“If I could do this, I feel anyone could:” The Design and Evaluation of a Two-Factor Authentication Manager

Garrett D. Smith
Brigham Young University
“If I could do this, I feel anyone could.” The Design and Evaluation of a Two-Factor Authentication Manager

Garrett D. Smith

A thesis submitted to the faculty of Brigham Young University in partial fulfillment of the requirements for the degree of Master of Science

Kent Seamons, Chair
Xinru Page
Daniel Zappala

Department of Computer Science
Brigham Young University

Copyright © 2022 Garrett D. Smith
All Rights Reserved
ABSTRACT

“If I could do this, I feel anyone could.” The Design and Evaluation of a Two-Factor Authentication Manager

Garrett D. Smith
Department of Computer Science, BYU
Master of Science

Two-factor authentication (2FA) is a strong defense against account compromise. However, usability studies reveal challenges with 2FA setup. The process to manually setup and remove 2FA methods differs across websites. We present a system design for a 2FA manager to automatically setup and remove 2FA methods. Potential benefits are reduced time, fewer mistakes, consistent terminology, a single workflow for users to learn, and the ability to rapidly transition to a new 2FA method—e.g., when replacing a lost 2FA method. We create two proof-of-concept implementations of our design, one as a browser extension and one integrated as a feature in an existing password manager. We evaluated the browser extension implementation approach using a between-subjects user study (N=60). Our results show fewer mistakes and reduced time compared to manually adding and removing 2FA methods. Qualitative results show that users found the automated process easy to use and were enthusiastic about the 2FA manager’s ability to help them rapidly replace 2FA methods in the case they lost their 2FA device.

Keywords: Usable Security, Two-Factor Authentication, automation, user study
ACKNOWLEDGMENTS

I would like to thank my advisor Kent Seamons, for allowing me to do this research and for his invaluable advice and guidance. I was fortunate to be introduced to this topic through Jonathan Dutson’s initial work. I appreciate the work that he did that led up to this project and his advice and feedback with this work. I would also like to thank Tarun Yadav for all of the help he provided in building the prototype, and his advice and effort while designing, and executing the user study. I’d also like to thank Paul Spencer for his help with the implementation of the prototype. I’d also like to thank all of those that helped provide feedback on my study design and final submission including Scott Ruoti, and my committee members Xinru Page and Daniel Zappala.

Lastly, I would like to thank my wife and daughter for all of their patience and support while I completed this project. I truly would not have been able to do this without them.
Contents

1  In Preparation: “If I could do this, I feel anyone could:” The Design and Evaluation of a Two-Factor Authentication Manager .......................... 1
Chapter 1

In Preparation: “If I could do this, I feel anyone could:” The Design and Evaluation of a Two-Factor Authentication Manager

This manuscript has not yet been accepted for publication.
"If I could do this, I feel anyone could:" The Design and Evaluation of a Two-Factor Authentication Manager

Garrett Smith  
*Brigham Young University*

Tarun Yadav  
*Brigham Young University*

Jonathan Dutson  
*Microsoft*

Scott Ruoti  
*The University of Tennessee*

Kent Seamons  
*Brigham Young University*

**Abstract**

Two-factor authentication (2FA) is a strong defense against account compromise. However, usability studies reveal challenges with 2FA setup. The process to manually setup and remove 2FA methods differs across websites. We present a system design for a 2FA manager to automatically setup and remove 2FA methods. Potential benefits are reduced time, fewer mistakes, consistent terminology, a single workflow for users to learn, and the ability to rapidly transition to a new 2FA method—e.g., when replacing a lost 2FA method. We create two proof-of-concept implementations of our design, one as a browser extension and one integrated as a feature in an existing password manager. We evaluated the browser extension implementation approach using a between-subjects user study (N=60). Our results show fewer mistakes and reduced time compared to manually adding and removing 2FA methods. Qualitative results show that users found the automated process easy to use and were enthusiastic about the 2FA manager’s ability to help them rapidly replace 2FA methods in the case they lost their 2FA device.

1 **Introduction**

Password authentication is vulnerable to remote attackers. Two-factor authentication (2FA) addresses this threat by requiring that in addition to a password (“something you know”) users must also authenticate using a factor that is difficult to steal remotely: “something you have” or “something you are”. While 2FA does not entirely prevent remote attack compromise, it does reduce the likelihood of such an attack and mitigate the impact of a successful attack [14, 15, 24].

Although 2FA provides security benefits, it is difficult for users to set up correctly [1, 7, 20]. This difficulty is driven by several factors. First, there is a wide variety of “something you have” implementations—for example, hardware security tokens, codes sent over SMS, and phone applications using push notifications—each of which is different to setup and use [19]. Second, there are hundreds of websites implementing 2FA [8], but each has a different setup interface, workflow, and terminology. For example, Google uses the term 2-step verification while sites like GitHub use the term two-factor authentication. Some sites require users to first setup 2FA using SMS before enabling other methods, while others allow any 2FA method to be enabled. This variation limits the ability for users to directly transfer experience from one site to another and may even cause mistakes if sites function differently from each other [20].

Third, there is no support to mass-enroll on multiple accounts, users must adopt 2FA manually, one account at a time. This can be time consuming. Later, if users need to replace their 2FA device (e.g., purchase a new phone), they have to manually re-enroll across these various accounts unless the 2FA method they are using supports synchronization across devices. Currently SMS is the only method that allows for a near seamless integration when getting a new device since the 2FA identifier is not unique to the mobile device but to the user’s phone number. For more secure methods of 2FA, such as push-based notifications or time based one time password (TOTP), this integration still requires user effort as synchronization is not enabled by default. Even then, only certain TOTP applications such as Twilio’s Authy [3] support the synchronization of TOTP secret keys across devices. As one renowned security researcher recently tweeted: “Upgraded to a new phone, which is like taking a 12 hour refresher course in configuring 2FA” [4].

We propose a novel solution to this problem—a 2FA manager that provides a unified, automated process to setup and remove 2FA methods on users’ accounts. To achieve our vision, this paper makes the following contributions.

1. We analyzed the workflow of 2FA enrollment at a number of websites to identify an abstract design of the 2FA setup process. We propose a 2FA manager that partially automates the 2FA setup process, providing a
unified, fast, and easy-to-use method for setting up 2FA methods across a wide range of websites. The manager can handle most of the enrollment process for the user: authenticating to their account, initiating the 2FA enrollment process, sending and receiving setup codes, completing the enrollment process, and ensuring a proper website configuration to begin using 2FA. The manager is especially well-suited to help users set up accounts en masse, such as when they first begin using 2FA or acquire a new 2FA device.

2. We describe two implementation architectures of the design: including a standard web-API to simplify, streamline, and speed up the setup and removal process. We discuss lessons learned from two prototype implementations of our 2FA manager as a Chrome Browser extension and an implementation that integrates with KeePass, an open source password manager.

