Evaluating User Behavior in Smartphone Security: A Psychometric Approach

Hsiao-Ying Huang[1], Soteris Demetriou[2], **Muhammad Hassan**[1], Guliz Seray Tuncay[3], Carl A. Gunter[1], Masooda Bashir[1]

[1] University of Illinois at Urbana-Champaign, {hhuang65, mhassa42, mnb, cgunter}@illinois.edu

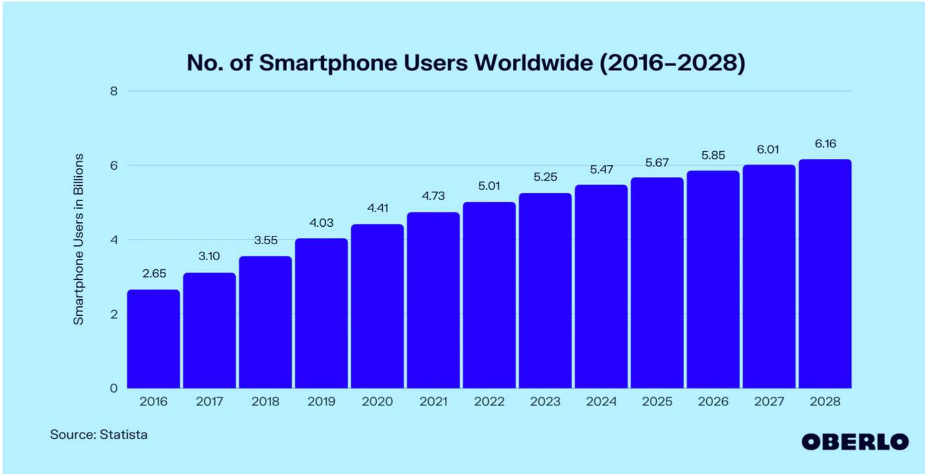
[2] Imperial College London, s.demetriou@imperial.ac.uk

[3] Google, gulizseray@google.com

Smartphone

Rising popularity of smartphone

- 85% of American own a Smartphone (Pew Research)
  - Up from just 35% in 2011.
- Convenience of communication, connectivity and entertainment.



Computer Security vs Smartphone Security

- Smartphone Security Behavior varies from other devices (such as laptops or PCs).
- On Smartphone, users often
    - Browse without vigilance *(Felt et al SOUPS '12, Kelley et al CHI '13*
    - Have inaccurate assumptions about Smartphone Security features *(Das et al '16)*,
    - Take minimal effort for Smartphone Security *(Kelley et al CHI '13, Chin et al SOUP '12, Mylonas et al C&S '13)*

Therefore, it is essential to study if Computer Security Scales can be used to study Smartphone Security Behaviors.

User Behavior & Smartphone Security

Field Observation		Self-reported Approach
✗ Time Consuming	⌛	Fast ✓
✗ Expensive (Equipment, time, etc)	$	Cheap ✓
✗ Limited	🔍	Explorative ✓
✓ Accurate	🎯	Approximate (soc desirability bias) ✗

User Behavior & Smartphone Security

Field Observation

Self-reported Approach

Smartphone Security Behavior

Two key gaps in current literature on Smartphone Security

- No standardized measurement of smartphone security behavior intentions across contexts
- Unclear if computer security behavior intentions can be applied to smartphone security behavior intentions

Goal: Develop a standardized measurement of smartphone security behavior intentions for different contexts.

Smartphone Security Behavior

Research Questions

- **RQ1:** Can we use computer security Behavior Intentions (BIs) measurement for smartphone security?
- **RQ2:** If not, how can we develop a smartphone security BIs measurement?

A Psychometric Approach

- **Psychometric:** Measuring human psychological attributes (personality traits, social attributes, cognitive abilities etc)
  - Conceptualize smartphone security behavior intentions as a psychometric construct

- Adopt the same approach as SA-6 and SeBIS scales – Based on Theory of Reasoned Action (TRA)
  - TRA proposes that people's behavior is determined by their attitude and subjective norms

Reference:

- Cori Faklaris, Laura A Dabbish, and Jason I Hong. A self-report measure of end-user security attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security,* 2019.
- Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (Sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015.

