Google

Account Protections

a Google Perspective

Elie Bursztein
Google, @elie

with the help of **many** Googlers

updated March 2021

Security and Privacy Group

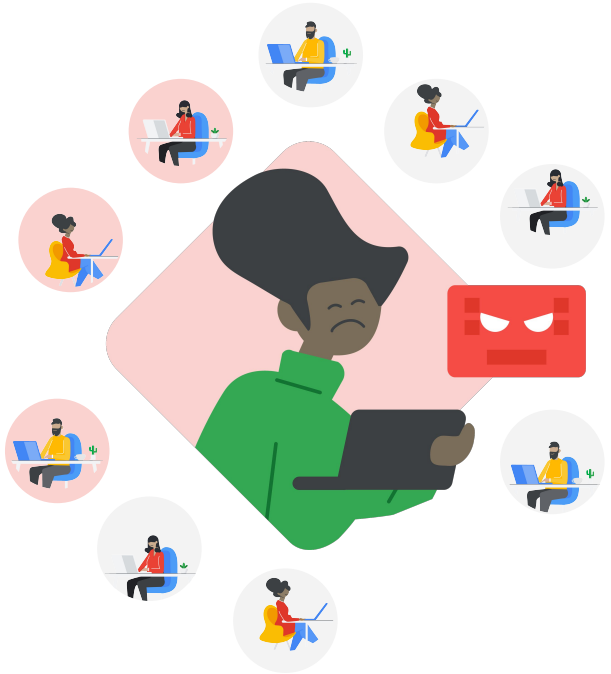
Slides available here:

https://elie.net/account

4 in 10

US Internet users report having their online information compromised

Source
the United States of P@ssw0rd$ - Harris / Google poll



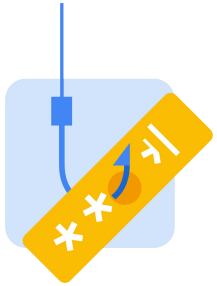
Google

Security and Privacy Group

How do attacker compromise accounts?

Main source of compromised accounts

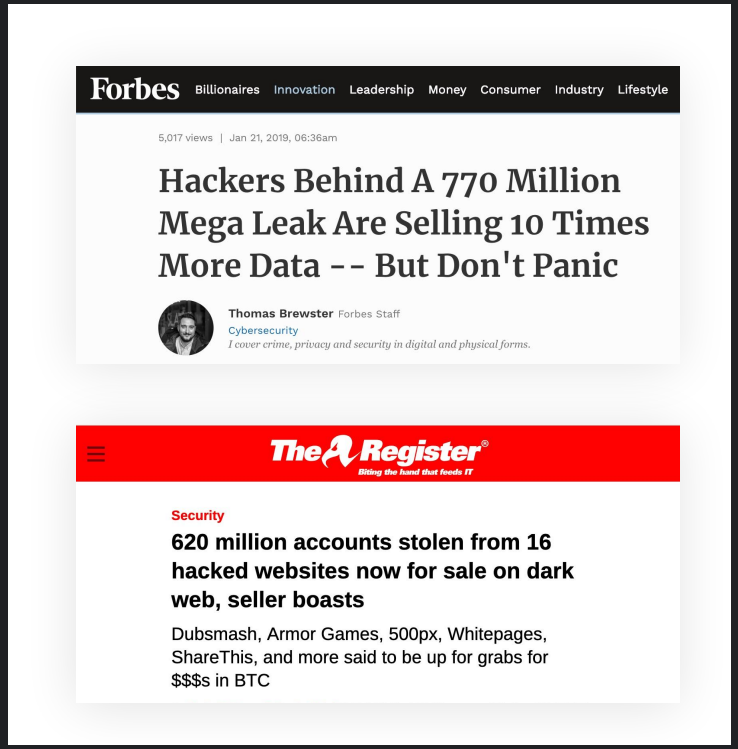
Data breach



Phishing

Keyloggers

The blackmarket is fueling the account compromised ecosystem



Forbes Billionaires Innovation Leadership Money Consumer Industry Lifestyle

5,017 views | Jan 21, 2019, 06:36am

Hackers Behind A 770 Million Mega Leak Are Selling 10 Times More Data -- But Don't Panic

Thomas Brewster Forbes Staff

Cybersecurity

I cover crime, privacy and security in digital and physical forms.

The Register®

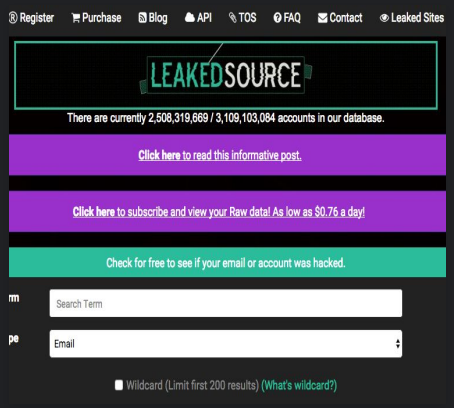
Biting the hand that feeds IT

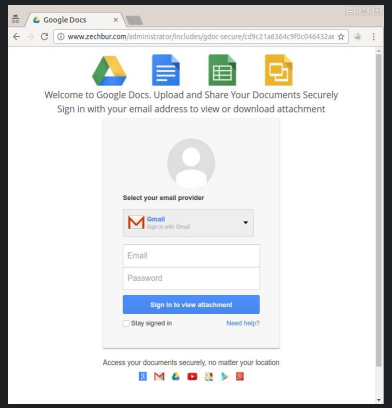
Security

620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts

Dubsmash, Armor Games, 500px, Whitepages, ShareThis, and more said to be up for grabs for $$$s in BTC

Accounts and hacking tools are readily available on the blackmarket



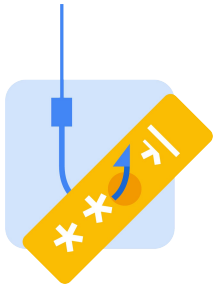


Google

Security and Privacy Group

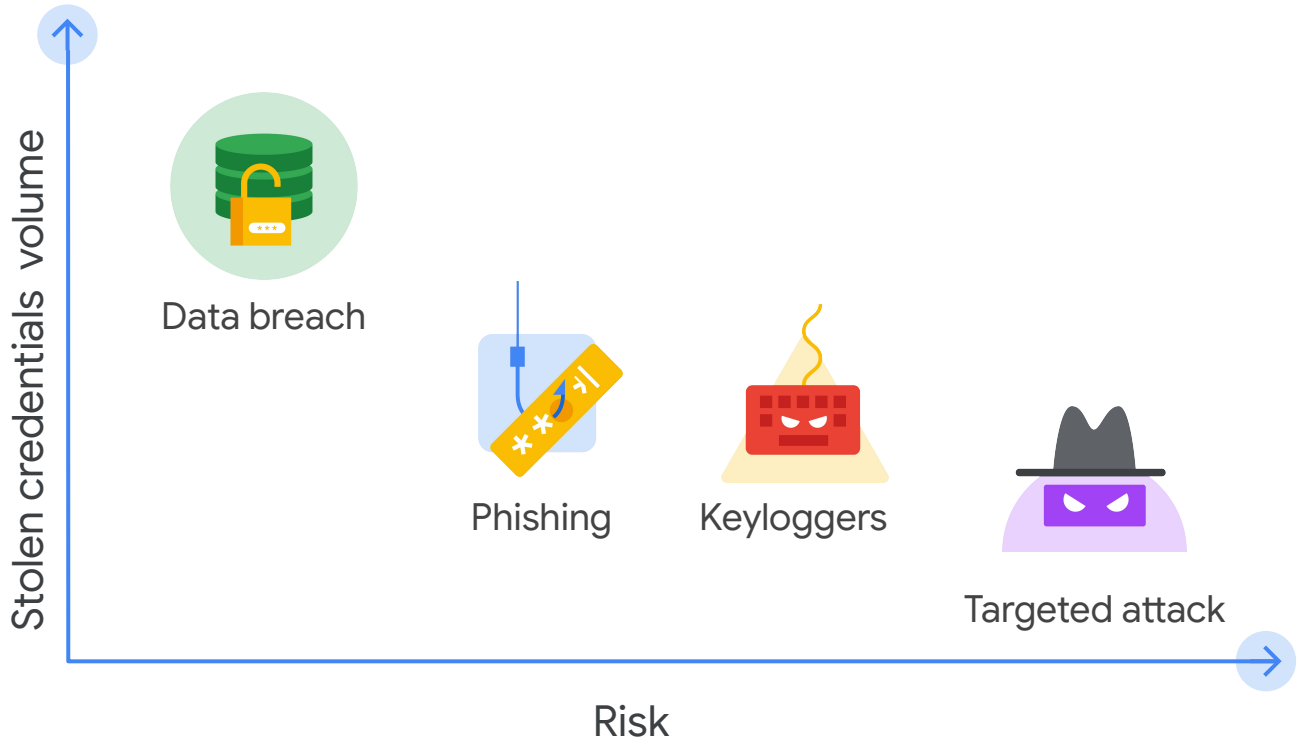
Volume of credentials stolen in 2016: *a lower bound*

Data breach
4.3B+



Phishing
12M+

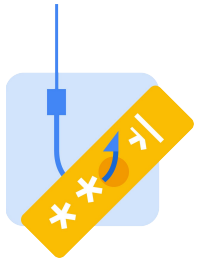
Keyloggers
1M+


Stolen credentials volume
Data breach
Phishing
Keyloggers
Targeted attack
Risk

Stolen credential origin takeaways

The black market fuels account compromise

Password reuse is the largest source of compromise



Phishing and keyloggers poses a significant risk

How can we prevent account compromise?

