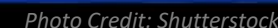
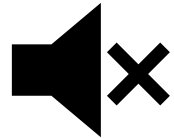


Identity and Access Management Fundamentals for Small Business



Notes and Reminders



Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.



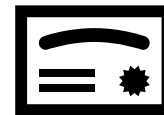
Webinar recording: This webinar will be recorded and posted to the event page here:

<https://www.nist.gov/itl/smallbusinesscyber/events>

Registrants will be notified via email when the recording is available.



Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.



CE/CPE credits: NIST does not provide specific information regarding CE/CPE credits. Attendees are welcome to use their registration confirmation email to self-report to their certification bodies.

NIST Small Business Cybersecurity Resources

SMALL BUSINESS CYBERSECURITY CORNER

Cybersecurity Basics

NIST Cybersecurity
Framework

Quick Start Guides

Events

Guidance by Sector

Guidance by Topic

Training

Videos

Get Engaged

Cybersecurity @ NIST



CONNECT WITH US



SPOTLIGHT

Cybersecurity Framework



Quick Start Guides



Videos



NIST Cybersecurity White Paper
NIST CSWP 28

Security Segmentation in a Small Manufacturing Environment

Dr. Michael Powell
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

John Hoyt
Aslam Sherule
Dr. Lynette Wilcox
The MITRE Corporation

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.28>

April 6, 2023

NISTIR 7621
Revision 1

Small Business Information Security: The Fundamentals

Celia Paulsen
Patricia Toth

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.7621r1>

A screenshot of the NIST Manufacturing Extension Partnership (MEP) website. The header includes the NIST logo and a search bar. The main heading is 'MANUFACTURING EXTENSION PARTNERSHIP (MEP)'. Below this, there is a section titled 'Cybersecurity Resources for Manufacturers' with a sub-heading 'WHERE TO START'. The page lists various resources and guides for manufacturers.

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide



www.nist.gov/itl/smallbusinesscyber

Identity and Access Management Fundamentals for Small Business

Ryan Galluzzo

Identity Program Lead

Applied Cybersecurity Division

Information Technology Lab



Digital Identity Functional Overview



Action

Seeks to answer the question



Identity Proofing

Who are you?

Identity proofing provides confidence that the person you are granting an account to is the person they claim to be.



Authentication

Are you the same you?

Authentication provides confidence that a returning user is the same person to whom you granted an account.



Federation

How can I receive and convey identity information?

Federation allows for the transmission of identity data to partners inside and outside your organization.



Authorization

What are you allowed to do?

Authorization limits a users access to the minimum needed for them to execute their defined roles and functions related to an applications, data, or service.

What is Multifactor Authentication?



Something you know

(e.g., Password, PIN)



Something you have

(e.g., phone, security key)



Something you are

(e.g., biometric)

Multifactor Authentication (MFA) combines more than one of these factors when authenticating users.

Why MFA Matters – Passwords stink.

Identity attacks in perspective: Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

More than
99% of identity
attacks are
password attacks

Breach replay
Password spray
Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1%
of attacks



MFA attacks

SIM swapping
MFA fatigue
AiTM

Post-authentication attacks

Token theft
Consent phishing

Infrastructure compromise

Source: Microsoft Threat Intelligence

Password Problems



Credential Stuffing,
Guessing, Brute Force



Offline and
Dictionary Attacks



Phishing, SMShing &
other fishing



Social Engineering &
Scams

Source: [Microsoft Digital Defense Report 2024](#)

Are you a target? A fun exercise...

Account | Your info | ... | ? | RG


- > 14 hours ago Unsuccessful sign-in
- > Yesterday 11:37 PM Unsuccessful sign-in
- > Yesterday 3:33 AM Unsuccessful sign-in
- > 10/19/2024 10:53 PM Unsuccessful sign-in
- > 10/19/2024 4:17 PM Unsuccessful sign-in
- > 10/19/2024 2:11 PM Unsuccessful sign-in
- > 10/18/2024 8:40 PM Unsuccessful sign-in
- > 10/18/2024 9:48 AM Unsuccessful sign-in
- > 10/16/2024 2:49 PM Unsuccessful sign-in
- > 10/16/2024 1:31 PM Unsuccessful sign-in
- > 10/16/2024 8:28 AM Unsuccessful sign-in
- > 10/16/2024 7:44 AM Unsuccessful sign-in
- > 10/16/2024 4:31 AM Unsuccessful sign-in

Account | Your info | ... | ? | RG

- > 10/16/2024 2:26 AM Unsuccessful sign-in
- > 10/16/2024 12:49 AM Unsuccessful sign-in
- > 10/16/2024 12:23 AM Unsuccessful sign-in
- > 10/15/2024 11:18 PM Unsuccessful sign-in
- > 10/15/2024 10:12 PM Unsuccessful sign-in
- > 10/15/2024 8:06 PM Unsuccessful sign-in
- > 10/15/2024 7:42 PM Unsuccessful sign-in
- > 10/15/2024 6:05 PM Unsuccessful sign-in
- > 10/15/2024 5:42 PM Unsuccessful sign-in
- > 10/14/2024 11:47 PM Unsuccessful sign-in
- > 10/14/2024 10:08 AM Unsuccessful sign-in
- > 10/14/2024 1:33 AM Unsuccessful sign-in

Account | Your info | ... | ? | RG

- > Yesterday 11:37 PM Unsuccessful sign-in
- ✓ Yesterday 3:33 AM Unsuccessful sign-in



