

Authentication @ Google

CS 155: Computer and Network Security

Diana Smetters
Google
smetters@google.com

Who am I?

My job is to make sure you can get into your Google Account, and bad people can't.

Uber-Tech Lead for Sign-in,
part of Google's Identity team.

Responsible for all the policies,
systems and UIs that decide who
gets into your Google Account, and
who doesn't.

This means balancing security,
access, and *reliability*.

To be more concrete....

Google
Sign in
Use your Google Account

Email or phone

[Forgot email?](#)

Not your com
[Learn more](#)

[Create acco](#)

English (United States)

Google
Welcome

magicrisktwo@gmail.com

Enter your password

Show password

[Forgot password?](#)

[Next](#)

English (United States)

Help Privacy Terms

Google
Account recovery

This helps show that this account really belongs to you

magicriskone@gmail.com

Get a verification code

To get a verification code, first co you added to your account (*** ** apply

Phone number

I don't have my phone

Google
Verify it's you

This device isn't recognized. For Google wants to make sure it!

[Learn more](#)

magicrisktwo@gmail.c

Try another way to sign in

- Get a verification code at (***).... Standard rates apply
- Call your phone on file (***)....99
- Use your phone or tablet to get a security code (even if it's offline)
- Get help

English (United States)

Help Privacy Terms

Google
2-Step Verification

This extra step shows it's really you trying in

magicgoodone@gmail.com

Check your Google Pixel 4

Google sent a notification to your Google Pixel 4. on the notification to continue.

Or open the Gmail app on your Apple iPhone SE (generation) to sign in from there.

Don't ask again on this device

[Try another way](#)

Google
Hi Sam

smetters.test3@gmail.com

To continue, first verify it's you

Enter your password

Show password

[Forgot password?](#)

[Next](#)

English (United States)

Help Privacy Terms



Google's strongest security helps keep your private information safe.

The Advanced Protection Program safeguards users with high visibility and sensitive information, who are at risk of targeted online attacks. New protections are automatically added to defend against today's wide range of threats.

[Learn how to get started](#)

Overview

- Review: What is authentication?
- Why is it hard, particularly at Google?
- Threats and defenses
- How do we work (what's my day job/team like)
- Questions

Authentication (authn)

Whether users are who
they claim to be

Authorization (authz)

What users are and aren't
allowed to access

Why should I
care?

With the shift to the cloud,
security is increasingly about
authentication.

How Does Authentication Work?

Stanford University

Stanford | Login

SUNet ID

Password

Login

Important Security Information: Logging in lets you access other protected Stanford websites with this browser, not just the website you requested.

[LOGIN HELP](#)

[FORGOT YOUR PASSWORD?](#)

Use of this system is subject to Stanford University's rules and regulations. See the [Stanford Administrative Guide](#) for more information.

How Does Authentication Work?

Stanford University

Stanford | Login

SUNet ID

Password

Login

Important Security Information: Logging in lets you access other protected Stanford websites with this browser, not just the website you requested.

 **FORGOT YOUR PASSWORD?**

Use of this system is subject to Stanford University's rules and regulations. See the [Stanford Administrative Guide](#) for more information.

Verify Identity

Enter your personal information below.

Last name

REQUIRED

University ID [what?]

REQUIRED

Last four digits of Social Security Number [why?]

REQUIRED

(or Individual Taxpayer ID Number)

Birthdate (MM/DD/YYYY)

REQUIRED

Password Reset Question:

City, town, or village of birth ?

Password Reset Answer

REQUIRED

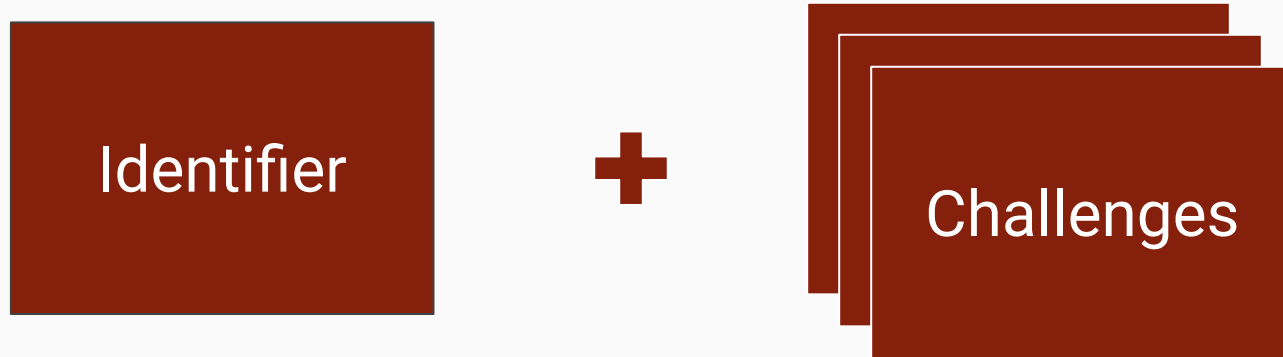
cancel

continue



If you have forgotten your password and are not able to provide the requested information, please submit a [help ticket](#) or call 650-725-4357.

How Does Authentication Work?



Quiz #1

- How many online accounts do you have?
- How many that really matter?
- Do you ever use the same password for multiple accounts?
- Do you ever use account recovery?
- To sign in?
- Have you turned on 2-factor authentication for any of your accounts?
- When you didn't have to?

Threats

- Credential breach
- Malware (keyloggers)
- (Offline) Phishing



SAVE



SHARE



TEXT



327

BUSINESS

‘We’ve Been Breached’: Inside the Equifax Hack

The crisis has sent shock waves through the industry, spooked consumers and sparked investigations



Equifax’s headquarters in Atlanta. Chief Executive Richard Smith has called the cyberattack the ‘most humbling moment in our 118-year history.’ PHOTO: RHONA WISE/EPA/SHUTTERSTOCK

By *AnnaMaria Andriotis*, *Michael Ranonort* and

Nylas

**Build
Features
Faster**

GET FREE API KEY

CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.

THEY WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!

THE FOOL!



HOW PEOPLE THINK HACKING WORKS

HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.

COOL, LET'S TRY THEM ALL ON VENMO.