To evaluate our proposed design, we conducted a between-subject user study (N=60) of a simulated prototype of our design. The user study was designed to answer the following research questions:

RQ1 Does automated 2FA setup/removal increase success rate?
RQ2 Does a user’s prior 2FA experience increase the success rate for 2FA setup/removal?
RQ3 Does automated 2FA setup/removal reduce completion time?
RQ4 Does a user’s prior 2FA experience reduce completion time for 2FA setup/removal?
RQ5 Does automated 2FA setup/removal increase the perceived usability of the setup/removal process?
RQ6 Does a user’s prior 2FA experience increase perceived usability of an automated 2FA setup/removal process?

The third contribution of our paper is our study results:

3. Our results show that the tested manager results in fewer mistakes and reduced time compared to manually setting up and removing 2FA methods. Qualitative results show that users found the automated process easy to use and were enthusiastic about the 2FA manager’s ability to help them rapidly replace 2FA methods in the case they lost their 2FA device.

2 Related Work

A few studies have focused on the usability of 2FA for banking systems in the UK. Gunson et al. studied a portable key fob which outputs a one-time code [12]. They found that while most customers perceived the 2FA method as offering a higher level of security, it was accompanied by significantly lower perceptions about usability and convenience. Fagan et al. shows that 71% of users reported inconvenience and cost as the reason to not use 2FA among the users who do not use 2FA [10]. The participants studied by Kol et al. were generally dissatisfied with the experience of using hardware tokens to authenticate, with one participant switching banks to avoid using the second-factor [16]. They recommend reducing the number of steps required for authentication to as few as possible to provide a more usable authentication experience. Our proposal builds off of this recommendation by attempting to reduce the number of steps for users to set up 2FA.

Das et al. examined the usability of the YubiKey Security Key. They found significant issues in the setup process, including unclear or confusing instructions, lack of validation, and a confusing demo [7]. Based on these findings, Yubico modified the instructions and simplified the workflow for the setup process. The researchers conducted a follow-on study and saw remarkable improvements. They provide suggestions to improve the acceptability and adoption of 2FA.

Reynolds et al. separated the study of the YubiKey’s day-to-day usability with the usability of the setup process [20]. Separating the setup and day-to-day usage of the device helped mitigate bias that may occur when a
negative or positive setup experience is reflected onto the day-to-day usability or vice versa. They found that while most users were pleased with the day-to-day usability of the YubiKey, the setup process was viewed poorly. They recommend that a standardized 2FA setup process could improve usability. Reese et al. similarly separated the study of day-to-day and setup usability [19]. They studied five second-factors and concluded that well-implemented 2FA could generally be usable in both setup and daily use. However, they acknowledge that the university population they studied is not representative of the general population, and recommend that other populations (such as the elderly or those without a college education) be studied.

De Cristofaro et al. compared the usability of three second-factors and found that perceptions of 2FA were more correlated with an individual’s background rather than the specific technology [9]. Most users studied found each of the methods studied to be highly usable. They find security tokens to be the most common second factor used in work environments, while email or SMS codes are the most often used in personal and financial environments. Colnago et al. studied the adoption of Duo, a cloud 2FA provider, at a university [6]. They found that users who have not tried 2FA anticipate it being more inconvenient and more difficult to use than it actually is. Once users tried 2FA, many thought it was easier to use than expected. They suggest that organizations should require the use of 2FA, with the understanding that once users begin to use 2FA they may have fewer usability concerns.

This previous work has highlighted many usability problems with 2FA and has provided suggestions for improving its user experience. While previous work has suggested standardizing the 2FA registration process, no work has developed such a system. Our work provides a first look into how to increase the usability of 2FA by simplifying the steps required of the user during the 2FA setup process.

Browsers have been automating password-based authentication using password managers for a long time. Nowadays browsers also offer integrated synchronization tools that allow configuring of devices to synchronize with each other. The synchronization allows autofill of credentials across devices for the stored accounts [11] [17]. To make 2FA based logins for phones seamless, Apple introduced a security code autofill feature for iOS 12 [2]. It allows a user to fill in the SMS code in the application automatically.

3 Design

To improve the usability and scalability of 2FA, we propose a 2FA manager for managing the setup process. Previous studies and our meta-analysis of some of the most common 2FA methods in use today helped us determine suitable tasks for a 2FA manager. Individual websites implement different terminology, instructions, requirements, and inconsistent 2FA setting’s location. We aim to provide a consistent and quick 2FA setup and removal experience into a single interface. A centralized place for setup/removal could avoid confusion caused by the wide variety of inconsistent 2FA setup processes websites offer today.

Design Goals After our analysis of setup processes we identified three high-level design goals: (1) Improve the setup success rate of 2FA; (2) Reduce the time to setup and remove 2FA; and (3) Provide a consistent user experience across websites (i.e., flow, terminology, requirements).

To accomplish these goals our 2FA manager brings the 2FA user experience into one unified interface, within the operating system or browser, similar to what a password manager does for single-factor authentication. For this system to be successful, we also propose a new standardized 2FA API that service providers can implement to simplify the interface between the 2FA manager and each service provider’s 2FA setup process.

3.1 Client-Side

We identified four steps to automating 2FA setup:

1. User authentication to an account
2. Selection of a second-factor method
3. The transfer of a 2FA identifier between the user and website
4. A challenge-response exchange to prove possession of the identifier

First, the manager facilitates user authentication to the website for which the user wants to set up 2FA. This typically involves providing the website with a username and password. The manager may store the user’s credentials, or it may prompt the user to input the credentials at the time of setup. If the user already enabled 2FA on the account, they will also have to authenticate with a second factor.

Second, the manager prompts the user to select a 2FA method from all the 2FA methods supported by the website and notifies the website. A manager might allow users to create a ranked list of their 2FA method preferences, allowing the manager to automatically select a 2FA method if the website offers one of the user’s preferred methods.

Third, the manager transfers a unique 2FA identifier between the user and the website. A 2FA identifier is a unique data-representation of a second-factor. For example, when selecting SMS as the 2FA method, a phone number is the unique identifier correlated with the user’s phone and is transferred from the user to the website. For some 2FA methods, the identifier originates at the website. For example, when selecting TOTP as the 2FA method, the identifier is a secret key transferred to the user through a QR or hexadecimal code.

Finally, the manager initiates a challenge-response process to verify that a user possesses the second factor. Websites
require users to prove possession of the 2FA identifier before enabling 2FA to prevent account lockout. This proof-of-possession occurs through challenge-response authentication. During challenge-response authentication, the website issues a challenge (a question for which the answer requires possession of the identifier) to the user, who must answer the question with the proper response (proof of possession of the identifier) to authenticate. The details of the challenge-response process depend on the chosen 2FA method. For example, for SMS 2FA the challenge is a text message sent to the user’s phone containing a code. The user responds by providing the website with the code they received in the text message. If the response matches the issued challenge, the website verifies that the user possesses the second factor.

