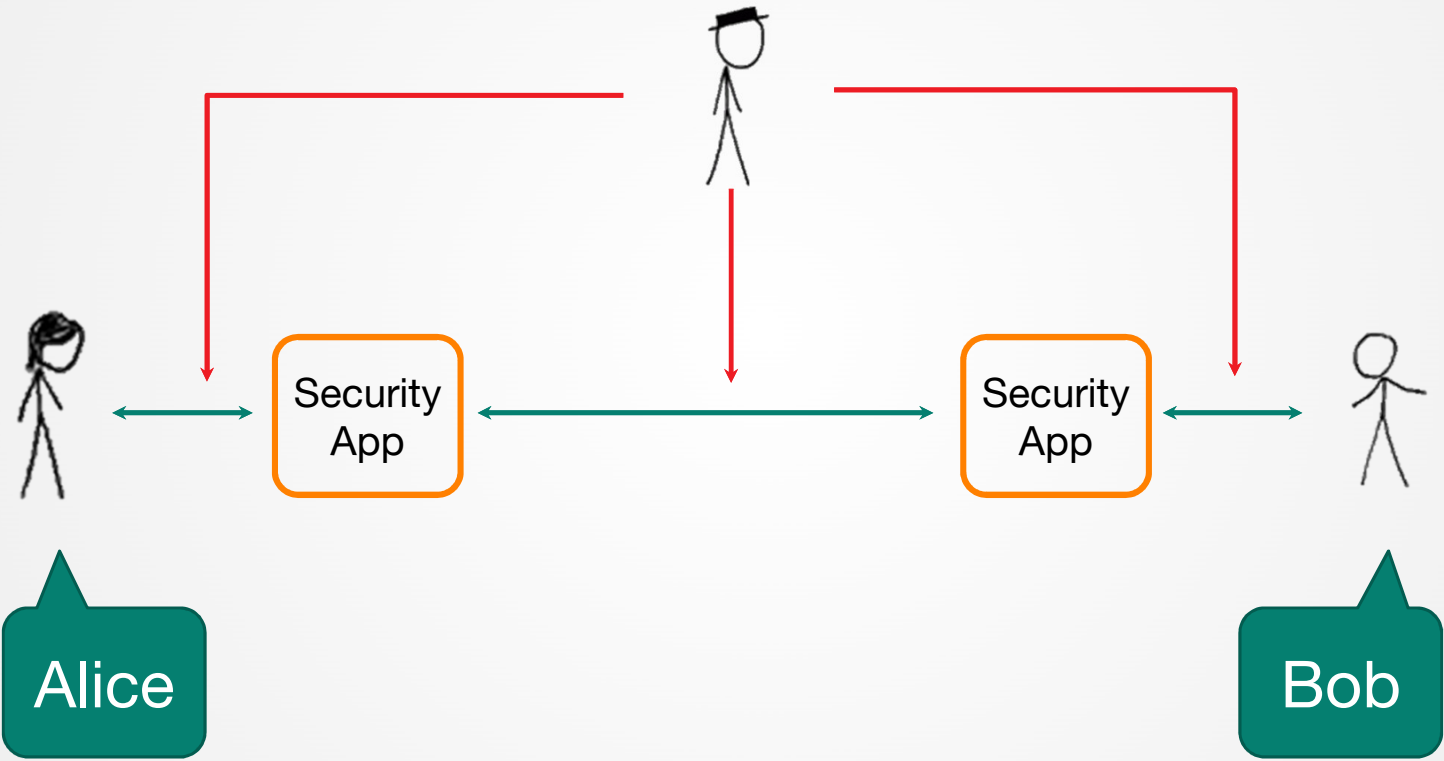
Humans and Security

The Traditional Cybersecurity Model



<https://xkcd.com/538/>

The Human in the Loop



Humans! a Growing Security Challenge

Sony Hackers Used Apple ID Phishing Scheme, Researchers Claim at RSA

By Sean Michael Kerner | Posted 2015-04-21 [Print](#)

[Tweet](#) [LinkedIn](#) 77 [Like](#) 23 [Share](#) 11 [Share](#) 100 [Email](#)



Cylance researchers provide new details into how Sony was hacked, and the allegation is that a phishing attack against Apple IDs was at the root of the attack.

SAN FRANCISCO—There have been a number of theories postulated about how the massive Sony [hack](#) in 2014 actually occurred, and at the RSA Conference here another set of theories are being put forward. In a session called "Hacking Exposed Live," Cylance Senior Security Researcher Brian Wallace and Cylance CEO Stuart McClure alleged that a phishing attack against Apple IDs was at the root of the Sony [hack](#).

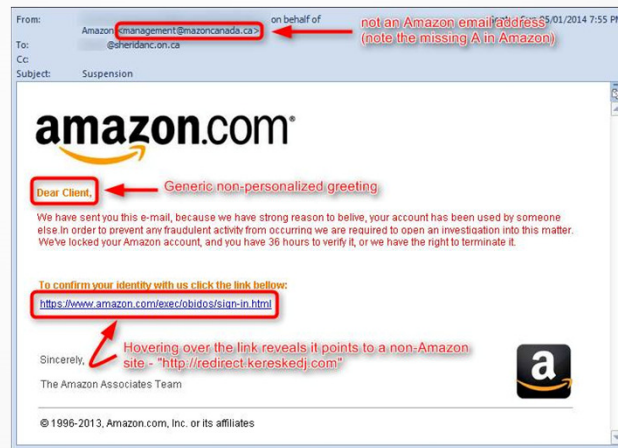
- 44.8% of security vulnerabilities required some sort user action (Microsoft Security Report, 2015)
- 73% of technology professionals perceive human errors to be one of the top three security threats (Deloitte cyber-security report, 2015)

What Humans do Wrong?