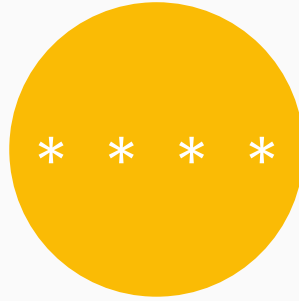
HOW IT ACTUALLY WORKS

Credential Breach



3.5B+

credentials leaked
in dumps



17%

minimum password
reuse rate



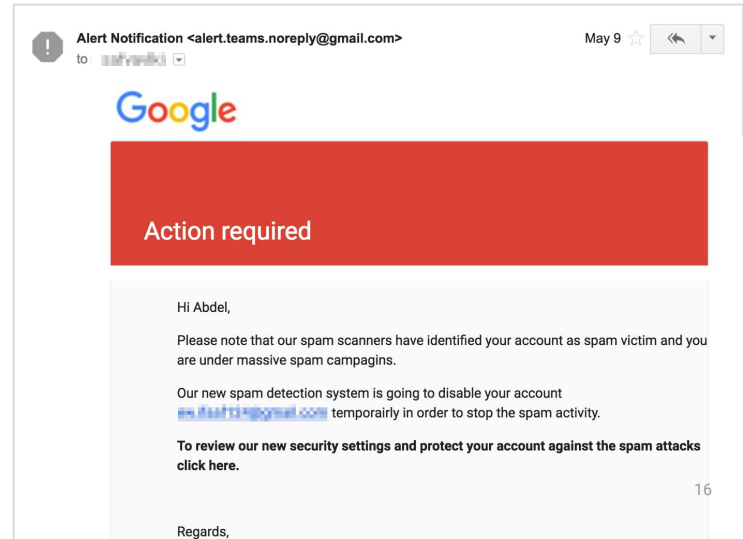
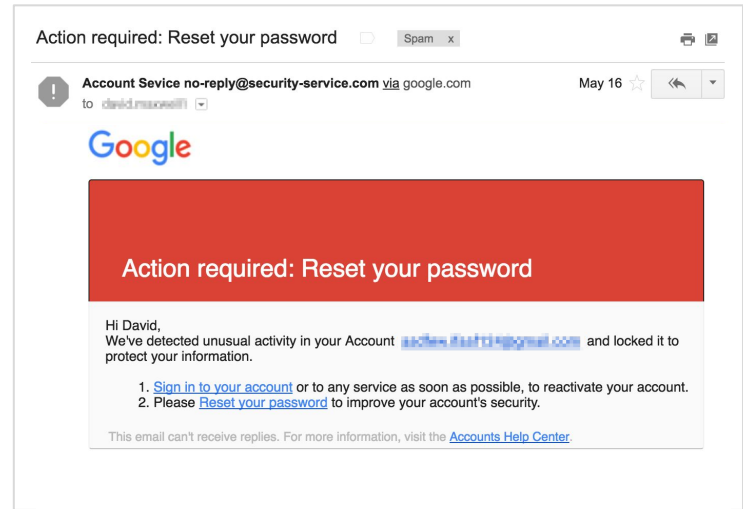
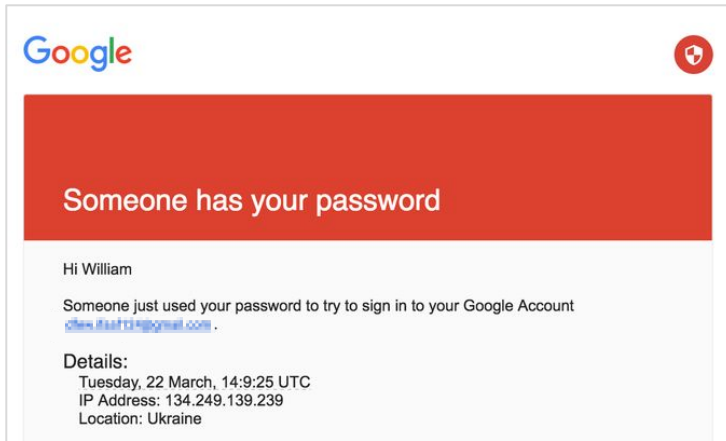
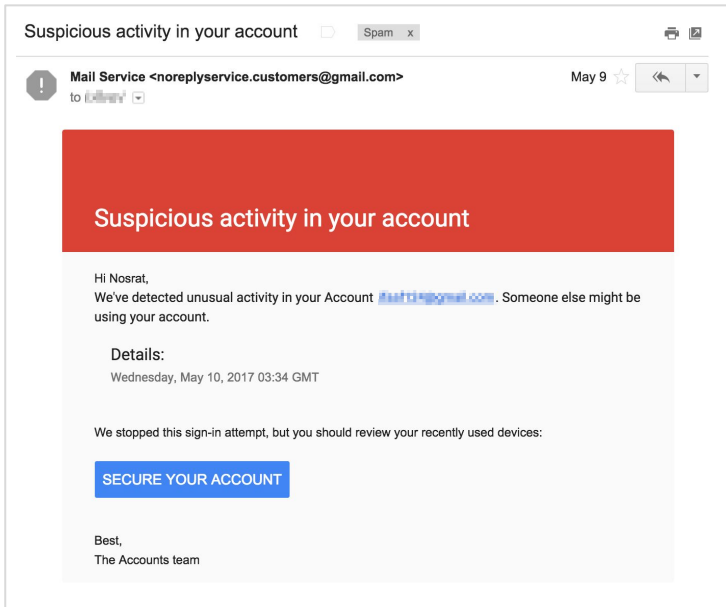
67M

