1 Suvey Instrument

1.1 Prolific ID and captcha

1. What is your Prolific ID? Please note that this response should auto-fill with the correct ID. [*Asked for preventing duplicate participation and for payment purposes*]
2. Before you proceed to the survey, please complete the captcha below. [*Asked to prevent bots*]

1.2 Non-demographic background info

1. Are you proficient in English?
   - o Definitely yes
   - o Probably yes
   - o Might or might not
   - o Probably not
   - o Definitely not
2. Do you have a degree in Computer Science, including a "minor," or any professional computer science certifications?
   - o Yes
   - o No
3. What kind of operating system does your computer use?
   - o Microsoft Windows
   - o Linux/Unix
   - o macOS
   - o Other
   - o I am not sure
4. Are you familiar with the term "public- key cryptography"?
   - o Yes
   - o No
5. Do you understand how cryptographic protocols work?
   - o Yes
   - o No
   - o I am not familiar with the term "cryptographic protocol"
6. Have you used FIDO authentication technology before?
   - o Yes
   - o No
7. Are you familiar with FIDO authentication technology?
   - o Yes, I am very familiar
   - o Yes, I am fairly familiar
   - o Yes, but I don't really know much about it
   - o Possibly, the name is vaguely familiar
   - o No, I am not familiar
8. Do you know what two-factor authentication or multi-factor authentication (a.k.a. 2FA or MFA) is?
   - o Yes
   - o No
   - o I am not sure
9. Do you currently use two-factor authentication or multi-factor authentication (a.k.a. 2FA or MFA) for any of your online accounts (e.g. official, personal or business email accounts etc.)?
   - o Yes
   - o No
   - o I am not familiar with two-factor authentication or multi-factor authentication

1.3 Technical knowledge of privacy tools scale (Kang *et al.* [1])

Please indicate true or false for each of the statements below. Please select "I am not sure" if you do not know the answer.

	True	**False**	**I am not sure**
Incognito mode / private browsing mode in browsers prevents websites from collecting information about you.			
Tor can be used to hide the source of a network request from the destination.			
A VPN is the same as a Proxy server.			
IP addresses can always uniquely identify your computer.			
HTTPS is standard HTTP with SSL to preserve the confidentiality of network traffic.			
A request coming from a proxy server cannot be tracked to the original source.			

1.4 Participant privacy attitude (before watching video)

Risk Perception

1. Please rate your level of concern for each of the following online threats.

	Not at all concerned	**Slightly concerned**	**Moderately concerned**	**Very concerned**	**Extremely concerned**
Having your personal email account password being compromised.	o	o	o	o	o
Having your social media account password being compromised.	o	o	o	o	o
Having your banking account password being compromised.	o	o	o	o	o
An attacker getting a hold of one of your passwords and using it to log into multiple other accounts.	o	o	o	o	o
Having your work email account password being compromised.	o	o	o	o	o
Please select "Slightly Concerned" for this statement.	o	o	o	o	o

2. **Perceived data value**
   For the following types of accounts, rate the sensitivity of the data for each account. If you do not use one or more of the listed accounts, select "Does not apply" for that account.

	Not sensitive at all	**Mildly sensitive**	**Moderately sensitive**	**Fairly sensitive**	**Extremely sensitive**	**Does not apply**
Online bank account	o	o	o	o	o	o
Personal Email account	o	o	o	o	o	o
Social media account	o	o	o	o	o	o
Work Email account	o	o	o	o	o	o
Online shopping/e-commerce account	o	o	o	o	o	o

1.5 Video modules

At this stage of the study, you are being asked to watch a set of {*NUMBER OF VIDEOS*} videos which is expected to take approximately a total of {*NUMBER OF MINUTES*} minutes and {*NUMBER OF SECONDS*} seconds.

A completion code is embedded in one of the videos. Please write down the code when you see it in the video. After you finish watching all the videos, you will need to enter the completion code embedded in the video to proceed to the next page of this survey and complete the rest of this survey.

You will be asked a mix of true/false, multiple choice, and short-answer questions based on the contents of the videos.

Please **click here** to access the video playlist for this study, or copy the link below and paste it in a new tab. For your convenience, a message containing the link will also be available at the beginning of future sections of this survey. {*link here*}

o I have watched all the videos in the playlist.

