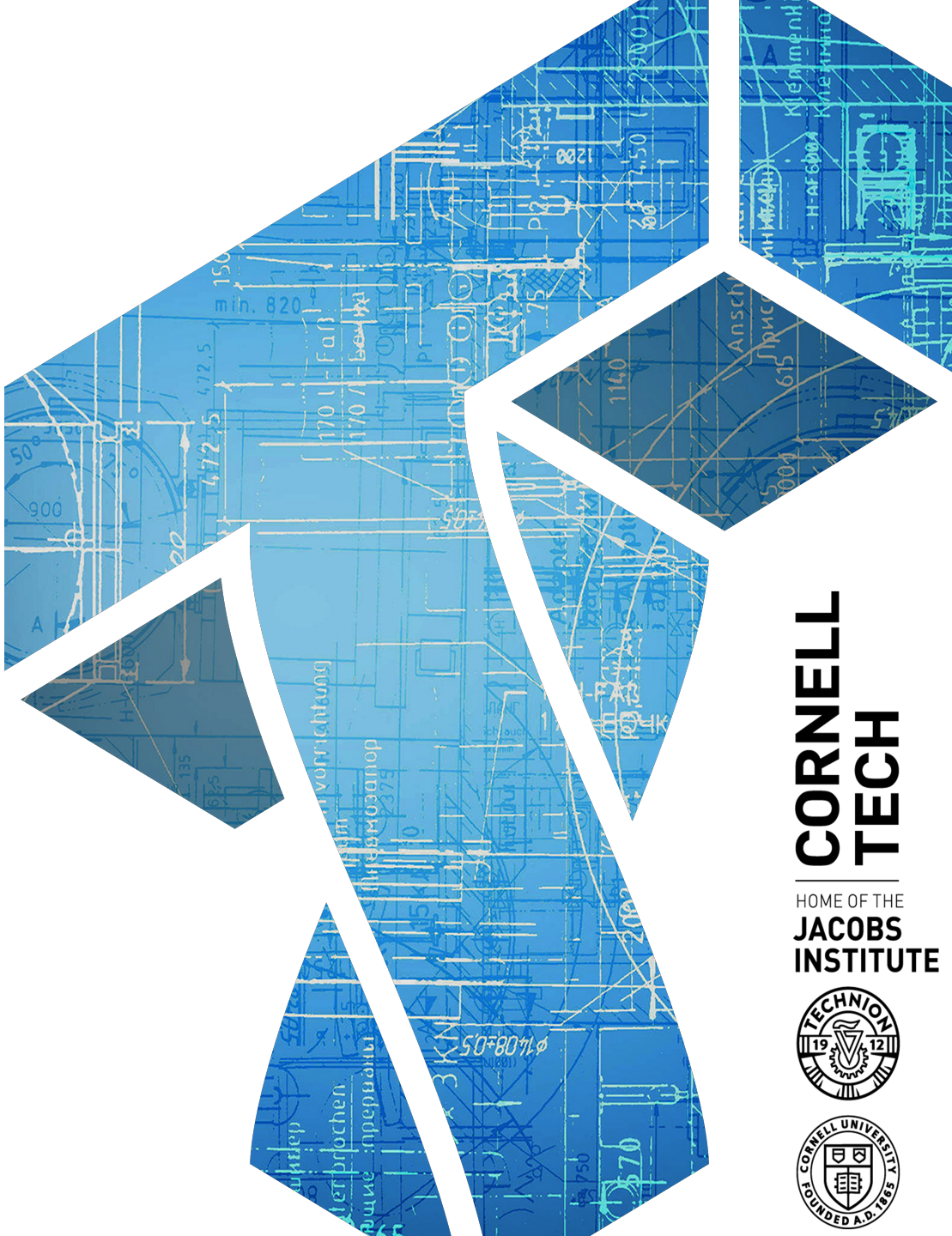
CS 5439:
Account security

Tom Ristenpart



CORNELL TECH
HOME OF THE
JACOBS
INSTITUTE

Today’s topic

Modern online account protections

Vectors for compromise - “Standard” and IPV threats

Discuss improvements to counseling and technology

Authentication systems

Goal: identify that system user is who they say they are

Some types of authentication mechanisms

- What you know (e.g., passwords)
- What devices you have (e.g., dongles, phone)
- What data you have (e.g., cookies)
- What features you have (e.g., biometrics)
- Where you are
- …

Evolution of computer authentication systems

Historically: password is only authentication check

Increasingly: password is one of many authentication checks

- “Hard” checks (must know password, must have matching fingerprint)
- “Soft” checks (same device being used, IP address of user, UA string of browser, etc.)

Machine learning viewpoint:
Use all the above as features to predict if it is correct user or not

Good summary:
http://www.jbonneau.com/doc/BHOS15-CACM-imperfect_authentication.pdf

Authentication systems

Three main phases:

(1) Account registration

(2) Login

(3) Account recovery

Account registration

Username: tom
Email: tom@tom.com
Password: password1

Login server

Initial registration of an account:

- Choose username
- Choose password
- (Almost always) give email address
- (Sometimes) choose security questions
- (Sometimes) set two-factor phone number

Sign Up

It's free and always will be.

First name | Last name

Mobile number or email

New password

Birthday

Sep | 8 | 1993 Why do I need to provide my birthday?