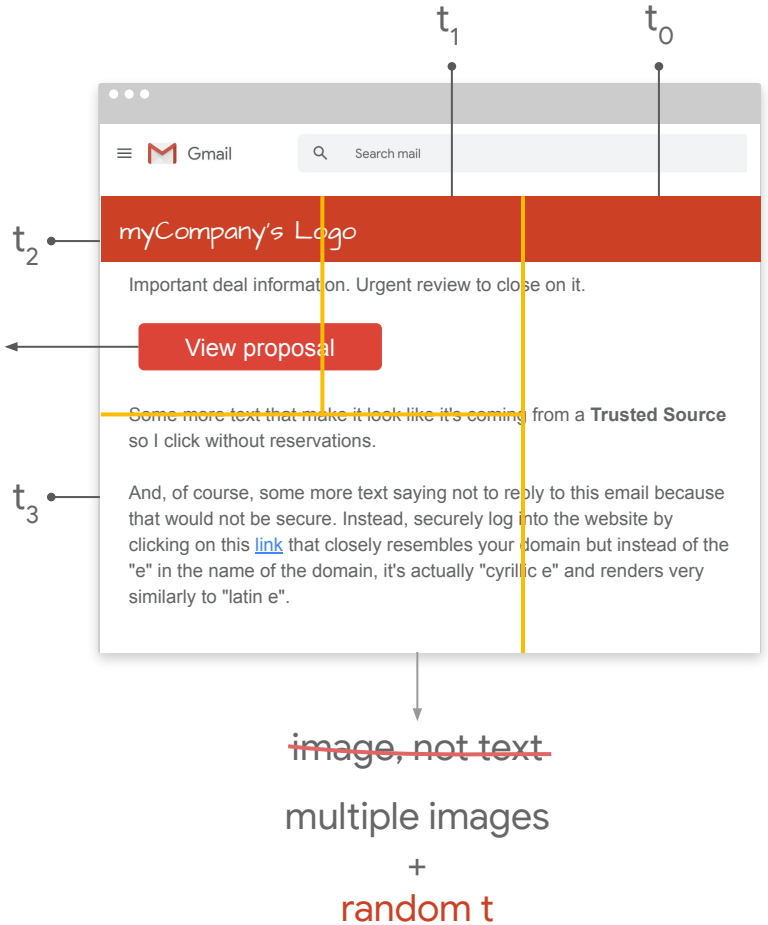
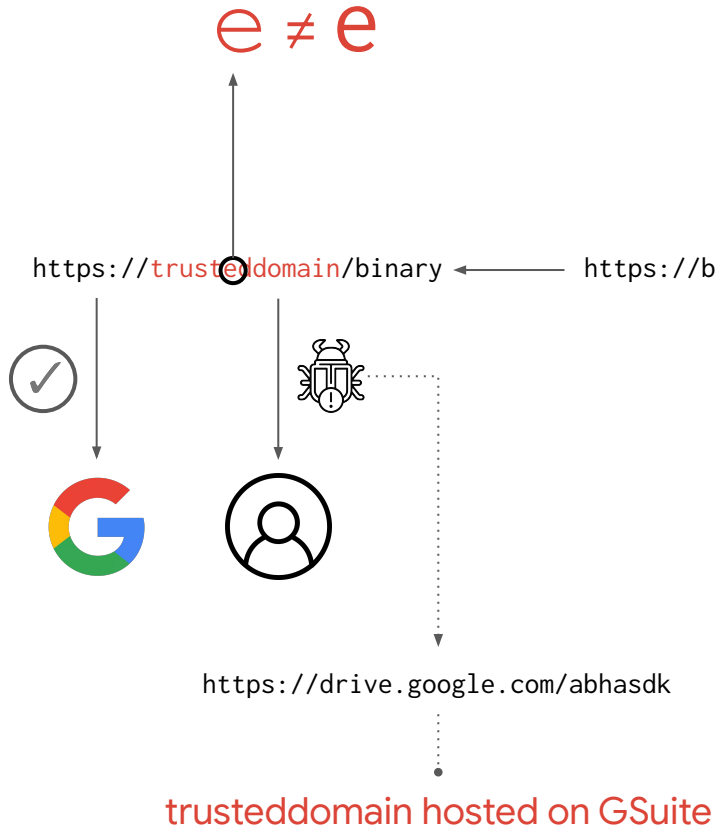
accounts proactively
re-secured

Source:

Data breaches, phishing, or malware? Understanding the risks of stolen credentials (Thomas et al., 2017) <https://research.google/pubs/pub46437/>

Phishing





Likelihood of Compromise



Involved in password
breach



Victim of keylogger

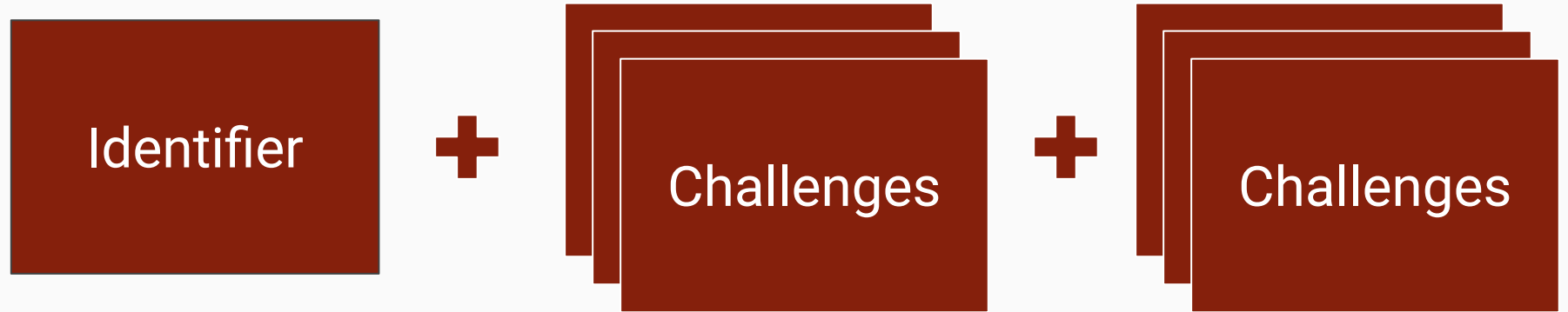


Phished

Source:
Anatomy of Account Takeover (Milka, 2019)
<https://www.usenix.org/conference/enigma2018/presentation/milka>

Mitigation

- Multi-factor authentication
- Risk-based authentication challenges
- Implicit signals



Multi-factor in the modern world



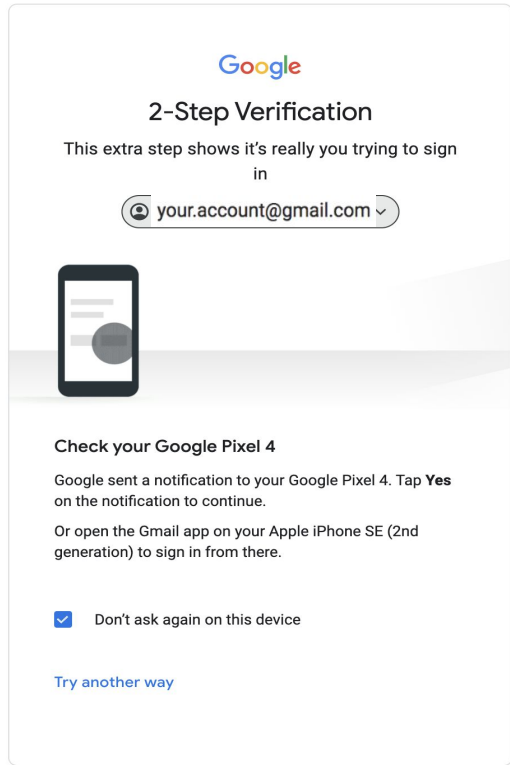
Controllable factors in Authentication

- When do we challenge you?
- What do we challenge you with?
- What "escape hatches" do we allow?
- What do we put under user control?

- What *implicit* signals do we get that help distinguish users from attackers?

When do we challenge you?