The combination of identifier and challenge-response is similar to the username and password authentication scheme. The identifier is similar to a username, but instead of representing a user, it represents a second-factor. The challenge-response process verifies the identifier similar to the use of passwords to verify usernames. Table 1 provides examples of identifiers and challenges for common second factors.

Verification of the challenge requires the user to interact with a second factor. The 2FA manager itself should not be used as a second factor, which means that the final step of the 2FA setup process requires some user interaction. However, the 2FA manager could completely automate the first three steps of the authentication process. For example, a 2FA manager that stores user credentials and 2FA identifiers might automatically authenticate a user, select a default second-factor method, and transfer the identifier before prompting the user to take action to verify the website-issued challenge. Automating steps in the setup process reduces the number of steps users need to perform to complete setup, providing a more usable experience [16].

Unifying these four steps into a single interface greatly simplifies the 2FA setup process. This is especially helpful when a user wants to set up 2FA on multiple accounts. If a user wants to set up 2FA on ten different websites, they currently have to navigate ten different menus with different workflows, interfaces, and requirements. With our 2FA manager, they can use the same workflow and interface for every website. This consistency removes one of the challenges of 2FA setup, making it easier for users to manage 2FA for multiple accounts.

3.2 Server-Side

We describe two proposals for simplifying the interface between a service provider’s authentication flow and a 2FA manager. The first is to introduce new standard HTML5 elements for 2FA, which are easier to support in the short term. The second is a standard API for 2FA assistants which could take longer to adopt but is more robust.

3.2.1 Web Standards

Currently HTML5 offers standard elements to define different user input fields required for authentication, including password and email [18]. Using these declared types allows password managers to automate some authentication processes such as auto-filling user’s account credentials [13]. We propose extending these input fields to include other authentication fields such as OTP code fields and QR codes for receiving the private keys for TOTP. Just as email and password fields have standard types, so should 2FA-specific fields. Websites that use these standard types would allow automated tools such as our 2FA manager to interface directly with them to simplify and automate much of the setup process.

Unlike password-based authentication, two-factor authentication and setup typically require multiple steps taken by the user. Without a standard, unified flow interfacing with the websites, custom web automation scripts would need to be written for each website. This may reduce the scalability of the automated setup process.

3.2.2 2FA Setup API

Even with having standard elements, password managers still have issues interfacing with some websites that do not properly implement those elements or don’t use the standards [13]. While expanding web standards to include 2FA fields could ease automation, it would not guarantee a consistent experience between websites unless they also standardized their 2FA setup flow.

Our second proposed approach is a 2FA Setup API that standardizes the entire 2FA setup process and enables a simple interface for automation tools. A standard API supports more scalable, robust 2FA automation because it eliminates customizing a script for each website.

We developed a proof-of-concept Web API based on the four steps discussed in section 3.1. The API is designed to be used by authenticated users (or 2FA managers), and facilitates the selection of a second-factor method, the transfer of the 2FA identifier, and the challenge-response exchange. Our API is designed to be relatively simple to implement but robust enough to support many second factors. Authenticated 2FA managers can use five endpoints to manage their 2FA methods (see Figure 3).

While available 2FA methods have to be hard-coded in web automation scripts, the API allows for dynamic discovery of what 2FA methods a website supports through the “supportedMethods” endpoint. The methods already enabled by a user can be discovered through the “enabledMethods” endpoint. The API facilitates the transfer
<table>
<thead>
<tr>
<th>Method</th>
<th>Identifier</th>
<th>Challenge Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Codes</td>
<td>Backup code</td>
<td>Backup code</td>
</tr>
<tr>
<td>Phone Calling</td>
<td>Phone number</td>
<td>Code received through call</td>
</tr>
<tr>
<td>Push Notification</td>
<td>Registration ID</td>
<td>Approval of authentication request</td>
</tr>
<tr>
<td>SMS</td>
<td>Phone number</td>
<td>Code received through text</td>
</tr>
<tr>
<td>TOTP</td>
<td>Shared secret</td>
<td>Code generated from shared secret and timestamp</td>
</tr>
<tr>
<td>U2F</td>
<td>Public key</td>
<td>Signed challenge</td>
</tr>
<tr>
<td>WebAuthn</td>
<td>Public key</td>
<td>Signed challenge</td>
</tr>
</tbody>
</table>

Table 1: 2FA method with corresponding identifier and response to the website’s challenge.

![API endpoints](image)

Figure 3: API endpoints

of the identifier and the challenge-response process through the exchange of three objects between the 2FA manager and website: (1) Request object, (2) Challenge object, and (3) Response Object.

For a 2FA method to be supported, it must specify what data it needs in each of the three objects. In some cases, method-specific data may not be required in all three objects. The assistant sends the request object to the “requestSetup” endpoint, providing the name of the 2FA method, along with any required method-specific information. The website returns the challenge object, which may contain user instructions from the website for how to complete the challenge and other information needed for the challenge may be transmitted in this object. In the response object (sent to the “response” endpoint), the manager returns the completed challenge-response to the website. Finally, the website notifies the manager whether the setup was successful. During this exchange, the method’s identifier is transferred between the manager and the website.

The website issues a challenge to the user and enables the 2FA method on successful completion of the challenge by the user. The three objects are method-specific, and some may be empty for some methods. For example, the request object contains the user’s phone number for SMS verification messages. The challenge object may be empty since the challenge is sent out-of-band through the phone network. On receipt of the response object (containing the SMS verification code received by the user) the website can enable SMS verification.

Authenticated users may disable a 2FA method through the “remove” endpoint.

4 Proof-of-Concept Implementations

We created two proof-of-concept 2FA managers to test the feasibility and usability of our design. One manager is a password manager extension, and the other is a browser extension. The first manager is an extension that integrates with the popular open-source password manager KeePass. The other extension is a browser extension.

We consider password managers and browsers (with built-in password managers) as ideal platforms. They already have a list of the user’s online accounts, and can compare this list with published lists of websites that offer 2FA to prompt users to set up 2FA on supported accounts. Password managers (stand-alone or in the browser) already store user credentials, allowing for easy automation of the authentication process. They could also be used to store 2FA backup codes created during the setup process, as is recommended by sites such as GitHub.

Both managers rely on browser automation scripts to interface with the different websites. The advantage is that it allows an extension to provide 2FA automation without website cooperation. A disadvantage of scripts is a lack of
scalability. Differences in user interfaces and 2FA setup workflow between websites make it necessary to implement a specialized web automation script for each supported website. The script depends on a website’s underlying HTML, so changes to a website’s flow, content, or design may break the script. Maintaining support requires regular website monitoring to detect errors and restore functionality.

2FA manager’s UX   The first step in our 2FA manager setup process is to select the account(s) where a new 2FA method will be set up. The menu shows all of the websites that the 2FA manager currently supports as seen in Figure 4.