Device/platform
iOS

Browser/app
Safari

IP address
223.81.131.111

Account alias
[Redacted]

Session activity
Incorrect password entered

Approximate location
China

Map is not available for activity on mobile devices

Look unfamiliar?
[Secure your account](#)

My Personal 365 Account

- **25 plus unsuccessful access attempts in one week**
- **Attempts from China, Vietnam, Brazil, Ukraine, Romania**
- **Yes, this is Office 365 but how many of you use Office 365?**

MFA Types



Less Secure

More Secure

	SMS OTP A code that is texted or delivered via audio	OTP Apps <i>App that generates timebound codes</i>	Push Authentication <i>App that sends approval requests to a user</i>	Cryptographic Apps <i>Key for authentication stored in software</i>	Security Keys <i>Key for authentication stored on a device</i>
Examples	“your verification code is 1234. Don’t share this with anyone else!”	Google & Microsoft Authenticators	“Press ‘approve’ if you are attempting to access...”	FaceID, Windows Hello, Google, PASSKEYS!	Yubikey, Google Titan, PIV Cards
The Good	<ul style="list-style-type: none"> ➤ Anyone with a phone can use it! 	<ul style="list-style-type: none"> ➤ SIM Swap protection ➤ Can be done offline 	<ul style="list-style-type: none"> ➤ SIM swap protection ➤ Minimal phishing protection 	<ul style="list-style-type: none"> ➤ Phishing resistant ➤ “Passwordless” ➤ Single device 	<ul style="list-style-type: none"> ➤ Phishing resistant ➤ Local MFA option ➤ Can be single device
The Bad	<ul style="list-style-type: none"> ➤ Highly phishable ➤ Connection required ➤ SIM Swap ➤ Network attacks ➤ Carrier reliance ➤ Plus a password 	<ul style="list-style-type: none"> ➤ Highly phishable ➤ App required ➤ Smart phone needed ➤ Plus a password 	<ul style="list-style-type: none"> ➤ Connection required ➤ App required ➤ “MFA exhaustion” ➤ Plus a password 	<ul style="list-style-type: none"> ➤ Smart device needed ➤ Not user friendly ➤ Limited market availability 	<ul style="list-style-type: none"> ➤ Another “thing” ➤ Expensive ➤ Loss/replacement ➤ Plus a Password (sometimes)

Some MFA is better than no MFA.

A word about Phishing Resistance...



Phishing is one of the primary means of compromising credentials, both passwords and some MFA types. Phishing resistance authenticators avoid these risks by mitigating

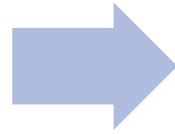
1. **User manipulation** by eliminating the need to manually enter codes or information
2. **Impersonated websites** by binding the authenticator to a specific website, domain, or a communication channel
3. **Attacker in the Middle** through cryptographic protocols and digital signing
4. **Replay of captured credentials** through techniques digital signing and time stamping

Not every application needs phishing resistance, but it should be used for high risk services and users such as system administrators and those with elevated privileges.

So what should you do?

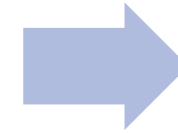
1. Take a Risk Based Approach

- Know your users
- Know your data
- Know your regulatory environment
- Understand the impact of unauthorized access to you and **your customers**
- Not every user or application needs the same level of authentication



2. Understand your options

- Know what your platforms, services, and IT providers offer
- Know what works for your employees, customers, and other users
- Know your threat and fraud environment
- Consider federation for external users



3. Layer your defenses

- Don't just rely on MFA, even phishing resistance
- Leverage platform, service, and IT provider tools to monitor for threats, risks, and events
- Integrate with authorization and access monitoring tools.