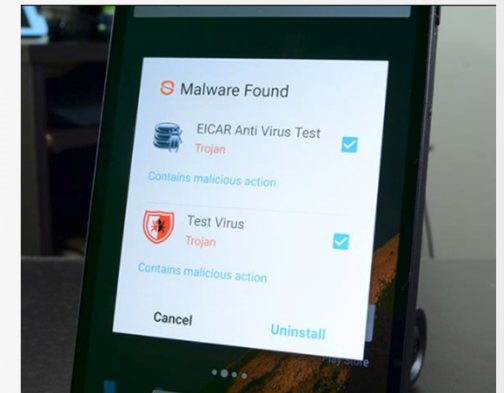
Mismanaging passwords



Clicking on the wrong link

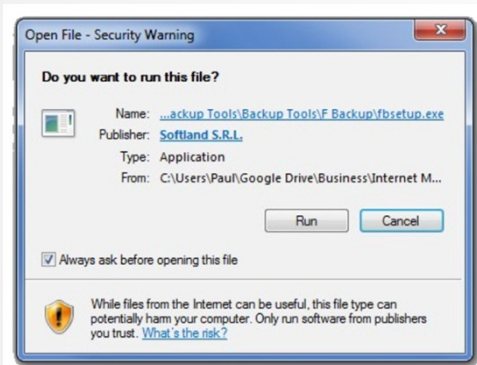


Download the wrong app

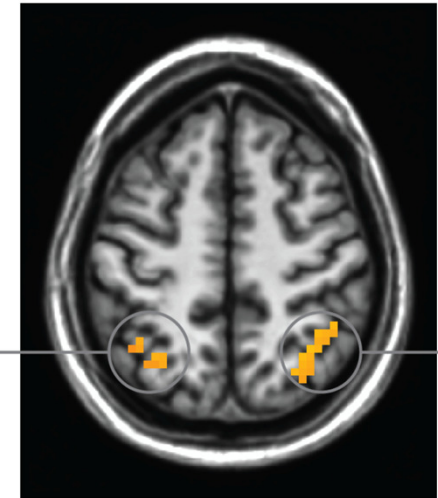
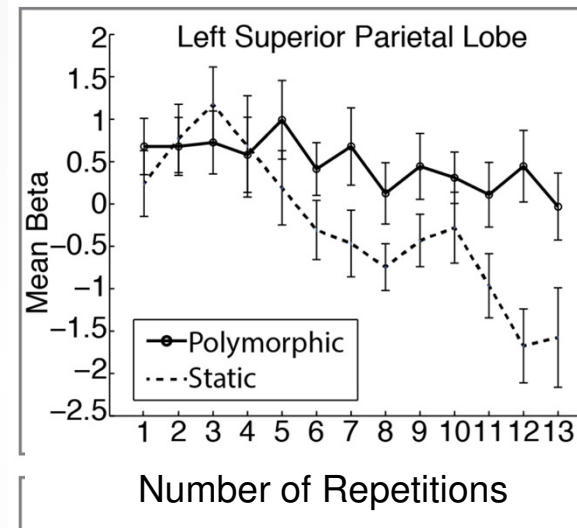


Security Warning Blindness

MRI shows reduced levels of activation for static messages, consistent with lower attention



(a) Original Warning Screenshot



Anderson, Bonnie Brinton, et al. "How Polymorphic Warnings Reduce Habituation in the Brain—Insights from an fMRI Study." CHI. ACM. 2015.

Cognitive Explanations

Security as a secondary task



Security threats are abstract



Security hurdles are concrete



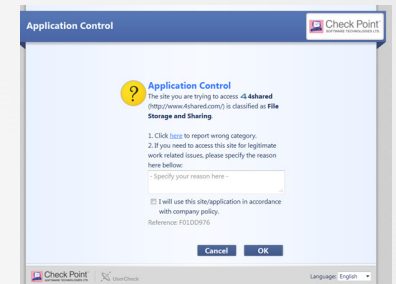
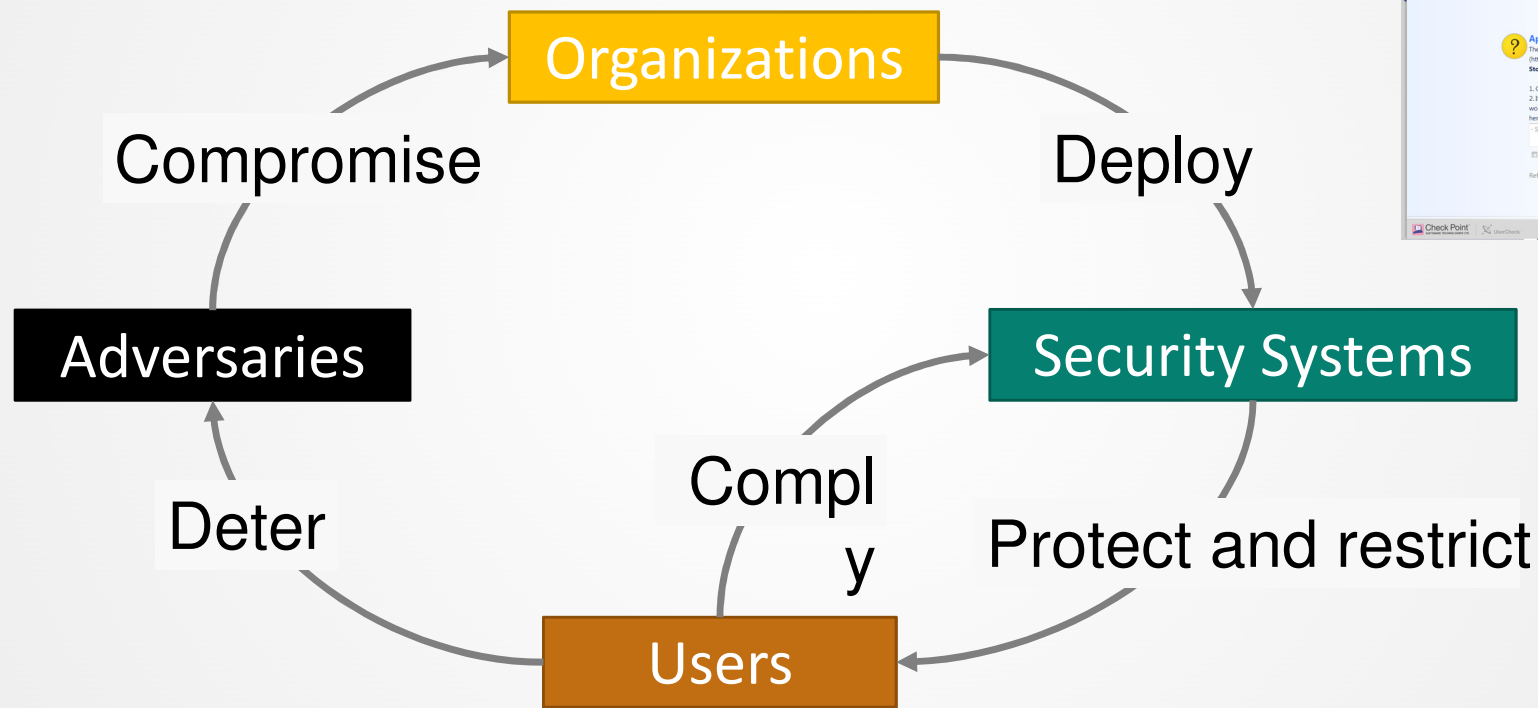
Security Compliance in the Organization