Please enter the completion code to continue:

_____

If answered incorrectly, participants were shown the following message:
The completion code that you have entered is incorrect. The code can be found within the videos. Please review the videos to find the correct completion code and try again.

1.6 Manipulation check

Manipulation check, participant cannot continue until answering the following two questions correctly. Correct answers are denoted in bold.

If you would like to refer to the videos again, please **click here** or copy the link below and paste it in a new tab.
{*link here*}

Please answer the following questions. You will need to answer both questions correctly before moving on to the next section of the survey.

1. What does the term "passkeys" refer to in the watched videos?

   - o Passwords created for online accounts
   - o **Automatically generated keys by the FIDO authentication protocol**
   - o PIN created for the USB security key
   - o All of the above
   - o None of the above
   - o I am not sure

   If answered incorrectly, participants were shown the following message:
   This response is incorrect. Please try again before moving on to the next section

2. How can you log into or recover an account if a USB security key is lost or damaged? Select all that apply.

   - o **Having a backup USB security key**
   - o Resetting the PIN of the USB security key
   - o **Having a one-time use code generated a priori**
   - o You cannot recover the account
   - o I am not sure

   If answered incorrectly, participants were shown the following message:
   This response is incorrect. Either one or more of the correct responses have not been selected, or one or more incorrect responses have been selected. Please try again before moving on to the next section.

1.7 Confidence regarding FIDO technology

If you would like to refer to the videos again, please **click here** or copy the link below and paste it in a new tab.
{*link here*}

1. Please answer the following questions using a scale of 0 to 10. **0: Not at all confident; 10: Extremely confident. [Slider options]**

   - How confident are you in your ability to setup FIDO authentication for your online account if asked?
   - How confident are you in your ability to use FIDO authentication technology once setup?
   - How confident are you in your understanding about the FIDO authentication technology?
   - How confident are you in your understanding of the security protocol that supports the FIDO authentication technology?

2. How likely are you to adopt FIDO authentication technology if it becomes available?

    1. Extremely unlikely
    2. Fairly unlikely
    3. Likely
    4. Somewhat likely
    5. Extremely likely

1.8 Security calculus

If you would like to refer to the videos again, please **click here** or copy the link below and paste it in a new tab. {*link here*}

1. **Perceived response efficacy**
   Please rate how much you agree with each of the following statements.

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
I understand the security benefits of using FIDO authentication for my online accounts.	o	o	o	o	o
Using FIDO is *more* secure than using just a password.	o	o	o	o	o
Using FIDO is *more* secure than using 2FA/MFA.	o	o	o	o	o

2. **Perceived response cost**
   Please rate how much you agree with the following statements.

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
If I were to use FIDO authentication for my online accounts, it would be too much of a hassle to set it up.	o	o	o	o	o

3. **Perceived response cost**
   Using a USB security key to log in would be

    o Much easier compared to using passwords
    o About the same level of difficulty compared to using passwords
    o Slightly more difficult compared to using passwords
    o Much more difficult compared to using passwords
    o I am not sure

1.9 FIDO understandability

Note: the scoring noted in the tables below was not displayed to participants.

If you would like to refer to the videos again, please **click here** or copy the link below and paste it in a new tab. {*link here*}

A total of 10 participants from your group will be selected from the top scorers based on their answers to the following questions, and will receive an additional $2 compensation as a bonus payment. If there are more than 10 top scorers due to ties in a group, we will use a lottery to select the 10 participants from the top scorers who will receive the bonus payment. Please try your best to answer the questions correctly.

1. **General conceptions of FIDO**
   Please indicate which of the following you believe to be true/false

	True	**False**	**Not sure**
Using FIDO technology, you can login to your account without your USB security key. *Score: 1*			
FIDO authentication technology transmits sensitive login information when you attempt to log in to your account. *Score: 1*			
You can setup multiple USB security keys for the same account. *Score: 1*			
You can use the same USB security key to setup different passkeys for different accounts. *Score: 1*			
Someone can steal the saved passkeys from the USB security key. *Score: 1*			
The passkey saved on the USB security key is never transmitted outside the USB device. *Score: 1*			
Please select"True" as your answer for this statement. *Score: 0*			

2. **Understanding of contingencies** Please indicate which of the following you believe to be true/false