Female Male

By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

Sign Up

Google

Create your Google Account

to continue to Gmail

First name | Last name

Username @gmail.com

You can use letters, numbers & periods

Password | Confirm password

Use 8 or more characters with a mix of letters, numbers & symbols

Sign in instead

Next

Account registration – standard threats

Username: tom
Email: tom@tom.com
Password: password1

Login server

Threat	Description	Defense?
Bot accounts	Automated scripts to setup accounts	IP-based rate limiting; proof of ownership checks; CAPTCHAs; other heuristics

Account registration – IPV threats

Username: tom
Email: tom@tom.com
Password: password1

Login server

Threat	Description	Defense?
Abuser sets up account	Abuser sets up account for victim	Setup separate account when safe to do so
Abuser & victim use shared password	Victim sets up account but uses shared password	Need to pick different passwords when safe to do so

"They'll hack into their phones and they'll hack into their accounts. Especially with intimate partner victimization . . . oftentimes these people share and know what is very personal information . . . because that was not something that they necessarily kept private when the relationship was a trusting, loving, good one." - Case manager

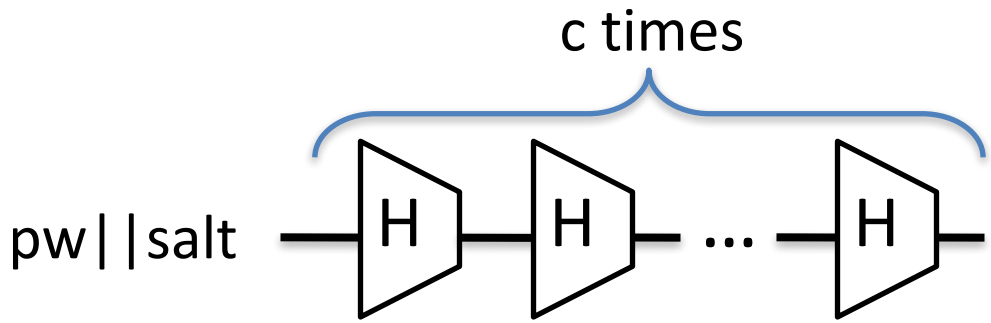
Digression: Password database compromise

Username: tom
Email: tom@tom.com
Password: password1

Login server

tom	$salt_1$, H^c(password1,$salt_1$)
alice	$salt_2$, H^c(123456,$salt_2$)
bob	$salt_3$, H^c(p@ssword!,$salt_3$)

Password hashing:



Cryptographic hash function H
(H = SHA-256, SHA-512, etc.)

Common choice is c = 10,000

More modern: scrypt, argon2

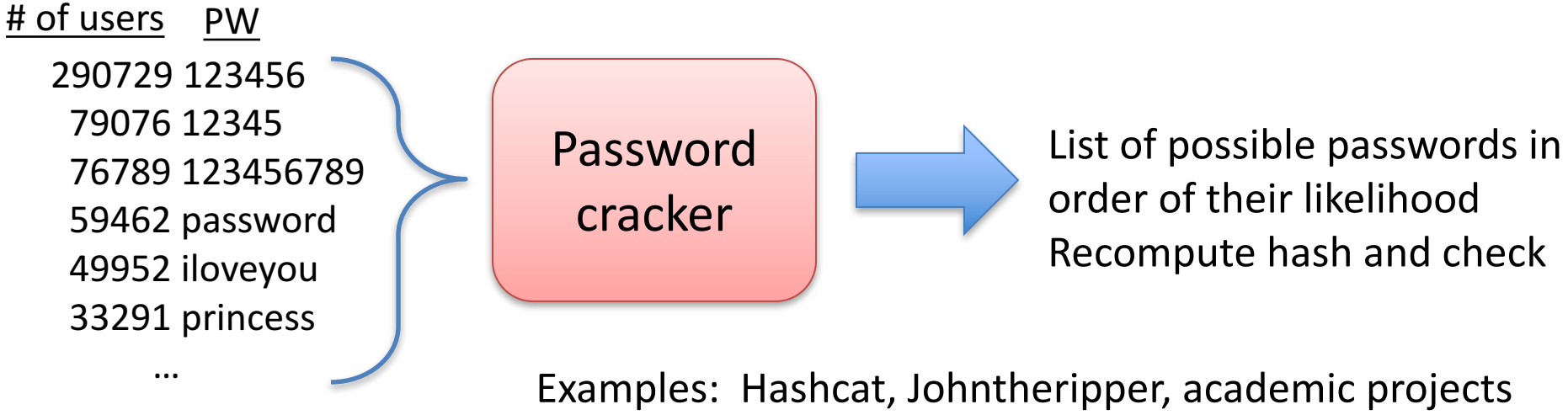
The idea is to slow down computation of the hash

Digression: Password database compromise

AshleyMadison breach: 36 million user hashes

Salts + Passwords hashed using bcrypt with c = 2^{12} = 4096

4,007 cracked directly with trivial approach



Examples: Hashcat, Johntheripper, academic projects

Digression: Password database compromise

AshleyMadison breach: 36 million user hashes

Salts + Passwords hashed using bcrypt with c = 2^{12} = 4096

4,007 cracked directly with trivial approach

CynoSure analysis: **11 million** hashes cracked

>630,000 people used usernames as passwords

MD5 hashes left lying around accidentally

http://cynosureprime.blogspot.com/2015/09/csp-our-take-on-cracked-am-passwords.html

Digression: Password database compromise

	year	# stolen	% recovered	format
⋮				
rockyou	2012	32.6 million	100%	plaintext (!)
LinkedIn	2012	117 million	90%	Unsalted SHA-1
Adobe®	2013	36 million	??	ECB encryption
YAHOO!®	2014	~500 million	??	bcrypt + ??
ASHLEY MADISON® Life is short. Have an affair.®	2015	36 million	33%	Salted bcrypt + MD5
⋮				

Digression: Password database compromise

Discussion:
How important is password database compromise as threat to IPV victims?