After selecting a website, the user is then prompted to authenticate unless the 2FA manager has access to the users credentials. The interface then allows the user to select one of the 2FA methods supported by the website, see Figure 5.

Depending on the 2FA method selected, the 2FA manager will then follow the method specific flow. For example, when a user selects TOTP-based 2FA the extension prompts the user to scan a QR code with an authenticator app and then enter the code provided from the app. Figure 6 and 7 shows this stage of TOTP setup for Github.

On successful completion of the second factor setup, the 2FA manager notifies the user, who can then return to the 2FA management menu.

2FA manager simulation for the user study   Our intent was to use the browser extension in our user study so that participants do not have to install standalone password managers on their devices to participate. However, during the pilot study described in Section 5.2 we found that a website’s 2FA user interface varied dramatically depending on the browser version and operating system of the machine running the extension. The changes in the interface created issues with our automated scripts that caused our manager to crash. We also found that the Chrome browser throttles any browser windows that are running in the background. This throttling was more severe on machines with limited resources, and caused many of our scripts to timeout without finding the necessary web elements needed to complete the process.

Due to the issues mentioned above we chose to create a version of the chrome extension that simulated the setup and removal process. To ensure that the experience was consistent across devices we used our working prototype to setup 2FA for Google, Facebook, and Dropbox 5 times on the same device using screen capture software to record the process. We then used the videos to calculate the average time that the extension would take in between user input and interfacing with each website. We used these average times to create artificial loading times into the simulated chrome extension.

5 Methodology

We conducted a 60-person between-subjects study approved by our institution’s ethics review board to evaluate the usability of our 2FA manager compared to the current 2FA setup/removal process. Due to the ongoing COVID-19 pandemic, and to obtain a more generalize-able sample, we elected to conduct the study remotely using Zoom.
5.1 Study Design

5.1.1 Independent and Dependent Variables

Our user study investigated how the method used to setup/remove 2FA affected the task success rate, completion time, and perceived usability of the setup/removal process. In this study we investigated two methods for 2FA setup and removal, manually using individual websites setup processes or using our simulated 2FA manager. Prior work [6] identified that prior usage of 2FA had an effect on the acceptance of 2FA. We wanted to test if the prior usage of TOTP influenced the success rate, setup time, or perceived usability of the setup/removal process of our simulated 2FA manager. We divided the 2FA usage into two groups, participants that used secure 2FA methods like TOTP or Security Keys, and participants that didn’t. To test these variables we first designed three different study groups:

<table>
<thead>
<tr>
<th>Group</th>
<th>Method Used</th>
<th>Prior Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td>Manual</td>
<td>Non-TOTP Users</td>
</tr>
<tr>
<td>Group B</td>
<td>Simulation</td>
<td>Non-TOTP Users</td>
</tr>
<tr>
<td>Group C</td>
<td>Simulation</td>
<td>TOTP Users</td>
</tr>
</tbody>
</table>

Table 2: User Study Conditions

Using a screening survey, we were able to assign participants to each Group. If a participant had experience using TOTP or Security Keys they were placed into Group C. Participants that did not have experience using either of those methods were randomly placed into either Group A or Group B. Organizing participants into these groups allowed us to compare Groups A and B to answer RQ1, RQ3, RQ5 while comparing Groups B and C helps us to answer RQ2, RQ4, and RQ6.

5.1.2 Study Setup

Participants were led through the study by a web-based Qualtrics survey and a study coordinator (shown in Appendix A.2). At the beginning of each session informed consent was obtained through the survey. Participants were then again asked about their usage of TOTP. Specifically participants were asked to look at the apps installed on their personal devices to see if they were using an authenticator app such as Twilio’s Authy or the Google Authenticator. If a participant’s answers differed from the answers in the scheduling survey the participant was reassigned to the correct group. For participants in either Groups A or B, the survey gave instructions on installing the Google Authenticator app. Participants in Groups B and C were then given instructions on installing the 2FA Automator Chrome extension. Study coordinators offered assistance if participants ran into issues installing the app or the Chrome extension (shown in Appendix A.3.1). Finally, participants were given unique login credentials for the Google, Facebook, and Dropbox test accounts and asked to get logged in to each of those accounts.

Before starting the tasks, participants were then given a brief introduction to 2FA, and specifically TOTP. Study coordinators read a short description of 2FA and TOTP with an explanation of the security benefits that 2FA provides (shown in Appendix A.3.3). The study coordinators then described the first task that the participants were assigned.
5.1.3 Group A - Manual Setup and Removal
The participants in Group A were tasked with setting up TOTP as the 2FA method for the three test accounts using each website’s 2FA setup process. Participants were allowed to use any resources they liked but were told that the study coordinators could not assist them with task. If the participants successfully completed the task, they were instructed to move on in the survey form and fill out a questionnaire about their experiences setting up TOTP. Once that was completed participants were then assigned their second task, removing TOTP from the test accounts. In describing the task, study coordinators explained that removing a 2FA method can be useful if a user obtains a new phone or if a device was lost or stolen. After completing the removal process participants filled out a second questionnaire about the removal process.

5.1.4 Groups B and C - Automated Setup and Removal
In groups B and C, participants were asked to use the 2FA Automator Chrome extension to setup TOTP as the 2FA method for the accounts. Again, participants were allowed to use any resources and were told that the coordinators would not be able to assist them. After completing the setup task they filled out a questionnaire about their experiences using the 2FA manager to setup 2FA. They were then instructed to use the 2FA manager to remove TOTP as the 2FA method on the accounts. The coordinators gave the same explanation about removal as was given to Group A. They then completed a final questionnaire about their experiences using the 2FA manager to remove TOTP from the accounts.

5.1.5 Questionnaire
The setup and removal questionnaire both used the System Usability Scale (SUS) to measure participant sentiment about the usability of the setup processes as a whole (i.e., not the usability of specific websites, but rather the usability of setting up 2FA across multiple accounts at one time). The System Usability Scale is composed of 10 Likert scale questions, with 1 being “Strongly disagree” and 5 being “Strongly agree” [5]. The responses to these questions are used to calculate a SUS score from 0 to 100. An analysis of over 5,000 users across 446 studies found that the average SUS score is 68, with a standard deviation of 12.5 [21]. These scores are often interpreted using percentile rankings or by assigning SUS scores a letter grade.

The questionnaire included questions to measure intention to adopt 2FA and perceived usefulness adapted from work by Colnago et al. [6]. Included with these questions were open-ended questions to investigate what aspects of the setup and removal process participants liked or disliked as well as reasons why they would or wouldn’t use TOTP or the 2FA manager for their own accounts.

5.2 Pilot Study
We conducted a pilot study over Zoom with 13 participants to test the functionality of our original Chrome extension and to test the study protocol. Of the 13 participants, 7 used our chrome extension. We found significant technical issues that made it difficult to ensure a consistent experience across user devices and operating systems. The pilot study prompted our decision to create a simulation of our 2FA manager for the user study to reduce development time and effort for the study.