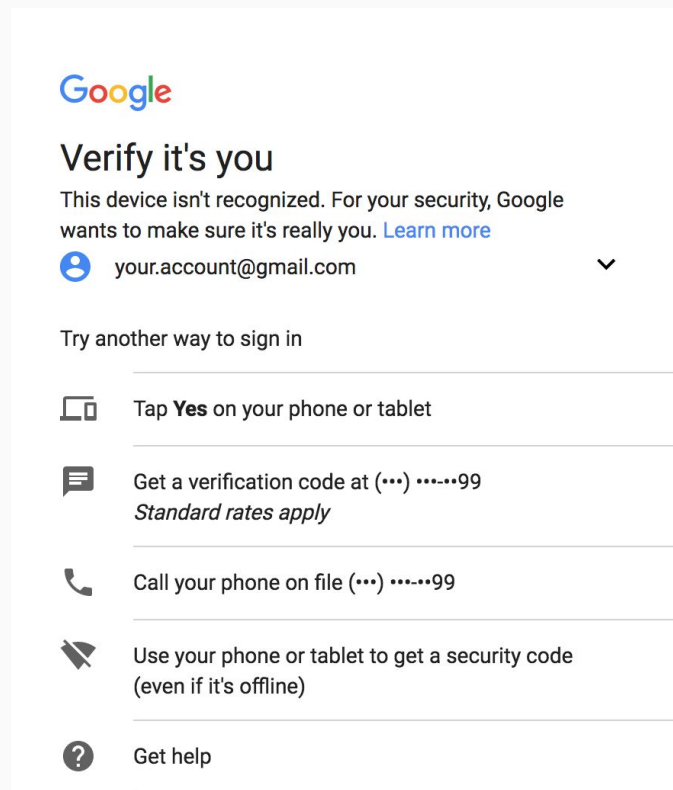
Deterministic (mostly)



English (United States) ▾

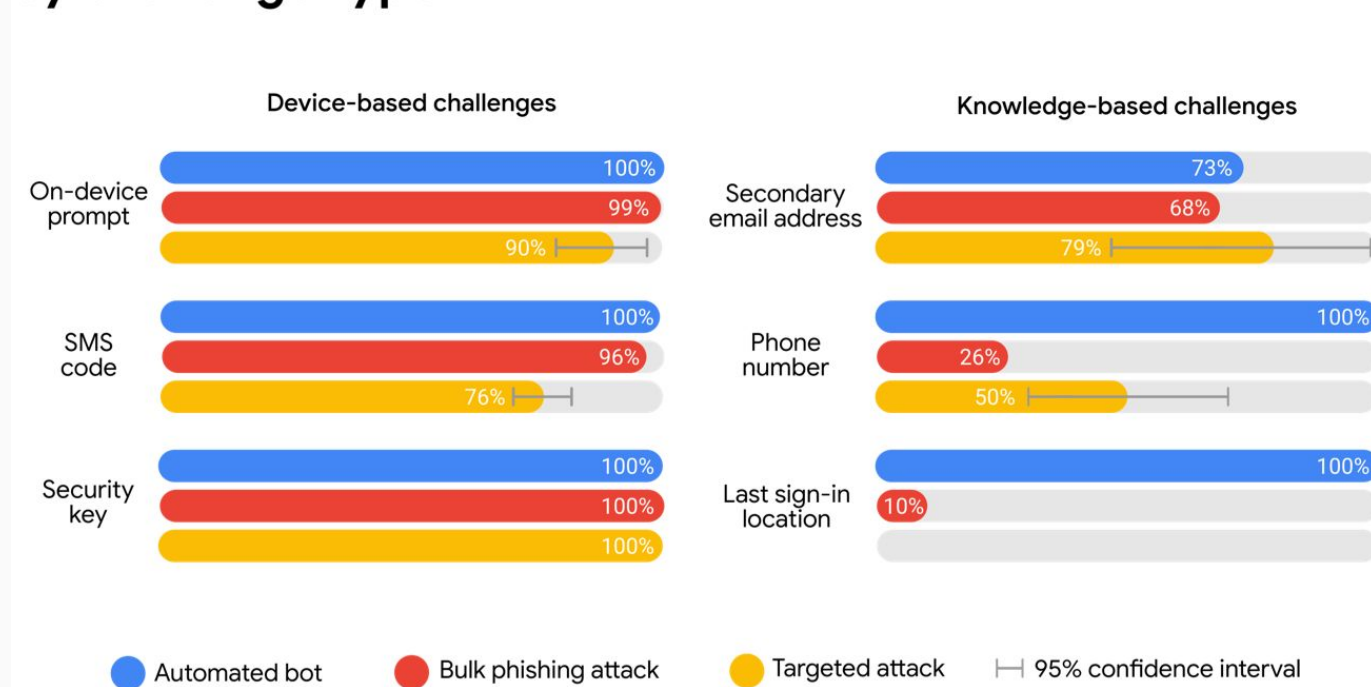
[Help](#) [Privacy](#) [Terms](#)

Risk-based



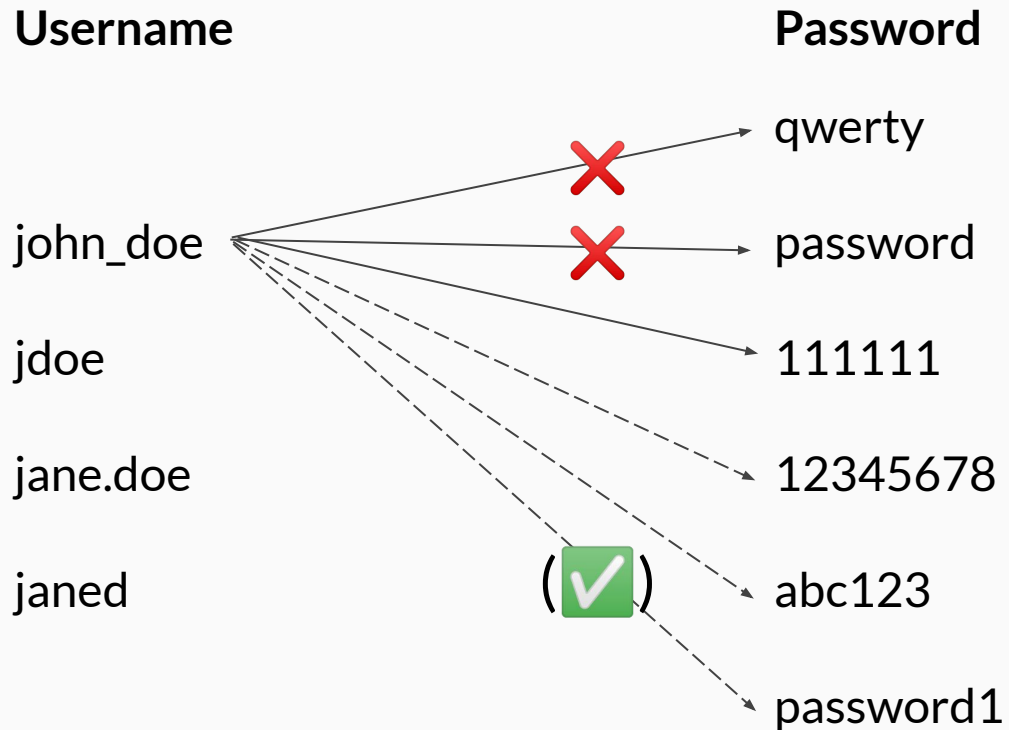
What do we challenge you with?