Account login

Username: tom
Password: password1

Login server

- Send username and password (over HTTPS)
- Password checked (hash with salt and compare to stored hash value)
- Apply ***heuristic checks*** that might indicate this is an attacker (with correct password)
  - Suspicious IP address?
  - Suspicious geographic location?
  - Suspicious browser user agent?
  - Password is in a breach?
- Generate second-factor challenge

Once passed, set an ***authentication cookie*** on device

Session cookies

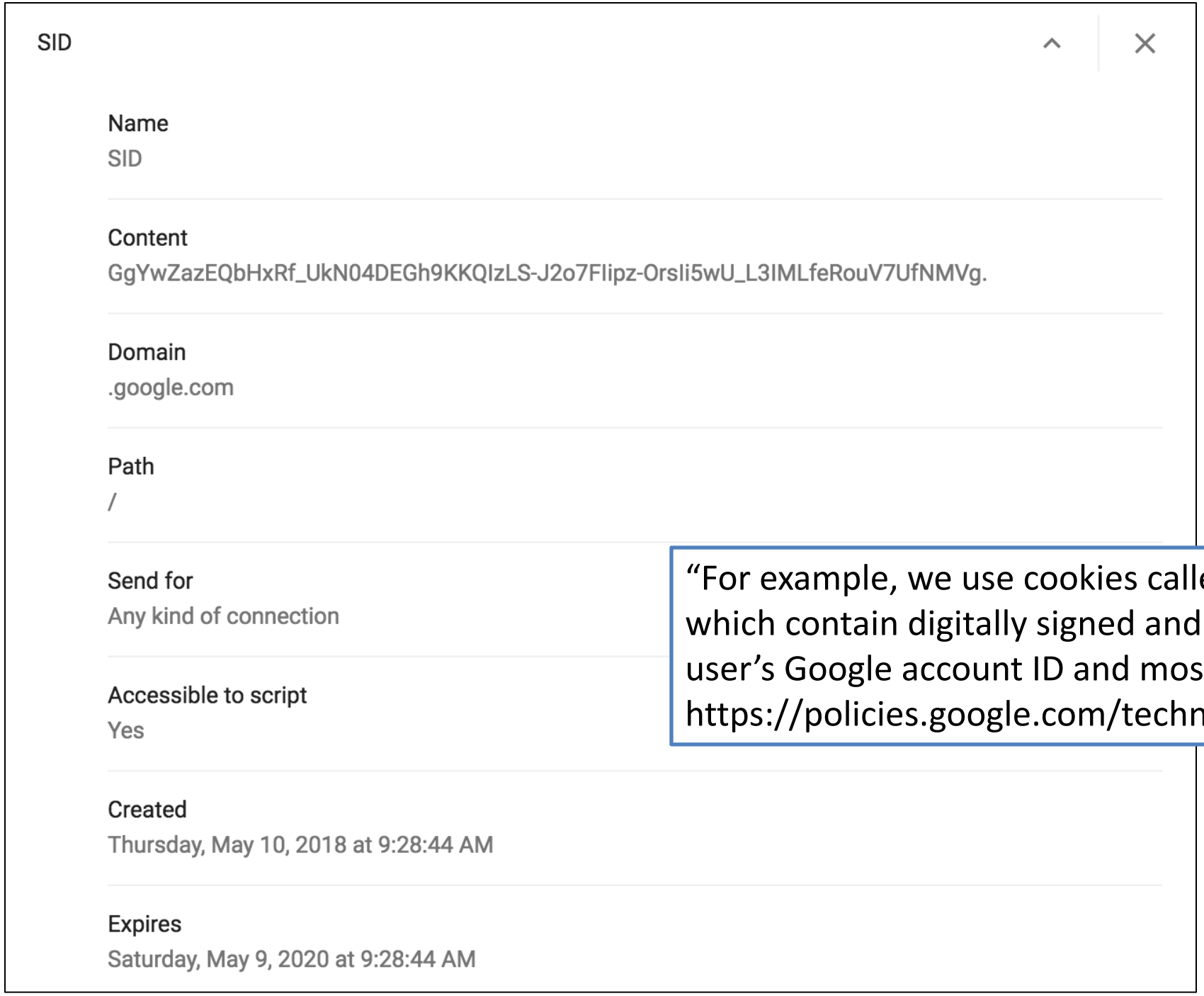
GET /login.html?username=tom&password=blah

HTTP/1.1 200 OK
Content-type: text/html
Set-cookie: loginToken=ab35h013490...

GET /info.html HTTP/1.1
Cookie: loginToken=ab35h013490…

Cookies used to have server set client state that is sent later on

Session cookies remain valid for long periods of time. Why?