Our participants were debriefed at the conclusion of the user study and informed that the chrome extension used in the study was not a working tool but a simulation of how the tool would work if they were to use it.

5.3 Recruitment
We recruited participants using the Prolific research platform. Eligibility criteria for the study required participants to be at least 18 years old, fluent in English, and willing to participate in a video interview. Participants first completed a scheduling survey (shown in Appendix A.1) delivered through Qualtrics. In the survey, participants reported their current 2FA usage and selected a time to participate in a live Zoom call.

Based on the participant’s reported 2FA usage, they were assigned to one of three groups. If they reported not having experience using a strong 2FA method such as TOTP or a security key, they were randomly assigned to either Group A or Group B. If they had experience with either of those methods, they were assigned to Group C.

5.4 Demographics
We specifically recruited equal numbers of male and female participants through Prolific. We found in our scheduling survey that males were more likely to report using an Authenticator App or security key. This resulted in Groups A and B having more female participants than males and Group C having more male participants than female. We attempted to balance the gender of participants in Groups A and B. A full breakdown of the demographic data for each group is shown in Table 3.

5.5 Compensation
Participants were compensated 8.55 USD for taking part in the study. The study lasted for approximately 30 minutes.

5.6 Limitations
The primary limitations in our study relate to our sampling methods. There may be a cultural bias in the data. Our participants were all located in the United States, and to sign
up for our study, they had to be fluent in English due to study coordinator limitations.

We recruited an equal number of male and female participants overall to balance the gender representation in the study. We did not foresee the dramatic difference in TOTP adoption by gender. This resulted in a balanced gender representation between Groups A and B, with more female participants than males. Since Group C had a significantly higher percentage of male participants than females, some of the differences between Group B and C results may be due to gender differences instead of their 2FA usage.

Unlike typical laboratory studies, we could not control the participant’s environment in a remote study, potentially biasing results. In addition, requiring participants to participate in a video call may have caused a sampling bias. We also measured participants’ intention to adopt TOTP after using our setup process to determine if participants were more likely to adopt TOTP after using a 2FA manager. Research has shown that users’ indication of their intention to adopt may not align with their actual adoption [22].

One limitation also comes from the implementation of the manager. For TOTP codes to be verified correctly, all devices that create or verify codes need to have closely synchronized clocks. Instead of relying on an API to verify the participants’ TOTP codes, we validated them locally in the extension. Thus, validation depended on the participants’ local system time. Some participants’ codes failed validation because their system time was too far out of sync. In one case, we detected the error, and the participant manually synced their computer. Other times the time difference between the authenticator app and the participants’ machine was less than 30 seconds allowing some codes to be accepted when they attempted to validate multiple times.

6 Quantitative Results

This section presents quantitative results from the user study. When comparing the means between task success rates we used a two-sample test of proportions. For comparing other means we used an independent t-test for two samples. We used the STATA 14.0 statistical software package for the quantitative analysis.

6.1 Task Success Rate—RQ1, RQ2

Participants completed the task successfully if they were able to setup TOTP as the 2FA method for each of the accounts. We wanted participants to experience the setup process for three major websites and evaluate the experience of setting up 2FA from a more general perspective than an individual website’s implementation. We hypothesized that our manager would have a significantly higher setup success rate than the manual setup. See Table 4 for a summary of the setup task success rate by Group. Of the five participants that failed to setup TOTP in Group A, two failed to setup TOTP on any accounts, two only failed to setup TOTP on Dropbox, and one failed to setup TOTP on only Google. We found a statistically significant difference in the success rate between the manual method and the 2FA manager (p = 0.0084), thus we can reject the null hypothesis. We also hypothesized that participants with experience using TOTP would also have a higher success rate when using the manager compared to participants who used our manager but didn’t use TOTP for their own accounts. The two participants in Group C that failed to complete the task were unable to setup 2FA on any of the accounts. For this hypothesis we fail to reject the null (p = 0.93) since we could not detect a significant difference in the success rate between Groups B and C.

For the removal task, we hypothesized that participants using our the 2FA manager would have a higher success rate than the manual method and that participants with experience with TOTP would also have a higher success rate. In Group A only one participant failed to remove 2FA, failing only on the removal process for Dropbox. Groups B and C did not have any task failure. We were unable to detect any significant difference between Groups A and B (p = 0.13). Since there were no failures in Groups B or C we can not perform a test of proportions between groups B and C.

6.2 Completion Time—RQ3, RQ4

Using the recorded video of each participant, we timed how long it took for each participant to complete the setup and removal tasks.
<table>
<thead>
<tr>
<th>Group</th>
<th>Setup Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A - Manual Setup</td>
<td>472</td>
</tr>
<tr>
<td>Group B - Automated Setup</td>
<td>315</td>
</tr>
<tr>
<td>Group C - Automated Setup</td>
<td>262</td>
</tr>
</tbody>
</table>

Table 5: Setup Completion Time by Group

<table>
<thead>
<tr>
<th>Group</th>
<th>Removal Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A - Manual Removal</td>
<td>162</td>
</tr>
<tr>
<td>Group B - Automated Removal</td>
<td>62.4</td>
</tr>
<tr>
<td>Group C - Automated Removal</td>
<td>59.67</td>
</tr>
</tbody>
</table>

Table 6: TOTP Removal Completion Time by Group

6.2.1 Setup

We used the video timestamps when a participant took their first setup action for each account and when they indicated that they had completed the setup for each site to calculate the completion time for each account. We subtracted the time that the participant asked the coordinator any questions, offered feedback, or if they decided to switch the website they were currently working on. Each of these website times were then added together to get the total setup task completion time. We only calculated this data for participants that completed the task successfully (Group A - 15, Group B - 20, Group C - 18).

We hypothesized that the manager would significantly reduce the amount of time required to setup TOTP on the three accounts. We rejected the null hypothesis and found a significant difference ($t(33) = 2.6602, p = 0.006$) between Groups A and B. We calculated a Cohen’s d of 0.904, indicating a large effect. We could not detect a significant difference between Groups B and C ($t(36) = 1.0694, p = 0.15$). A summary of this timing data can be found in Table 5.

6.2.2 Removal

We used the same method of calculating the removal timing as we did for the setup timing removing the timing data for the participant in Group A that failed to complete the task. Once again, we hypothesized the manager would significantly reduce completion time. We found a significant difference ($t(32) = 3.5054, p = 0.0007$) in the mean removal time between Groups A and B, so we can reject the null hypothesis. We did not find a significant difference between Groups B and C ($t(36) = 0.506, p = 0.31$). These results are shown in Table 6.

6.3 System Usability Scale—RQ5, RQ6

After participants completed each task they completed the System Usability Scale questionnaire. We hypothesized that our manager would be perceived to be more usable than the manual method, indicated by a higher SUS score for both the setup and removal process. Since the setup process is known to be difficult [1, 20]. We also hypothesized that participants with experience using TOTP would rate the manager higher than those without experience using TOTP.

