authenticate 2023

THE FIDO CONFERENCE

find me online

timcappalli.me

# Passkeys 101

**Tim Cappalli**

Identity Standards Architect @ Microsoft


Signature Sponsors:

1Password | Microsoft | yubico | Google

authenticatecon.com

SC MEDIA
A CyberRisk Alliance Resource

LOG IN REGISTER

Email security, Phishing

# Zimbra credentials targeted in global phishing campaign

Simon Hendery August 18, 2023

Log In

0% 20% 40% 60% 80% 100% 0% 20% 40% 60% 80% 100%

83% of breaches involved External actors (n=5,177)

74% of breaches involved a human element (n=4,482)

Creds

Phishing

we all know how prevalent phishing has become

siliconANGLE

## Credential phishing volume increases 527% in the first quarter

BY DUNCAN RILEY

A new report released today by phishing detection and response solutions company Cofense Inc. details a stagg credential phishing volume in the first quarter and an overall increase in active threats.

In the first quarter, Cofense detected a 527% increase in credential phishing volume from the previous quarter, a as "volatile." The volume increase year-over-year was more moderate, though still a significant 40% increase fro quarter of 2022. Notably, the main spike in credential phishing volume occurred in March, significantly exceeding February.

Emotet, long a favorite among cybercriminals and once described as "the world's most dangerous malware," was the most

CHECK POINT

SECURITY JUNE 19, 2023

## 'Sign in to continue' and suffer : Attackers abusing legitimate services for credential theft

By Itamar Biran And Golan Cohen

# Hackers don't break in.
# They log in.

username + password

+ OTP (SMS)

+ OTP (app)

+ OTP (email)

+ app push

username + email magic link

username, then OTP (SMS), then password

username, then magic link, then password

password

SMS OTP

email OTP

magic link

app push

password

SMS OTP


email OTP


magic link

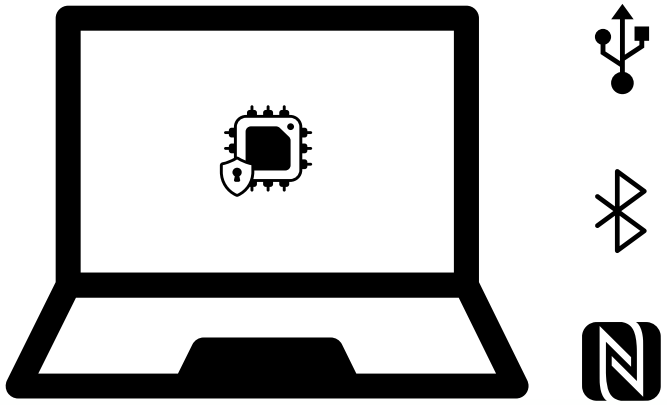

app push

username, then password, then ***FIDO security key***

phishing resistant

# Phishing Resistance

## proximity



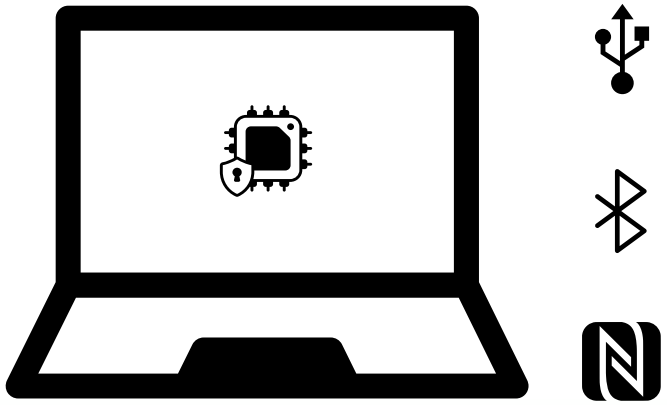
## verifier name binding

tim@mymail.com
`login.capptoso.com`

- ✓ login.capptoso.com
- ✗ login.capptoso.com.site.xyz
- ✗ myaccount.com
- ✗ login.capptoso.com