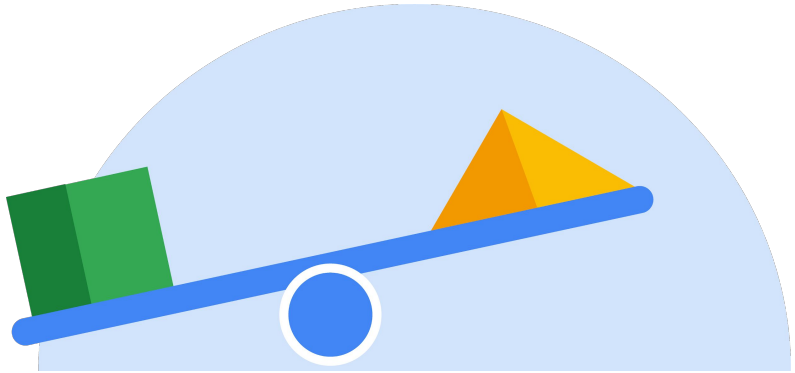
Defense in depth leveraging many competing technologies

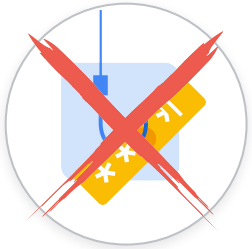
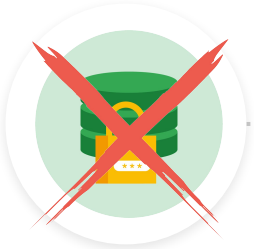
Google

Security and Privacy Group

Increasing security comes at the expense of additional friction including lock-out risk, monetary cost, and user education

Each security solution offers a different trade-off which makes security a complex balancing act between usability and security

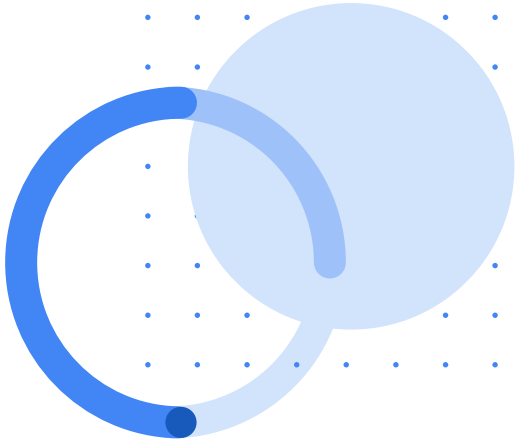


Credentials are stolen	Stolen credential database is built	Accounts are compromised	At risk users face advanced attacks
			
Preventing credential theft	Resetting leaked credentials proactively	Preventing unauthorized login	Advanced protection

Today: combining key technologies to offer the best account security and usability possible

Part 1

Preventing credentials theft



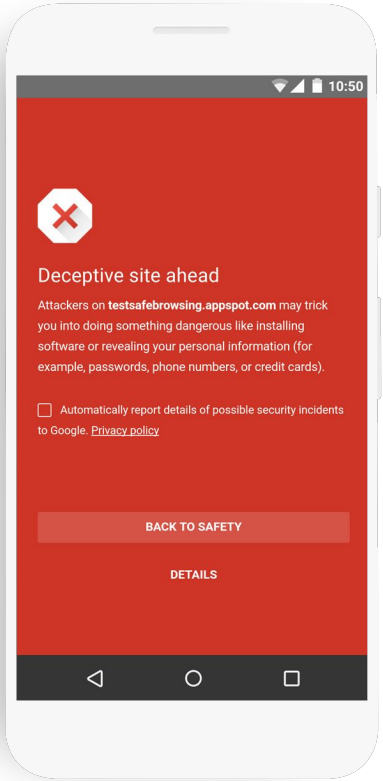
Google

Security and Privacy Group

Build large scale AI powered systems to detect and block threats at scale before they reach users