6.3.1 Setup

We found the mean SUS scores for our manager to be higher than the manual method. Our manager had a median SUS score of 77.5 in Group A, while the manual method was 70.38. Figure 8 shows the distribution of SUS scores for participants in each group. We included all participants regardless of whether they successfully completed the task in calculating the mean SUS score for each Group. The scores suggest the 2FA setup process can be improved through automation, however we found that the differences in ratings between Groups A and B ($t(38) = 1.1339, p = 0.132$) and Groups B and C ($t(38) = 0.1866, p = 0.57$) were not statistically significant. In both cases we can’t reject the null hypotheses.

6.3.2 Removal

The results for the removal SUS scores are shown in Figure 9. Participants that failed to setup TOTP on any of the accounts did not attempt the removal task and were not asked the removal SUS questionnaire. We can reject the null hypothesis ($t(37) = 2.7986, p = 0.0041$) for the scores between Group A and Group B with a Cohen’s d of 1.02. There was no significant difference detected between Groups B and C ($t(36) = -0.6560, p = 0.74$).
7 Qualitative Results

After completing both tasks, participants answered open-ended response questions about their experiences with the setup and removal processes. To analyze these responses, two researchers used an inductive coding process [23] to identify common themes and ideas expressed by participants. First, the researchers independently read through all responses making a list of common themes and ideas they found. The researchers then discussed their lists and created an initial codebook. Researchers then independently coded 1/6th of the data, met to resolve differences in the codes and finalized the codebook. Finally, each researcher coded each response independently, then discussed the responses where there was disagreement in the codes until reaching agreement for all responses. Here we discuss the common themes and ideas observed in the responses. In total we identified 8 primary codes with 52 subcodes. The final codebook is included in Appendix A.4.

7.1 Setup

We first asked participants what they liked and disliked about the setup process. 41 participants (68%) expressed that the setup process was easy and took little effort. This response was consistent regardless of which setup process they used.

**Discoverability of 2FA settings** In Group A, 9 participants (45%) mentioned that they disliked searching for the correct page to set up 2FA. Our prototype resolved the concern of discovering 2FA by including 2FA settings as part of the automation process. None of the users from Group B or C reported an issue regarding the discoverability of 2FA settings.

**P26:** “It was hard to find the right place to do it on some sites. Google was the hardest.”

Once they found the correct page participants typically had little trouble. Participants liked that once they set up TOTP for one account they could largely use the same process to do it on more accounts.

**P26:** “Once you found the right place, it was easy to do. And the more I did it, the more comfortable I felt with it.”

**Inconsistency** One thing that some participants disliked across all systems was the inconsistency in the requirements for each account. Specifically, Dropbox and Facebook only required one 2FA method if the user wanted to set up TOTP while Google required participants to enable SMS first.

**P40:** “While I liked most aspects about the setup process, I did not like how my phone number had to be used with my Google account.”

**2FA Manager** Five participants (25%) in Group C mentioned the convenience of using the manager to set up 2FA on multiple accounts at a time.

**P10:** “This was *incredibly* easy. Install the extension, select multiple websites, and go. Setting up multiple websites is great, as I can just plug in credentials from my password manager.”

35% of participants groups B and C mentioned the usefulness of the 2FA manager while setting up 2FA.

**Others** Ten percent of participants from group A reported issues with the instructions but no participants from group B or C reported issues regarding instructions.

7.2 Removal

In general, participants (Group A - 11 55%, Group B - 18 90%, Group C 16 80%) also indicated how easy the removal process was. Participants in Group C again recognized that the 2FA manager could be helpful when managing 2FA for multiple accounts. Five participants (25%) mentioned liking removing 2FA en masse from accounts.

**P55:** “I liked that I could select multiple types of accounts (from multiple services) at one time instead of having to go through the whole process, repetitively, one service at a time.”

Some participants even found that knowing how easy it was to remove 2FA if they needed to switch devices would encourage them to use 2FA more.

**P23:** “This process makes the disabling of 2FA so easy that I’d want to use it on more websites.”
7.3 Extension Limitations

Group C participants had more experience with 2FA and we anticipated they would appreciate the idea of automating the setup and removal of 2FAs, however, we did not find a significant difference in the usability of the manager. We believe this is because of how we implemented our prototype. In group C, 40% of participants had implementation-specific concerns that wouldn’t exist if browsers incorporate our proposed design. 20% participants reported issues with our implementation (no Firefox support, no other 2FA method supported, being an extension, and UI) and other 20% participants mentioned their lack of trust in the extension.

P40: “I would likely use this automated tool on my own accounts based on how seamless the whole setup process was without having to delve into the website settings. Although with most Chrome extensions, I don’t exactly trust them given some that I have used in the past have “went rogue”. Nonetheless, I would likely use this automated tool for accounts that I use frequently that do not have sensitive information.”

8 Observations

There were several errors and pain points that participants encountered in the setup and removal process. The errors participants encountered were largely dependent on the setup process they used.

Manual Setup  Participants that used the manual method had a challenging time finding the 2FA settings page for each account. For example, on Facebook, participants often looked for the 2FA settings page in the Privacy settings instead of the Security and Login settings. For Google, participants often started looking for the 2FA settings page in Gmail settings instead of Google Account settings. As a result, many participants gave up trying to navigate to the correct settings page and instead resorted to using a search engine to find the settings page.

Once a participant found the 2FA settings page, the next issue they would encounter would be on the select a 2FA method page. Unlike Dropbox and Facebook, Google does not allow a user to enable TOTP unless they setup SMS or Google Prompt (push-based) first. There is no indication that Google supports TOTP unless the participant uses another method first. One participant gave up trying to setup TOTP on Google because they could not find the page to add TOTP.

Dropbox didn’t have as many pain points as Facebook and Google. However, there was a significant issue in the final step of Dropbox. Unlike Google and Facebook, Dropbox has several additional steps that participants go through even after entering the TOTP code from their authenticator app. Once a participant enters their secret code, Dropbox provides them with some backup codes that they should save for use when they lose access to their second factor. The two participants that failed to setup TOTP on Dropbox assumed they were at the end of the process and closed the 2FA popup window. This interrupted the setup process, never enabled 2FA for the account, and did not notify the user that they did not complete the process. This phenomenon has been identified before [20] but still remains an issue five years later. Users would think they have secured their account when in reality their account is still only protected with a password.

The final two participants in the manual group that were unable to complete the setup task didn’t understand how TOTP worked. One person setup SMS for each of the accounts, telling the study coordinator that they added the authenticator app to each of their accounts. The other participant could not figure out how to scan the QR code on the authenticator App.