Security in the Organization

- With Bring Your Own Device (BYOD), devices cannot be inherently trusted
- Users can choose to evade security altogether (Pfleeger et al., 2014)

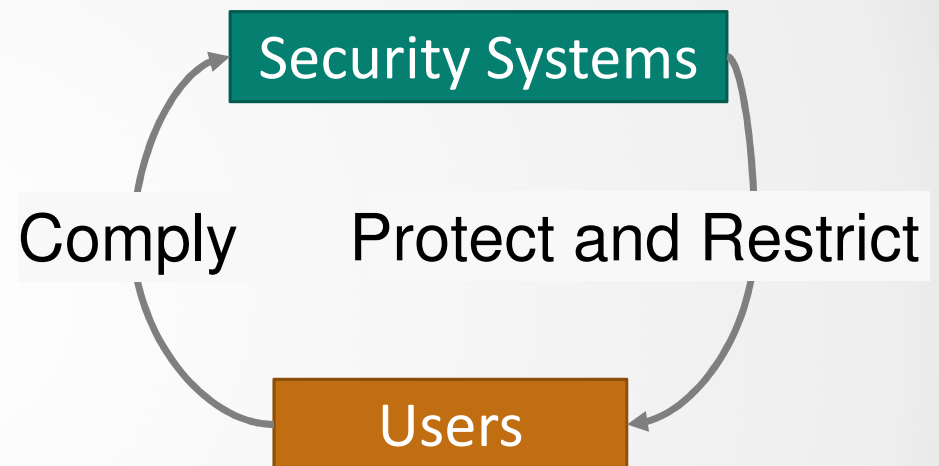


The User/Organization Dynamics



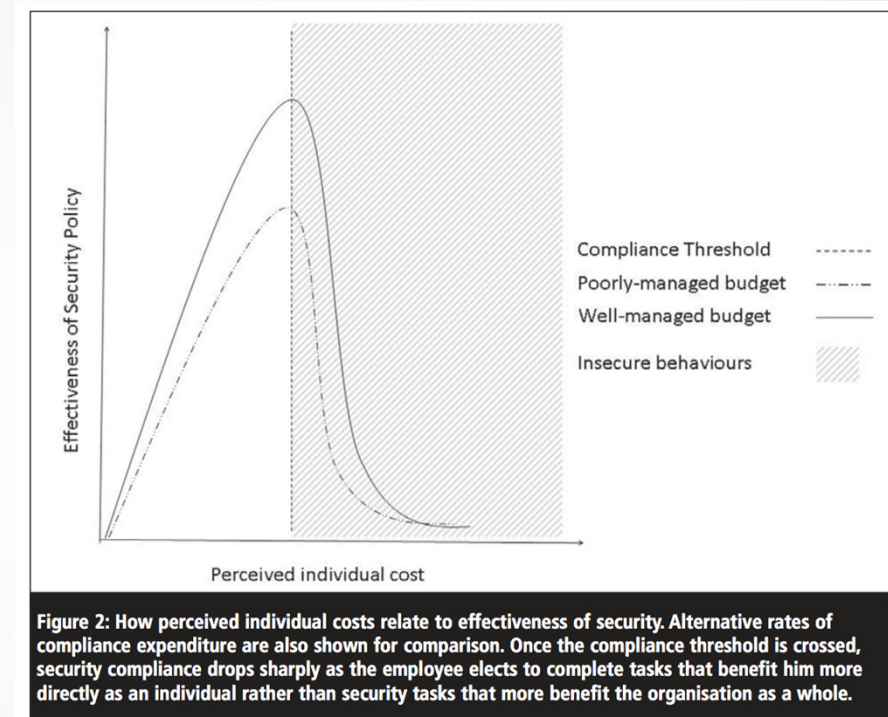
Why Compliance is Difficult

- Security is a secondary task (Johnston and M. Warkentin. 2010; Smith, 2012)
- In many cases, it complicates the primary task (think passwords, dlp)