Methodology

Two-phase study to measure smartphone security behavior intentions

- Recruited participants from United States via Mturk
- Ensured data quality by using attention-check questions in each section of the survey

Phase 1 Testing if 4 dimensions of SeBIS can be applied to smartphone (mSeBIS)

Phase 2 Developing new measurement for smartphone security Bis (SSBS)

Phase 1: Smartphone SeBIS

Revised SeBIS to fit smartphone context

- Four types of item modifications
  1. Word/phrase substitution (*“laptop/tablet” -> “smartphone”*)
  2. Word/phrase revision *(e.g “I regularly change my password … using my **smartphone**.”)*
  3. Item deletion (“*When browsing websites, I mouse-over links to see where they go, before clicking them.”*)
  4. Item addition *(“I turn on the **‘lost my device’** feature on my smartphone.”)*

Smartphone-SeBIS: A revised version of SeBIS for Smartphone Security BIs, comprehensive scale with 20 items on a Likert Scale, was conducted on MTurk.

Phase 1: Results of Smartphone SeBIS

Data Analysis

- **Internal reliability** is 0.68 (Cronbach's alpha, Cutoff point: >.70, Nunnally, 1978)
- **Confirmatory factor analysis** was conducted to confirm if the measurement was fit for the model of SeBIS.
    - Comparative Fit Index (CFI)= 0.565 (Cut-off point: >.90 recommended by Netemeyer et al. 2003)

Conclusion: Poor fit of the data, 4-dimensions of SeBIS may not be suitable for measuring smartphone security behavior intentions

SSBS Methodology

Two-phase study to measure smartphone security behavior intentions

- Recruited participants from United States via Mturk

Phase 1 Testing if 4 dimensions of SeBIS can be applied to smartphone (mSeBIS)

Phase 2 Developing new measurement for smartphone security Bis (SSBS)

Phase 2: Developing SSBS

- Generated a list of 45 smartphone security behaviors based on security experts' views
  - Ensured no important smartphone security behavior was missing (referred to US-CERT as a standard)
  - Ensured compliance with principle of applicability and acceptance
- MTurk Survey (n=487) on 5-point scale survey
  - Average age of participants was 34.6 years
  - Average time to complete 6.3 minutes

Gender	Percentage
Female	44.8%
Male	55.2%

Results: SSBS

- 3 rounds of EFA to extract the effective items
  - Resulted in 14 items loading onto 2 factors
- Identified two factors: *Technical and Social*

Evaluation

- EFA to extract effective items
- Scale Reliability
- Convergent Validity
- Conformity Factor Analysis

TECHNICAL	T1	I reset my Advertising ID on my smartphone.
	T2	I hide device in my smartphone's bluetooth settings.
	T3	I change my passcode/PIN for my smartphone's screen lock at a regular basis.
	T4	I manually cover my smartphone's screen when using it in the public area (e.g., bus or subway).
	T5	I use an adblocker on my smartphone.
	T6	I use an anti-virus app.
	T7	I use a Virtual Private Network (VPN) app while connected to a public network.
	T8	I turn off WiFi on my smartphone when not actively using it.
SOCIAL	S1	I care about the source of the app when performing financial and/or shopping tasks on that app.
	S2	When downloading an app, I check that the app is from the official/expected source.
	S3	Before downloading a smartphone app I ensure the download is from official application stores.
	S4	I verify the recipient/sender before sharing text messages or other information using smartphone apps.
	S5	I delete any online communications (i.e., texts, emails, social media posts) that look suspicious.
	S6	I pay attention to the pop-ups on my smartphone when connecting it to another device (e.g. laptop, desktop).