Google

Security and Privacy Group

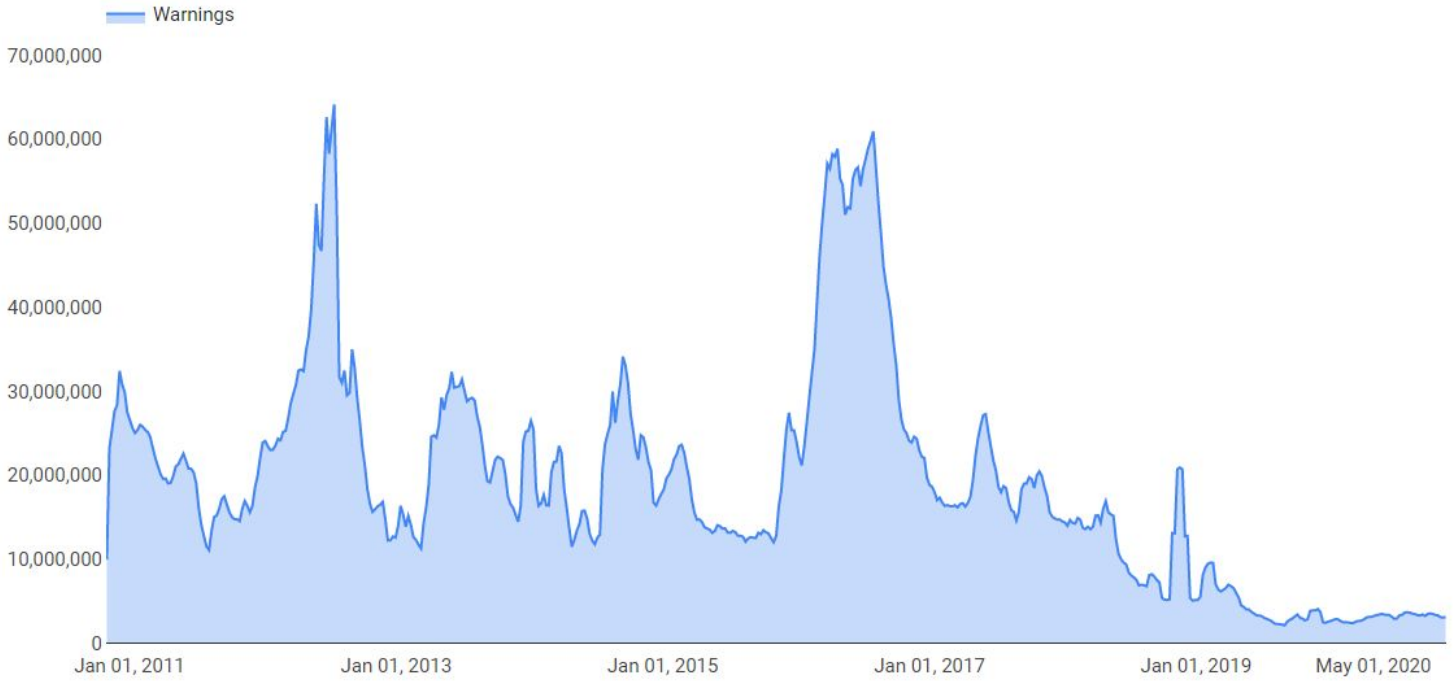


Safe Browsing warnings protects over 4 billions devices from phishing, malware

Google

Security and Privacy Group

Millions of warnings displayed weekly

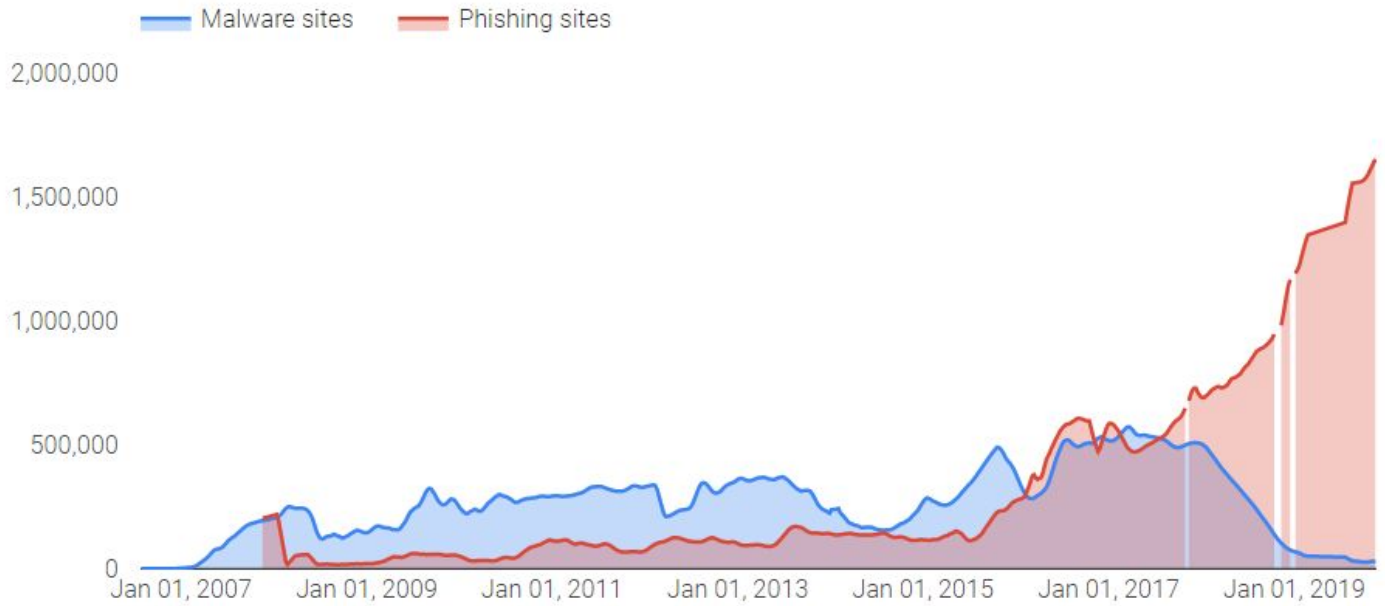


Google

https://transparencyreport.google.com/safe-browsing/overview

Security and Privacy Group

Attackers are shifting to phishing



Everyday Gmail blocks over 100M+ phishing emails

Cats through the age

2000 BC

1200 AC

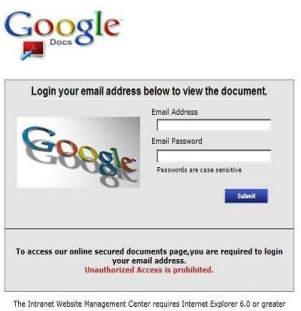
1800 AC

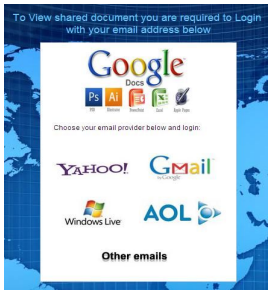
2020 AC

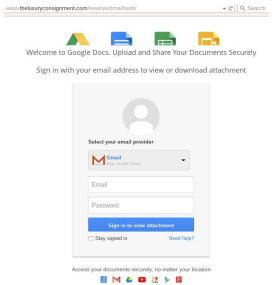
Google

Security and Privacy Group

Drive phishing through the ages





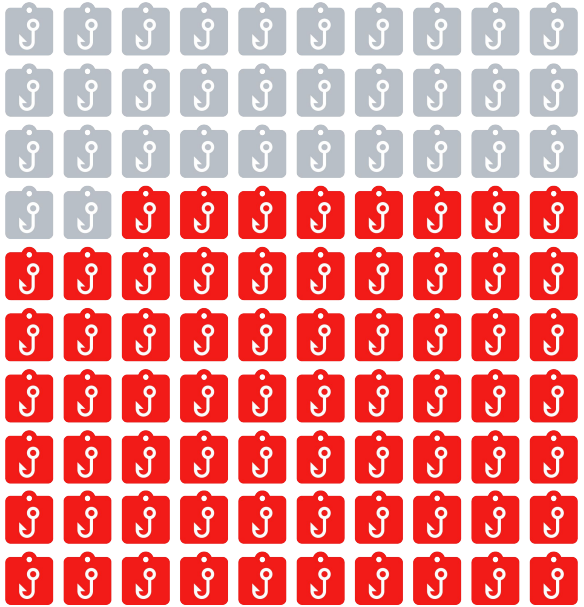


Google

Security and Privacy Group

68%

of phishing emails blocked by Gmail are different from one day to the next



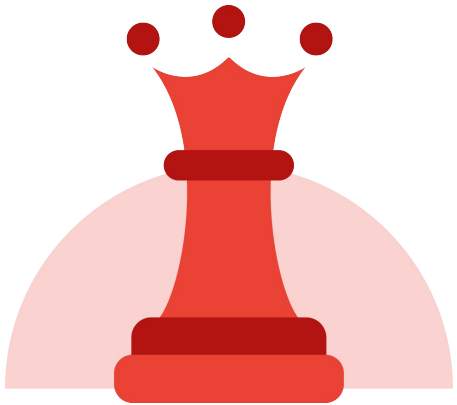
Google

[Deconstructing the Phishing Campaigns that Target Gmail Users]

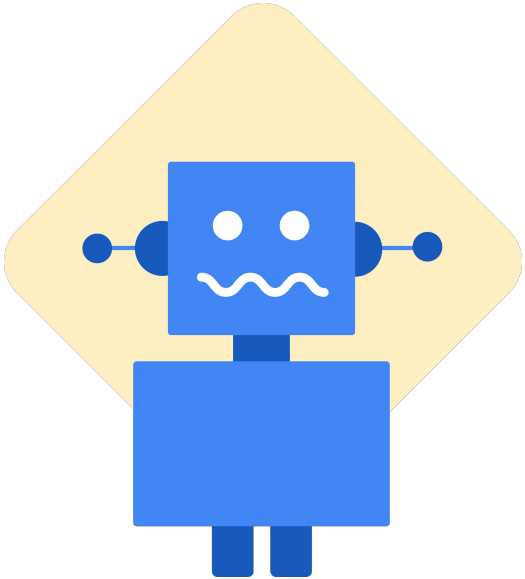
Security and Privacy Group

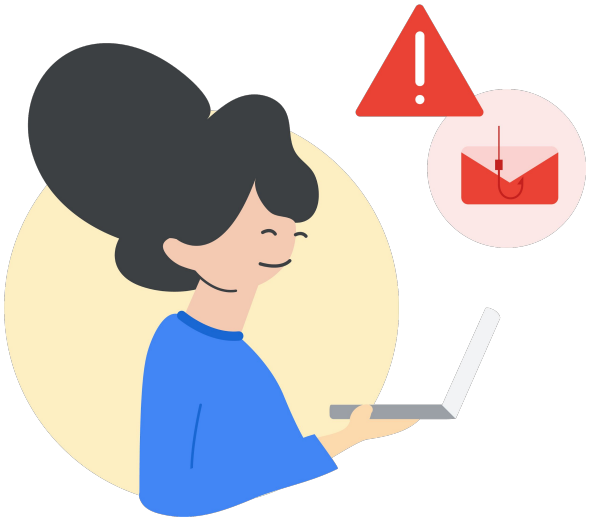
Keeping up with constantly evolving attacks requires continuously improving and retraining detection systems.

As in evolution the red queen hypothesis applies: it takes all your running to stay ahead of attackers.