"For example, we use cookies called 'SID' and 'HSID' which contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time."
https://policies.google.com/technologies/types?hl=en

Account login – standard threats

Username: tom
Password: password1

Login server

Threat	Description	Defense?
“Horizontal” online guessing attacks	Try a handful of popular passwords across many accounts	Strong passwords; track & block IP addresses; heuristic checks
“Vertical” online guessing attacks	Try popular passwords against a single account	Strong passwords; track & block IP addresses; heuristc checks; lock account after # of failed attempts
Credential stuffing	Use password exposed in breach against targeted account	Heuristic checks; breach detection checks
Phishing	Trick victim into disclosing password, e.g., via email	Heuristic checks; 2FA

Account login – IPV threats

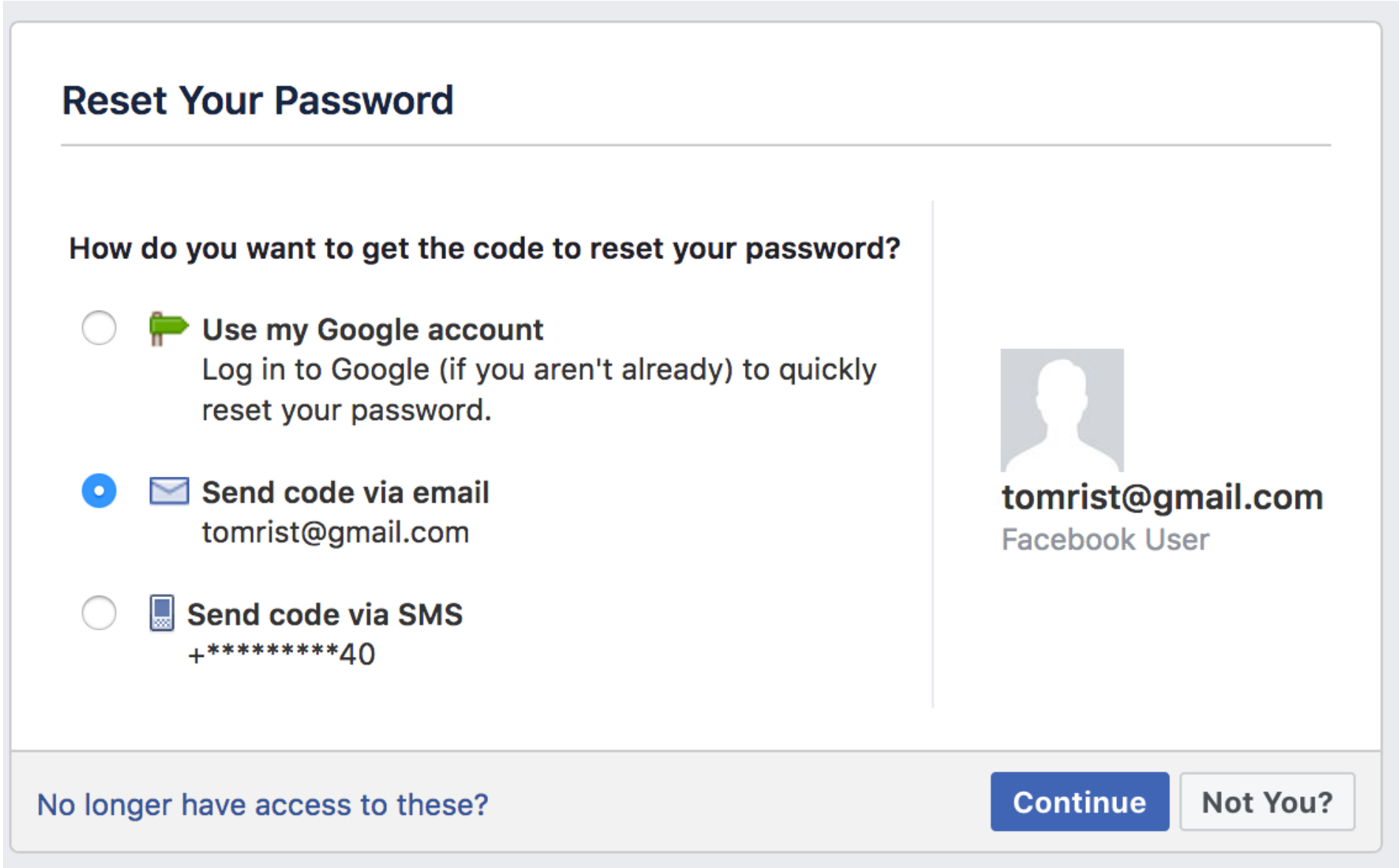
Threat	Description	Defense?
Abuser knows password (different location)	Abuser knows password and logs in from different location	Two-factor authentication; heuristic checks
Abuser knows password (same location)	Abuser knows password and logs in from same household or even device	Change password; use two-factor authentication
Abuser compels password disclosure	Abuser forces password disclosure (emotional or physical coercion)	Decoy passwords?
Abuser uses device to gain access	Session cookies allow abuser to login from device without auth checks	Delete session cookies