Compliance Budget

- In most cases, damages are paid by the organization (Johnson and Goetz, 2007)
- In most cases, lost productivity is paid by users (Beautement et al., 2008)
- Users tend to think in terms of “compliance budget” (Beautement and Sasse, 2009)



Beautement and Sasse (2009)

Incentivizing and Nudging

Incentivized Cyber Security

- Incentives, both positive (encouragements) and negative (punishments), are regularly used in many fields
- Initial studies show that they have an effect in information security (Coventry et al., 2014; Turland et al., 2015)
- Users tend to consider only a limited set of factors in compliance (Beautement and Sasse, 2009) and are prone to underweight rare events (Hertwig et al., 2004)

Research Questions

How can we nudge users to comply with security warnings?

1. What is the effect of presenting information about incentives?
2. What is the effect of presenting “almost hit” messages?

Nudging Mechanisms

Points

Showing a salient and gamified feedback on the current history of the user, as a sum of the prior applied incentives



Probabilistic Warning

Showing specific warnings to the user according to the probability of the threat (Perry et al., 2002)

For example, in PW-60, the message is shown when the expected probability of malware is higher than 60%



Assumptions and Questions

Assumptions

- Negative incentives for bad security outcomes
- Positive incentives for achieving productivity goals – number of tasks completed per time quantity
- Users are not malicious

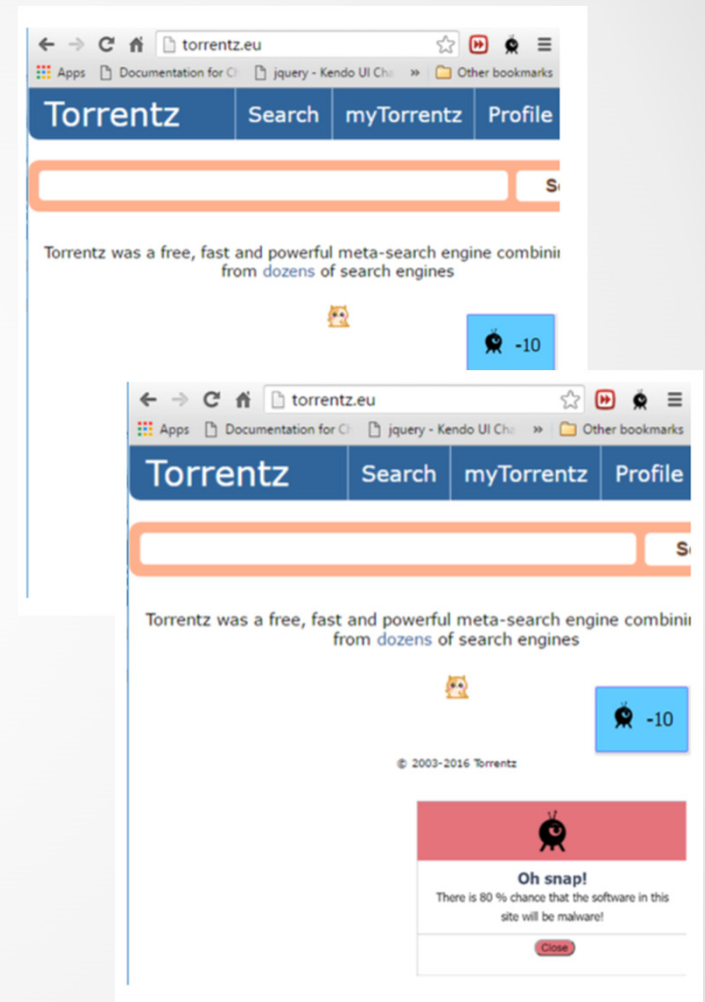
Questions

- How do points and PW affect compliance?
- What is the effect on user learning?

Our Experiment

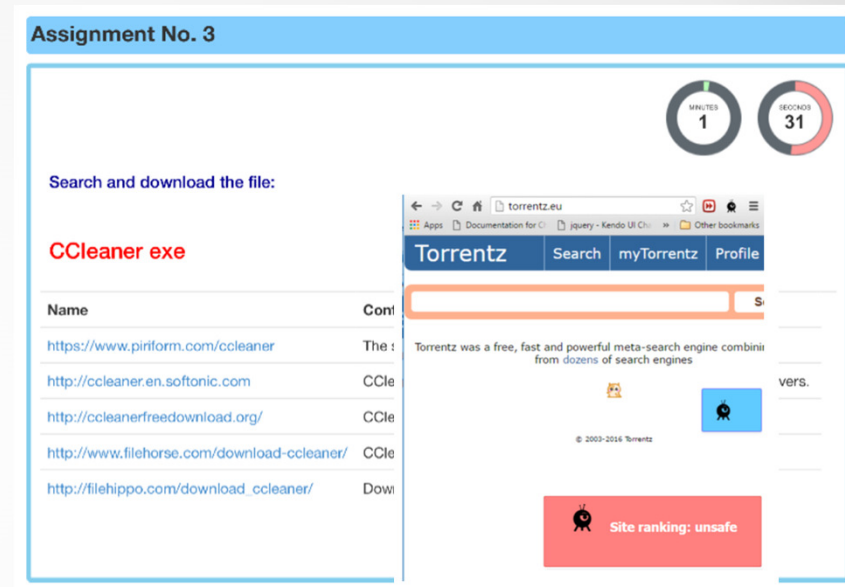
Security-Robot

- A malicious website and download filtering system
- Information about websites taken from Google Safe Browsing API
- Implemented as a Chrome Extension
- Shows Website Safety Rank (WSR) notification
- As well as points and probability warnings