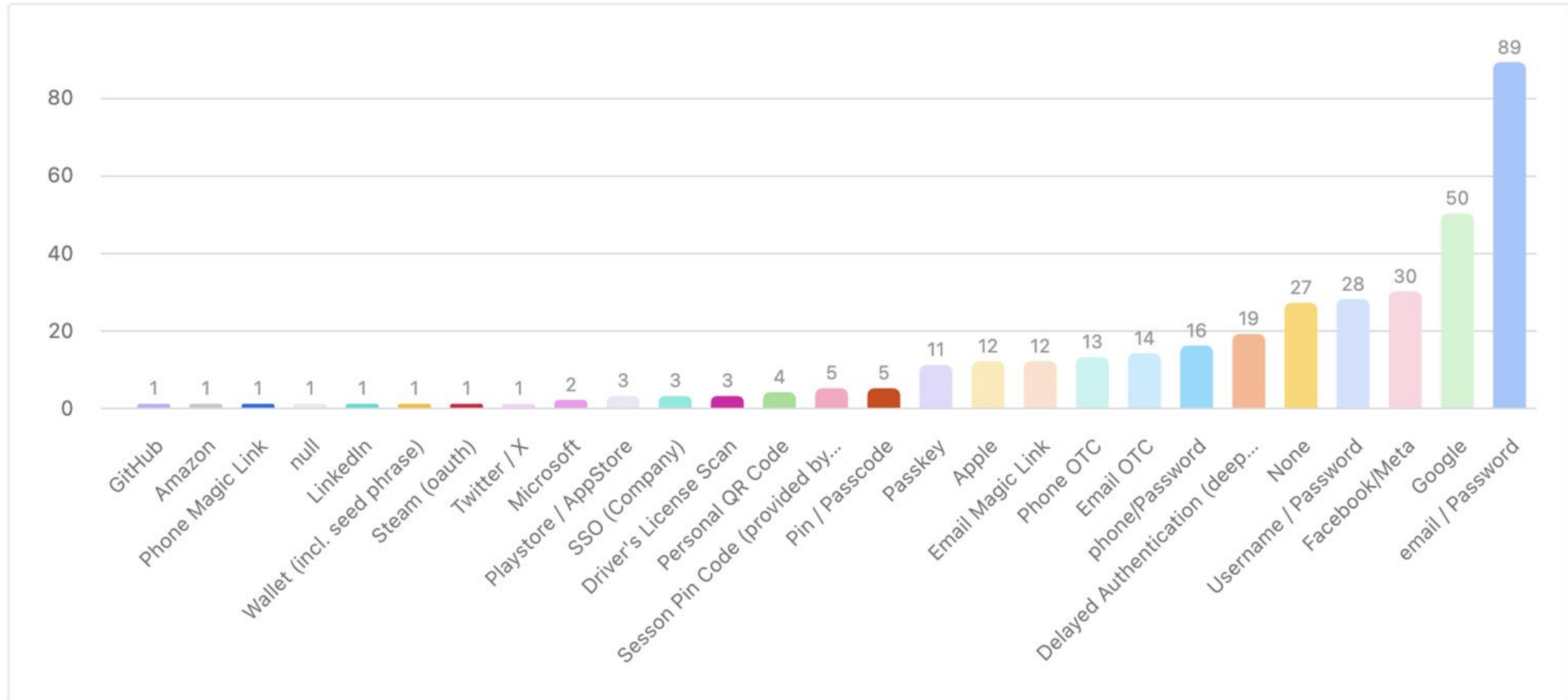


The Password Paradox - Why Passwords persist and how we can mitigate their risk.

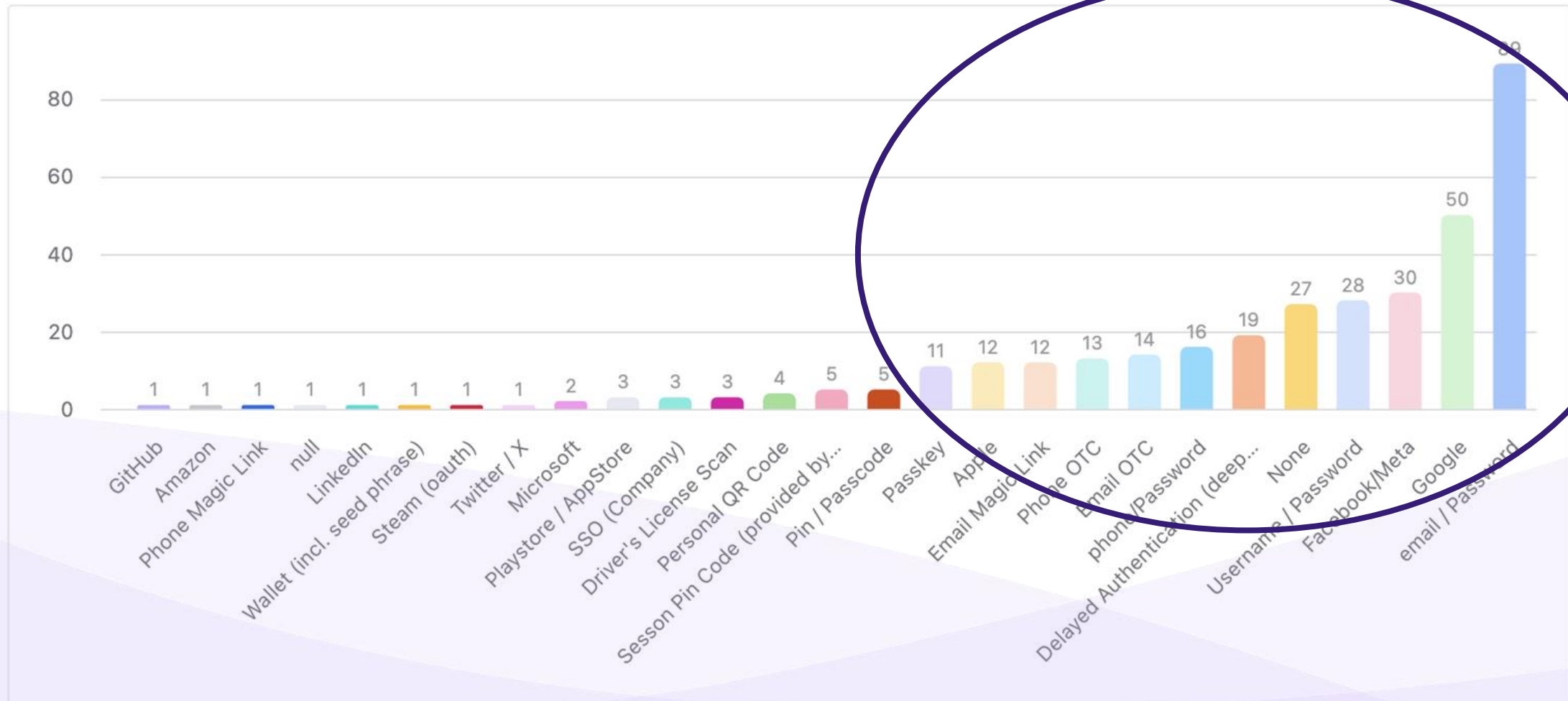
Rob Thelen; CEO, Rownd - robert@rownd.com