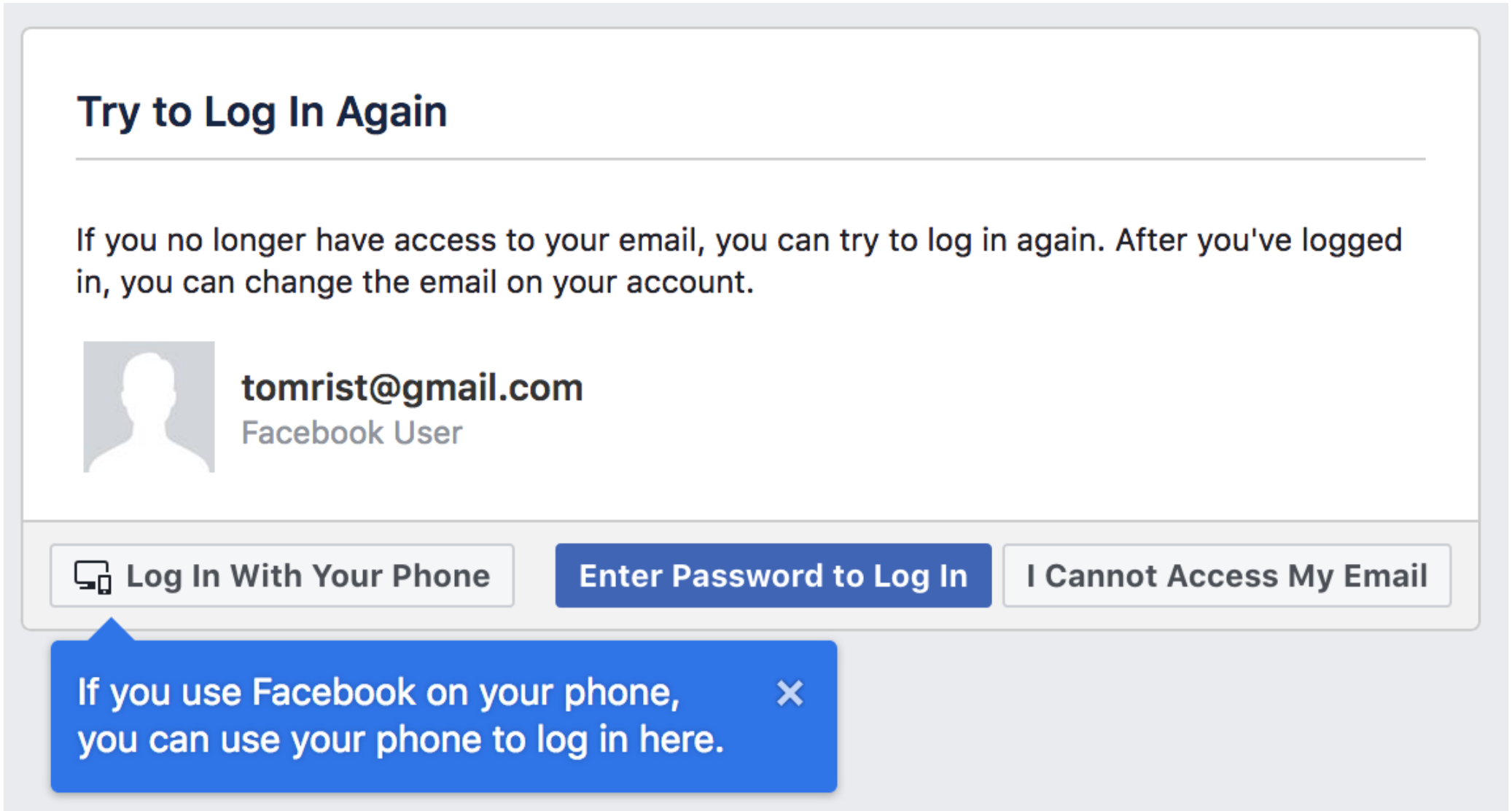
"[The abuser] stole her computer and was able to access all this information . . . her school applications, her bank accounts, all sorts of things, and gain access and control of these things. That . . . had a totally traumatizing effect."
- Case manager

Account recovery

Users often forget their passwords & login cookies will (eventually) expire

Account was compromised and victim wants to regain control


Reset Your Password
How do you want to get the code to reset your password?
Use my Google account
Log in to Google (if you aren't already) to quickly reset your password.
Send code via email
tomrist@gmail.com
Send code via SMS
+**********40
tomrist@gmail.com
Facebook User
No longer have access to these?
Continue
Not You?

