DREU Final Report

Ashley Bochner
Indiana University

July 2021

1 Introduction

Phishing is a chronic risk online, with severe results. The hacking of the Democratic Party in 2016 and other major hacks in history all began with phishing. Defeating phishing requires ubiquitous use of two factor authentication.

Cryptographic fobs are the only widely used two factor authentication option which has not been documented to be vulnerable to users. Phone-based methods of 2FA are not as strong as the fobs. A most simple version occurs when attackers claiming to be customer service representatives obtain the cooperation of victims who dutiful read off their short-messaging service, such as texting, in order to authentication themselves [YA14]. Other successful attacks against phone-based two factor which cryptographic fobs are far less vulnerable include malware [Dmi+14], man-in-the-middle [KVB16],and pop-up femtocells which control all traffic to a phone [GRB12].

In this work we examine the case where the keys are provided and there is certainty of exchanging information. The keys were provided by the university and the recipients of the key participated in learning remotely. If the uncertainty were removed and the devices provided at no cost, would the keys be perceived as useful and acceptable?

To answer the questions about the acceptability of Yubikeys we provided incoming students to a university in the Midwest with free Yubikeys in the fall of 2020. We asked them about their self-reported authentication practices, compared this to their actual authentication practices and authentication use for the incoming class as a whole. We then interviewed a small number for further insight. All interactions except for the interviews were anonymous and data was shared as distributions for comparison rather than individual records as possible. All the data sharing and experimental protocols were documented and approved by the IRB.
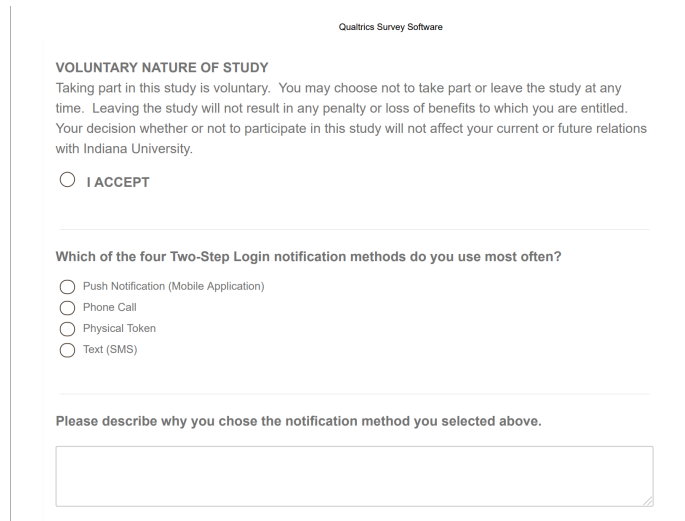
2 Methodology

Two hundred randomly selected first year students were delivered Yubikeys to their homes or dorms upon enrollment to the University. All students that

attend the university are required to use two factor authentication to login to university websites.

At the end of the academic year the students who received a Yubikey and were identified by the university as still enrolled were sent a separate survey invitation from those who did not receive the key at the beginning of the year. The number of first year students who received Yubikeys that were still active at the end of the first year dropped from 200 to 123 (61.5%).

The survey had a combination of multiple choice questions and open answer, as pictured below.

Qualtrics Survey Software

VOLUNTARY NATURE OF STUDY
Taking part in this study is voluntary. You may choose not to take part or leave the study at any time. Leaving the study will not result in any penalty or loss of benefits to which you are entitled. Your decision whether or not to participate in this study will not affect your current or future relations with Indiana University.

○ **I ACCEPT**

Which of the four Two-Step Login notification methods do you use most often?
○ Push Notification (Mobile Application)
○ Phone Call
○ Physical Token
○ Text (SMS)

Please describe why you chose the notification method you selected above.

Figure 1: A screenshot of our survey sent out to the students.

The survey asked about their preferences and use of two-factor authentication. The survey contained questions that inquired participants to reflect on their experience with two-factor authentication on the likert scale. We also inquired about the participants technical expertise and demographics. From the email sent to the groups, we received 68 survey responses, 15 from the Yubikey group and 53 responses from the general student group.

Survey question asking about gender reference [**spiel2019gender**]. This article tackles the topic of how to ask participants about their gender identity respectfully within research surveys.

3 Findings

When analyzing our survey we found that 75% of our respondents reported using 2FA for services outside the university context. With the majority (82%) reporting to use push notifications and only 3% reporting using a physical token at the end of the period. The most common responses given for changing from

physical tokens to another authentication method focused on the fear of losing the physical token, a lack of compatibility with specific device (such as a phone or tablet without the correct USB port), and not perceiving a benefit compared to a phone they already had.

4 Acknowledgements

I would like to thank the DREU for the funding provided for this summer. I would also like think Professor L. Jean Camp and doctoral candidate Jacob Abbott for providing exceptional mentorship and guidance throughout my research journey.

References

[Dmi+14]   Alexandra Dmitrienko et al. "On the (in) security of mobile two-factor authentication". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2014, pp. 365–383 (cit. on p. 1).

[GRB12]   Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. "Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications." In: *NDSS*. 2012 (cit. on p. 1).

[KVB16]   Radhesh Krishnan Konoth, Victor van der Veen, and Herbert Bos. "How anywhere computing just killed your phone-based two-factor authentication". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2016, pp. 405–421 (cit. on p. 1).

[YA14]   Ezer Osei Yeboah-Boateng and Priscilla Mateko Amanor. "Phishing, SMiShing & Vishing: an assessment of threats against mobile devices". In: *Journal of Emerging Trends in Computing and Information Sciences* 5.4 (2014), pp. 297–307 (cit. on p. 1).