Experiment Design: Tasks

1. Users were asked to download software applications under time pressure
2. The more applications they downloaded in 2 minutes, the higher their bonus was
3. When entering the website, WSRs were shown to all participants
4. Users actually downloaded the application
5. If the application was “found” to be malicious, participants were fined



Website Risk	Probability	Fine	Reward
Green	0.2	-10	5
Yellow	0.6	-10	10
Gray	0.5	-10	10
Red	0.8	-10	15

Experimental Design: Variables

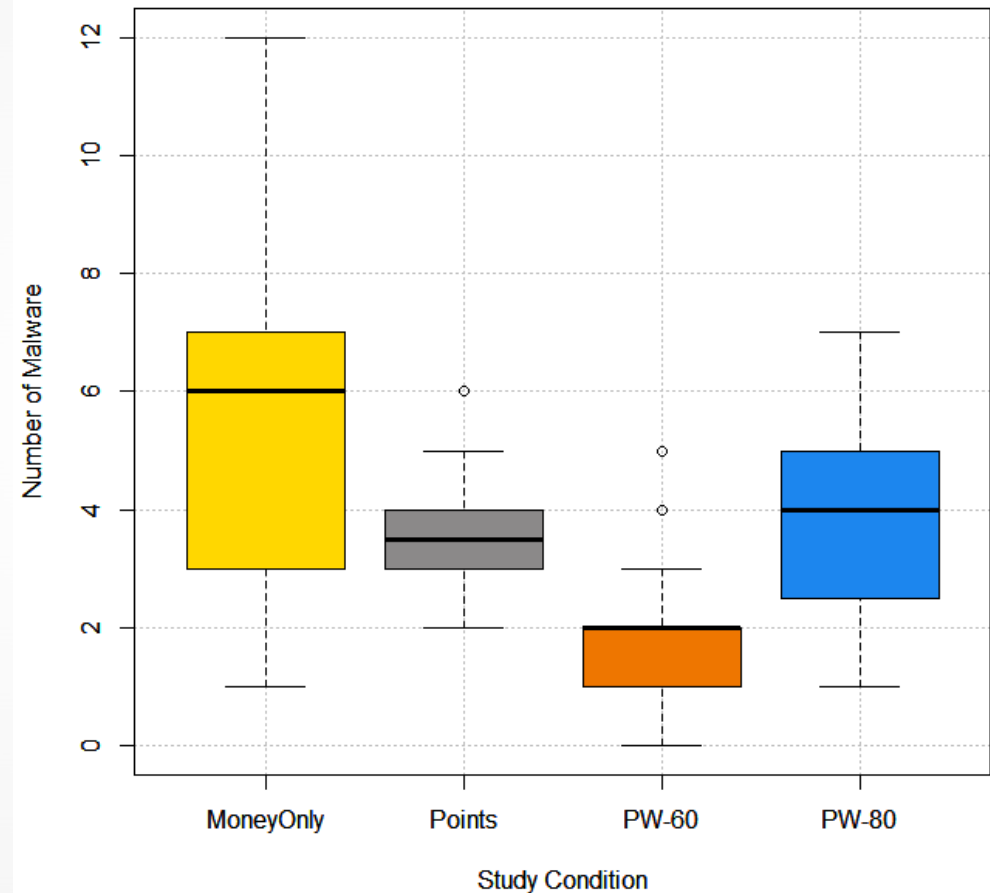
To maximize their bonus, participants needed to balance their desires and fears

Independent Variables	Dependent Variables
<p>Conditions:</p> <ul style="list-style-type: none">• MoneyOnly• Points• PW-60 (+Points)• PW-80 (+Points)	<ul style="list-style-type: none">• Malware: Number of downloaded malware applications• Downloads: Number of downloaded applications• Score• Productivity: Number of safe downloaded applications

We had roughly 20 participants in each condition, each carrying out 6 counter-balanced tasks