	True	**False**	**Not sure**
If the same USB security key is used for different accounts, the passkeys used for different accounts are the same. *Score: 1*			
If different USB security keys are setup for the same account, the passkeys generated for different USB security keys are the same. *Score: 1*			

3. **Response efficacy**
   Please indicate which of the following you believe to be true/false

	True	**False**	**Not sure**
The use of FIDO technology prevents attackers from logging into my account even if they have my USB security key and know my PIN for the USB security key. *Score: 1*			
The use of this technology prevents attackers from logging into my account if they have my USB security key but **do not** know my PIN for the USB security key. *Score: 1*			
Once successfully logged in, this technology encrypts all further communication between my device and the service provider to protect sensitive data being transmitted. *Score: 1*			
The use of this technology eliminates the threat of having login credentials stolen from the login server for passkey-enabled accounts. *Score: 1*			
A FIDO enabled account cannot be compromised by a phishing attack. *Score: 1*			

1.10 Adoption/non-adoption motivation

If you would like to refer to the videos again, please **click here** or copy the link below and paste it in a new tab.
{*link here*}

1. If you were asked to consider adopting FIDO authentication technology, which of the following accounts would you consider for adopting FIDO authentication? Please select all that apply.

   o Personal Email account
   o Official Email account
   o Online banking account
   o Social media account
   o Credit card account
   o Online shopping account
   o None of the above options apply

2. Please list any other account(s) for which you would consider adopting FIDO authentication. If listing multiple accounts, please separate each account type with a comma.

   _____

3. If you were asked to consider adopting FIDO authentication technology, on a scale of 0 to 10, how relevant each of the following reasons would be in your decision to adopt FIDO authentication technology? **0: Not at all relevant; 10: Highly relevant. [Slider options]**

   - The convenience of a passwordless experience
   - Eliminating the need to create different passwords for different accounts
   - Eliminating the risk of passwords being stolen
   - Improved security
   - Eliminating the need to remember passwords
   - Eliminating the need to write down passwords

4. Please list/explain below any other reasons that would be relevant in your decision to adopt FIDO authentication technology.

   _____

5. If you were asked to consider adopting FIDO authentication technology, on a scale of 0 to 10, how relevant each of the following reasons would be in your decision to **not** adopt FIDO authentication technology? **0: Not at all relevant; 10: Highly relevant. [Slider options]**

   - The monetary cost of the USB security key
   - The difficulty to remember the PIN for the USB security key
   - The fear of losing the USB security key
   - The inconvenience of learning the FIDO technology
   - The inconvenience of using FIDO technology
   - The lack of necessity in my opinion
   - I believe 2FA or multifactor authentication is more robust

6. Please list/explain below any other reasons that would be relevant in your decision to not adopt FIDO authentication technology.

   _____

1.11 Demographic questions

1. What is your age (in years)? Leave it blank you prefer not to answer.

   _____

2. What is your gender?

   o Female
   o Male
   o Prefer not to disclose
   o Prefer to self-describe _____

3. For what kind of online account(s) do you use/have you used two-factor authentication or multi-factor authentication (a.k.a. 2FA or MFA)? Please select all that apply.

   o Personal account
   o Office/business account
   o School/college account
   o None
   o Other (Please specify)

4. What is the highest level of education you have received?

   o Less than high school
   o High School graduate or GED
   o Some College
   o 2-year degree
   o 4-year degree
   o Master's degree
   o Doctoral degree
   o Professional degree

5. Which of these describes your personal income last year?

   o $0
   o $1 to $9,999
   o $10,000 to $24,999
   o $25,000 to 49,999
   o $50,000 to 74,999

- o $75,000 to 99,999
- o $100,000 to 149,999
- o $150,000 and greater
- o Prefer not to answer

6. Do you have any other comments or feedback about the study?

_____

2 Video Transcripts

2.1 Introduction: FIDO Authentication, USB security keys, and"passkeys"

Hello, today I'm going to be demonstrating and talking about FIDO authentication. FIDO authentication is a new form of authentication that aims to replace passwords to offer a more secure and simpler authentication mechanism.

To login using FIDO authentication, you can either use your own smartphone or you can use a special kind of USB security key that you can buy from Amazon or other vendors. In this video we use a USB security key such as the one shown in the picture here.

