Incentives for Enabling Two-Factor Authentication in Online Gaming

Kyle Crichton
Carnegie Mellon University
Pittsburgh, PA 15213, USA
kcrichto@andrew.cmu.edu

Jason Lee
Carnegie Mellon University
Pittsburgh, PA 15213, USA
dongyool@andrew.cmu.edu

Meihan Li
Carnegie Mellon University
Pittsburgh, PA 15213, USA
meihanl@andrew.cmu.edu

Abstract

Despite proven security benefits, adoption of two-factor authentication (2FA) for online accounts remains low [12]. To encourage users to enable 2FA Epic Games, the company behind the enormously popular online game Fortnite, began offering free in-game content as a reward for those who adopt [15]. To assess the incentive's effectiveness, we conducted an online survey study with 200 active Fortnite players. Since the incentive offered was not randomly assigned to participants, we employed an instrumental variables design to estimate the causal effect. While the analysis revealed no statistically significant effect, the data suggests incorporating the social aspect of player interactions may lead to a significant result in future work. In addition, our qualitative analysis identified several shortcomings in end-user communication regarding the availability of 2FA, the incentive being offered, and the value and risk associated with user's account.

Author Keywords

Two-factor authentication; Incentives; Video games; Fortnite; Account security

ACM Classification Keywords

H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous; K.6.5 [Security and Protection]: Authentication; J.5 [Social and Behavioral Science]: Economics

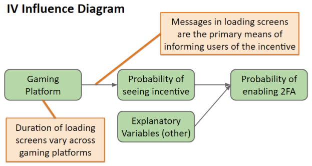

IV Influence Diagram
Messages in loading screens are the primary means of informing users of the incentive
Gaming Platform
Probability of seeing incentive
Probability of enabling 2FA
Duration of loading screens vary across gaming platforms
Explanatory Variables (other)

Figure 1: Influence diagram for instrumental variable (IV) model.

Adopted 2FA	
Reasons	*Count*
Better security	84
Incentive	11
Ease or comfort	7
Tournament rule	3

Table 1: Participant's reasons for adopting 2FA.

Not Adopted 2FA	
Reasons	*Count*
Account not vital	36
Extra hassle	19
Unaware of option	11
Secure enough	3

Table 2: Participant's reasons for not adopting 2FA

Introduction

Released in 2017, Fortnite has become one of the most popular games of all time with over 250 million active users [6]. Generating $2.4B in revenue in 2018, the platform has become a target for social engineering attacks aimed at compromising user accounts and stealing financial information [8, 14]. In response, Fortnite's parent company Epic Games began offering free in-game content to players who enabled two-factor authentication (2FA) for their account. As one of the first examples of an incentive offered to encourage positive security behavior in the private sector, Fortnite's initiative provides a unique opportunity to examine incentives for security in practice. Understanding how this affected the security decision-making of users is critical for the design of future incentives in the field.

Background and Related Work

Multifactor authentication is a process that requires a user to provide a combination of something they know, something that they are, and something that they have in order to identify themselves. 2FA is a subset requiring only two of these factors, most often a password and smartphone authentication code. However with each additional factor required, a system trades usability for security [11]. Despite the growing ubiquity of smartphones, which has lowered barriers to enabling 2FA, users have shown resistance to its adoption [9, 12]. Recent studies have demonstrated the usability and perceived difficulty, real or not, of initial 2FA configuration poses the greatest hurdle for users [4, 1]. This is further compounded by evidence that even for users already motivated by security, intentions don't necessarily translate into positive outcomes [5].

To address these challenges, incentives in the security field, like those more broadly, are often employed to shift cost tradeoffs and motivate "users to behave according to their stated preferences [2]. However, their effectiveness is dependent on the interaction of many factors including the value of the incentive offered, how the individual values what they are protecting, and the perceived effectiveness of the encouraged behavior [13, 3, 7]. While the majority of previous work is based on controlled laboratory experiments, our study provides insight into real-world behavior in response to a security incentive. As such, we are able to validate many of these findings and contribute additional insight into user preferences.

