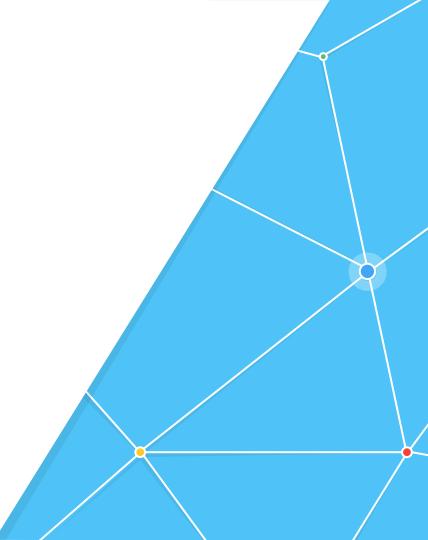
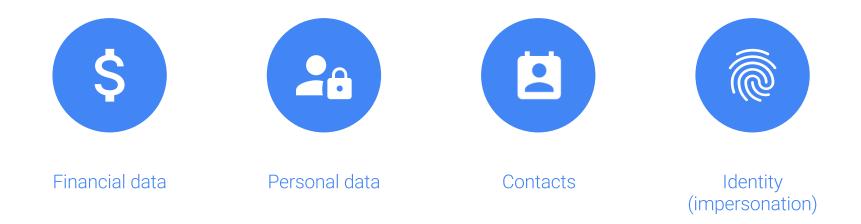
Research at Google

The Anatomy of Account-Takeover

Grzegorz Milka (grzegorzmilka@google.com)



Online accounts are valuable targets



Data breaches are always there

SECURITY

Dropbox data breach: 68 million user account details leaked

	The New York Times	
	TECHNOLOGY	
FORTUNE Tech	Yahoo Says 1 Billion User Accounts Were Hacked	
CHANGING FACE OF SECURITY LinkedIn Lost 167 Mil Breach	lion Account Credentials in Data	

And so are targeted hijacks

I was hacked Posted Aug 23, 2017 by John Biggs (ejonnbiggs)



https://techcrunch.com/2017/08/23/ i-was-hacked/

We want to protect **all users,** and today we discuss **passwords**.



Modern password authentication requires a **risk-aware**, **defense-in-depth** system.

Password theft ecosystem



The three avenues of password theft





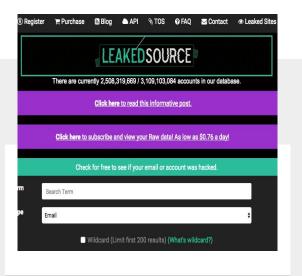


Commoditization of abuse

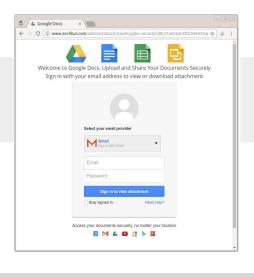




The wares on sale







Data breach market

Keyloggers

Phishing kits



Markets can be tracked

In 2016, we have collected over 4000 data breach dumps with over 3.3B credentials.



Users reuse passwords



12%-43%* reuse rate

*"Data breaches, phishing, or malware?"



Users reuse passwords





* internal estimate

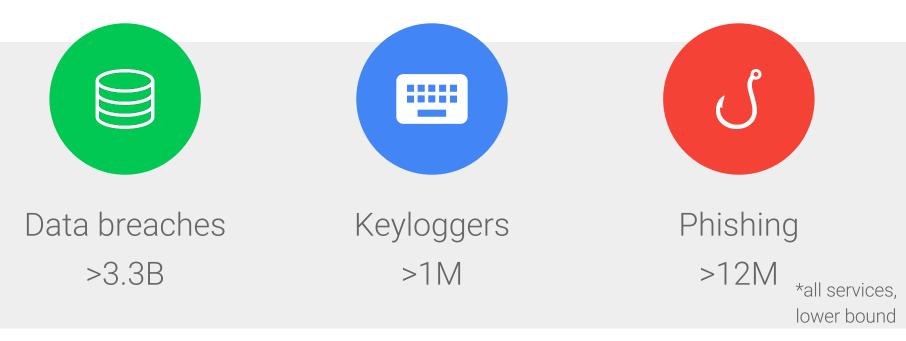


Number of valid Google passwords found in data breaches:

67 Million



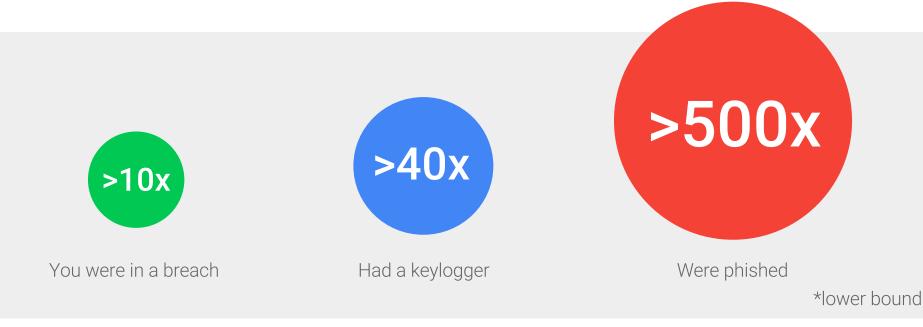
Volume of credentials stolen in 2016*





Hijacking likelihood*

Compared to a general active account, how much more likely it is that you will be a victim of hijacking if we know:





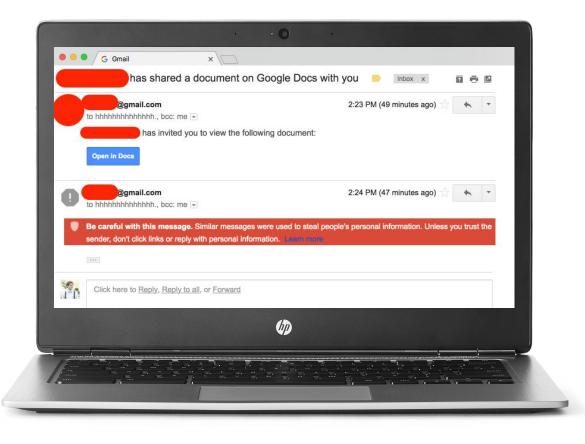
Prevention Sign-in risk detection Challenges



Key takeaway

Modern password authentication requires a risk-aware, **defense-in-depth** system.







A Safe Browsing

Deceptive site ahead

Attackers on **esty.adelawarriewood.com.au** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). <u>Learn more</u>

Automatically send some <u>system information and page content</u> to Google to help detect dangerous apps and sites. <u>Privacy policy</u>

DETAILS

Back to safety



We notify compromised users and ask them to change their password.



Prevention Sign-in risk detection Challenges





Password-only authentication is risky.



Adoption of additional security is low





Of active Google accounts Of Americans *Pew Research Center



Sign-in risk detection



Image courtesy of Dr Frank Stajano, "Passwords and the Evolution of Imperfect Authentication"



Dimensionality of risk

How surprised we are to see you login like that?

Unusual location, device, time

How suspicious does the login look?

- Similarity to known hijacking patterns
- Is user at risk?



Hijackers adapt.



Geocloaking

\$message .= "-----\n";

\$message .= "Email : ".\$_POST['Email']."\n";

\$message .= "Password : ".\$_POST['Passwd']."\n";

\$message .= "-----+ IP Address & Date +-----\n";

\$message .= "IP Address: ".\$ip."\n";

\$message .= "Country: ".\$country."\n";

\$message .= "Date: ".\$adddate."\n";

~83% phishing kits

In the end, we don't look at user's location for many users.



Prevention

Sign-in risk detection

Challenges



Dynamic 2FA: Ask for additional verification



When the sign-in is risky



That is solvable by the user



Key takeaway

Modern password authentication requires a **risk-aware**, defense-in-depth system.