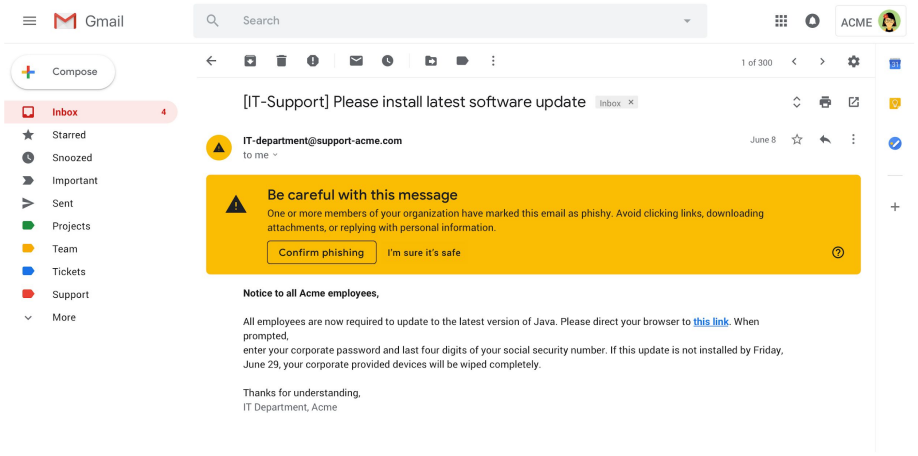
How to deal with a borderline case?





Provide as much context as possible and rely on user to make the final decisions

Gmail inbox soft warnings help users decide which emails are phishing



Google Cloud

45%

of Internet users don’t know what phishing is

Google

Security and Privacy Group

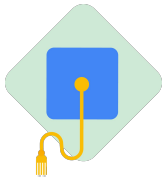
Takeaways

Prevention is a critical first defense layer

It protects billion of users across the world from being phished and infected

Keeping up with attack evolutions requires constant improvements

Attackers actively attempt to evade detection thas are major hurdles to them



Education and warning design are a must

Make sure that users understand the risks and don’t get warning fatigue is very challenging

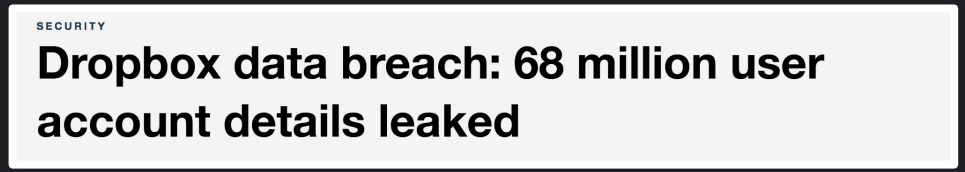
Section 2

Resetting compromised credentials proactively

Google

Security and Privacy Group

Third party data breaches keep surfacing


SECURITY

Dropbox data breach: 68 million user account details leaked


FORTUNE | Tech

SEARCH

CHANGING FACE OF SECURITY

LinkedIn Lost 167 Million Account Credentials in Data Breach


The New York Times

TECHNOLOGY

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

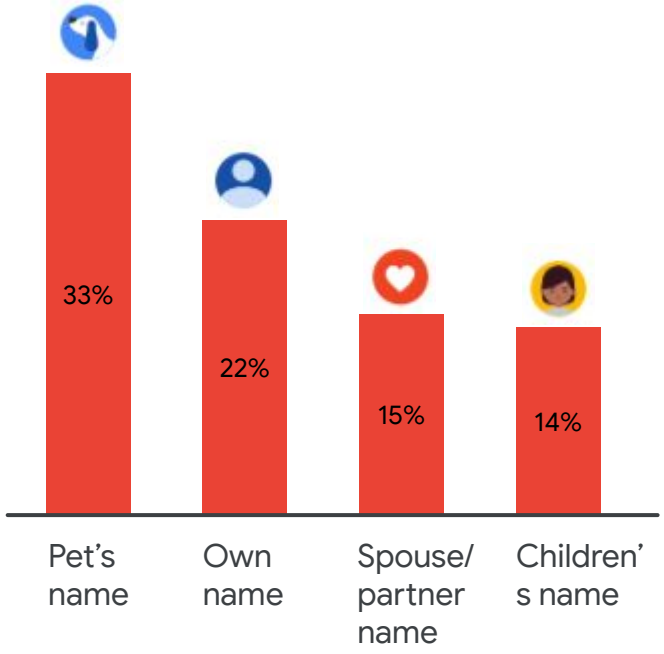
66%

Of US users reuse passwords across online services

Source: the United States of P@ssw0rd$ - Harris / Google poll

Google

Security and Privacy Group



59%

Of the U.S. adults use a name or a birthday into some of their online password

Source
[The United States of P@ssw0rd$ - Harris / Google poll]

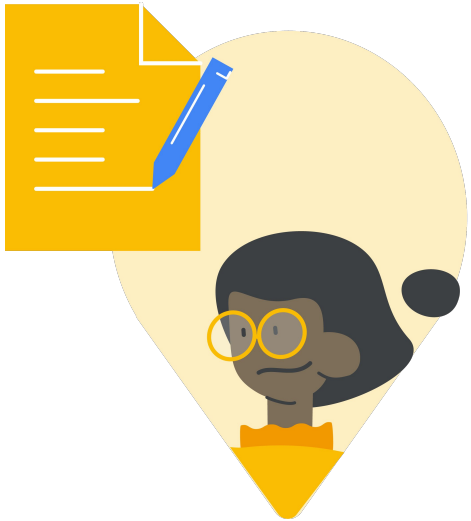
Get users to use a password manager

Google

Security and Privacy Group

15%

of US Internet users use a password manager. 36% use a piece of paper....



Source
[The United States of P@ssw0rd$ - Harris / Google poll]

Google

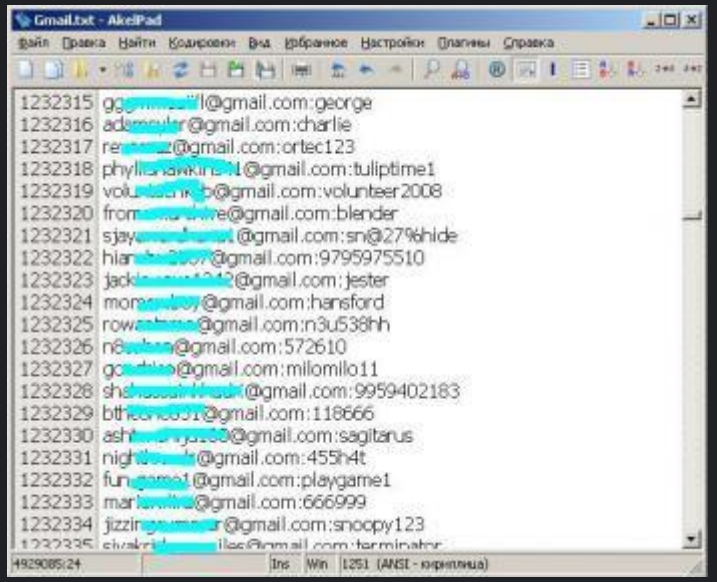
Security and Privacy Group

We need additional defenses to mitigate password reuse until password managers are ubiquitous

Google

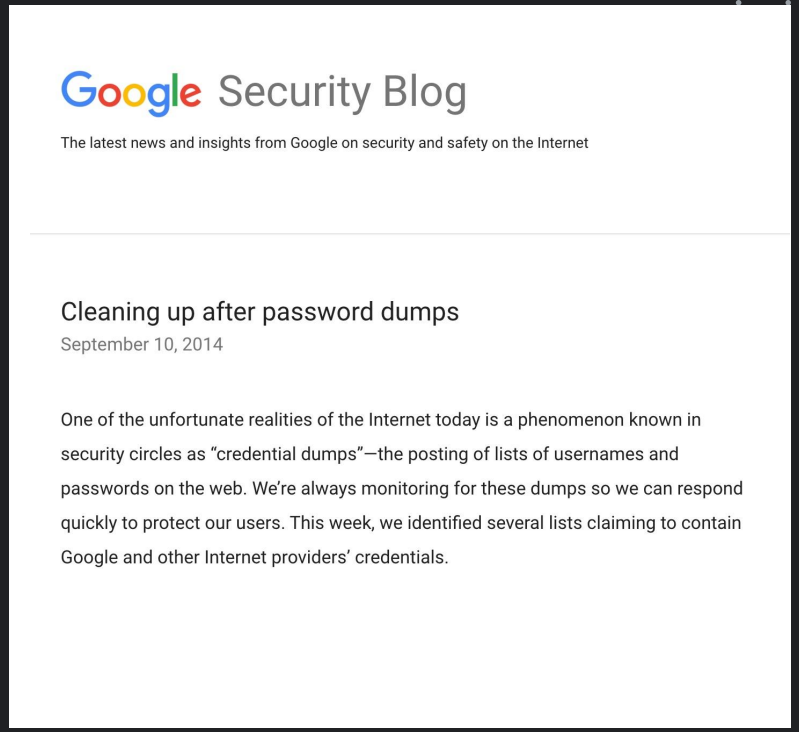
Security and Privacy Group

2014



Google

Security and Privacy Group



Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Cleaning up after password dumps

September 10, 2014

One of the unfortunate realities of the Internet today is a phenomenon known in security circles as “credential dumps”—the posting of lists of usernames and passwords on the web. We’re always monitoring for these dumps so we can respond quickly to protect our users. This week, we identified several lists claiming to contain Google and other Internet providers’ credentials.