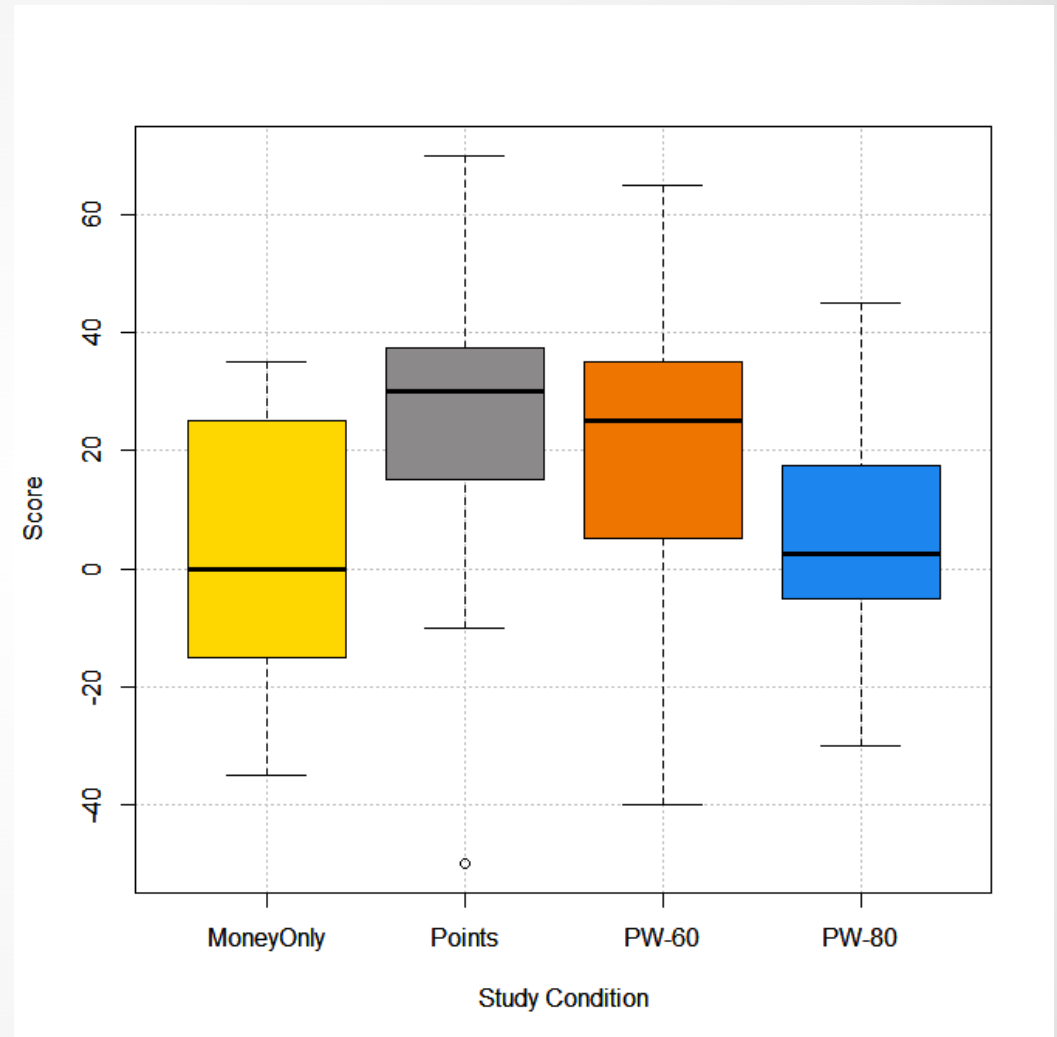
Results: Malware

- Participants in the PW-60 have downloaded significantly less malware than other conditions ($p = .0000006$)
- Participants in the Points ($p = .01$) and PW-80 ($p = .008$) have downloaded significantly less malware applications than the MoneyOnly condition (($F(3, 78) = 11.58, p < .000001$))



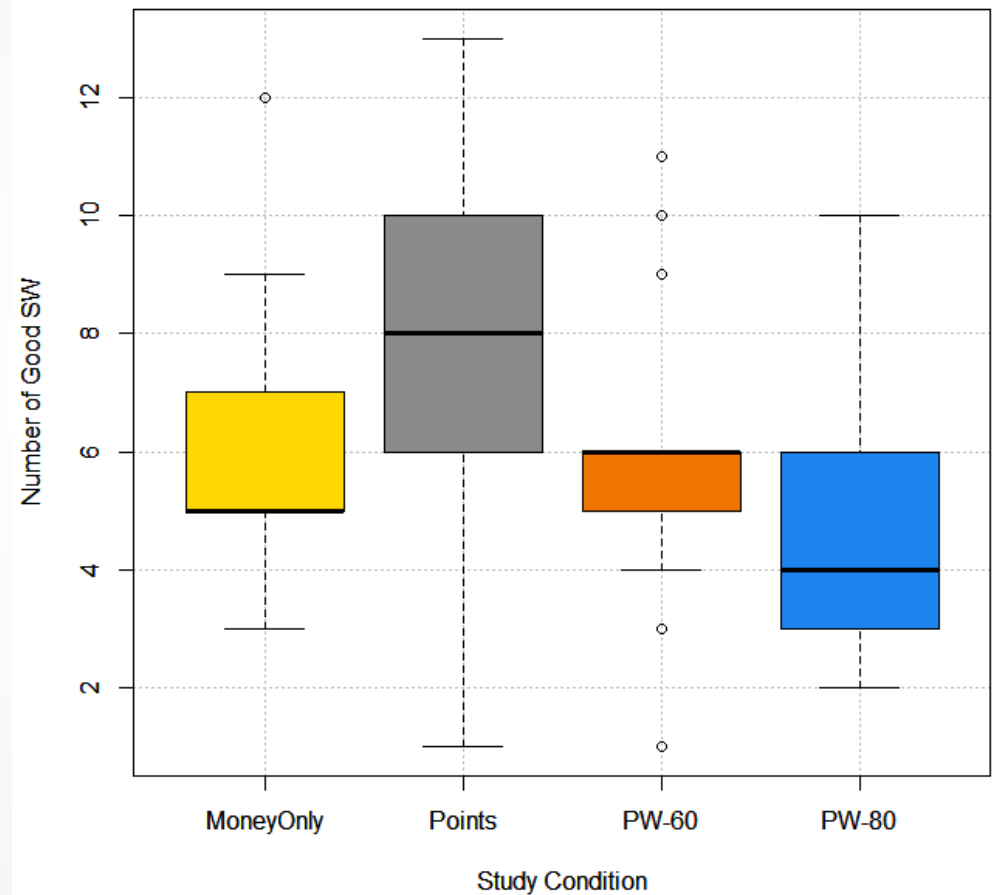
Results: Score

Participants in the points ($p = .009$) and PW-60 ($p = .028$) had earned significantly more than the other conditions ($F(3, 78) = 5.026, p = .00309$)



