

“It’s Stored, Hopefully, on an Encrypted Server”:

## Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur

August 11, 2021 | 30<sup>th</sup> USENIX Security Symposium



## Tired of passwords?

If you use your fingerprint, face, or PIN to sign in to your phone or tablet, you can use it to sign in to eBay.

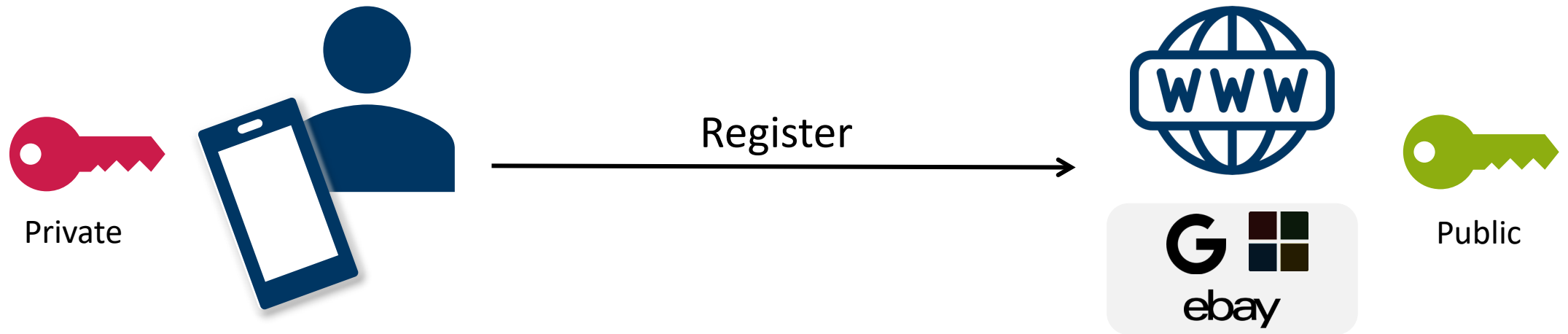
Turn on

Maybe later

# WebAuthn



# Registration | FIDO2 Protocol



# Authentication | FIDO2 Protocol



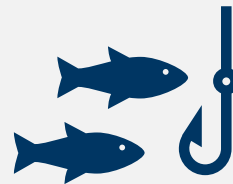
# Advantages | WebAuthn



Fast



Nothing to remember



Phishing resistant



# Notification



## Tired of passwords?

If you use your fingerprint, face, or PIN to sign in to your phone or tablet, you can use it to sign in to eBay.

