

Hacktion: Building a More Cyberliterate Public Through Public Play

Frank J. Lee, Ph.D.

Professor of Digital Media at Drexel University, Director of the Entrepreneurial Game Studio (EGS)

I. INTRODUCTION

Hacktion is a pervasive mixed-reality (PMR) mobile game that educates the general public in simple, accessible cybersecurity measures in order to better protect American society from large scale cyberattacks. The unique PMR format of *Hacktion* places it at the forefront of games-based interventions in education, behavior modification, and civic engagement.

II. KEY INNOVATIONS

A. Improving Game-Based Education

Hacktion is the product of a unique design model in which learning objectives are built directly into the game experience rather than grafted on as an afterthought. The model follows Bogost, who argues that a successful educational game must integrate its rules with its fiction to be effectively immersive and intrinsically motivating.^{1,2}

B. Foregrounding Human Behavior in Cybersecurity

While it is tempting to think about network security as a matter of objective elements such as the resilience of data structures, our research suggests that the cyberliteracy of key personnel and populations within targeted systems is far more significant^{3,4}. *Hacktion* aims to inoculate the American population from likely future hacking incidents such as DDOS and other IOT attacks.

C. Public Playtesting as Data Analysis

During a period of open play the *Hacktion* application will gather a suite of anonymized information pegged to particular players in the test population. With this data we can evaluate the change in our population's knowledge of cybersecurity practices and confidence in cyberliteracy. Further, we can use customized analytical tools to evaluate game progress with a level of granularity specific to our game experience. We can, for example, isolate a group of players that only completed three of the seven mini-games and evaluate how their understanding of a given cybersecurity principle differs from the control group.

III. SCREEN SHOT

PMR games like *Hacktion* and *Pokemon GO!* use GPS and high-speed wireless networks to create public play experiences outdoors. Here, a tester plays a minigame that teaches users the importance of strong password management.

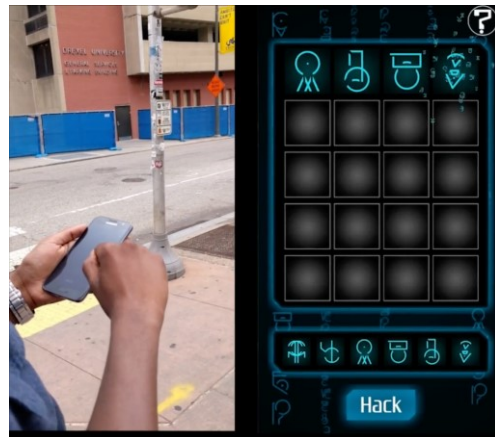


Figure 1: Pass-Cracker Minigame

ACKNOWLEDGEMENTS

Hacktion is made possible by National Science Foundation (NSF) funding through the Secure and Trustworthy Cyberspace (SaTC) initiative.

REFERENCES

1. Bogost, "The Rhetoric of Video Games." In K. Salen Tekinbas (Ed.), *The Ecology of Games: Connecting Youth, Games and Learning*. Cambridge, MA. MIT Press. [PDF]. Retrieved Nov. 20, 2017.
2. Bogost, *Persuasive Games: The Expressive Power of Video Games*, Cambridge, Mass: MIT Press, 2010.
3. National Science and Technology Council, "Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security," [PDF], 2016
4. IBM Global Technology Services, "IBM Security Services 2014 Cyber Security Intelligence Index," [PDF] 2014.