The world's most powerful onboarding platform

Majority of Top Mobile Apps still use Passwords

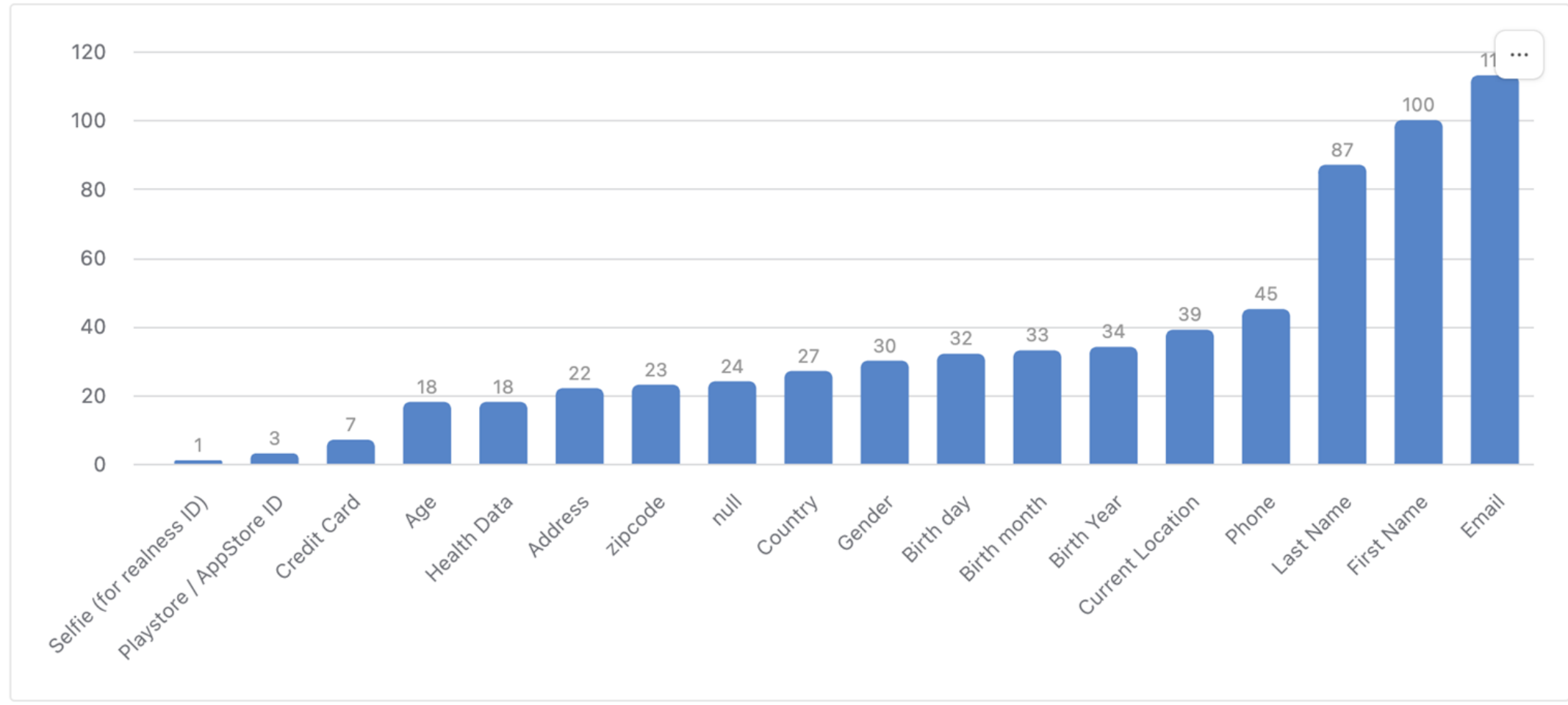


Majority of Top Mobile Apps still use Passwords



42% have at least one social login

Vast majority of Mobile apps collect PII



Why are passwords still used?

Top reasons (from CEOs and CTOs):