Turn on

Maybe later



## STUDY 1

### Identify Misconceptions



Task / Survey



42 Participants



## STUDY 2

### Design Notifications



7 Focus Groups



29 Participants



## STUDY 3

### Compare Notifications



Experiment



345 Participants





## STUDY 1

### Identify Misconceptions



Task / Survey



42 Participants



## STUDY 2

### Design Notifications



7 Focus Groups



29 Participants



## STUDY 3

### Compare Notifications



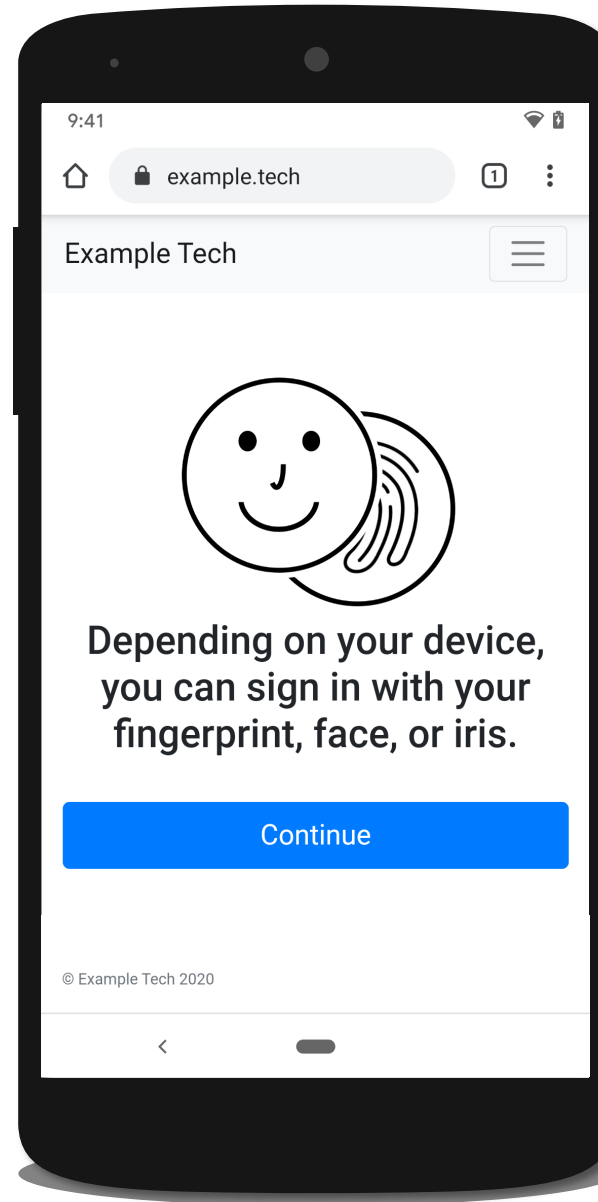
Experiment



345 Participants

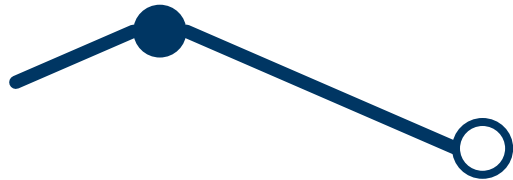
# Methodology | Study 1

## Notification

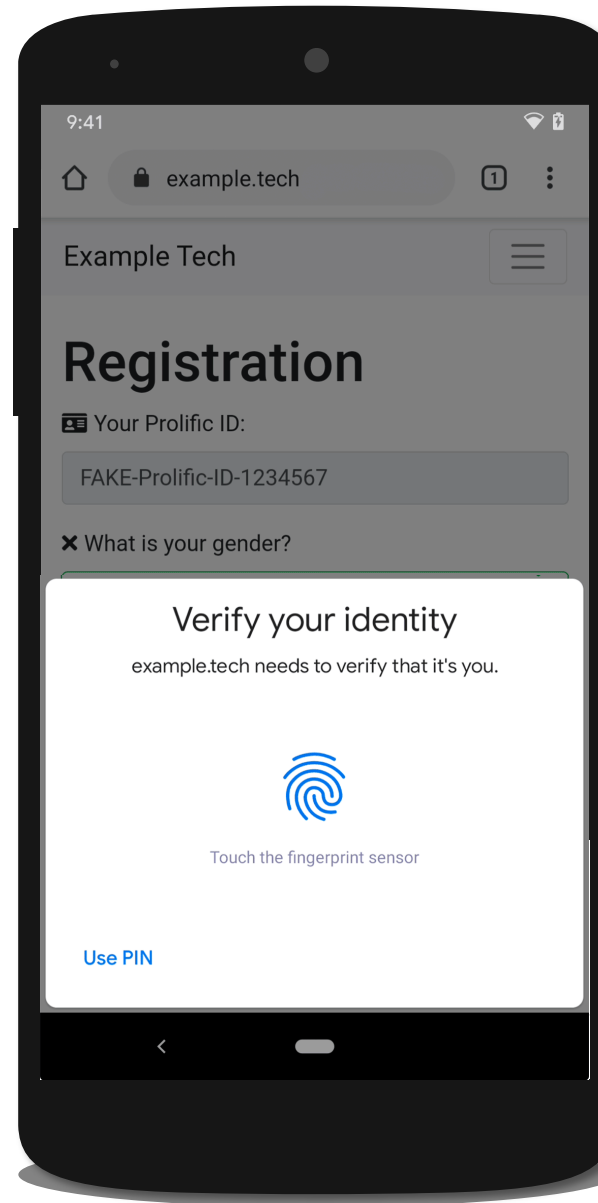


# Methodology | Study 1

Notification



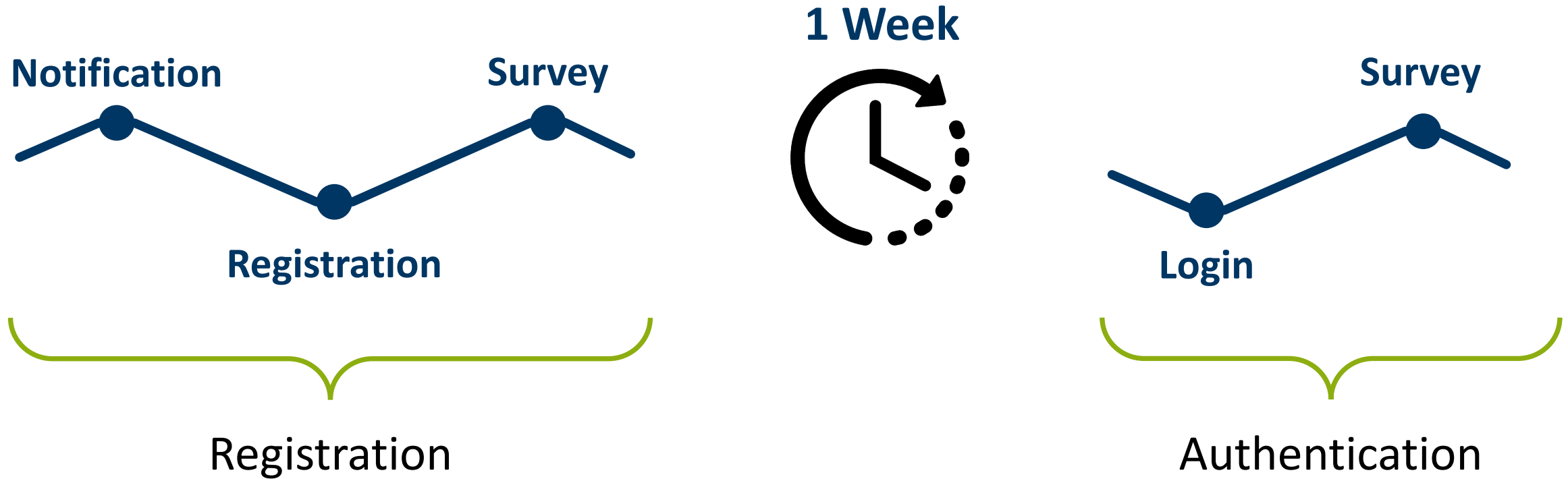
Registration



# Methodology | Study 1



# Methodology | Study 1



# Misconceptions | Study 1

**67%** think biometric sent to website



# Misconceptions | Study 1

67% think biometric sent to website