Results: SSBS

Reliability metrics assessed with success

- Cronbach's alpha (full scale) = 0.8 > 0.7 ✓
- ITC (each item) > 0.2 ✓
- IIC (both subscale) between 0.2 & 0.4 ✓

Evaluation

- EFA to extract effective items
- Scale Reliability
- Convergent Validity
- Conformity Factor Analysis

Table 3: Factor loadings and reliability statistics of finalized scale

ID	Item	Technical	Social	Inter-total correlation
T1	I reset my Advertising ID on my smartphone.	.787		0.52
T2	I hide device in my smartphone's bluetooth settings.	.639		0.47
T3	I change my passcode/PIN for my smartphone's screen lock at a regular basis.	.629		0.51
T4	I manually cover my smartphone's screen when using it in the public area (e.g., bus or subway).	.621		0.55
T5	I use an adblocker on my smartphone.	.614		0.51
T6	I use an anti-virus app.	.612		0.53
T7	I use a Virtual Private Network (VPN) app while connected to a public network.	.604		0.42
T8	I turn off WiFi on my smartphone when not actively using it.	.544		0.47
S1	I care about the source of the app when performing financial and/or shopping tasks on that app.		.723	0.24
S2	When downloading an app, I check that the app is from the official/expected source.		.677	0.36
S3	Before downloading a smartphone app I ensure the download is from official application stores.		.677	0.21
S4	I verify the recipient/sender before sharing text messages or other information using smartphone apps.		.609	0.41
S5	I delete any online communications (i.e., texts, emails, social media posts) that look suspicious.		.552	0.25
S6	I pay attention to the pop-ups on my smartphone when connecting it to another device (e.g. laptop, desktop).		.526	0.39
	Cronbach's alpha	0.84	0.79	
	Inter-item correlation	0.40	0.39	

Results: SSBS

Convergent Validity

- N = 66
- Pearson's correlation between avg. score of SeBIS and SSBS (r=.403 > 0, p=0.008 < 0.005). ✓

Evaluation

- EFA to extract effective items
- Scale Reliability
- Convergent Validity
- Conformity Factor Analysis

…participants who showed higher intentions in protecting their general security were also more likely to protect their smartphone security.

This confirms that our scale is measuring a similar construct with SeBIS, that of security behavior.

Table 2: Pearson's Correlation between SeBIS and SSBS

	Correlation coefficient (p-value)	
SeBIS / SSBS	Technical approach	Social approach
Device securement	-.017 (p=.896)	.060 (p=.628)
Password generation	.290 (p=.018)	.229 (p=.064)
Proactive awareness	-.090 (p=.471)	.614 (p<.0001)
Update	.301 (p=.014)	.431 (p=.0003)

Results: SSBS

Confirmatory Factor Analysis

- CFA to compare data within two-component model
- N = 358

Evaluation

- EFA to extract effective items
- Scale Reliability
- Convergent Validity
- Confirmatory Factor Analysis

- Reliability ✓
  - *Full SSBS scale alpha = 0.79*
  - *Technical Subscale Alpha = 0.81*
  - *Social Subscale Alpha = 0.85*
- **PCA** ✓
  - Two components: *Technical* and *Social*

- CFI = 0.954 > 0.90 ✓
- TLI = 0.942 > 0.90 ✓
- RMSEA = 0.054 < 0.06 ✓
- SRMR = 0.059 < 0.08 ✓
- Pearson's Correlation ✓
  - No significant correlation between the two components

Applications and Role of the SSBS

- SSBS can contribute to the modelling of smartphone security behavior, such as:
  - end-users' security behavior intentions
  - risk of accidental insider threats from smartphone use
  - Designing interventions or policies
  - cultures, languages, personality trait affects smartphone security
- The scale can also be used for educational and training purposes
- Integrated with other scales (SeBIS, SA-6) to model behavior across different device types

Limitation & Future Works

- Investigating other factors
  - Established goodness of fit for *Technical* & *Social* components.
  - Other variables could include; security knowledge, risk perception, personality traits etc.
- Studying Smartphone Privacy Behaviors
- Predicting actual behavior from intentions:
  - Explore the gap between intentions and actions
- Addressing low Average Variance Extracted (AVE) for *Technical* subscale

Conclusion

- Smartphone security behavior differs from general security behavior
- Developed and validated a new scale: SSBS
  - 14 items and two subscales: Technical and Social
  - high internal consistency, unique item loading, and no subscale correlation
  - convergent validity with SeBIS, an existing security behavior scale
- SSBS can be a valuable instrument for
  - Understanding smartphone security behavior
  - Improving smartphone security design

Thank you for your attention!

Muhammad Hassan
PhD Student, School of Information Sciences
University of Illinois at Urbana-Champaign
mhassa42@illinois.edu