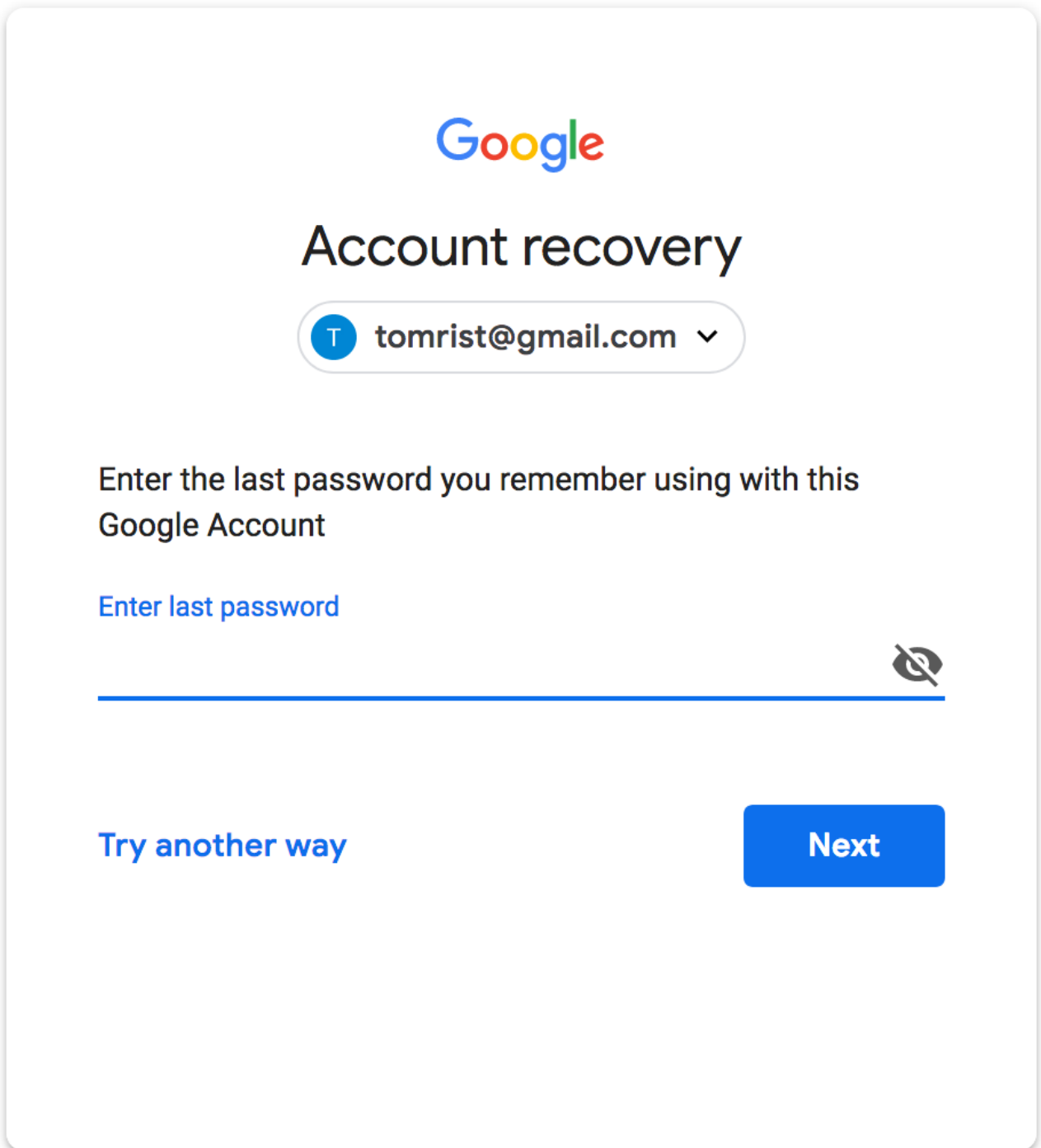

Try to Log In Again
If you no longer have access to your email, you can try to log in again. After you've logged in, you can change the email on your account.
tomrist@gmail.com
Facebook User
Log In With Your Phone
Enter Password to Log In
I Cannot Access My Email
If you use Facebook on your phone, you can use your phone to log in here.

No Email Access

We're sorry you're having trouble recovering your email address. Unfortunately, this means we can't verify who you are or give you access to the Facebook account you're trying to log into. We may hide the information on your Facebook account if we detect that you cannot regain access to it.

Learn more about how to access your Facebook account

Done


Google
Account recovery
T
tomrist@gmail.com
Enter the last password you remember using with this Google Account
Enter last password
Try another way
Next

Google Verification Code

Dear Google User,

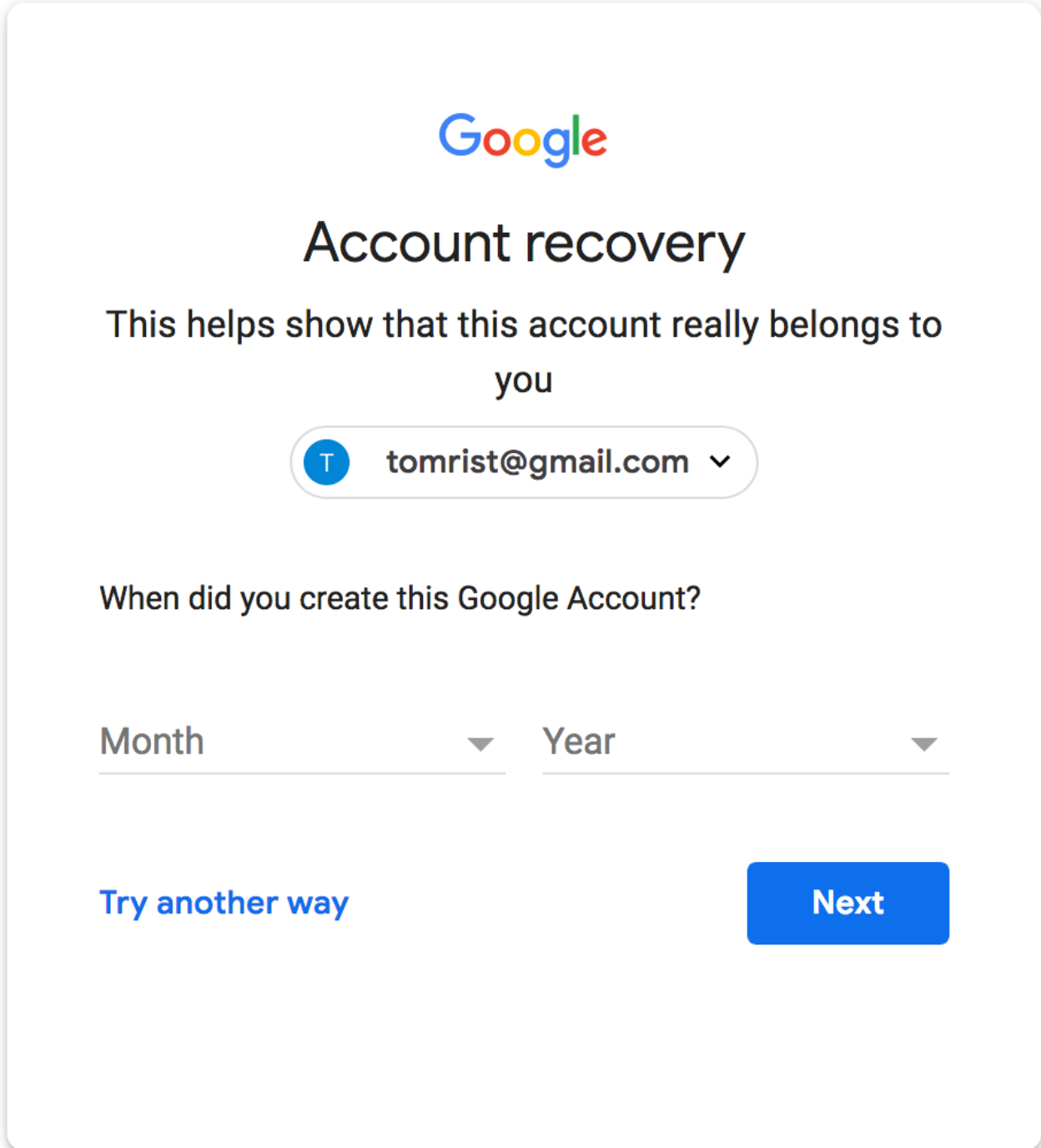
We received a request to access your Google Account through your email address. Your Google verification code is:

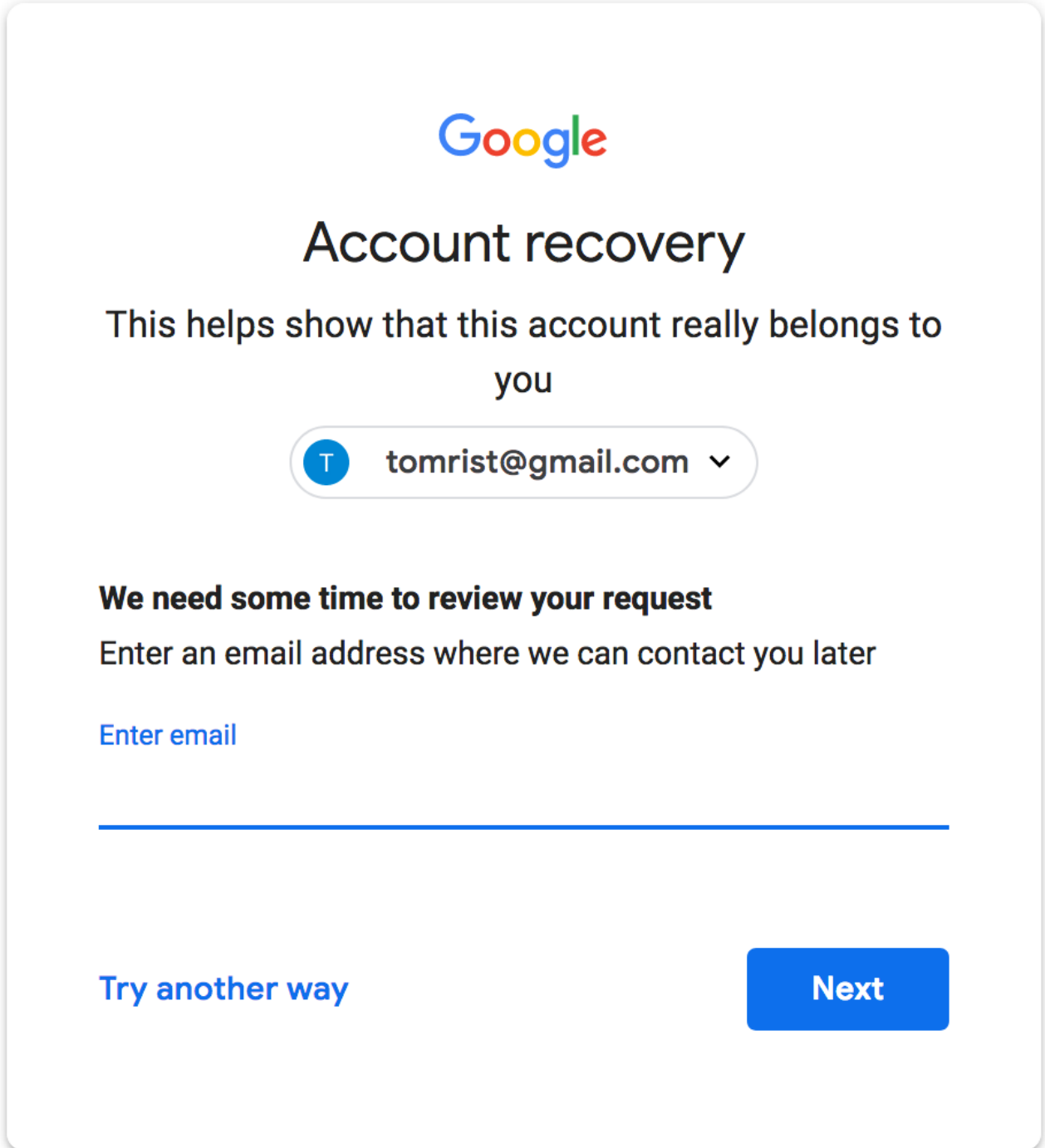
884159

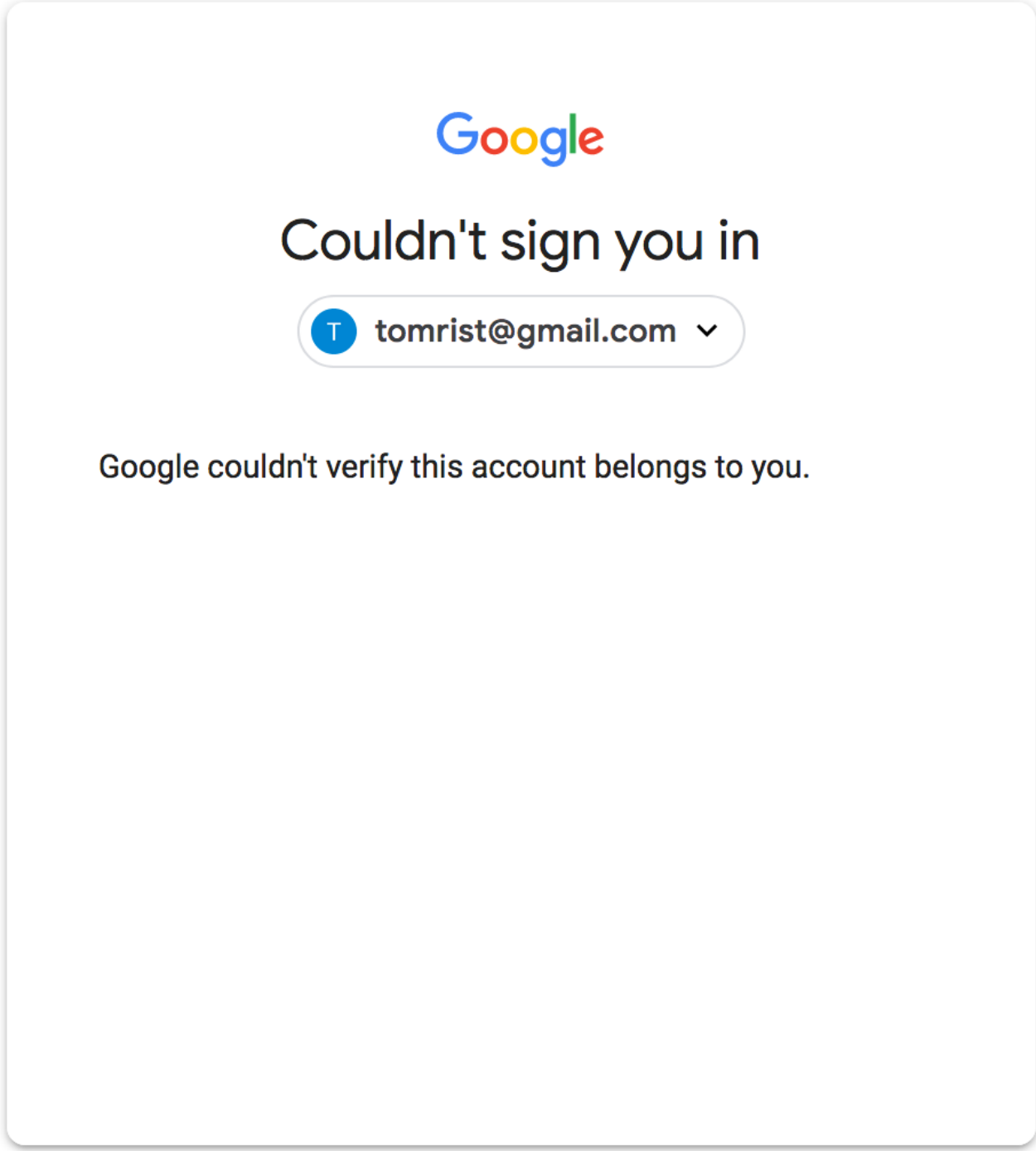
If you did not request this code, it is possible that someone else is trying to access the Google Account . **Do not forward or give this code to anyone.**

Sincerely yours,

The Google Accounts team


Google
Account recovery
This helps show that this account really belongs to you
T
tomrist@gmail.com
When did you create this Google Account?
Month
Year
Try another way
Next


Google
Account recovery
This helps show that this account really belongs to you
T
tomrist@gmail.com
We need some time to review your request
Enter an email address where we can contact you later
Enter email
Try another way
Next


Google
Couldn't sign you in
T
tomrist@gmail.com
Google couldn't verify this account belongs to you.

Account recovery

Users often forget their passwords & login cookies will (eventually) expire

Account was compromised and victim wants to regain control

- Bootstrap authentication off another account
- Use second factor to authenticate
  - Email, phone, second factor app
- Facebook: setup trusted friends
- Answer security questions
- Answer personal questions

Big services (target) using only automated systems

http://gmailaccountrecovery.blogspot.com/

Account recovery – standard threats

Users often forget their passwords & login cookies will (eventually) expire

Account was compromised and victim wants to regain control

Threat	Description	Defense?