1. Cost to move (Expensive to add auth choices)
 2. If it ain't broken, don't fix it
 3. Fear of negative metrics
- 

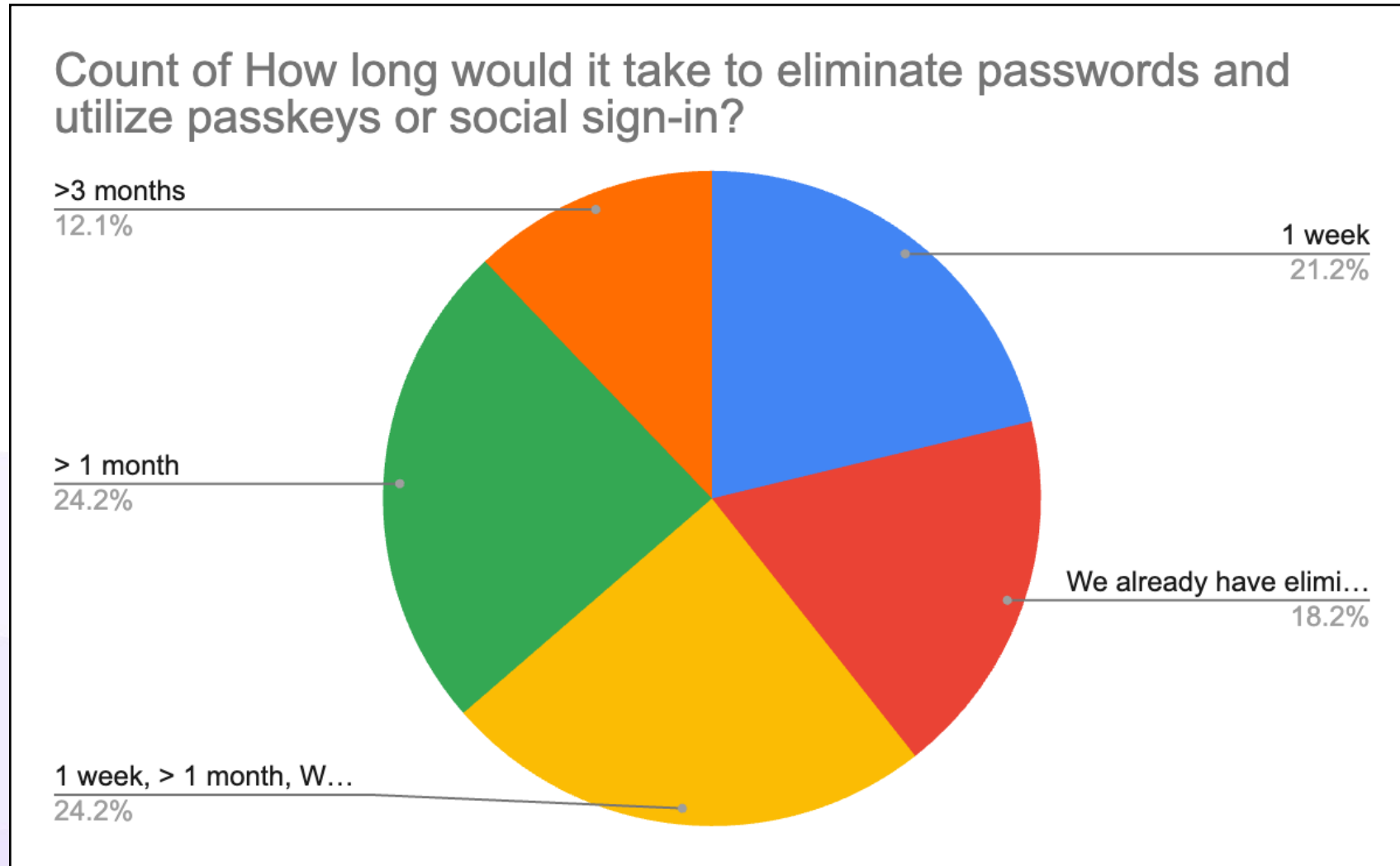
Why are passwords still used?

Top reasons (from CEOs and CTOs):

1. Cost to move (Expensive to add auth choices)
2. If it ain't broken, don't fix it
3. Fear of negative metrics

Over the next few slides, I hope to show that each of these are false.

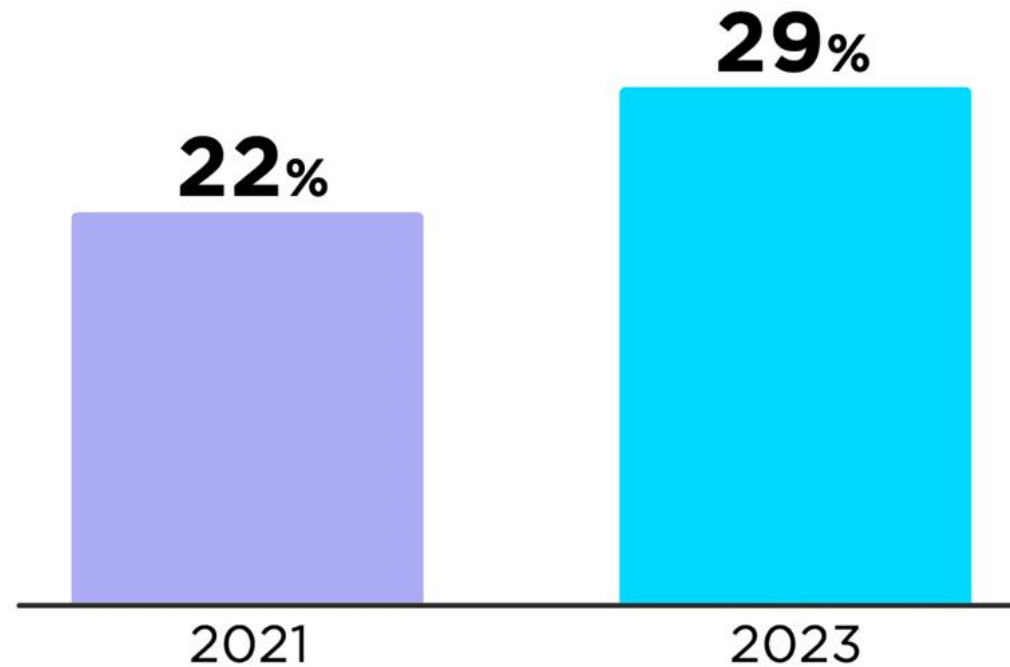
Survey of CTOs showed majority of apps COULD get rid of passwords in under a month