To set up FIDO authentication for an account, you will need to create a PIN for the USB security key the first time you use it. Once the PIN is created, you can begin using the USB security key for FIDO authentication. To do so, you will need to register the USB security key with the login server for your online account, for example an email account, where the system will auto generate passkeys that will be used to authenticate you once FIDO is setup.

In the next videos, I will demonstrate how you can set up passkeys for an account to enable FIDO authentication using a USB security key, and how you can log in once FIDO authentication is set up for an account. You can use the same USB security key to setup FIDO authentication for different online accounts. You can also use multiple USB security keys to set up multiple passkeys for the same account. Please proceed to the next video to learn more details.

2.2 Demonstration: setting up a USB security key and FIDO authentication

in this video, I'll be first demonstrating how you setup a USB security key, and then how you use the USB security key to setup FIDO authentication.

To demonstrate, I'll be setting up passkeys for FIDO authentication for a new Microsoft account that I've created for this demonstration. To create a passkey, I've navigated here to account.microsoft.com and I've signed into my account. From the management page, which is this page, I'll go to the Security tab on top. Now I'll click on "Advanced Security Options". And then I will click on "Add a new way to sign in or verify". I want to add an external security key, so I'll select the fourth option shown here. Now I will click next and follow the prompts on my laptop. So, I'll click to add an external security key and continue with the prompt. Now I will insert the USB security key into my laptop. This is the first time I am using this USB security key, so I'll have to complete the first time setup step.

This means that I have to set up a PIN for this USB security key. This same PIN will be used whenever I use this USB security key to setup passkeys for a new account, or login to an existing account using this USB security key.

So I'll create my PIN here. Now it will ask me to tap my USB security key to confirm that I'd like to use my USB security key for this request. And it will now ask me to name my USB security key so I know which one I am using on this account, so I'll name it "Blue Yubikey". This concludes the process of setting up FIDO authentication and creating passkeys for my account.

Thank you for watching. Please proceed to the next video.

2.3 Explanation: setting up a USB security key and FIDO authentication

So what's happening here? Let's say some user Jane wants to set up her USB security key for her Microsoft account. When she initiates that request, first she'll have to unlock her USB security key using the PIN. The USB security key needs to be unlocked using the PIN before you can register a USB security key with an account, or use it to login to a previously registered account. Creation of the PIN upon the first time use of a USB security key was demonstrated in the previous video.

To unlock her USB security key, Jane will plug her key into her laptop and be prompted to enter her PIN. If her pin is correct, she will have to touch the touch sensor on the USB security key. This is not a fingerprint sensor, this is just a touch sensor. This action is done as a final verification step to verify that Jane indeed wants to use this USB security key for some task.

So again, when Jane first requests to register her USB security key for her account, she'll be required to unlock her USB security key by entering the PIN. The rest of the process is automatic. Now, her laptop will reach out to Microsoft and say "hey, I would like to create a passkey for my account using this USB security key". Microsoft will then respond to Jane with some random message, let's say a picture of a cat for example. Now, Jane's USB security key will create two digital keys. These digital keys are the core of how we login using passkeys. This pair of keys consists of a secret passkey (the red key) and an unlocking passkey (the green key). The secret passkey can be used to lock a message as seen here. And the unlocking passkey can unlock a message locked by its corresponding secret passkey. The use of a different unlocking passkey to try and unlock the message will not work, it must be the same unlocking passkey that was

generated with the secret passkey.

So now, Jane's USB security key will use the secret passkey to lock the message of the cat in a box. Her laptop will then send this locked message, along with the unlocking green passkey to Microsoft. This green key can only be used to unlock the box to check whether the original message is inside the box or not. As only Jane's USB security key can put the original message in the box and lock it using the secret passkey, Microsoft can use the corresponding green passkey to verify that the locked message is indeed from Jane. This way Microsoft can use the unlocking passkey to verify that the message that was sent by Jane was indeed a locked version of the original message. If this check fails, then an error has occurred in the communication line and this registration process is discarded. If this verification is successful, Jane's USB security key will save the secret passkey for her Microsoft account, and Microsoft will save the unlocking passkey for Jane's account.

Thank you for watching. Please proceed to the next video.

2.4 Explanation: using the same USB security key for multiple accounts

It's important to note that a single USB security key can be used for multiple accounts.