Account takeover prevention rates, by challenge type

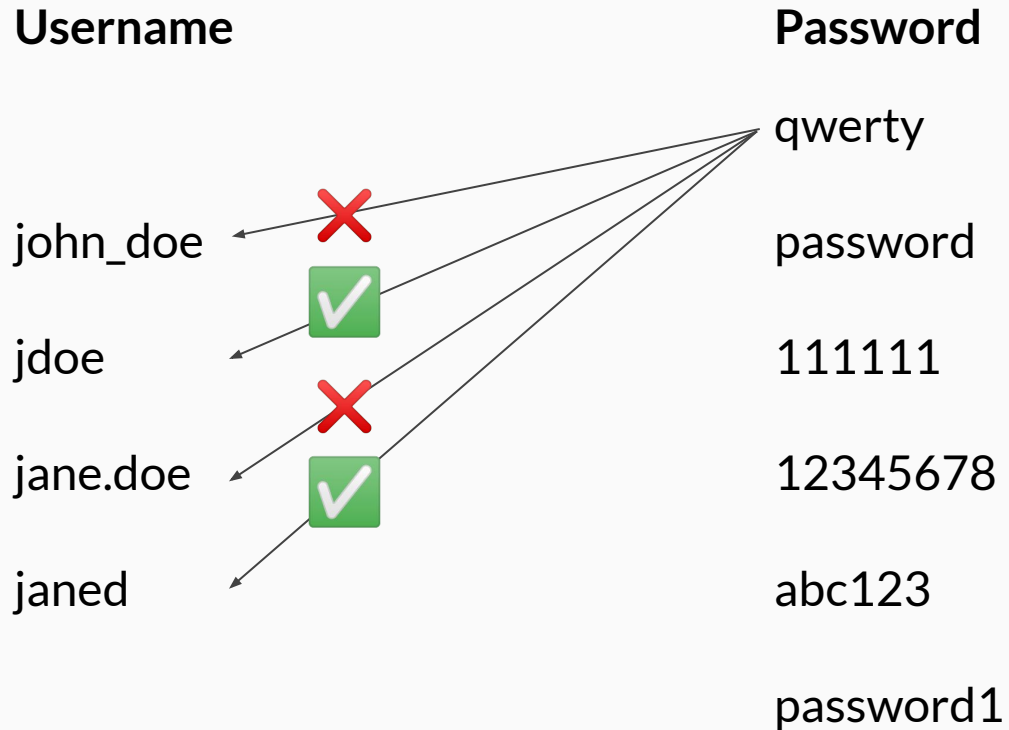


Source:
Evaluating Login Challenges as a Defense Against Account Takeover
(Doerfler et al.) <https://ai.google/research/pubs/pub48119>

Password Brute-Forcing: Defeatable with Per-User Quotas



Password Spraying



Predator Logger

About the Crack Cure RS PINS

PREDATOR 13

Delivery

Recovery

Settings

Binder

Downloader

Options

Tools

Build

Delivery

PHP FTP E-Mail

http://www.DeceptiveEngineering.com/path/logs.php Test

ftp.host.com username ***** Show Test

e-mail@host.com smtp.host.com ***** Show Test

Enable SSL Port: 587

Save these settings Interval for all: 10 minutes

Predator Logger

About the Crack Cure RS PINS

PREDATOR 13

Delivery

Recovery

Settings

Binder

Downloader

Options

Tools

Build

Recovery

Enable stealers

IMVU No-IP Paltalk Firefox

Minecraft AIM Nimbuzz Chrome

Bitcoin Wallet Pidgin jDownloader Opera

Runescape Pins Trillian FlashFXP Safari

RSBot Recovery FileZilla CoreFTP IE (6-11)

EpicBot Recovery System Info SmartFTP Outlook

RareBot Recovery IDM Win Key CD Keys (400+)

FTP Commander

Predator Logger

About the Crack Cure RS PINS

PREDATOR 13

Delivery

Recovery

Settings

Binder

Downloader

Options

Tools

Build

Settings

General Other Misc

Keylogging Clipboard Logging Disable CMD

Clear Steam Screenshot Logging Disable Regedit

Melt Clear Chrome data Disable Msconfig

USB Spread Clear IE data Disable TaskManager

P2P Spread Clear Firefox data Run Confirmation E-Mail

Add to Startup Delay Execution 10 seconds Select all

Predator Logger

About the Crack Cure RS PINS

PREDATOR 13

Delivery

Recovery

Settings

Binder

Downloader

Options

Tools

Build

Multi Binder

Files

Run bound files Add files Remove Clear all

Predator Logger

Predator Logger

Why is this hard?

And maybe harder for Google than others?

- Moving target w/evolving attackers
- Defenses themselves pose (availability) risks

The Security - ~~Usability~~ Availability Continuum

Availability

Security



Can you get access to your stuff?

- Fast?
- Easily?
- Eventually?

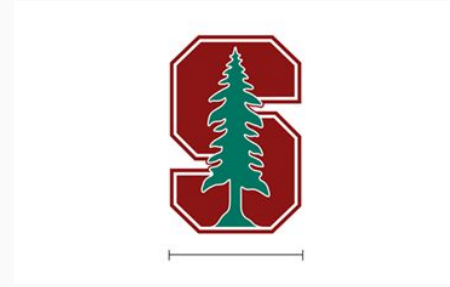
Increased security means you have to say **no**, at least some of the time.

Different accounts pose different protection problems



Subscription video-streaming:

- Large user base (e.g. 100M)
- **Potential damage:**
 - Theft of service/content
 - Theft of personal data
 - Ratings fraud (abuse)
- **Lockout prevention:**
 - Customer support/payment info
- **User cost of account loss:** low



Educational institution:

- Small user base (< 100K)
- **Potential damage:**
 - Theft of personal data
 - Content manipulation/DoS
- **Lockout prevention:**
 - Administrator fallback prevents account loss
- **User cost of account loss:** N/A

Different accounts pose different protection problems



Google:

- Large user base ([2B+ active](#)), many products
- **Potential damage:**
 - Theft/damage of personal data
 - Loss of income (e.g. for YouTube creators/App developers)
 - Leapfrog attacks against other accounts
 - Recovery email
 - "Sign in with Google"
 - Abuse against others
 - Spam, Ad click fraud, Review fraud
- **Lockout prevention:**
 - User-configured account recovery + devices
- **User cost of account loss:** ranges from zero to irreplaceable

Quiz #2

How many Google Accounts do you have?

How many do you care about/pay attention to?

Weaponized protection mechanisms



If you build something to let users protect themselves, hijackers will turn it against them.