Automated Setup  Every participant in Group B successfully setup TOTP on their accounts. Because our extension created a popup window, some participants had a difficult time finding the window when navigating to different windows. The two participants in Group C that were unsuccessful in setting up TOTP couldn’t figure out how to scan the QR code in the authenticator app. This was surprising, since both participants had indicated that they were already using TOTP on their own accounts.

Manual Removal  Each website had two primary methods for removing a 2FA method from the account. For each website there was both a single “Turn Off” 2FA button and some type of edit or manage button that was associated with each 2FA method that was enabled on the account. The main pain points participants encountered with this task was that each edit button behaved a bit differently. For Google, even though participants had to enable TOTP and SMS, when trying to use the edit/remove button to remove TOTP, Google would give an error that says, ”Two-Step Verification is not allowed without this method” even though participants had SMS setup as a backup method. This led all of the participants to simply turn off 2FA, removing both methods instead of just TOTP. On Facebook, the manage button would allow a user to either add a new TOTP app or turn off 2FA entirely. All participants were able to remove TOTP from Facebook. On Dropbox the edit button allows a user to choose a different 2FA method in place of the one they had enabled. One participant did not notice the small slider for turning off 2FA above the edit button and upon clicking the edit button and seeing the 2FA setup page assumed they had successfully removed the authenticator. This error is especially concerning. If users believe they have removed a method from their account and dispose of their authenticator...
(e.g., uninstalled their authenticator app, changed phone numbers) they could be locked out of their account.

**Automated Removal** No participants had issues removing TOTP from their accounts using the 2FA manager.

### 9 Discussion and Future Work

Our user study confirms previous work showing that the 2FA setup process suffers from usability issues. Specifically, our results indicate that significant fatal errors in the setup process that were discovered in 2018 [20] still exist in the current implementations of the setup process. Our user study also uncovered a similar issue in the removal process where users attempting to turn off 2FA could end up locked out of their accounts. The fact that these issues still exist shows the importance of improving the setup and removal processes of 2FA. While our study confirms the existence of these issues, future work could investigate how often issues such as these occur to users when they use their own accounts.

The results also show that the specific implementation of 2FA setup and removal affects the success rate, time to setup/remove, and usability of the process. With our tool, we showed that the setup and removal process can be improved through automation to increase the likelihood of success, decrease the amount of time needed, and potentially increase the perceived usability of the systems. Further, we find that fatal errors that users experienced in the manual method can be prevented when using our automated 2FA manager. Further work should investigate whether these improvements can increase the acceptance and adoption of 2FA.

While previous work has found that novice users of 2FA have lower acceptance and lower perceived usability of 2FA, our work shows that automation may reduce that effect. Participants that used the simulated 2FA manager and did not have experience using advanced methods of 2FA had similar rates of success, task time, and perceived usability as more advanced users. This result indicates that automating the 2FA setup/removal process could reduce the burden for novice users to be nearly the same burden as users with significant experience. Further work should investigate whether such a tool could also improve the adoption of 2FA in novice users due to decreased burden.

### 10 Conclusion

We design a 2FA manager that unifies and automates the 2FA setup and removal process for 2FA methods across multiple accounts. This manager is designed to make these processes more uniform and seamless.

To evaluate whether we met these goals, we conducted an evaluation of a browser-based implementation of our 2FA manager. Our results show that our manager results in fewer mistakes and reduced time compared to manually setting up and removing 2FA methods. Qualitative results show that users found the automated process easy to use and were enthusiastic about the 2FA manager’s ability to help them rapidly replace 2FA methods in the case they lost their 2FA device.

Furthermore, our user study reveals that when manually setting up 2FA methods, some users will add the method, but fail to enable 2FA on their account, leaving it protected only by a password. This problem was first identified by Reynolds et al. [20] in 2017, and remains a problem five years later. Similarly, we find that users can fail to complete the process for removing a 2FA method, leaving their account inaccessible if they dispose of the method. In contrast, our 2FA manager ensures that adding and removing completes as intended by the user, obviating these issues.

These results call for increased efforts to unify and automate the 2FA setup and removal process. Our long-term vision is that there is a role for 2FA managers to assist with 2FA, much like password managers help users manage passwords.

### References


A.1 Screening Survey

1. Which of these websites do you currently have an account with? (Select all that apply)
   Google, Amazon, Yahoo, Facebook, Reddit, LinkedIn, Twitter, Dropbox, Github, Pinterest, Outlook

2. Description: Many online services offer a method to increase the security of your accounts called Two-Factor Authentication (2FA). In addition to providing something you know (a password), 2FA typically requires that you also prove possession of something you have such as a phone or security key. To prove you possess this device a website will request information from the device. This information comes in one of these ways: (1) a code sent to your phone via SMS, (2) a notification on your phone, (3) a code generated by an authenticator app on your phone, (4) a press on a USB security key

   Question: Do you currently use any of these 2FA methods on any of your accounts?
   Yes, No, Not Sure
3. Do you currently use an authenticator app that generates a code that you provide when you login to any of your accounts, such as Authy, or Google Authenticator shown below? <We included logos of Twilio Authy and Google authenticator app for reference>
   yes, No, Not Sure

4. Do you currently use a USB security device such as the one in the picture to login to any of your accounts? <We included photo of a yubikey for reference>
   Yes, No, Not Sure

5. For each of the websites that you have an account with please indicate the 2FA method that you use to login to each account.
   A code sent to your phone via SMS, A notification on your phone, A code generated by an authenticator app on your phone, A press on a USB security key, None - I only have to use a username and password

6. Do you use the Google Chrome web browser?
   Yes, No, Not Sure

7. Do you currently have Google Chrome installed on your computer?
   Yes, No, Not Sure

A.2 Study survey

1. Please open your mobile phone and look through your apps. Which of these apps do you have installed on your account? <This question was used to put people in different group based on their answers>
   Authy, Google Authenticator, Both, Neither

2. Please open the app that you have installed. How many accounts are setup in your authenticator app? <Group C specific>
   0, 1-5, 6-10, More than 10

3. Please select which type of phone you have and press the next button
   iOS - iPhone iPad etc, Android - Samsung Pixel LG etc
   <Device-specific installation instruction for Google authenticator app provided along with the screenshot>

4. <For Group B & C, Installation instruction for our chrome extension is provided along with the screenshots>

5. <Test account details for Google, Facebook, Dropbox provided and users were asked to login manually into each test account>

6. <For Group B and C, instructions on how to open chrome extension along with screenshots were provided.>

7. Participants perform 2FA setup task

8. 2FA Usability Questions In this survey, the words “setup process” refer to the process of setting up the authenticator using the chrome extension. All questions must be answered. If you feel you cannot answer one of the items, mark the center of the scale. Please record your initial reaction to the questions rather than thinking for a long time.