Up until this point, we have a USB security key that has a single passkey stored on it. Jane can simply register the same USB security key with another account, and her USB security key will create a new passkey for the other account.

Passkeys are not shared across accounts or services, they are unique for each account.

Thank you for watching. Please proceed to the next video.

2.5 Demonstration: multiple USB security keys for one account

We can also add multiple USB security keys for a single account.

The process is nearly identical to when we registered our first USB security key. We'll start again from account.microsoft.com We'll navigate to the security tab, and then to "Advanced Security Options". And again, we'll add another way to sign in, select security key, and follow the prompts for our second USB security key. This is an older USB security key, so I've already set it up previously, so I will not need to create a new PIN, but rather I will use the PIN that I created the first time I used this USB security key. Finally, I will tap the USB security key as a final verification that I would like to use this USB security key. Now, my USB security key has been registered and I can name it.

Thank you for watching. Please proceed to the next video.

2.6 Demonstration: one-time use recovery codes

In addition to setting up multiple USB security keys for a single account, there are other account recovery options. Namely, you can use pre-generated one-time use passcodes to recover access to your account.

To generate this code, from account.microsoft.com, you can go to the security tab and click "Advanced security options". From here if you scroll all the way down, you can select this option to generate a recovery code. This code can be used in the case of an emergency to recover access to your account. This code is not to be used as your normal way to access your account, rather only to recover the account. The code should be stored in a secret location, such as a safe, so that it cannot be accessed by anybody other than you.

Thank you for watching. Please proceed to the next video.

2.7 Demonstration: logging in using FIDO

Now that we have passkeys added to our account, we can log in with any of the two USB security keys that we have registered. I've logged out. Now I can navigate to any Microsoft site, we've been using account.microsoft.com for this demonstration, so I'll continue to use that. I can enter my email, and now I can follow the prompt to authenticate using a USB security key. So, I'll insert the USB security key into my laptop. Type in my PIN that was set up for this USB security key, continue through the prompts, and then tap the USB security key to verify that I want to complete this request. And now, I've successfully logged into this account.

Thank you for watching. Please proceed to the next video.

2.8 Explanation: logging in using FIDO

Using Jane again as our example, when a user like Jane tries to log in, she'll first have to unlock her USB security key. Now the automatic login process takes place: The laptop reaches out to Microsoft attempting to login as user "Jane". Microsoft will retrieve the unlocking passkeys that were saved during the setup process for Jane, Microsoft will then send a message, for example an image of a flower, to Jane's laptop. Jane's USB security key will then retrieve the secret passkey associated with her Microsoft account, and use it to lock the image of the flower.

The laptop will now send this locked image to Microsoft. Microsoft will attempt to unlock the message with each of the unlocking passkeys stored during the setup process. If the first unlocking passkey on top is successful, then Microsoft knows that it must have been locked by Jane's black USB security key. If the second unlocking passkey on the bottom is successful, then Microsoft knows that the message must have been locked by Jane's blue USB security key. In either case, this tells Microsoft that the user trying to authenticate is using one of the enrolled USB security keys, so it must be Jane. So, if either of these is successful, then Jane will be successfully logged into her account.

Thank you for watching. Please proceed to the next video.

2.9 Explanation: Benefits of using FIDO authentication

Let's discuss some of the benefits of adopting FIDO authentication technology.

To begin with, this eliminates the need to remember and manage many passwords for your accounts. The USB security key stores the corresponding secret passkey for each account you create, securely, on the device.

Secondly, this eliminates the ability of an attacker to steal your password. We're no longer sending passwords to log in, instead we're using our secret passkeys stored on our USB security key to generate new messages every time we want to authenticate. The secret passkey is securely stored in the USB security key and never leaves the USB security key.

To reiterate, the benefits of using passkeys is that you no longer need to remember your password, and nobody can impersonate you without your USB security key and PIN.

Thank you for watching, please proceed to the next video.

2.10 End of video modules

This marks the end of the video modules. Thank you for watching the videos. We hope you enjoyed learning about FIDO authentication. At this time, you may copy the completion code displayed on the screen into the Qualtrics survey and proceed to the remainder of the study. You may come back to this playlist at any point in the study to review any of the videos as you please.

References

[1] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "my data just goes everywhere:" user mental models of the internet and implications for privacy and security," in *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*. Ottawa, 2015, pp. 39–52.