# Phishing Resistance

## proximity



## verifier name binding

tim@mymail.com
`login.capptoso.com`

- ✓ login.capptoso.com
- ✗ login.capptoso.com.site.xyz
- ✗ myaccount.com
- ✗ login.capptoso.com
  `Iogin.capptoso.com`

# OK, problem solved, right?

# RIGHT?!

# No.

still need a password

need multiple security keys

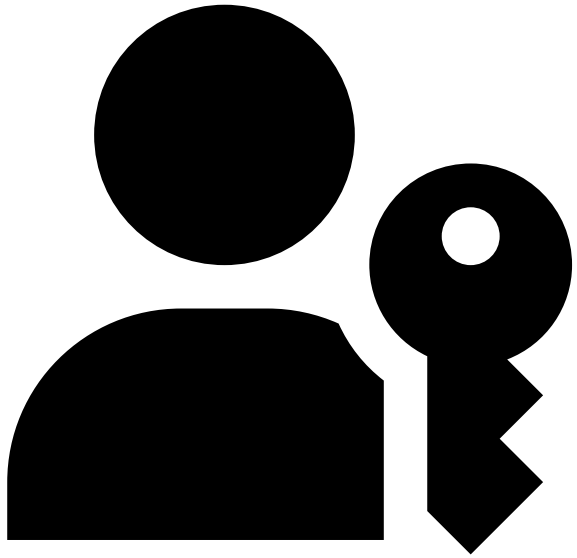
confusing user experience

what if we had just ***one*** credential

that was ***phishing-resistant***

with a great ***user experience***

that was ***always available*** when you need it?



# passkeys

# **passkeys**

are replacements for

*passwords*

*(and all the baggage that comes with them)*

# Four Pieces

a new name

a new icon

a new flavor

new features

# A New Name!

discoverable credentials

FIDO credentials

WebAuthn
discoverable credentials

FIDO2 credentials

***passkeys***

a password

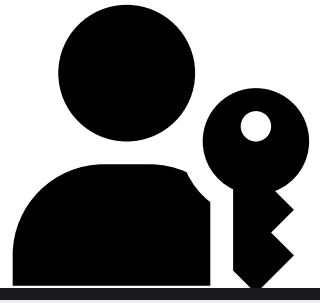
a passkey

common noun

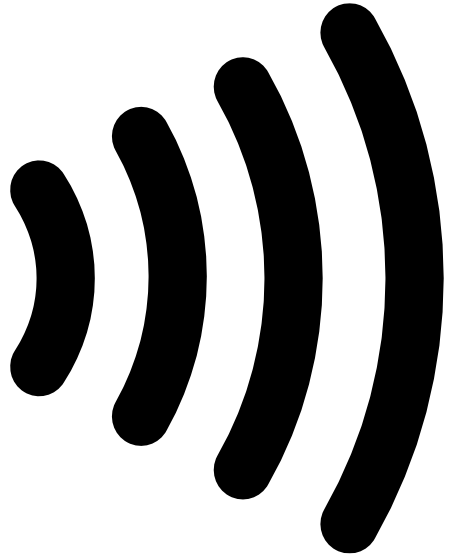
passwords

passkeys

# but what actually is it?

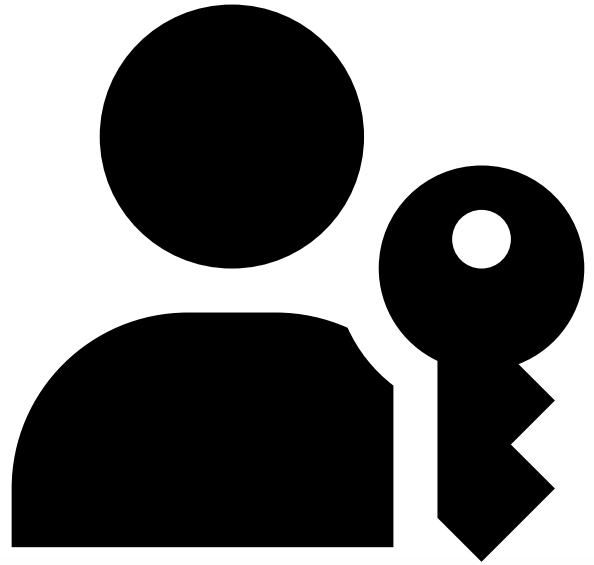


| | | | | | |
|---|---|---|---|---|---|
| `1a2b3c` | | | `uid9a8b` | `capptoso.com` | `Tim Capptoso` |
| credential identifier | private key | public key | user identifier | relying party identifier | metadata |



# A New Icon!

???