**43%** biometric not safe from attacker



# Misconceptions | Study 1



67% think biometric authentication is not safe to website

43% biometric authentication is not safe from attacker

**93%** unaware of fallback





## STUDY 1

### Identify Misconceptions



Task / Survey



42 Participants



## STUDY 2

### Design Notifications



7 Focus Groups



29 Participants



## STUDY 3

### Compare Notifications



Experiment



345 Participants

# Focus Groups | Study 2



© "Focus group on working principles" by Kennisland licensed under CC BY-SA 2.0

# Methodology | Study 2

Welcome



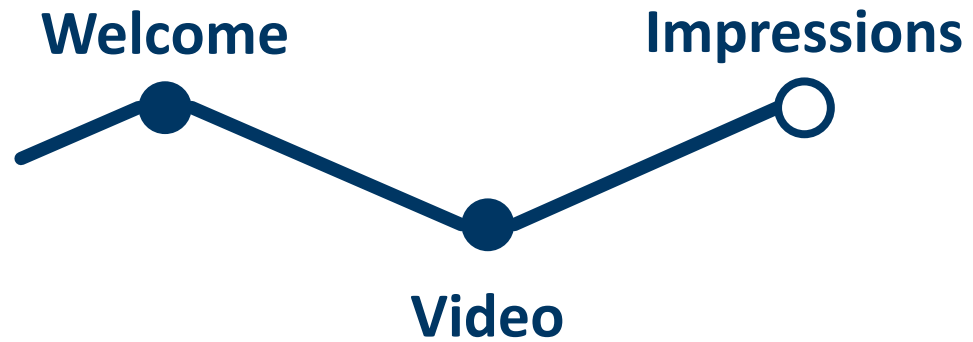
# Methodology | Study 2

Welcome

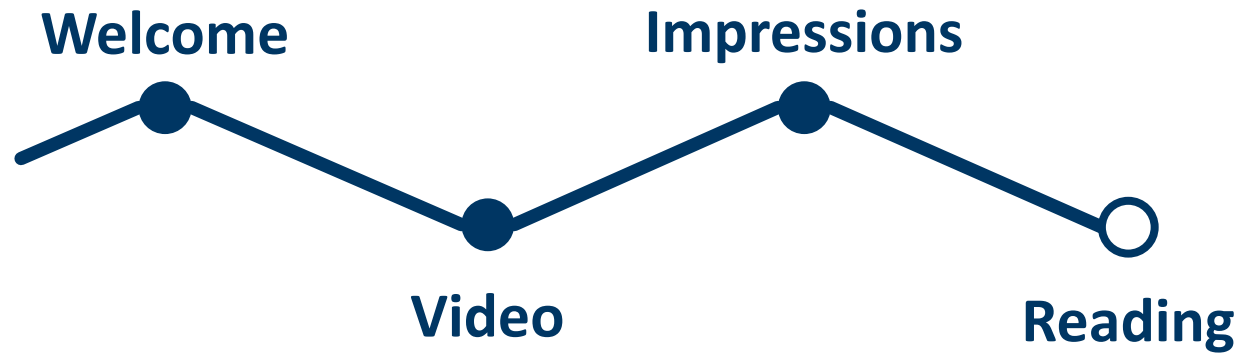
Video



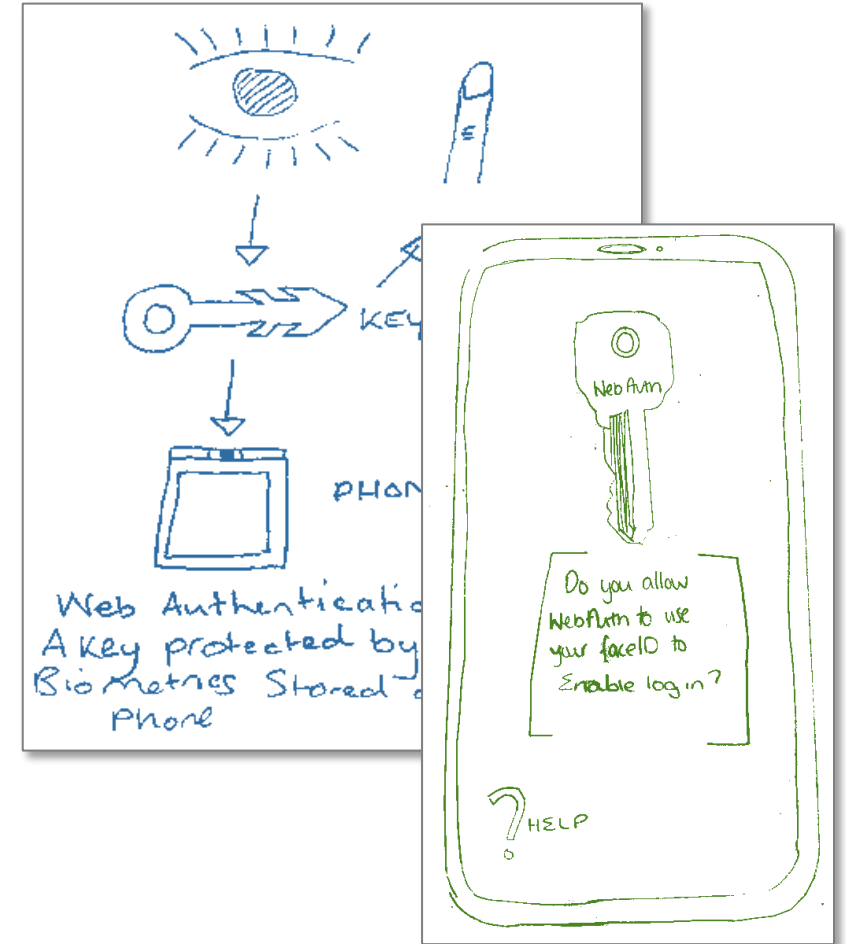
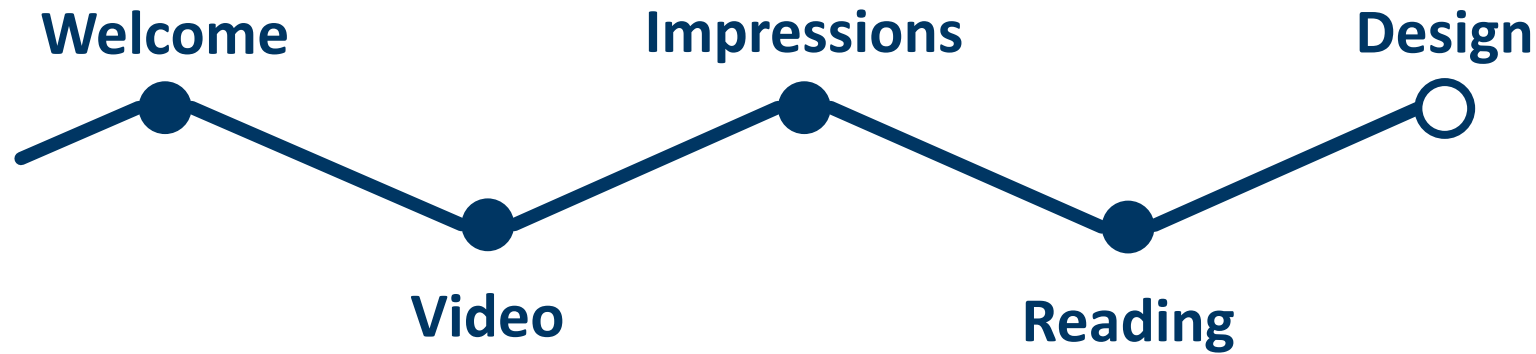
# Methodology | Study 2