Attacker guesses answers to recovery questions	Adversary gathers information about victim from public sources	Need more unpredictable recovery question answers; get rid of security questions
Use compromised 2FA route to gain access	Adversary compromised email or phone associated with account	Send notification to old email / phone; time delay on access via second factor

Paper measuring poor security and usability of security questions:
http://www.jbonneau.com/doc/BBCJW15-WWW-google_personal_knowledge_questions.pdf

Account recovery – IPV threats

Users often forget their passwords

Session cookies will expire: How to regain access to account?

Threat	Description	Defense?
Abuser knows answers to recovery questions	Personal questions likely to have known answers	???
Abuser has locked victim out of account	Frequent tactic is to takeover account and lock victim out by changing PW and email/phone	Changes should trigger notification sent to old email (with recovery secret)
Session cookies not invalidated	Resetting passwords may not invalidate session cookie on abuser device	Need to give option to invalidate old cookies

"The [abuser] hacked their Facebook, hacked their email, hacked the phone. So you know how Facebook will send you a text message, like a code to let you in. So trying to somehow report it and give her access so she can change everything again was hard, because the phone number that was listed was a number that he had in his possession. So it was impossible." - Case manager

Discussion

How do we advise victims about account compromise & recovery?

How do we improve account security workflows for IPV threat models?