# New Flavor!

***synced***

passkeys

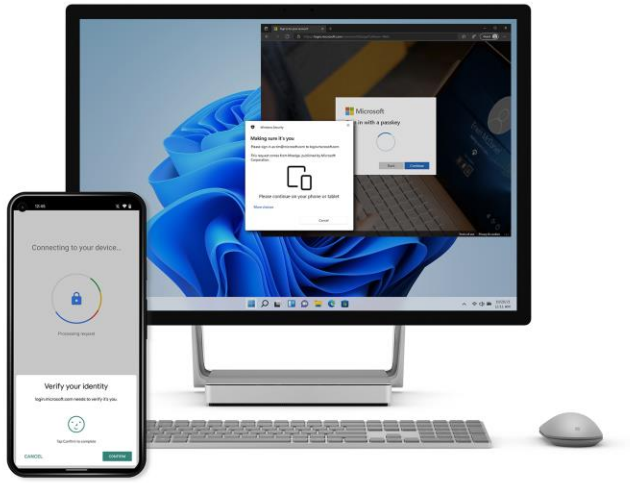
# What About Security Keys?

***synced***
passkeys

***device-bound***
passkeys

# Some New Features!

Autofill UI



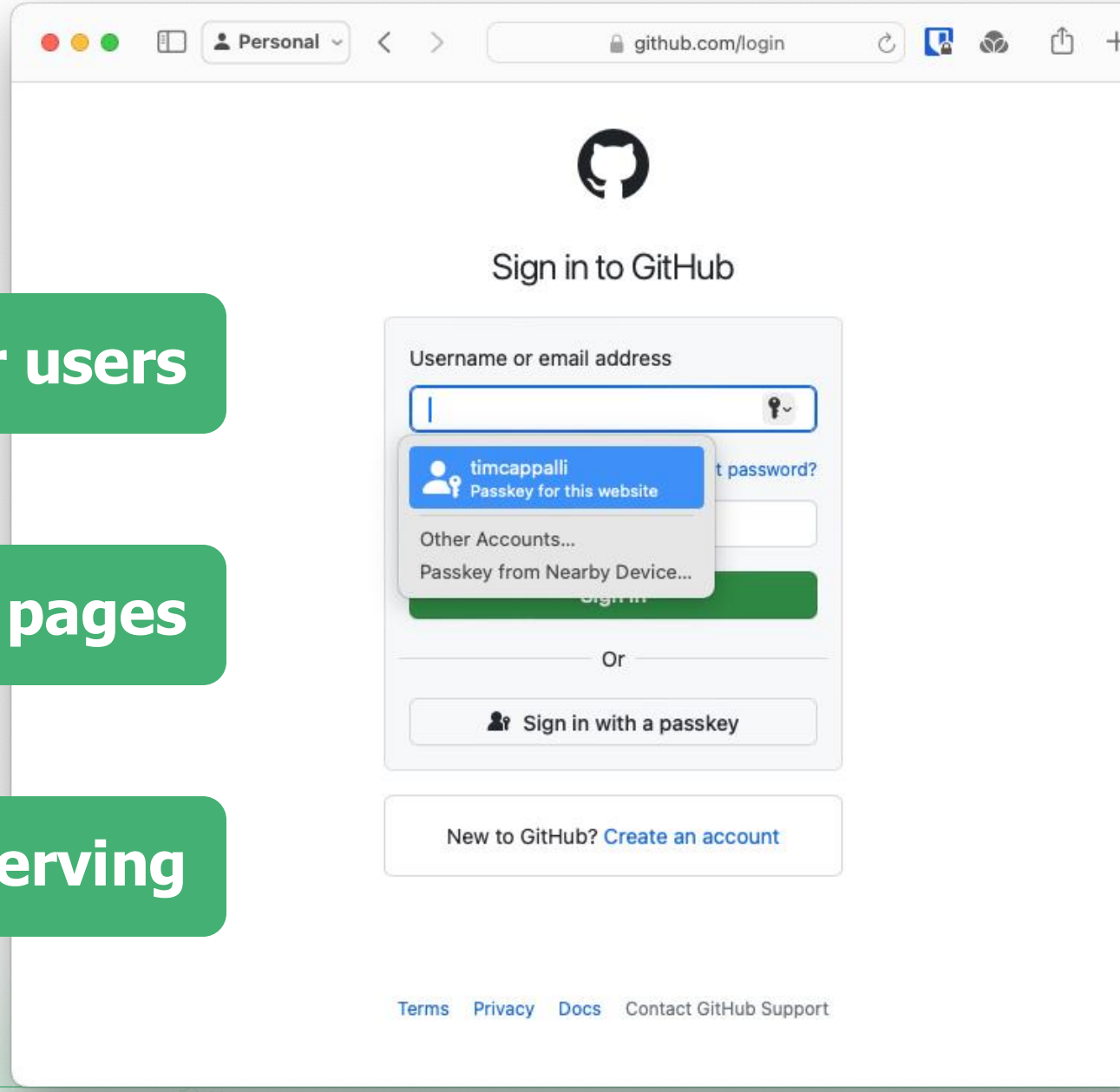
Cross-Device Authentication

# Autofill UI

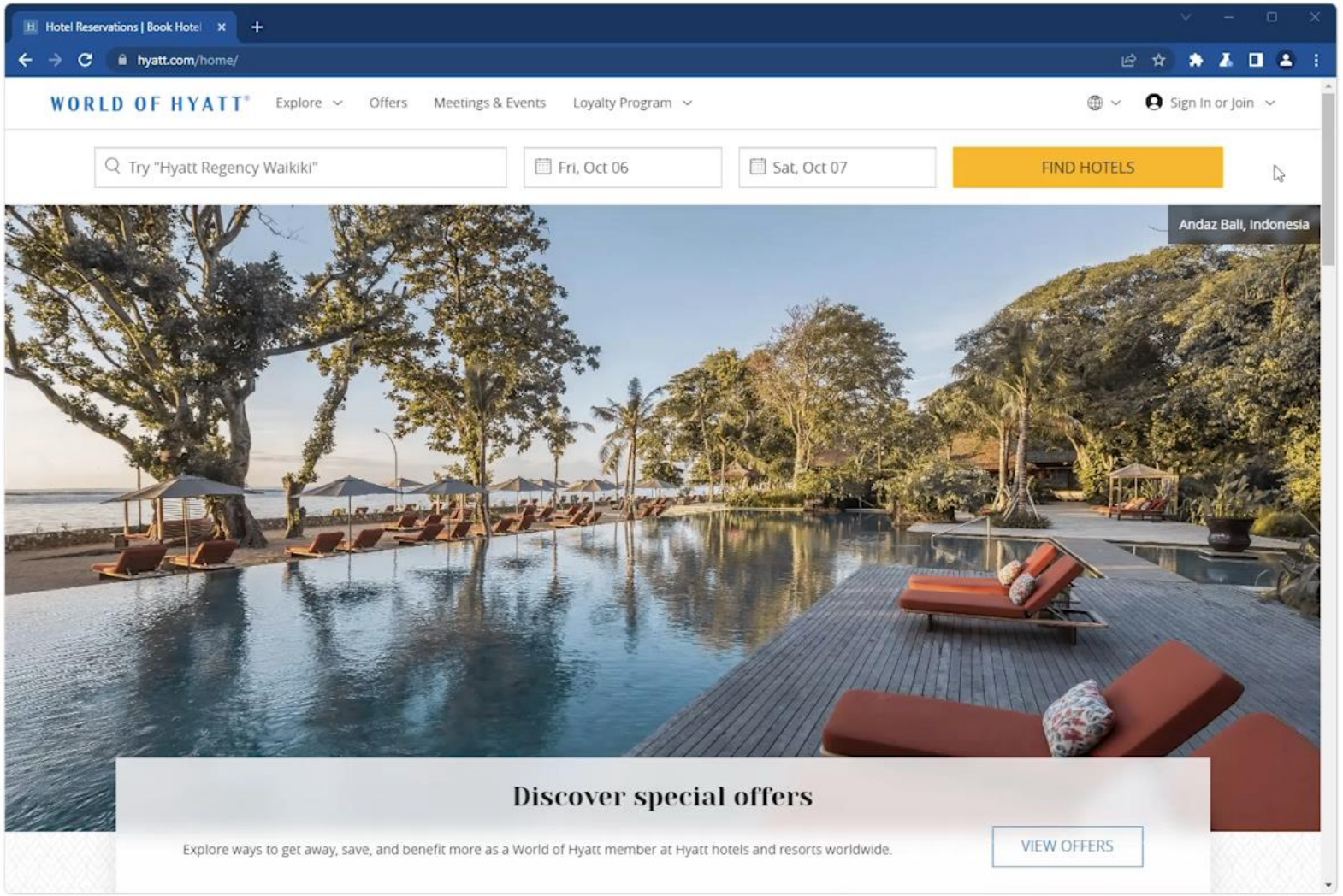
familiar experience for users

easy addition to existing sign in pages