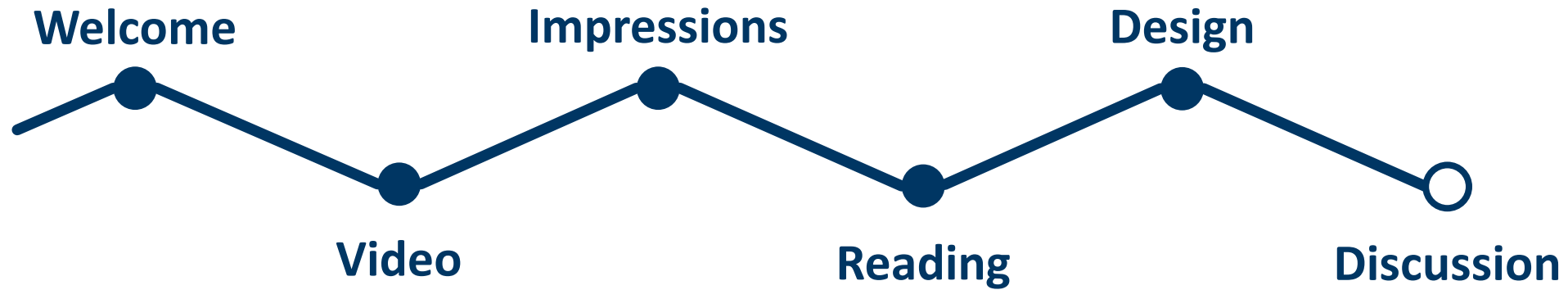
# Methodology | Study 2



# Methodology | Study 2



# Methodology | Study 2





# Results | Study 2



Convenience



Security

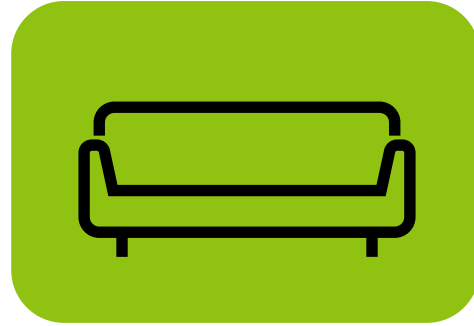


Passwords



Availability

# Results | Study 2



Convenience



Security



Passwords

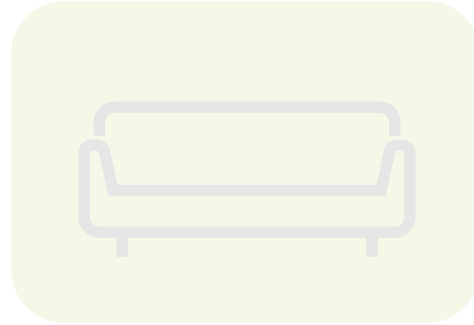


Availability

# Results | Study 2

”

No one except  
you has access



Convenience



Security

”

Never leaves  
your phone

”