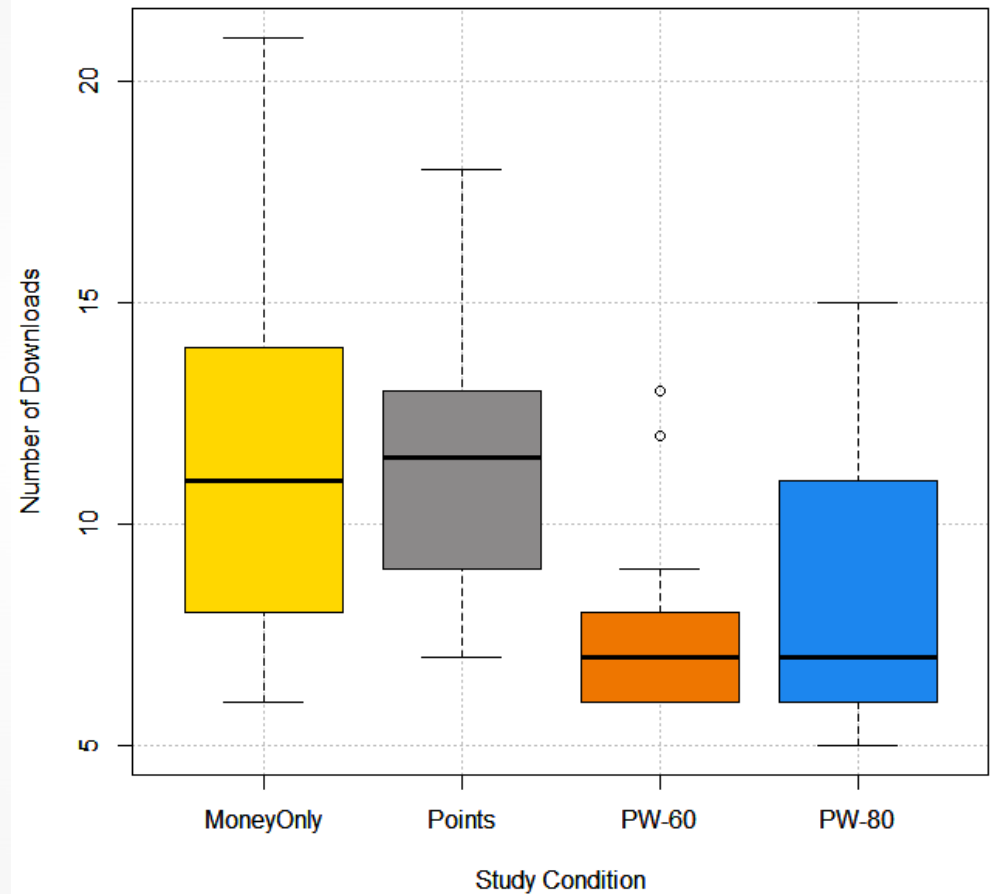
Results: Productivity

Participants in the Points condition were significantly more productive than all other conditions

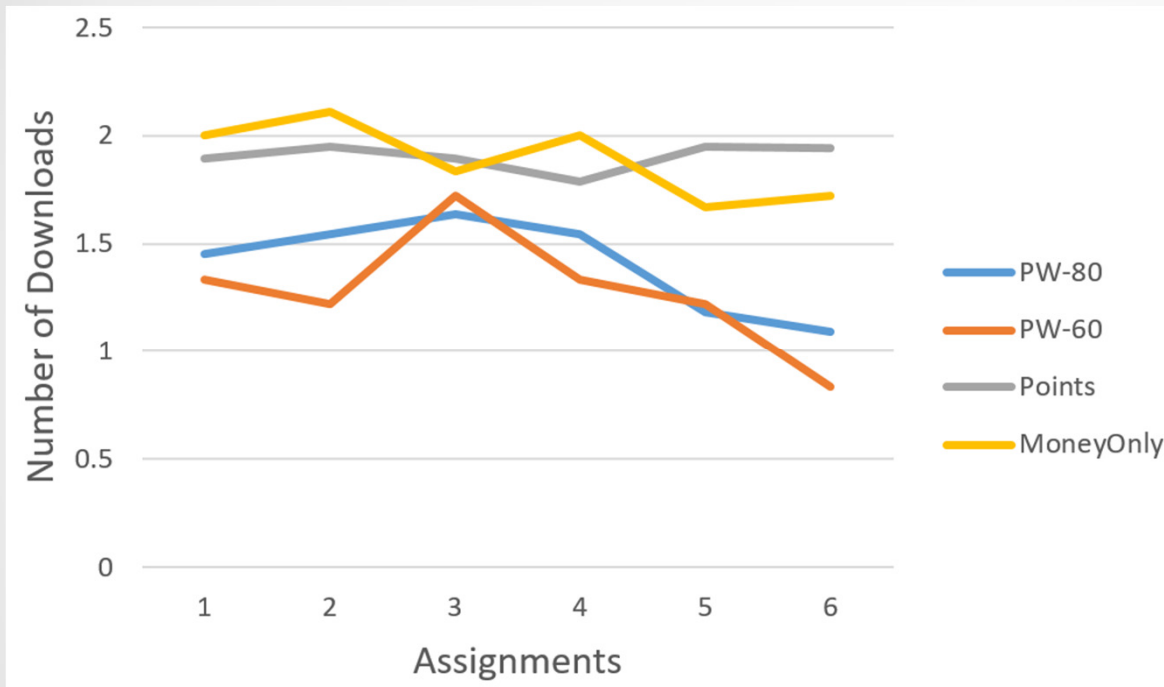


Results: Downloads

Participants in the PW-60 and in the PW-80 download significantly less applications than in the other conditions ($p = .001$ and $p = .018$, respectively, $F(3, 78) = 8.167$, $p < .00001$)



Learning



- The number of downloads and malware for PW-60 was significantly lower in the second half of the study.
- Weaker results were found for PW-80 and none for the other conditions

Implications

Thinking about the results

1. Points and probability warnings make the users' behavior safer
2. And even do not significantly harm productivity
3. Users are just more selective.