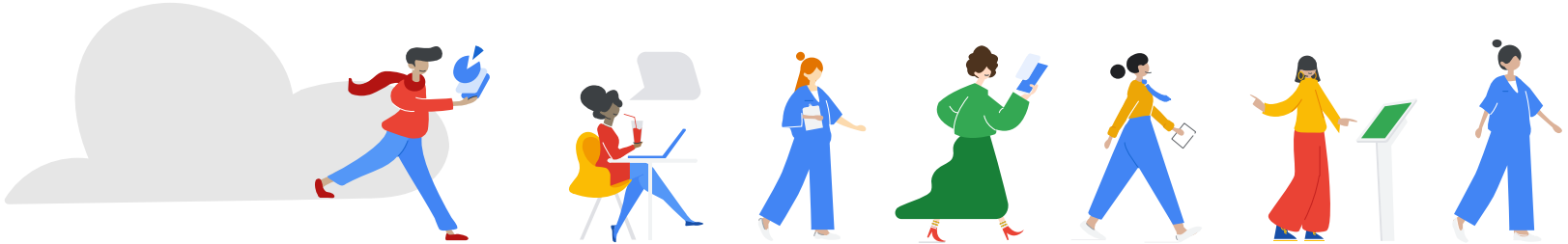
Disclosing the existence of our proactive breach password reset program

Google

Security and Privacy Group

110M+

Google accounts proactively re-secured



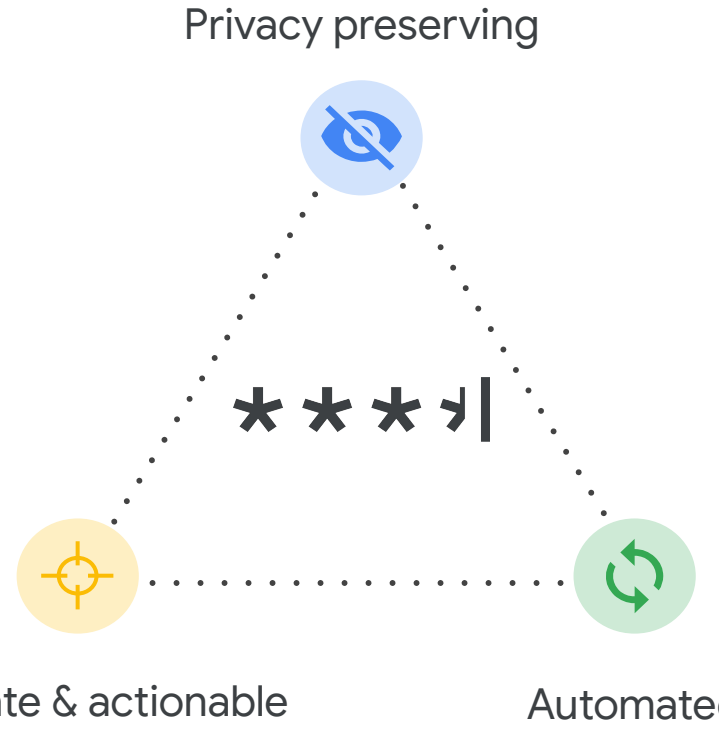
Google

Security and Privacy Group

How to protect all internet accounts against compromised password reuse?

Google

Security and Privacy Group



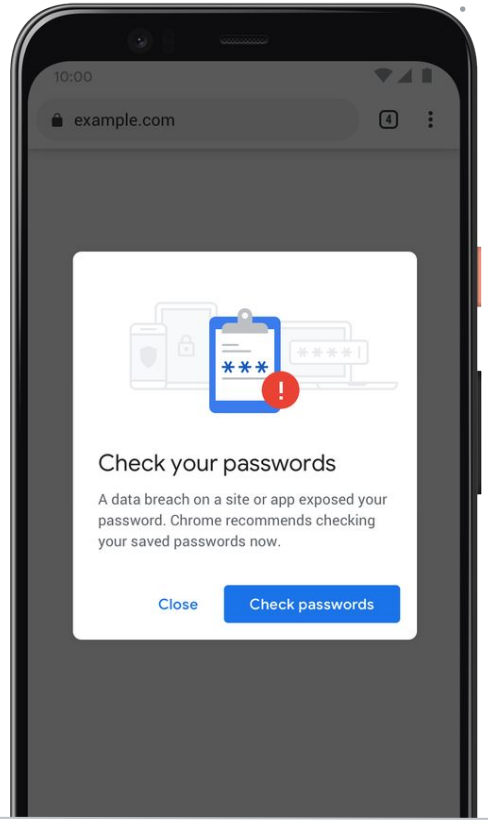
Ideal password warning system properties

Private set intersection

Allows users to query Google about the breach status of their usernames and passwords without revealing the information queried.

Additional cryptographic mechanism ensure that malicious actors can’t use the system to learn leaked username and password.

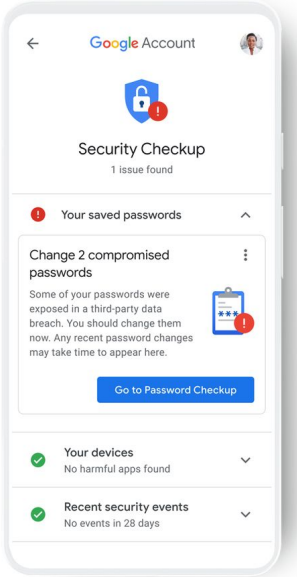
Password Checkup protects hundreds of millions of users from leaked passwords by displaying tens of millions of warnings weekly



Google

https://blog.google/technology/safety-security/keeping-private-information-private/

Security and Privacy Group

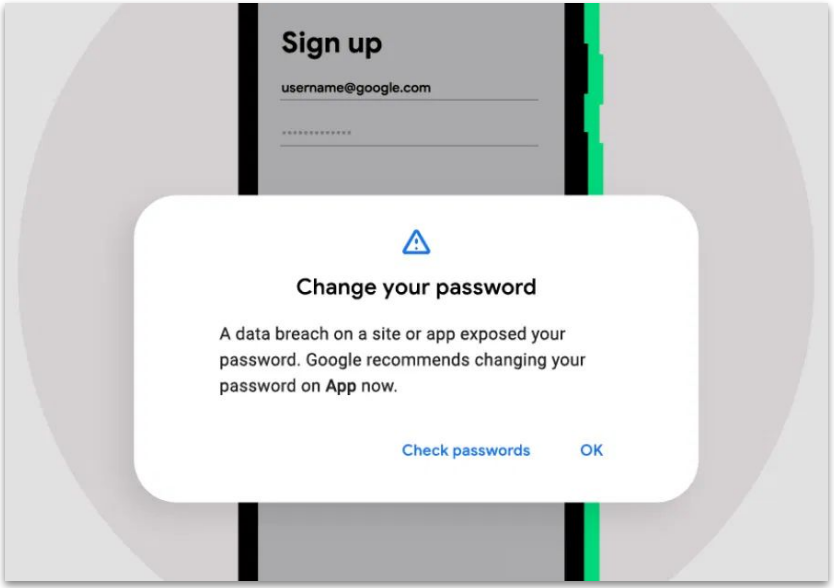


100M+ people have used Password Checkup, and they've seen a 30% reduction in breached credential usage