Only stored on  
your device

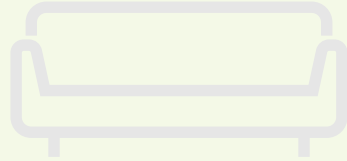


Passwords



Availability

# Results | Study 2



Convenience



Security

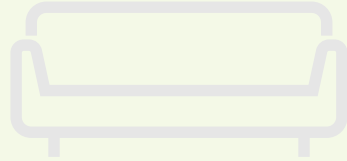


Passwords



Availability

# Results | Study 2



Convenience



Security



Passwords



Availability



## STUDY 1

### Identify Misconceptions



Task / Survey



42 Participants



## STUDY 2

### Design Notifications



7 Focus Groups



29 Participants



## STUDY 3

### Compare Notifications

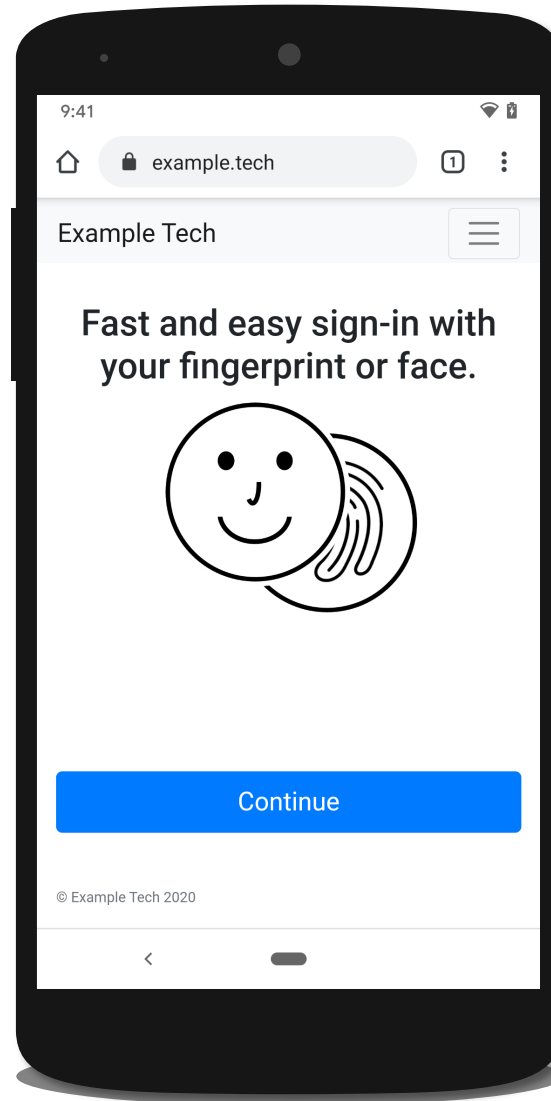


Experiment



345 Participants

# Notifications | Study 3



# Notifications | Study 3

Fast and easy sign-in with  
your fingerprint or face.



Your fingerprint or face is  
only stored on  
your personal device.

Continue

Fast and easy sign-in with  
your fingerprint or face.



Your fingerprint or face is  
never shared with  
Example Tech or third parties.

Continue

Fast and easy sign-in with  
your fingerprint or face.



Your fingerprint or face  
never leaves your  
personal device.

Continue

Fast and easy sign-in with  
your fingerprint or face.



Unlike passwords  
it can't be hacked.

Continue

Fast and easy sign-in with  
your fingerprint or face.



Backed by Microsoft,  
Google, and Apple.

Continue



## Stored



## Shared



## Leaves



## Hacked

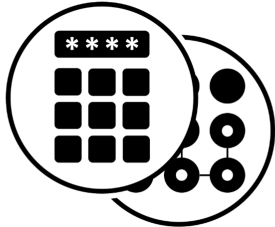


## Brands



# Notifications | Study 3


Fast and easy sign-in with your device's PIN, pattern, or password.



Continue




## Registration

 Your Prolific ID:

FAKE-Prolific-ID-1234567

✕ What is your gender?

Please select...

 How old are you?