But remember:

- This is a lab experiment
- However, in similar methodologies, the results usually scale to real-world behaviors

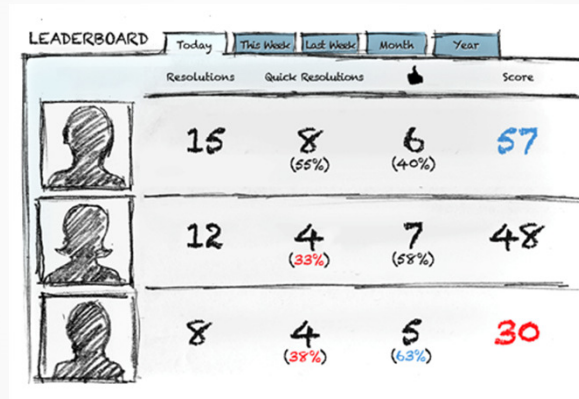
Practical Incentive Systems




Actual incentives



How much would a breach cost?

Social incentives



LEADERBOARD					
	Today	This Week	Last Week	Month	Year
	Resolutions	Quick Resolutions			Score
	15	8 (55%)	6 (40%)		57
	12	4 (33%)	7 (58%)		48
	8	4 (38%)	5 (63%)		30

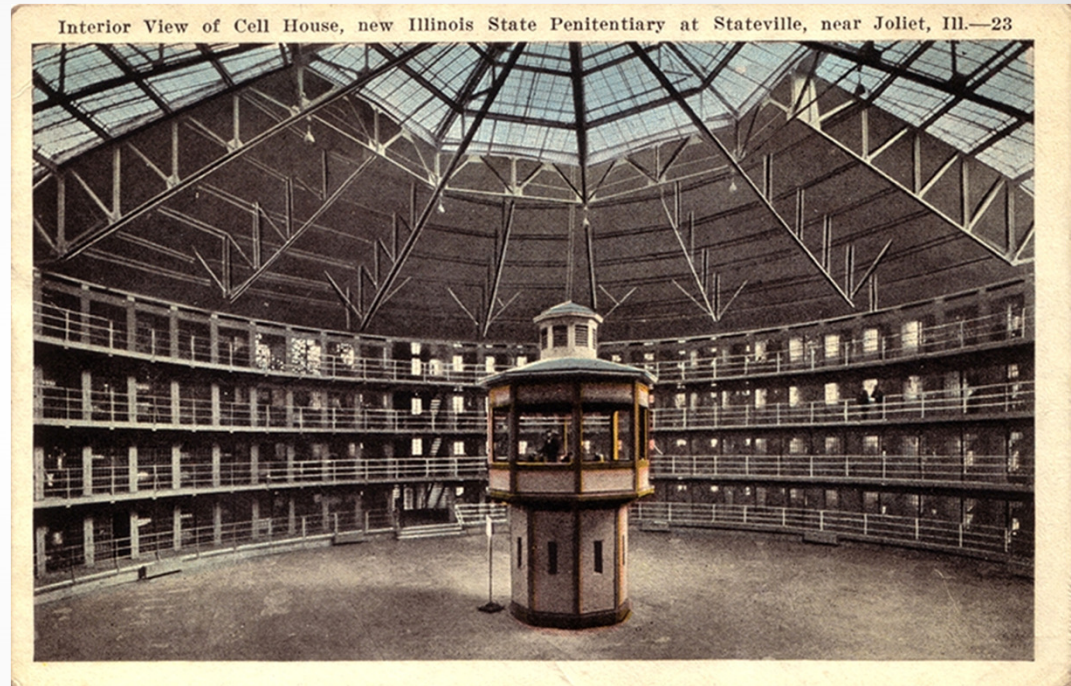
Cognitive Penalties

Please Wait..
1 seconds



Discipline and Punish

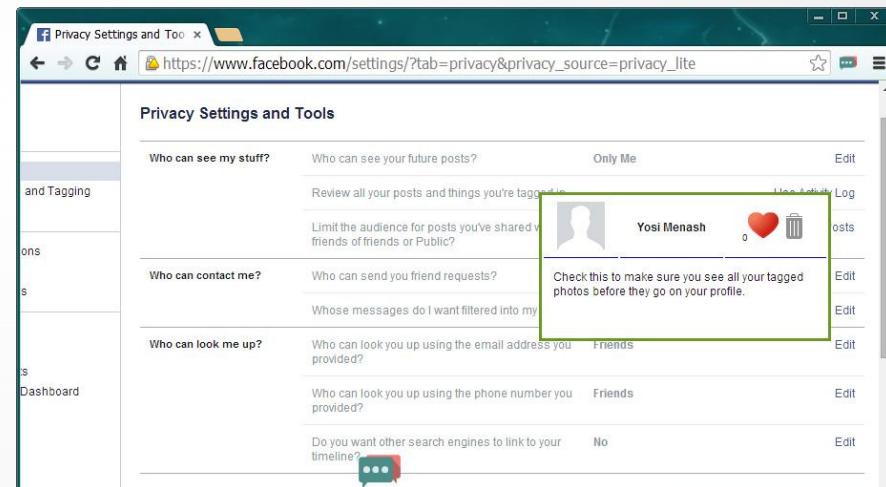
- Can nudging become a sophisticated way of disciplining users?
- Can it serve as a basis for negotiation?
- Would we would like to be users of Security-Robot?



Future Studies

Extending gamification to social comparison and pressure mechanisms

	Resolutions	Quick Resolutions	👍	Score
	15	8 (55%)	6 (40%)	57
	12	4 (33%)	7 (58%)	48
	8	4 (38%)	5 (63%)	30



Thank You!

Thanks!

Lena

Israel's National Cyber
Bureau

<http://toch.tau.ac.il/>

Twitter: @erant

erant@post.tau.ac.il



IWiT

Interacting with Technology