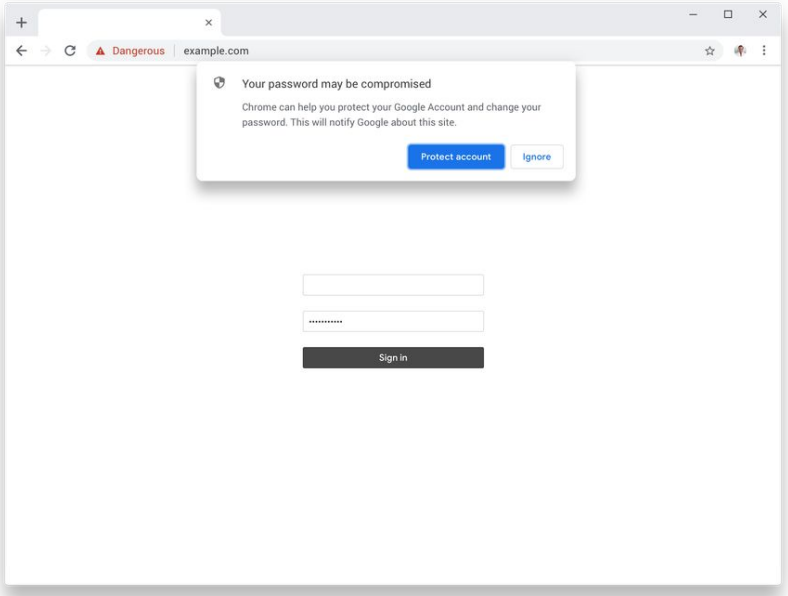
Google

https://blog.google/technology/safety-security/keeping-private-information-private/

Security and Privacy Group



Password check up on android



Predictive anti-phishing protection

Google

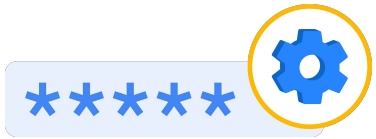
https://security.googleblog.com/2021/02/new-password-checkup-feature-coming-to.html

Security and Privacy Group

Takeaways

Proactive password protections greatly reduce malicious sign-in

People all too often choose easy to guess passwords

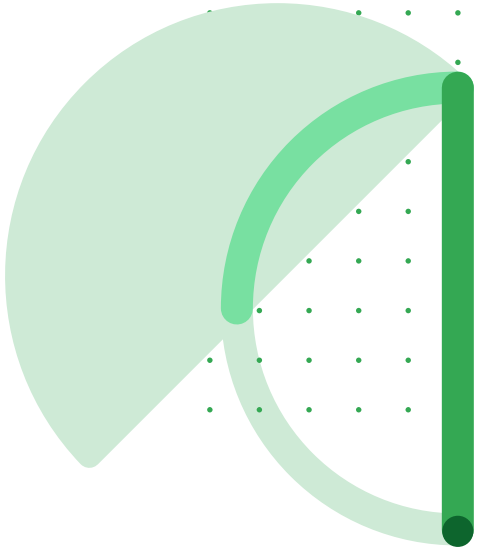


Password manager can solve a lot of those issues

Get users to realize how important this is for them

Section 3

Preventing unauthorized logins



Password only authentication is dangerous

Google

Security and Privacy Group

Use additional information

To prevent hackers logging in with compromised credentials

Google

Security and Privacy Group

Types of additional information

Who you are

What you have

What you know

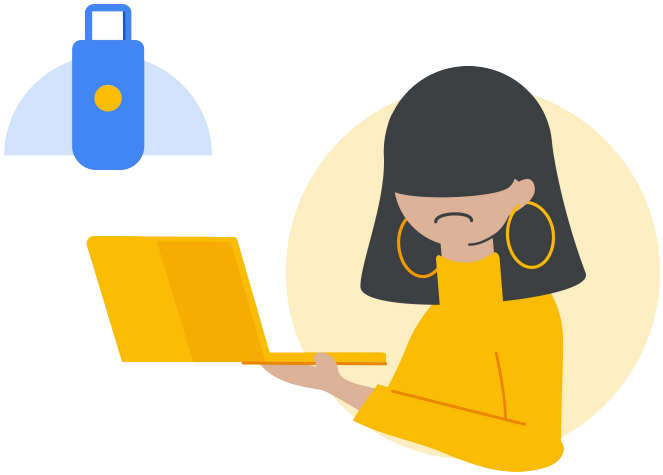
Mass adoption of two factor authentication is challenging

Google

Security and Privacy Group

37%

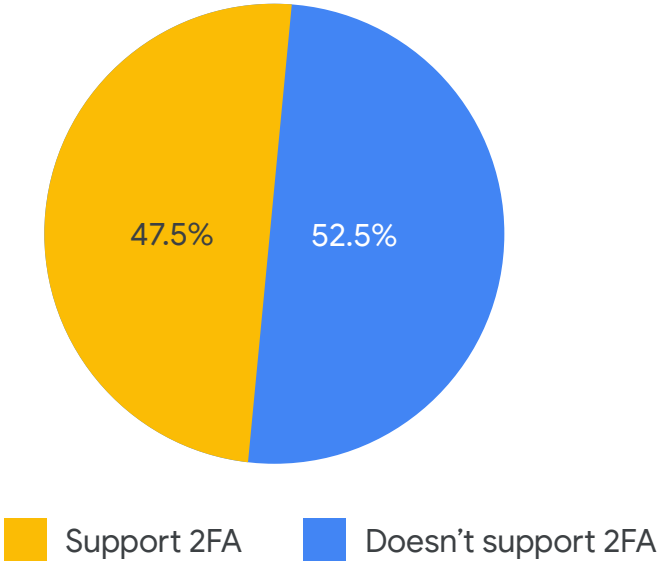
Of US internet users use two-factor authentication



Source
[The United States of P@ssw0rd$ - Harris / Google poll]

Google

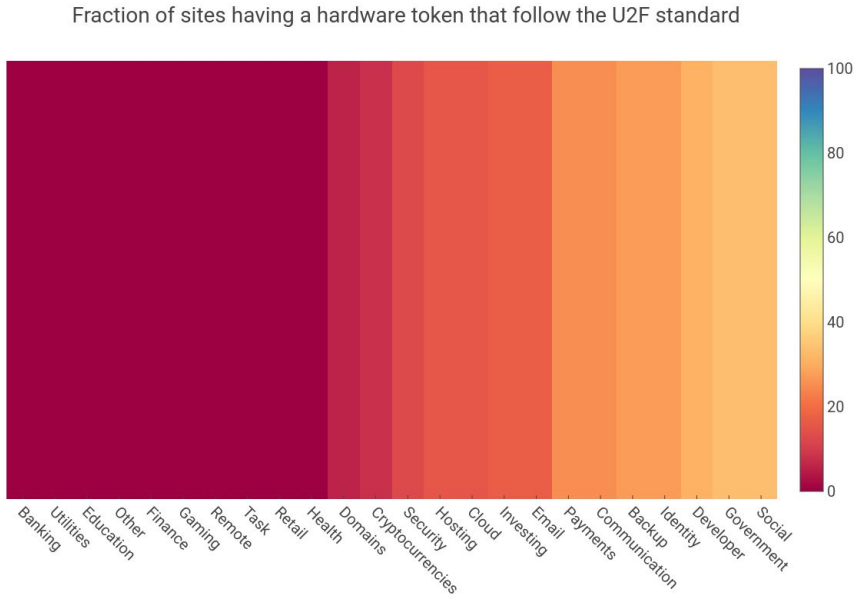
Security and Privacy Group



52.5%

of the online service don’t offer two factor authentication

Source
https://elie.net/blog/security/the-bleak-picture-of-two-factor-authentication-adoption-in-the-wild/



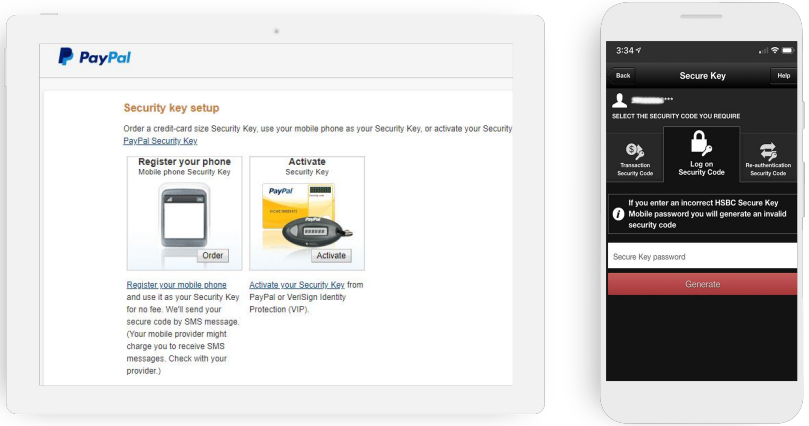
Some industries don't use standards

Google

https://elie.net/blog/security/the-bleak-picture-of-two-factor-authentication-adoption-in-the-wild/