Threats

- Credential breach
- Malware (keyloggers)
- (Offline) Phishing
- Challenge compromise

SMS: Not so hot anymore

SIM swap scam: What it is and how to protect yourself



SIM Swapping Attacks: What They Are & How to Stop Them

Fraudsters with social engineering skills are hijacking cell phone SIM cards to access victims' bitcoin and social media accounts.

Fraudster has your number, literally and otherwise

BRIAN BARRETT

SECURITY 08.19.2018 07:00 AM

How to Protect Yourself Against a SIM Swap Attack

Your phone number is increasingly tied to your online identity. You need to do everything possible to protect it.

Mitigation

- Multi-factor authentication
- Risk-based authentication challenges
- Implicit signals
- Dynamic challenge policies

Dynamic challenge policies

Google

2-Step Verification

This extra step shows it's really you trying to sign in

nobody.000@somedomain.com ▾

Try another way to sign in

- Tap **Yes** on your phone or tablet
- Use your phone or tablet to get a security code (even if it's offline)
- Get a verification code at (***).*13
Standard rates apply
Unavailable on this device
- Enter one of your 8-digit backup codes
- Get help
For security reasons, this may take 3-5 business days

English (United States) ▾

Help

Privacy

Terms

- Automatically offer the strongest challenges available
- Suppress weaker challenges in risky situations where the user has better options

Strengthening 2-Step Verification by showing phone prompts to more users

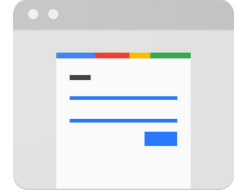
Tuesday, June 16, 2020

What's changing

Starting on July 7, 2020, we will make [phone verification prompts](#) the primary 2-Step Verification (2SV) method for all eligible users, unless they are already using security keys as their 2SV method of choice. This means that if you sign in to your Google

Threats

- Credential breach
- Malware (keyloggers)
- (Offline) Phishing
- Challenge compromise
- Active Man-in-the-Middle (MITM)



1 Click link

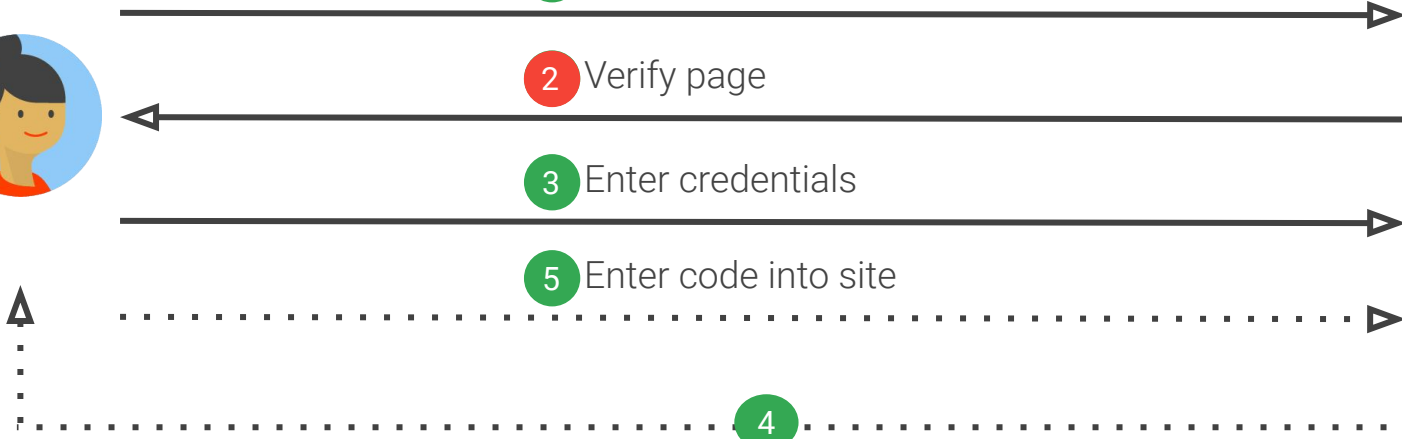
2 Verify page

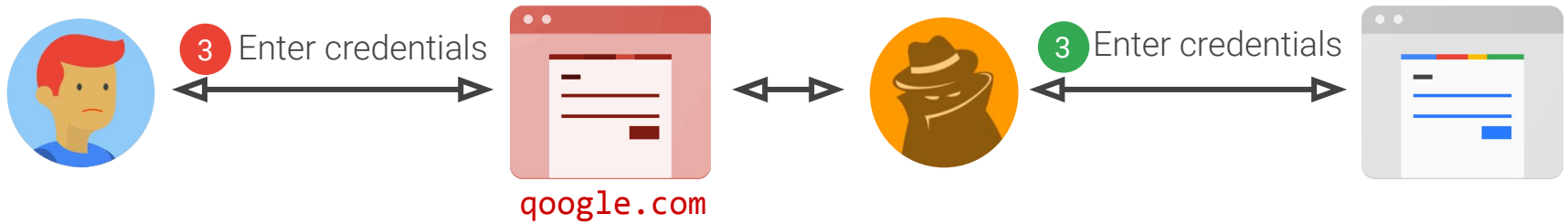
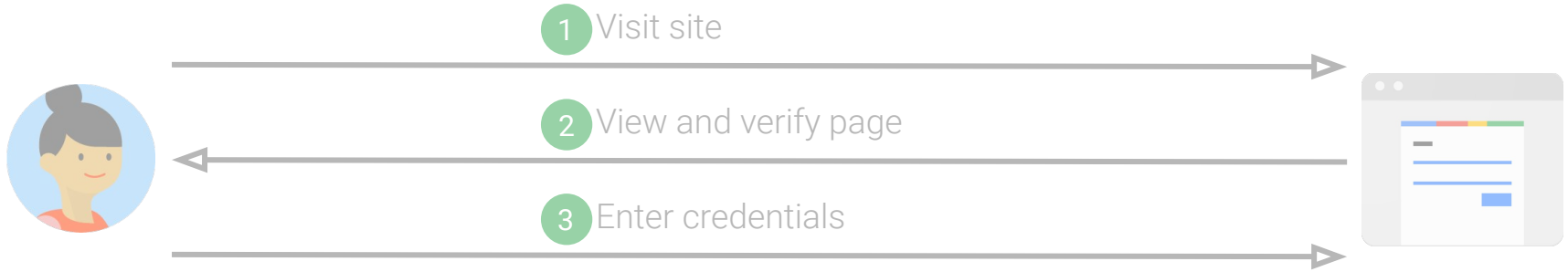
3 Enter credentials

5 Enter code into site

4

Send SMS code







Evilginx - Advanced Phishing with Two-factor Authentication Bypass

06 APRIL 2017 on hacking, research, phishing, mitm



YouTube 'influencers' get 2FA tokens phished

24 SEP 2019



2-factor Authentication, Google, Security threats, Social networks



Sign in

with your Google Account

Email or phone

[Forgot email?](#)


[More options](#)

NEXT

← <https://accounts.google...> 3



One account. All of Google.