Increasing threat of account take over

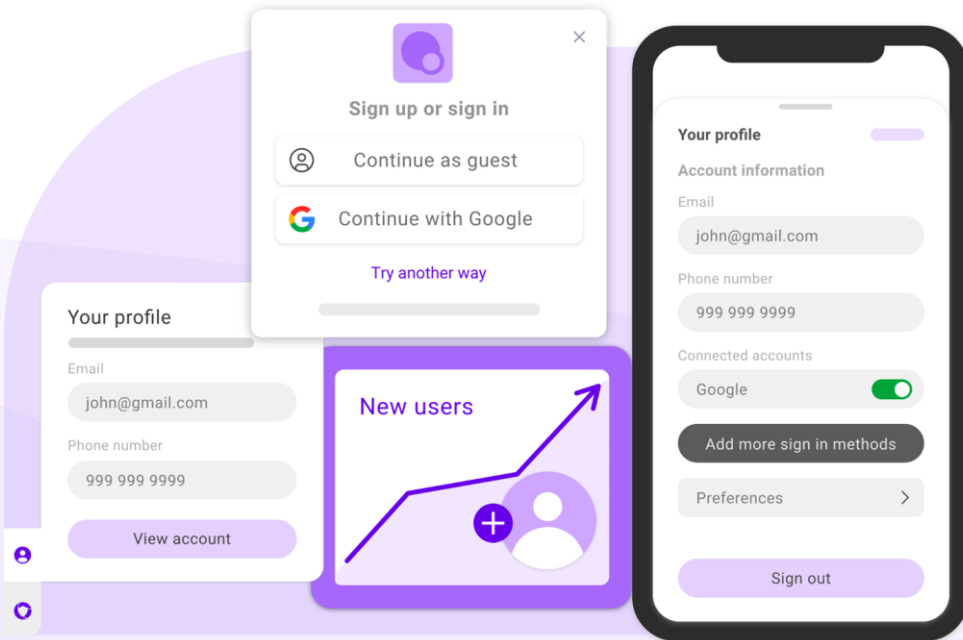
ACCOUNT TAKEOVER HAS INCREASED SINCE 2021

PERCENT WHO'VE HAD AN ACCOUNT TAKEN OVER
(SOMEONE ACCESSED THEIR ONLINE ACCOUNT BY OBTAINING THEIR SIGN-ON CREDENTIALS)



Most account takeovers focus on changing email/phone numbers

Wide suite of services that will give a risk score and ownership information over phone numbers and emails.



Your support team is a threat vector

Support usually has the ability to change recovery email addresses or phone numbers, ensure procedures are in place to make sure the new email is safe.



Phishing to get in

Attackers will use advanced phishing (one-time code phishing or targeted password phishing) to gain access, then change recovery emails to take over the account



Compare with known data


If you already have the data, compare known information with what is listed on a phone record - address, zip-code, and last 4 of SSN to verify users.



Encourage users to have multiple recovery methods

Backup email address and phone numbers are useful if an account is locked without putting a burden on support.

Users will pick the first choice most of the time.




Get the latest updates from Schrute Farms


Email


you@domain.com

Continue

OR

 Continue with Okta


 Continue with Google

 Continue with MobileConnect (test)


Try another way


By continuing, you agree to Schrute Farms's terms and conditions and privacy policy.


Powered by Rownd




Get the latest updates from Schrute Farms

 Continue with a passkey

 Continue with Okta

 Continue with Google

 Continue with MobileConnect (test)

OR

Email


you@domain.com

Continue


Try another way


By continuing, you agree to Schrute Farms's terms and conditions and privacy policy.

Powered by Rownd



Get the latest updates from Schrute Farms

 Continue with Google

 Continue with a passkey

Try another way

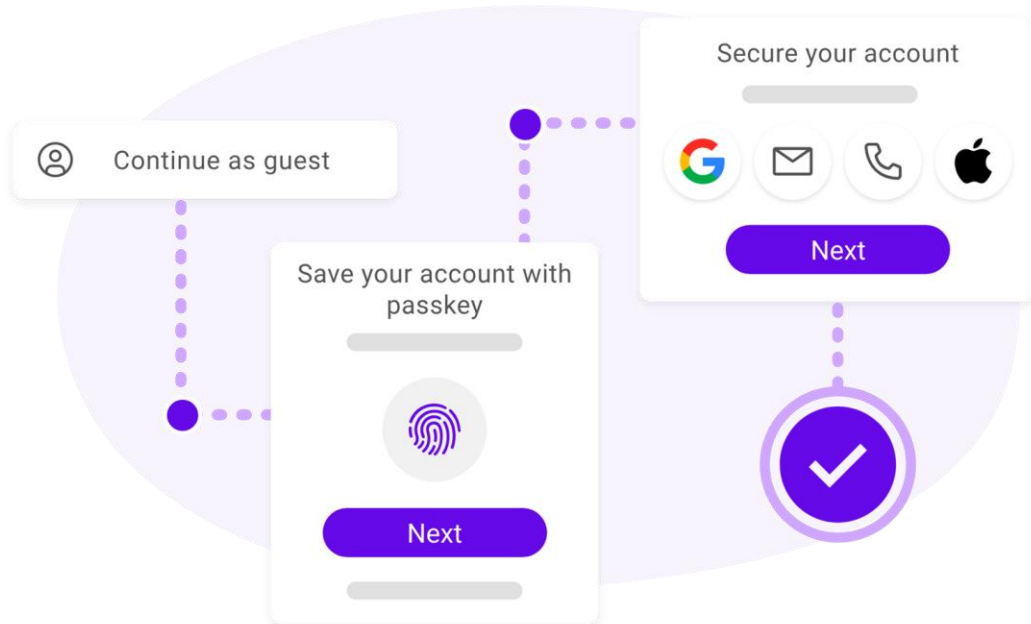
By continuing, you agree to Schrute Farms's terms and conditions and privacy policy.