Security and Privacy Group

Many sites marketing reuse terminology incorrectly and end-up confusing users

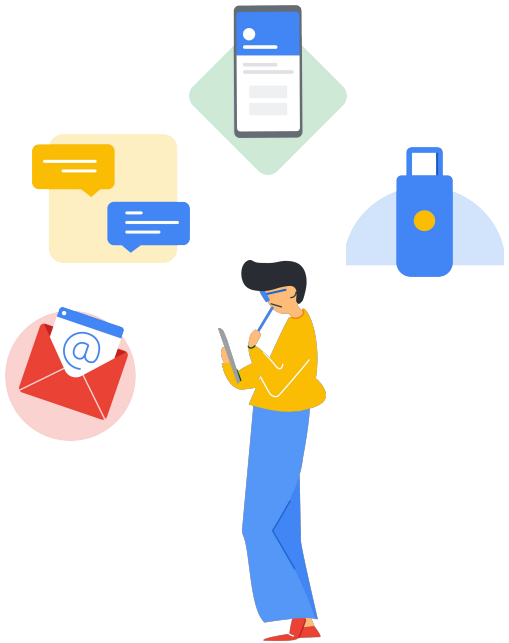


https://elie.net/blog/security/the-bleak-picture-of-two-factor-authentication-adoption-in-the-wild/

Google

Security and Privacy Group

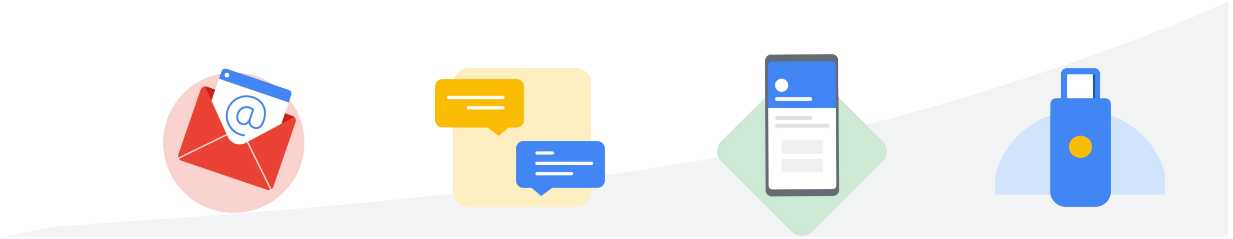
Which type of two factor authentication should we push for?



Google

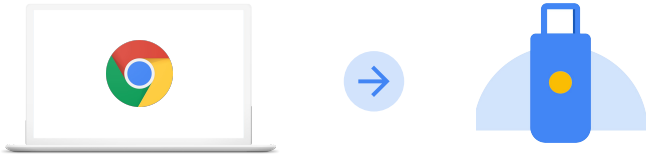
Security and Privacy Group

Not all 2FA technologies are equal



	Secondary email	SMS verification	Device prompt	Security key
Boutique phishing	68%	96%	99%	100%
Spear-phishing	53-100%	76%	90%	100%

Security keys are the most secure second factor against phishing



Physical key

Security key built into your phone

Google

Security and Privacy Group

How to speed up security key adoption?

Google

Security and Privacy Group

OpenSK

Say hello to OpenSK an open-source security key written in RUST

Google

Security and Privacy Group

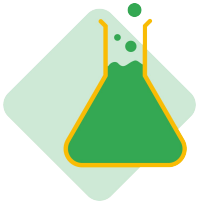
OpenSK: Design Philosophy

Open

Open source, no patents,
no NDAs, affordable.

Secure by design

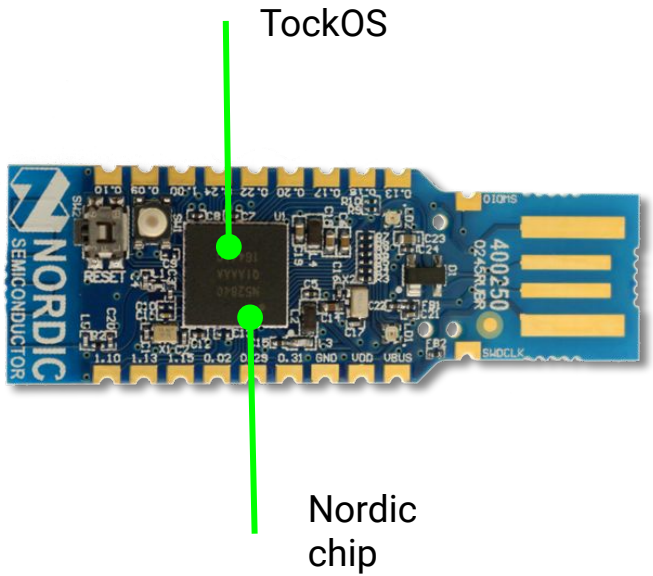
Memory-safe programming language, and secure OS.

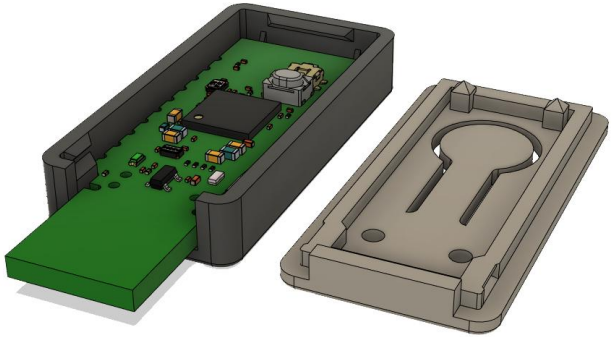


Research friendly

Cheap & easy to audit your own key, and attack it.

OpenSK: hardware





[Case 3D blueprint]

Paul Rascagnères @r00tbsd · Jan 30

New open source project from Google: **OpenSK**. A FIDO U2F and FIDO2 implementation for Nordic nRF52840 board. I'm not an expert but it looks like a #yubikey but with an open source firmware and 5 times cheaper... and great STL files to 3D print the case ;) github.com/google/OpenSK/...

Gary Explains @garyexplains · Feb 5

My @NordicTweets nRF52840 Dongle has arrived, so now I can try out @Google's **OpenSK** and build my own security key using TockOS and Rust!

The Register®
Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | DEVOPS | BUSINESS | PERSONAL TECH | SCIENCE | EMERGENT TECH | BOOTNOTES | VENDOR VOICE

{* SECURITY *}

Google's OpenSK lets you BYOSK – burn your own security key

Now there's no excuse

Tue 4 Feb 2020 // 10:30 UTC 33 GOT TIPS?

Tim Anderson BIO EMAIL TWITTER SHARE

OpenSK, a new open-source project from Google, lets folk make their own security key for less than £10.

You flash the OpenSK firmware on a Nordic dongle – and voila. The USB dongle includes the nRF52840 SoC (32-bit Arm Cortex-M4), supports Bluetooth Low Energy and NFC (Near Field Communication), as well as a user-programmable button. If you have a 3D printer to hand, you can also print a suitable enclosure.

// MOST READ

1 Microsoft's OS joins macOS and Linux at the Flutter party, but guess which one performs best? Hint: It's not Windows

2 Ethernet failure on Swiss business jet prompted emergency descent, say aviation safety bods

Help manufacturing OpenSK-based affordable security key for everyone

Since Feb'21 Feitan OpenSK research edition key [available on Amazon for $9.90](#) (not ready for production!)

Kayla Laree

★★★★★ Really cool project to bring FIDO2(CTAP2), FIDO U2F, W3C WebAuthN to mass adoption.

Reviewed in the United States on February 6, 2021

OpenSK implements FIDO2(CTAP2) and FIDO U2F specifications, it can support any website leveraging W3C WebAuthN.

Helpful | Report abuse

Edward Hugley

★★★★★ Great value

Reviewed in the United States on March 9, 2021

Verified Purchase

Supports most websites. Nice and small. Good design. Good value for what it does.