2 things that can go wrong



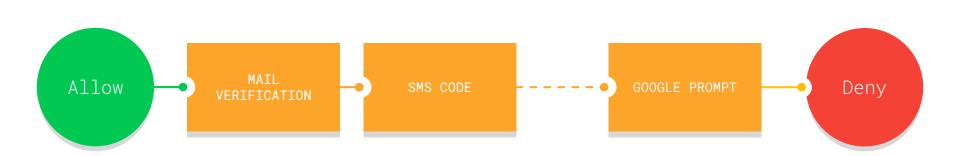


Hijacker gets in

User is locked out



Choose the challenge that minimizes damage





Secondary e-mail verification

Google

Verify it's you This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more 😑 maganini wataona @gmail.com V 8 **** Get a verification code Google will send a verification code to mag.....@gmail.com SEND More options



have problems passing this challenge



Secondary e-mail verification

Google

Verify it's you This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more estimation (a constraint of the constraint of V 8 **** Get a verification code Google will send a verification code to mag.....@gmail.com SEND More options

Vulnerable to password reuse

Google

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

your.account@gmail.com

V

Try another way to sign in

Tap **Yes** on your phone or tablet

Get a verification code at (···) ·····99 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



SMS code

Vulnerable to phishing...

18% of observed phishing kits collect phone data.

... and other methods

There are multiple ways to get the SMS code besides phishing.



I was hacked Posted Aug 23, 2017 by John Biggs (ejohnbiggs) I f V in 8° & C V I



https://techcrunch.com/2017/08/23/i-was-hacked/



Google

ГП

1

(?

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

V

your.account@gmail.com

Try another way to sign in

Tap Yes on your phone or tablet

Get a verification code at (•••) •••••99 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



SMS code

Most successful hijackings of high-value 2FA-accounts involve breaking the SMS code.

SMS code interception happens in targeted attacks as well as in opportunistic ones.

Google

Гп

1

2

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

S your.account@gmail.com

~

Try another way to sign in

Tap Yes on your phone or tablet

Get a verification code at (•••) •••••99 Standard rates apply

Call your phone on file (•••) •••-••99

Use your phone or tablet to get a security code (even if it's offline)

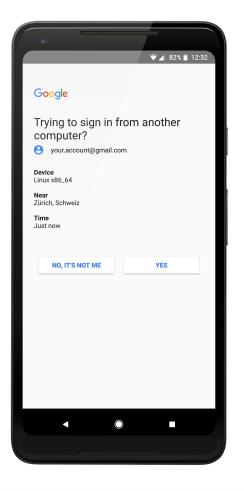
Get help



SMS code

"by January 2016, [the number of phone hijackings] had increased to **2,658**."

Lorrie Cranor, FTC Chief Technologist





Google Prompt

Nothing stops the user from just clicking "Yes"

More flexible

We can present more data and use additional signals for risk-analysis

In-session detection

Hijacking monetization



Theft of personal data



Viral-phishing and scams



Spamming and product abuse

Bringing the user into the loop 0

Google

Suspicious activity in your account

Hi Grzegorz.

Someone recently signed into your Google account grzegorzmilka@google.com and created unusual Gmail message filters.

Details:

Thursday, January 11, 2018 2:14 PM (Israel Time) Tel Aviv-Yafo, Israel*

Review your recently used devices to make sure no one else has access to your account.

REVIEW YOUR DEVICES NOW

Go to the Help Center to learn more about Gmail filters.

The Google Accounts team

Googlers, please file any feedback here. This email can't receive replies. For more information, visit the Google Accounts Help Center.

Finding the hijacker in-session

20:54:24 | LOGIN (new)

20:55:51 | MAIL_DELETE | 1 (new device notifn.)



Finding the hijacker in-session

- 20:54:24 | LOGIN (new)
- | 1 (new device notifn.) 20:55:51 MAIL DELETE
- 21:01:30 | EXPORT CONTACTS



Finding the hijacker in-session

20:54:24 | LOGIN (new)

20:55:51 | MAIL_DELETE

- 21:01:30 | EXPORT_CONTACTS
- 21:06:45 | MAIL_SEND
- 21:07:50 | MAIL_FILTER

21:08:07 | LOGOUT

1 (new device notifn.)

with phishing links "hacked"->Trash





Modern password authentication requires a **risk-aware**, **defense-in-depth** system.