[Next](#)
[Find my account](#)

[Create account](#)

One Google Account for everything Google



Mitigation

- Multi-factor authentication
- Risk-based authentication challenges
- Implicit signals
- Dynamic challenge policies
- Detecting and blocking active MITM
- Relying on trusted devices
- Phishing-resistant challenges

Detecting/Blocking Active MITM

Announcing some security treats to protect you from attackers' tricks

October 31, 2018

Posted by Jonathan Skelker, Product Manager

Guidance to developers affected by our effort to block less secure browsers and applications

Friday, August 28, 2020

Posted by Lillian Marie Agerup, Product Manager

We are always working to improve security protections of Google accounts. Our security systems automatically detect, alert and help protect our users against a range of security threats. One form of phishing, known as “[man-in-the-middle](#)”, is hard to detect when an embedded browser framework (e.g., [Chromium Embedded Framework - CEF](#)) or another automation platform is being used for authentication. MITM presents



Couldn't sign you in

The browser you're using doesn't support JavaScript, or has JavaScript turned off.

To keep your Google Account secure, try signing in on a browser that has JavaScript turned on. [Learn more](#)

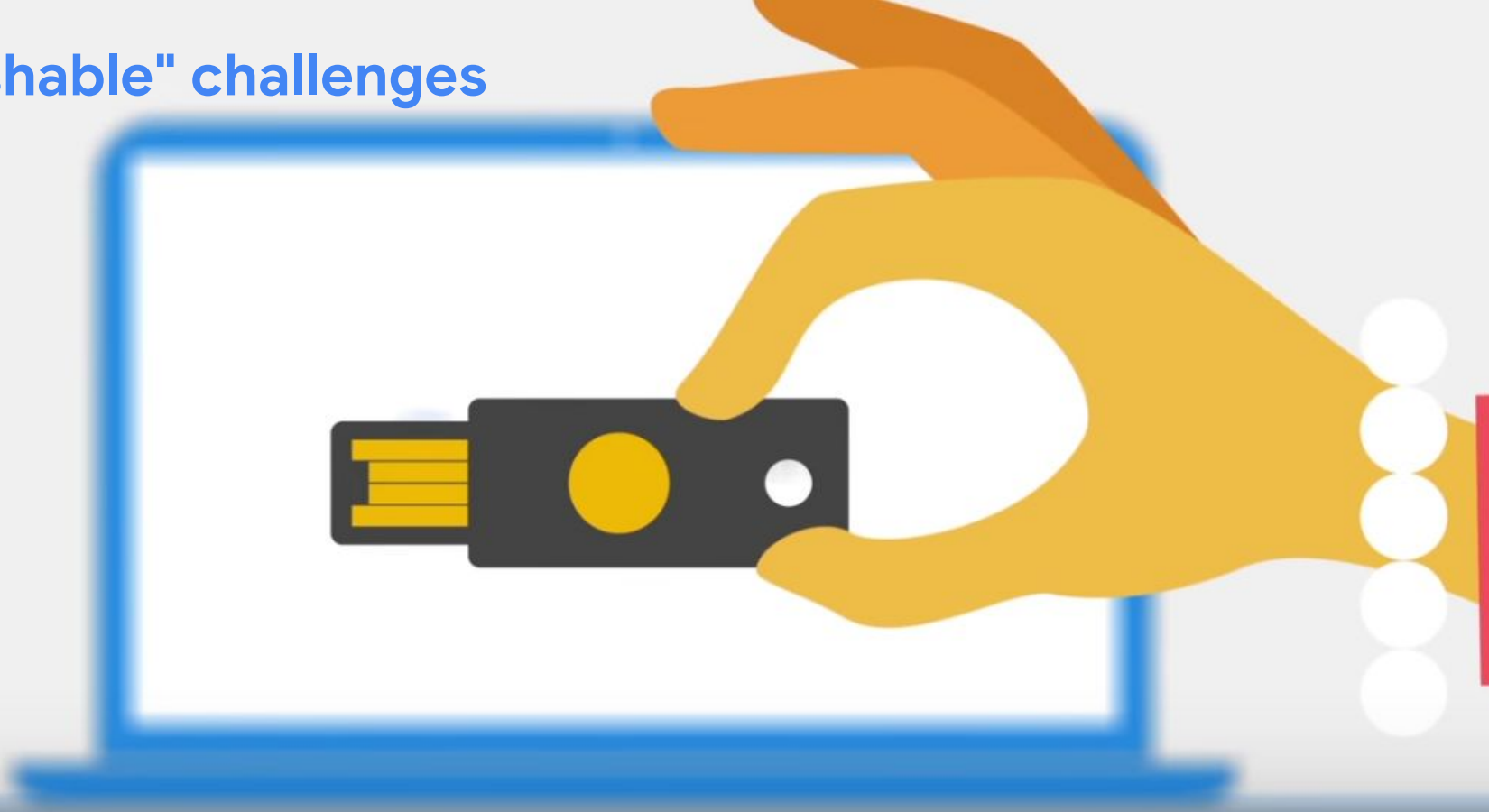
Trusted/Known Devices

Cardinal Key

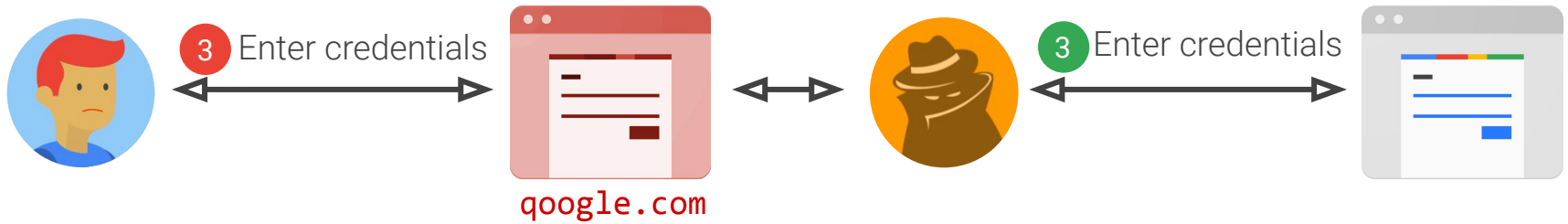
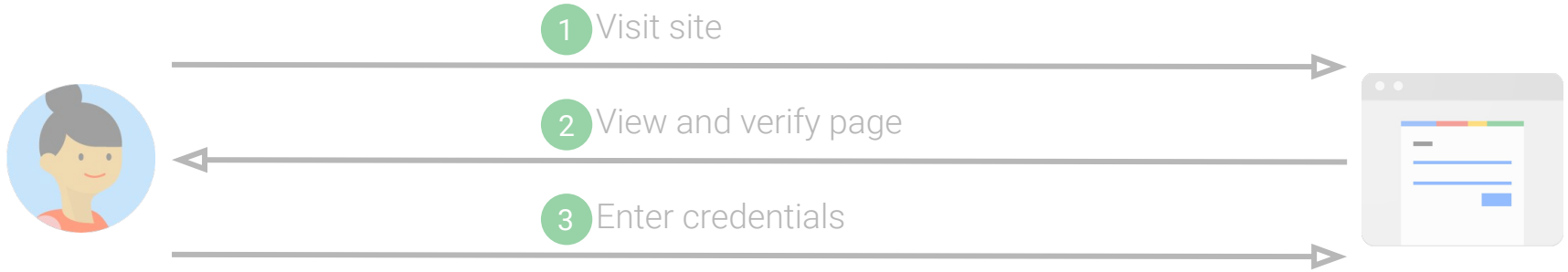
Simplicity and Security