Study Design

This study employed a between-subjects design to examine the differences in players who enabled 2FA and those that did not. Participants were recruited using Amazon's Mechanical Turk platform over a 3-week period spanning from April to May 2019. Initial pilot studies indicated that a screening process was necessary to ensure the study only recruited active Fortnite players. Only 13% of the initial responses contained verifiable Fortnite usernames. Many provided fabricated handles or those of famous streamers. To address this, we verified player usernames through an API call to a public facing database of known Fortnite accounts and asked general knowledge questions of the game's mechanics.

In total, 1,010 responses were collected for the screening survey, of which 24% were found to be eligible for the study. A total of 200 out of the 242 eligible participants went on to complete the full survey. Participants were compensated $0.05 for completing the screening process and $2.50 for the full study survey.

Methodology

The primary challenge of conducting this study outside of a laboratory setting was the inability to randomly assign

Incentive and 2FA Adoption		
Adopted	*Seen Incentive*	
	No	*Yes*
No	73	4
Yes	68	55

Table 3: Breakdown of participants based on whether they were aware of the incentive and enabled 2FA. Strong positive correlation (OR 14.76).

Social Effect and Incentive		
Incentive	*Friend Adopted*	
	No	*Yes*
No	100	41
Yes	16	43

Table 4: Breakdown of participants based on whether they had a friend who enabled 2FA on Fortnite and if they were aware of the incentive offer. The positive correlation (OR 6.55), unaccounted for in the model, likely dampened the effect of the incentive.

the incentive across participants. To address this issue, an instrumental variables (IV) method was employed using logistic regression. IV is an econometric method commonly used when there are endogenous explanatory variables. A suitable instrument can be used to predict the independent variable, but does not have an effect on the dependent variable except through the independent variable [10].

In our study, we chose the primary gaming platform that the participant plays Fortnite on as a viable instrument. Loading screens within the game are the primary means through which Epic Games can communicate information regarding 2FA to its users. The duration that loading screens are visible to players varies across platforms. Personal computers offer much greater computational resources than other devices. As a result, the loading screens are visible much longer on phones and consoles, making it more likely that a player received information about the incentive. While the instrument is unlikely to be directly correlated with 2FA adoption, it is possible that unmeasured usability differences across platforms may generate potential bias.

In total, five proposed multivariate models were tested: one baseline without IV and four two-stage IV models with different covariates. Each model was constructed based on an exploratory analysis using a random 20% of the sample and evaluated using 5-fold cross-validation on a different 60% subset. This method used the average area under the Receiver Operating Characteristic (ROC) curve as the assessment metric. Reported outcomes are based on the 80% of the data that was not used to design the models.

In addition to the quantitative analysis, participant's open-ended responses regarding their reasons for adopting, or not adopting, 2FA were coded using emergent coding techniques. The codebook was validated by two separate coders for acceptable inter-rater reliability using a subset of 50 responses (Cohen's Kappa: 0.649). User preferences for enabling 2FA in response to different incentives and accounts were also collected and aggregated to assess the rationality and strength of user security preferences.

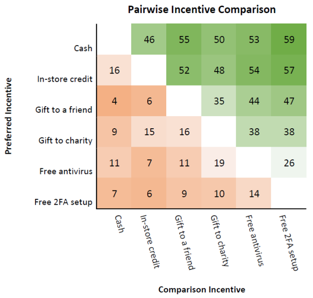
Effect of the Incentive

Overall, the data revealed a strong positive correlation ($p<0.01$) between the following independent variables and enabling 2FA.

- Being aware of the incentive being offered.
- Having a friend who enabled 2FA for Fortnite.
- Having an account that was previously compromised.