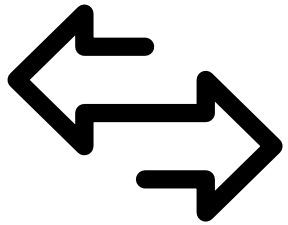
dynamic & privacy preserving



# Cross-Device Authentication

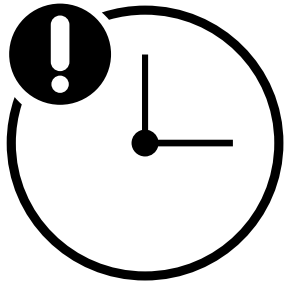


# Cross-Device Authentication



Bootstrapping

Shared Devices



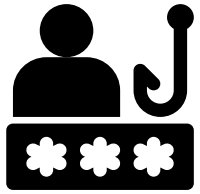
Temporary Access

# Why Passkeys?

**1:1**

Unique Credential
Per Service

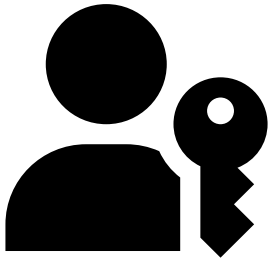
Standards-based



Phishing
Resistant

Asymmetric Cryptography
without a PKI

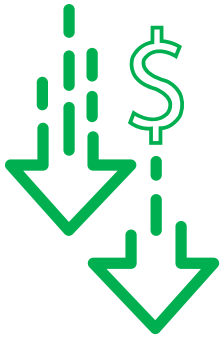
Natively
Supported



# passkeys

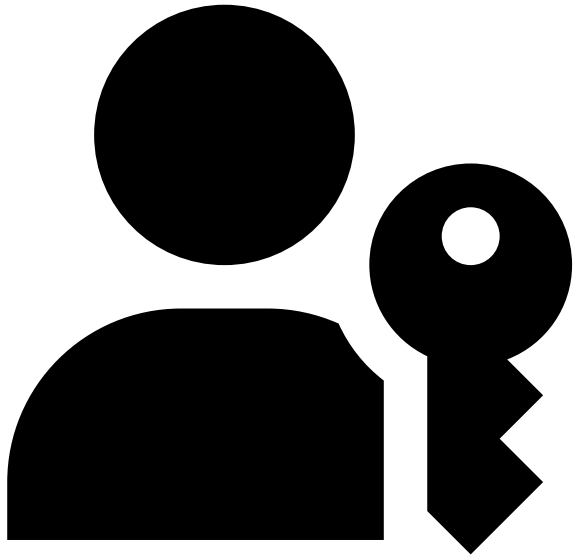
phishing resistant

happier users



lower costs

better account security



# Start your journey towards passkeys!

authenticate 2023

THE FIDO CONFERENCE

# Thank you.

Signature Sponsors:

1Password | Microsoft | yubico | Google

authenticatecon.com