Powered by Rownd

Small changes can lead to better user-behavior

Progressive Sign-up

Start with limited options and then sprinkle in 2FA and other options later in the process.



Adaptive by Device

Understand how each type of device works. Sign-in with Apple is hard on Android, for example.



Passive options

Default to passive options early in the funnel. When authentication is required, ensure safer options are presented first.



Progressive sign-up

Allow users add new sign-up methods over time. Let them add passkey, sign-in with social, etc. Don't make it mandatory right off the bat - or your metrics will hurt.

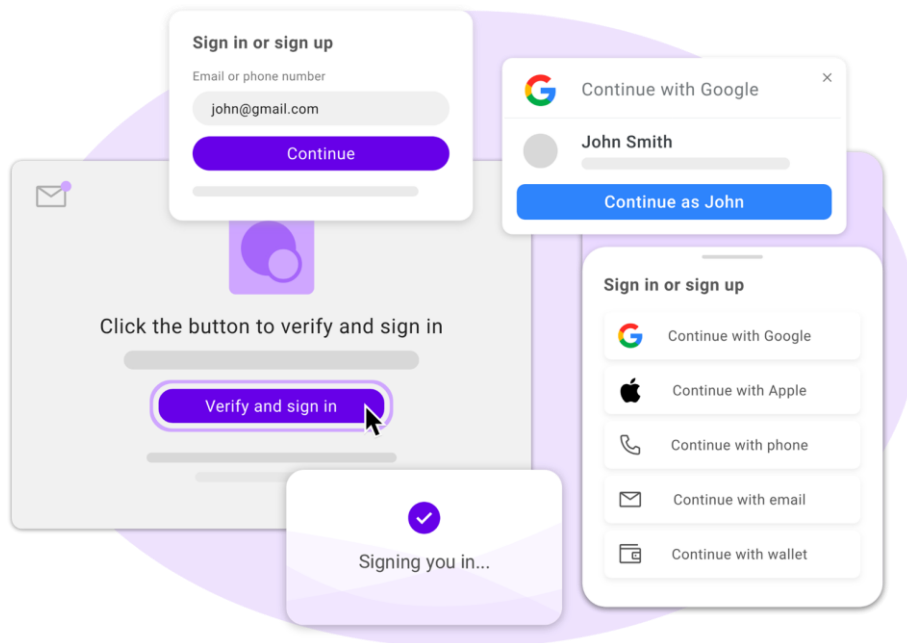


Iterate and experiment

There is a constant tug of war between the CISO/risk and the growth/product team. Security and ease do not have to be a trade off. Experiment and iterate based on data.

Passwordless also enables more sign-ins

Convert more users by simplifying your sign-up and sign-in experiences - also make them more secure



One click options

Add Login with Google and Apple or other social to verify emails faster and with less friction. Note how they work on different devices.



Email and Phone verification

But don't overly rely on them for authentication due to risks.



Add Passkeys ASAP

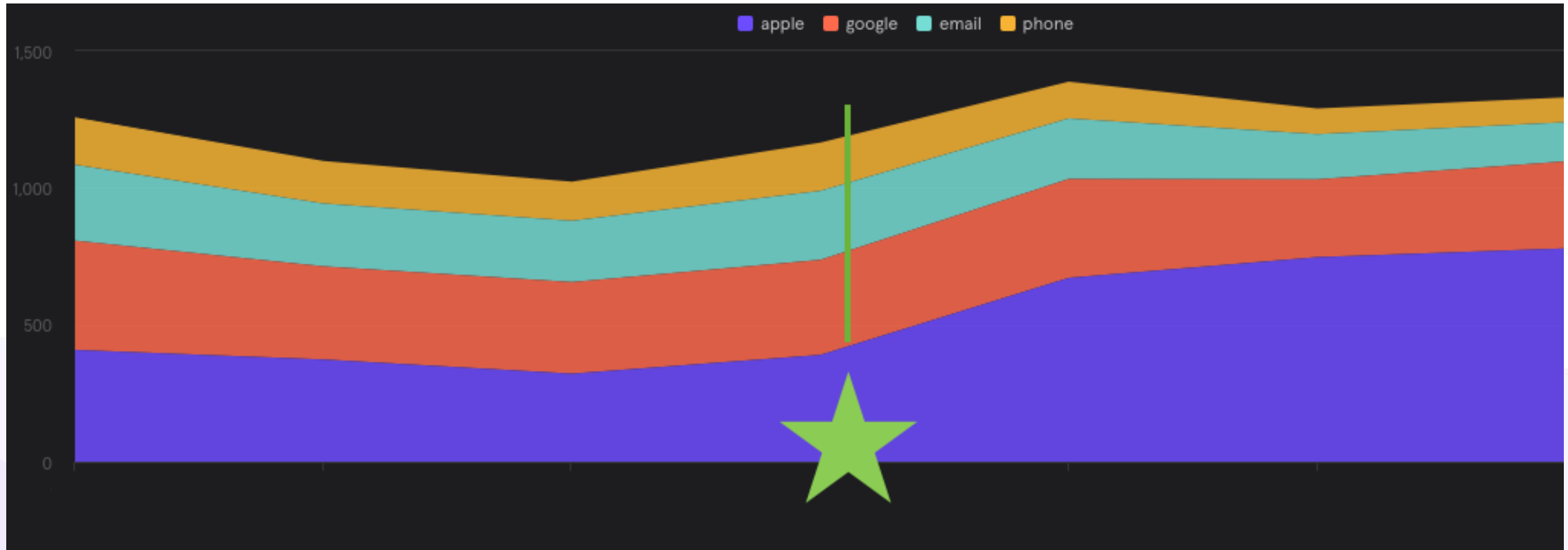
Passkeys are tied to a user's account, meaning they can login even after they switch devices.