Across the sample, the odds of adopting 2FA was 14 times greater for those who had seen the incentive compared to those who had not (OR 14.76). However, since this is only a descriptive statistic, we attempted to isolate the causal relationship using IV methods. Two IV models performed well under cross-validation, but Model 3 (AUC 0.803) was chosen as the best representation of the data as it involved fewer covariates and would be less likely to overfit the data. However, no statistically significant effect was found for the incentive in any of the IV models tested.

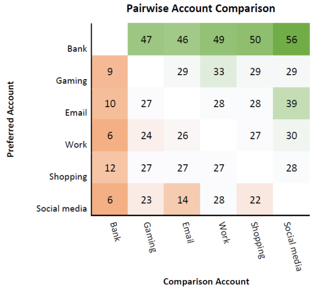
While this result might indicate that the effect of the incentive was too small for our sample size to capture, it may also be the case that further refinement of the IV model is required to accurately model the data. Our analysis showed that the odds of knowing about the incentive being offered was 6 times greater for those who had a friend who adopted 2FA for their Fortnite account (OR 6.55). While the research team hypothesized that social effects would influence 2FA adoption, we did not anticipate the important role it would play in spreading awareness of the incentive being offered. This dampened the true effect of the proposed IV in our models. Isolating this aspect of the overall social effect and



Pairwise Incentive Comparison

Preferred Incentive \ Comparison Incentive	Cash	In-store credit	Gift to a friend	Gift to charity	Free antivirus	Free 2FA setup
Cash		46	55	50	53	59
In-store credit	16		52	48	54	57
Gift to a friend	4	6		35	44	47
Gift to charity	9	15	16		38	38
Free antivirus	11	7	11	19		26
Free 2FA setup	7	6	9	10	14	

Figure 2: Number of participants who strictly prefer to enable 2FA for the incentive on the y-axis compared to that on the x-axis. The prevalence of darker colored areas indicates strong preferences between alternatives.



Pairwise Account Comparison

Preferred Account \ Comparison Account	Bank	Gaming	Email	Work	Shopping	Social media
Bank		47	46	49	50	56
Gaming	9		29	33	29	29
Email	10	27		28	28	39
Work	6	24	26		27	30
Shopping	12	27	27	27		28
Social media	6	23	14	28	22	

Figure 3: Number of participants who strictly prefer to enable 2FA for the account on the y-axis compared to that on the x-axis. The light colored areas indicate greater user uncertainty.

accounting for it in future work shows promise toward finding a significant result moving forward.

Reasons for Adopting

In our analysis of the open-ended responses, summarized in Table 1 and 2, we found that the majority (68%) of participants who adopted 2FA were primarily motivated by the extra layer of security. This is a positive sign for the general perception of 2FA in the population. However, only 11 participants (9%) mentioned the free in-game content as a major factor in their decision despite the strong positive correlation observed in the data. This is likely a result of the offer being salient only for those participants on the margin where the incentive would be most influential.

Of the participants who did not adopt 2FA, 54% reported being unaware that 2FA was available and 15% explicitly mentioned it as the reason for not adopting. In addition, 58% were uninformed of the incentive offer before taking the survey. This indicates that many users did not notice the notifications, likely a result of habituation to the many messages displayed in the loading screens. As such, future communication-based interventions targeting user awareness would likely improve adoption outcomes. Of greater concern, 47% of non-adopters viewed their Fortnite account as not important enough to enable 2FA for and another 4% felt 2FA was ineffective at providing additional security. This validates findings from previous work and reinforces the need for improved risk communication to end users.

User Preferences

Overall, we found participants exhibited rational preferences when presented with choices between different incentives and accounts. Shown in Figure 2, participants displayed strong preferences across the spectrum of incentives. Monetary rewards were found to be the most attractive, with each subsequent offer favored less. This suggests that users have well-defined preferences in this area. As such, organizations should focus their efforts towards using cash, or cash-like rewards. Instead of rewarding users with a fixed in-game emote as Epic Games currently does, allowing users to choose their reward, thereby making it more cash-like, would likely increase the offers attractiveness.