Enter password

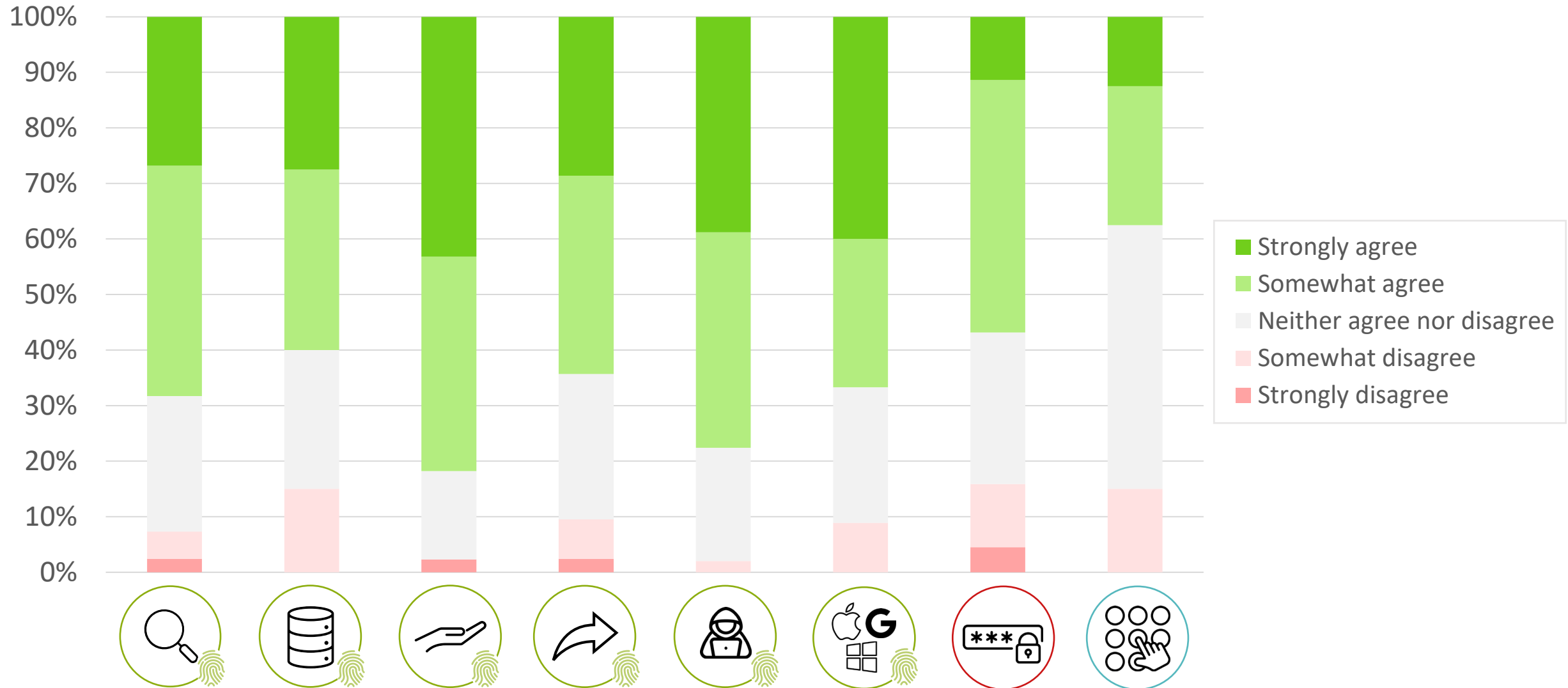
Confirm password

Must be at least 8 characters long.

Register

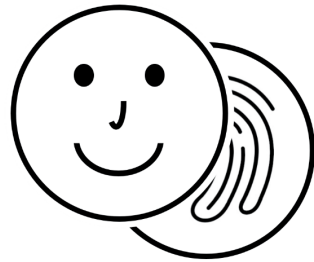


# Perception of Security | Study 3



# Notifications | Study 3

Fast and easy sign-in with  
your fingerprint or face.



Your fingerprint or face is  
only stored on  
your personal device.

Continue

Fast and easy sign-in with  
your fingerprint or face.



Your fingerprint or face  
never leaves your  
personal device.

Continue

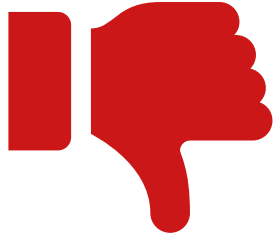


**Stored**



**Leaves**

# Misconceptions | Study 3

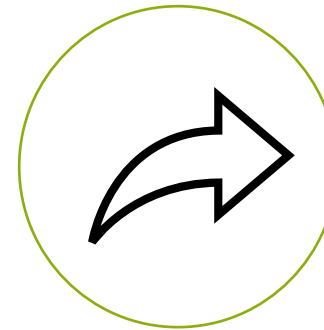


**66%** in ***Control*** think biometrics sent to website



***Stored***

**45%**



***Leaves***

**50%**

# Takeaways

## Perceptions



Misconceptions about where biometrics are stored



Biometric WebAuthn perceived very positively

## Notifications



*Stored* and *Leaves* notifications most effective



Emphasize speed and ease, not comparison to passwords

# “It’s Stored, Hopefully, on an Encrypted Server”: Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

Leona Lassak

leona.lassak@rub.de



Annika Hildebrandt

ahildebrandt@uchicago.edu



Maximilian Golla

maximilian.golla@rub.de



Blase Ur

blase@uchicago.edu



## Takeaways



Biometric WebAuthn  
perceived positively



*Stored and Leaves*  
notifications effective



Emphasize speed / ease



Extended  
Version