Helpful | Report abuse


fido™
CERTIFIED
L1
FIDO2

What's next? Major milestones

1	**FIDO 2.1 Certification**	OpenSK on track to be the first FIDO 2.1 certified key
2	**Bleeding edge features**	New features to make keys more secure and usable are actively developped
3	**Improved manufacturing**	Keep partnering with the industry to develop high quality affordable security keys

More information at:

https://github.com/google/opensk

Takeaways

Password are not enough

Password reuse and phishing makes credentials only login very risky

Strong two factors is the way to go

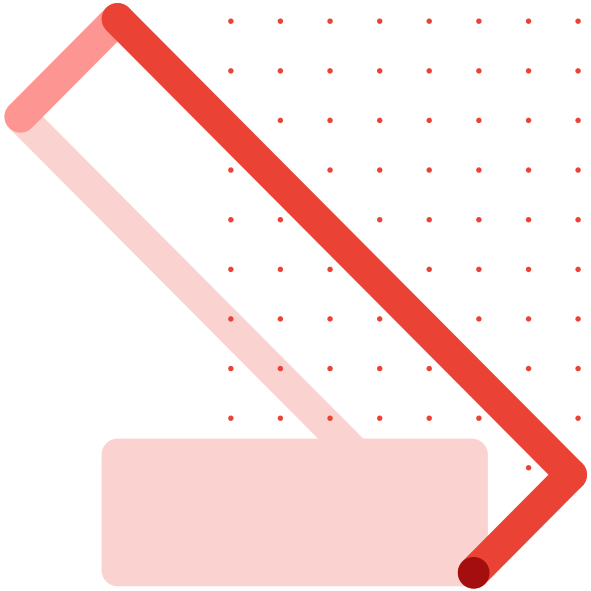
Not all 2nd factors are created equals we need to focus on strong two factor adoption

Industry wide adoption is still very distant

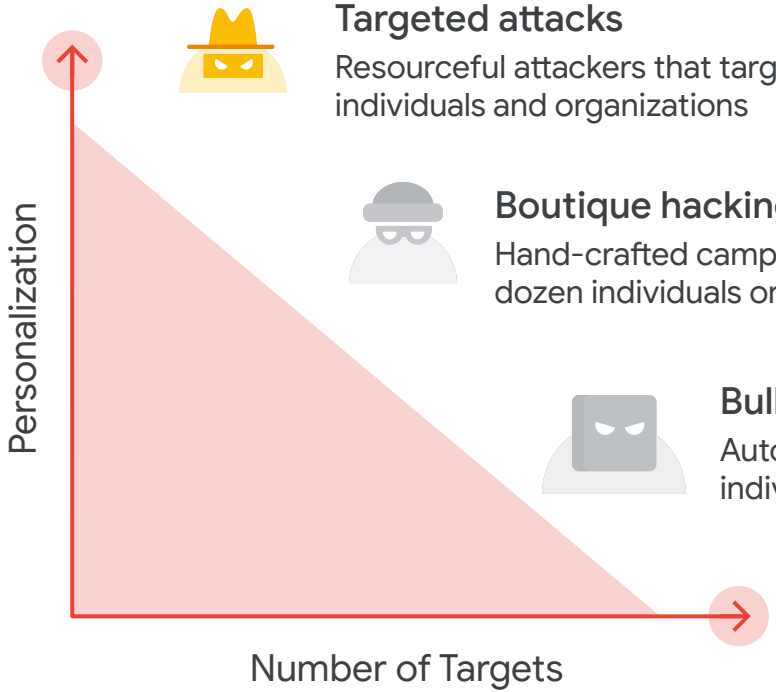
There are a lot of structural problem to solve before we get 2FA as universal as HTTPS

Section 4

Advanced protection



Large scale attacks don’t care which accounts they target



Targeted attacks

Resourceful attackers that target specific individuals and organizations

Boutique hacking

Hand-crafted campaigns targeting a few dozen individuals or organizations

Bulk hacking

Automated campaigns targeting many individuals and organizations

Accounts at risk of targeted attacks

Journalists & hacktivists

Politicians & campaign teams

Executives & Fintech users

Celebrities

Key threats faced by targeted users

Spear-phishing

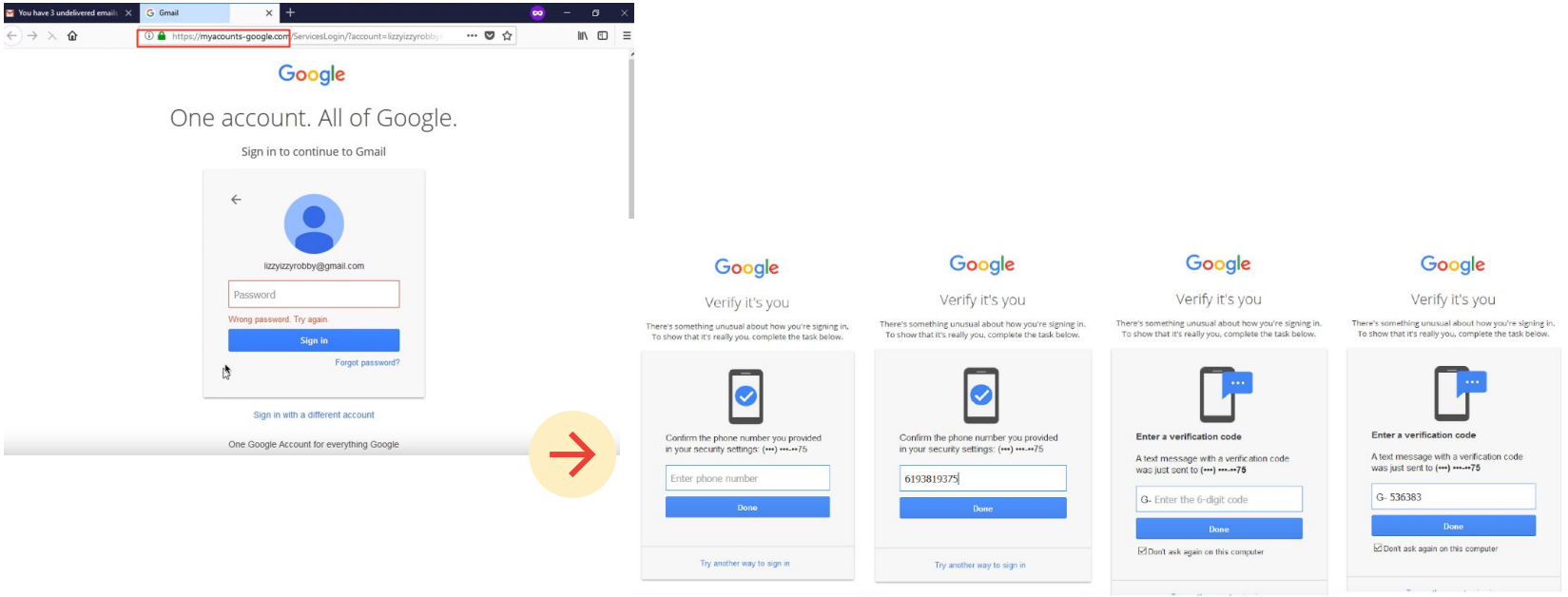
Handcrafted phishing attacks with two factor phishing is a common tactic against targeted users

Malicious oauth app

Attackers use oauth app to maintain persistent access to targeted users

Advanced account recovery impersonation

Attackers research their target background and use the collected data for impersonation and phishing purpose

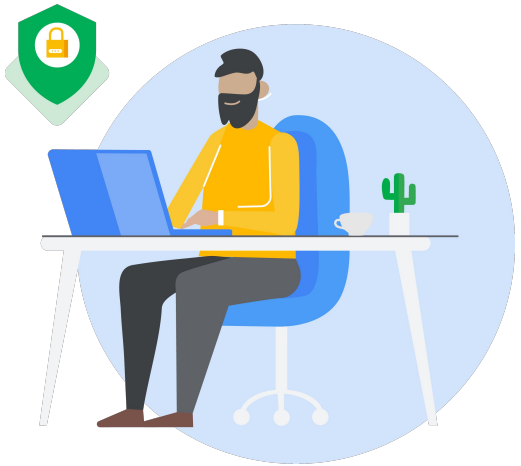


Realtime password verification and then phishing the SMS code

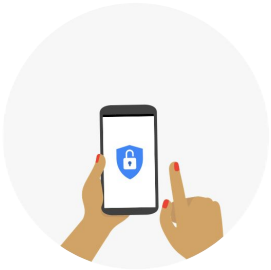
Google

Security and Privacy Group

Increase security further at the expense of additional friction

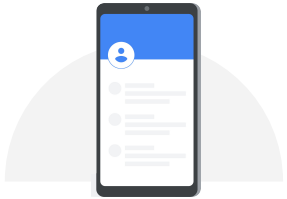


Lock-down login
Mandatory security keys



Protecting Session
Limit API Data Access

Protecting Session
Squeeze out malware



Account Recovery
Stronger Verification

Takeaways

Strong account security requires a defense in depth strategy

Constant improvements are needed to keep-up with adversaries

Additional protections are need for targeted users

Google

Effective account security requires tailoring your protections to meet your users needs

https://elie.net/account

Security and Privacy Group