   Strongly agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Strongly disagree

   (a) I think that I would like to use this setup process frequently.
   (b) I found the setup process unnecessarily complex.
   (c) I thought the setup process was easy to use.
   (d) I think that I would need the support of a technical person to be able to use this setup process.
   (e) I found the various functions in this setup process were well integrated.
   (f) I thought there was too much inconsistency in this setup process.
   (g) I would imagine that most people would learn to use this setup process very quickly.
   (h) I found the setup process very awkward to use.
   (i) I felt very confident using the setup process.
   (j) I needed to learn a lot of things before I could get going with this setup process.

9. Please select how much you agree with the following statements about two-factor authentication.

   Strongly agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Strongly disagree

   (a) Setting up two-factor authentication makes my account less likely to be compromised.
   (b) Setting up two-factor authentication means I do not have to worry as much about my account safety.

10. How satisfied or unsatisfied are you with the level of protection which is offered by Two-Factor Authentication?

    Strongly unsatisfied, Somewhat unsatisfied, Neither satisfied nor unsatisfied, Somewhat satisfied, Strongly satisfied

11. After using this tool how likely are you to start using an authenticator app to secure more of your personal accounts?

    Extremely unlikely, Somewhat unlikely, Neither likely nor unlikely, Somewhat likely, Extremely likely

12. If the automated tool you used in this task was available to you how likely would you be to use it on your own accounts?

    Extremely unlikely, Somewhat unlikely, Neither likely nor unlikely, Somewhat likely, Extremely likely
13. Please click and drag the following websites into these three categories:

Items: Google, Amazon, Yahoo, Facebook, Reddit, LinkedIn, Twitter, Dropbox, Github

options: I currently use an authenticator on this website, I plan to secure this website using an authenticator, I don’t plan to secure this website using an authenticator, I don’t use this website

14. What did you like about this setup process?
   <free response>

15. What didn’t you like about the setup process?
   <free response>

16. <conditional question based on previous response> You indicated you would be <likely/unlikely> to use an authenticator app for more of your own accounts. Why would (or wouldn’t) you want to use the authenticator app for more of your accounts?
   <free response>

17. <conditional question based on previous response> You indicated you would be <likely/unlikely> to use this automated tool on your own accounts. Why would (or wouldn’t) you want to use this tool for your own accounts?
   <free response>

18. Participants perform 2FA Removal task

19. 2FA Usability Questions In this survey, the words “removal process” refer to the process of removing the authenticator app from the account using the automated tool. All questions must be answered. If you feel you cannot answer one of the items, mark the center of the scale. Please record your initial reaction to the questions rather than thinking for a long time

   Strongly agree, Somewhat agree, Neither agree nor disagree, Somewhat disagree, Strongly disagree

   (a) I think that I would like to use this removal process frequently.
   (b) I found the removal process unnecessarily complex.
   (c) I thought the removal process was easy to use.
   (d) I think that I would need the support of a technical person to be able to use this removal process.
   (e) I found the various functions in this removal process were well integrated.
   (f) I thought there was too much inconsistency in this removal process.
   (g) I would imagine that most people would learn to use this removal process very quickly.
   (h) I found the removal process very awkward to use.
   (i) I felt very confident using the removal process.
   (j) I needed to learn a lot of things before I could get going with this removal process.

20. Now that you have used this removal process has it changed your opinion of whether you would like to use an authenticator app on your own accounts?
   No, Yes

21. Has your opinion changed of whether you would like to use the automated tool for your accounts?
   No, Yes

22. What did you like about this removal process?
   <free response>

23. What didn’t you like about this removal process?
   <free response>

24. <conditional question> You indicated that this task changed your opinion about using an authenticator app for more of your accounts. What was it that made your opinion change?
   <free response>

25. <conditional question> You indicated that this task changed your opinion about using this automated tool. What was it that made your opinion change?
   <free response>

26. <Debrief>

A.3 Instructions provided during the study

The following instructions were read to the participants during the study. The chrome install instructions were excluded from group A and the app install instructions were excluded from group C.

A.3.1 Instruction regarding installation of app and chrome extension

The app that you installed on your phone is an authenticator app that will generate secure codes that you can use to login to an online account. You will use this as part of the user study today. Go ahead and select the B option and click the next button to go to the next page in the survey. The next step to setting up your computer is to install a chrome extension that you will use in the study. The chrome extension you will install is used to set up Two-Factor Authentication on multiple websites. This page of the survey includes instructions for installing and enabling the extension. Please follow those instructions. I am here to help you if you run into any issues.
A.3.2 Instructions regarding opening incognito

The tasks you will be asked to do are related to the login process of three different online accounts: gmail, facebook, and dropbox. To protect your personal accounts, you will not be using your own accounts in these tasks but will use test accounts. We are also going to have you use incognito mode today. May I assist you in opening an incognito window, or are you already familiar with how to do it?

A.3.3 Instruction regarding setup task

For this task we would like you to set up 2FA on these three accounts. 2FA provides an extra layer of protection to an online account. In addition to providing something you know (like a password), 2FA typically requires that you also prove possession of something you have such as a phone or security key. To prove you possess this device a website will request information from the device. The app you installed on your phone is one such method. When logging in to an account that has an authenticator app setup, you will be asked to provide a secret code that is generated by the app. This secure code is unique and is linked to your account and your phone. In order for an attacker to gain access to your account they would need to not only have access to your password but would now also need to have access to your phone.

A.4 Codebook

1. Setup Usability
   (a) Discoverability of 2FA Settings
   (b) Learnability - after doing once it gets easier
   (c) (In)Consistency
   (d) Visibility of System Status
   (e) Multiple Accounts
   (f) Backup Method
   (g) Number of steps
   (h) Specific Requirements
   (i) Adding account to Auth App
   (j) Time/Effort to setup
   (k) Instructions
   (l) Easy/Intuitive process
   (m) QR Code Scanning

2. Security Strategy
   (a) Selective Securing
   (b) Mandatory Security
   (c) Proactive Securing
   (d) Reactive Securing

3. Removal Usability
   (a) Discoverability of 2FA Settings
   (b) Learnability
   (c) (In)Consistency
   (d) Visibility of System Status
   (e) Multiple Accounts
   (f) Number of steps
   (g) Specific Requirements
   (h) Time to remove
   (i) Easy/Intuitive process

4. 2FA Usability
   (a) Concerns for Losing Device
   (b) Annoyance of login
   (c) Require multiple devices
   (d) Ease of Use
   (e) 2FA Method type
   (f) Easy removal leads to increased usage

5. Security concern
   (a) Easy Removal means Security Concern
   (b) Trust
      i. Authenticator App
      ii. Extension
      iii. Websites
   (c) Lack of Awareness about Security Benefit

6. Extension Implementation
   (a) Firefox Support
   (b) Other 2FA method Support
   (c) Extension
   (d) UI

7. Usefulness of Automated Tool

8. Usefulness of 2FA
   (a) Risk Based Authentication is enough
   (b) Security Benefits
   (c) User doesn’t have accounts of value
   (d) Wasn’t aware of 2FA offering or how easy it is