In contrast to the user's strong incentive preferences, Figure 2 shows that participant's preferences towards different types of accounts were much weaker. With the exception of bank accounts, which participants had clear preference for over the alternatives, users exhibited a high degree of uncertainty when faced with other comparisons. This indicates that individuals either have very disparate preferences or, more likely, have difficulty assessing the value and security risks associated with different accounts. As such, it is imperative organizations make the case to their users why a certain account is worth protecting.

Conclusion and Future Work

The results of our study validate previously identified factors that contribute to security decision-making and behavior in response to incentives. In addition, we confirm that individuals exhibit rational preferences and show they face uncertainty when assessing the security risk and value of different accounts. Along with low rates of incentive and 2FA awareness, this highlights the vital role of effective end-user communication. While we were unable to find a statistically significant effect for the incentive, we believe that future refinement of our proposed IV model that isolates social effects may lead to a significant result going forward.

Acknowledgements

We thank Lorrie Cranor, Hana Habib, and Sarah Pearman for their helpful suggestions and guidance during this study.

REFERENCES

1. Claudia Ziegler Acemyan, Philip Kortum, Jeffrey Xiong, and Dan S. Wallach. 2018. 2FA Might Be Secure, But Its Not Usable: A Summative Usability Assessment of Googles Two-factor Authentication (2FA) Methods. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62, 1 (2018), 1141–1145. DOI:http://dx.doi.org/10.1177/1541931218621262

2. Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users&Rsquo; Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. DOI: http://dx.doi.org/10.1145/3054926

3. Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags. 2012. It's All About the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice. In *Proceedings of the 15th International Conference on Financial Cryptography and Data Security (FC'11)*. Springer-Verlag, Berlin, Heidelberg, 16–30. DOI: http://dx.doi.org/10.1007/978-3-642-27576-0_2

4. Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 456, 11 pages. DOI: http://dx.doi.org/10.1145/3173574.3174030

5. Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 97–111. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/forget

6. Ben Gilbert. 2019. How big is 'Fortnite'? With nearly 250 million players, it's over two-thirds the size of the US population. *Business Insider* (Mar 2019). https://www.businessinsider.com/how-many-people-play-fortnite-2018-11

7. Tejaswini Herath and H.R. Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47 (05 2009), 154–165. DOI:http://dx.doi.org/10.1016/j.dss.2009.02.005

8. Tom Hoggins. 2019. Fortnite earned record 2.4bn in 2018, the most annual revenue of any game in history. *The Telegraph* (Jan 2019).

9. Andy Kemshall. 2011. Why mobile two-factor authentication makes sense. *Network Security* 2011 (04 2011), 9–12. DOI: http://dx.doi.org/10.1016/S1353-4858(11)70038-1

10. Gangadharrao S. Maddala and Kajal Lahiri. 1992. *Introduction to Econometrics*. Vol. 2. Macmillan. 354–356 pages.

11. Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. 2018. Multi-Factor Authentication: A Survey. *Cryptography* 2 (01 2018). DOI: http://dx.doi.org/10.3390/cryptography2010001

12. Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. Two-factor Authentication: Is the World Ready?: Quantifying 2FA Adoption. In *Proceedings of the Eighth European Workshop on System Security (EuroSec '15)*. ACM, New York, NY, USA, Article 4, 7 pages. DOI:http://dx.doi.org/10.1145/2751323.2751327

13. Elissa M. Redmiles, Michelle L. Mazurek, and John P. Dickerson. 2018. Dancing Pigs or Externalities?: Measuring the Rationality of Security Decisions. In *Proceedings of the 2018 ACM Conference on Economics and Computation (EC '18)*. ACM, New York, NY, USA, 215–232. DOI: http://dx.doi.org/10.1145/3219166.3219185

14. Matt Tatham. 2019. While Youre Playing Fortnite, Fraudsters Are Looking to Play You. *Experian* (Mar 2019).

15. Dave Thier. 2018. How To Unlock The Free 'Boogie Down' Emote In 'Fortnite: Battle Royale'. *Forbes* (Apr 2018).