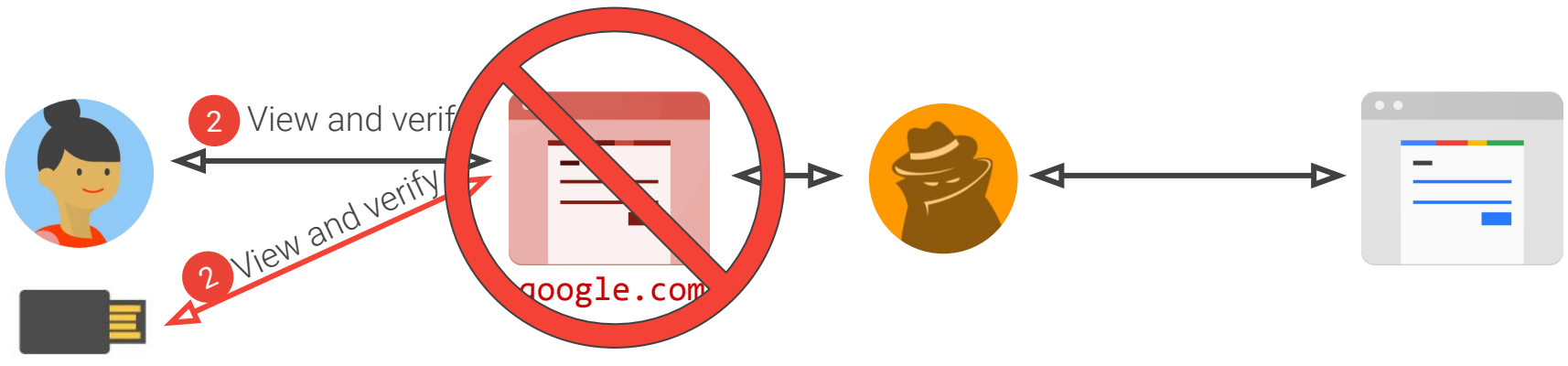
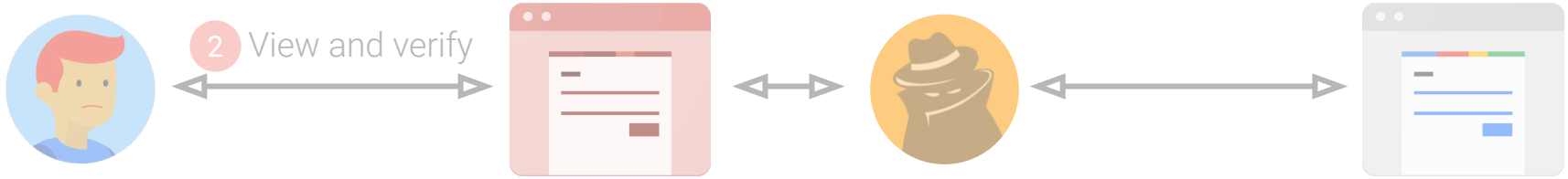
[Get a Cardinal Key](#)

"Unphishable" challenges



WebAuthn/U2F





Even Better - Phones as (free) Security Keys



Google Smart Lock 4+

Google LLC

★★★★☆ 3.7 • 184 Ratings

Free

Now, your Android phone is also a security key



Enhanced account protection

Strongest 2FA protection against phishing



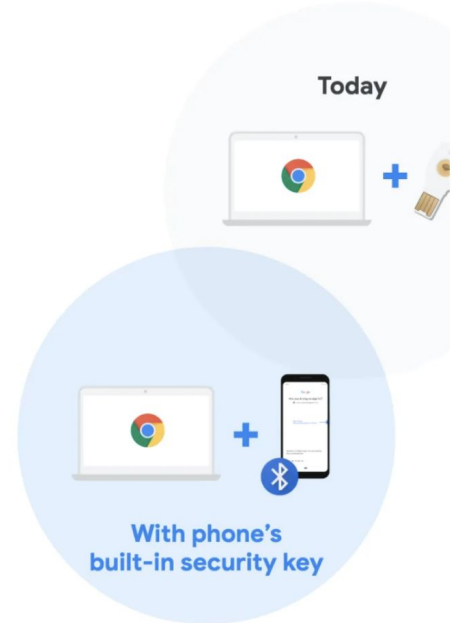
Easy to use

Simple, one-time enrollment process, no app required



Convenient for users

Use the phone which is already in your pocket.



APPLE \ GOOGLE \ TECH \

Google now treats iPhones as physical security keys ¹

With an update to the Google Smart Lock app

By [Jon Porter](#) | [@JonPorty](#) | Jan 15, 2020, 5:02am EST

Multifactor: the new normal

SAFETY & SECURITY

A simpler and safer future — without passwords

GOOGLE

Google will soon automatically enroll users in 2FA

You'll have the option to opt-out

[Home](#) > [News](#) > [Security](#)

Google to Opt People Into Two-Factor Authentication Automatically

Google will start with those who regularly engage with Google products on mobile and have recovery options saved to their accounts, but going forward, 2FA will be opt out rather than opt in.



By [Michael Kan](#) May 6, 2021



Threats

- Credential breach
- Malware (keyloggers)
- Phishing
- Challenge compromise
- Active MITM
- Malware (session theft)

Cookie/Token Theft: When it's too hard to get in the front door...

You go in through the window



What's it like to do this job?

We're hiring!

Team:

- Identity org of ~400
 - Sites in Sunnyvale, San Francisco, Munich, Zurich and Tel Aviv
- Sign-in team of ~55 engineers
 - Divided into 6 subteams with different specializations (not all security)
 - 25% female

What do we do?

- Write code
- Do & review design
- Do data analysis
- Work with xfn partners
 - Product managers
 - UX designers & writers
 - UX researchers
 - Data analysts
- Go to a lot of meetings (at least me)

Questions?