Move sign-up later with "Guest users"

The world's best brands delays sign-up until users have tried the app. "Guest users" can convert to full users but also reduce the threat of account take over

Case-study: Hiding choices led a 15% increase in sign-up rates

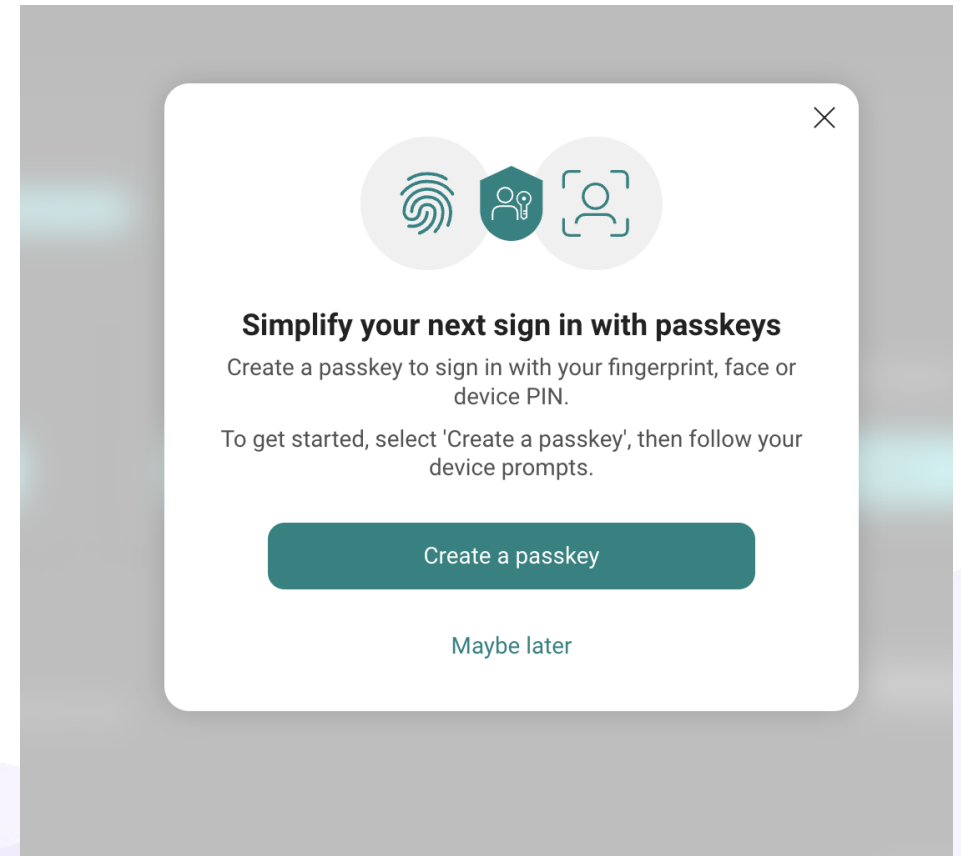


With Passkeys, optional nudges are key

Pop-up once every few weeks,
until a passkey is created.

Let users know what passkeys
are prior to kicking off a flow.

**Leads to 3x more users with
passkeys as secondary factors.**



Why are passwords still used?

Top reasons (from CEOs and CTOs):

- ~~1. Cost to move (Expensive to add auth choices)~~
- ~~2. If it ain't broken, don't fix it~~
- ~~3. Fear of negative metrics~~

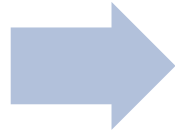
Things that can be done right now:

1. Change order of sign-up options
2. Reduce choices, spread out 2FA
3. Add passkeys as optional, but be persistent
 1. Create processes for your support team

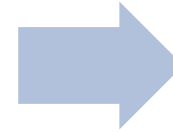
ROWND

robert@rownd.io

1. Take a Risk Based Approach



2. Understand your options



3. Layer your defenses

- Digital Identity Guidelines
 - Digital Identity Model & Risk Management ([SP 800-63-4](#))
 - Identity Proofing & Enrollment ([SP 800-63A-4](#))
 - Authentication & Authenticators ([SP 800-63B-4](#))
 - Federation & Assertions ([SP 800-63C-4](#))
- Digital Identity Guidelines – Implementation Resources ([NIST SP 800-63-3 Implementation Resources](#))
- Digital Identity – Mobile Driver's License (<https://www.nccoe.nist.gov/projects/digital-identities-mdl>)
- MFA for e-Commerce (<https://www.nccoe.nist.gov/multifactor-authentication-e-commerce>)



Questions?

Thank You for Joining Today's Webinar!

FOR FURTHER INFORMATION OR QUESTIONS ABOUT NIST'S
SMALL BUSINESS CYBERSECURITY RESOURCES:



smallbizsecurity@nist.gov