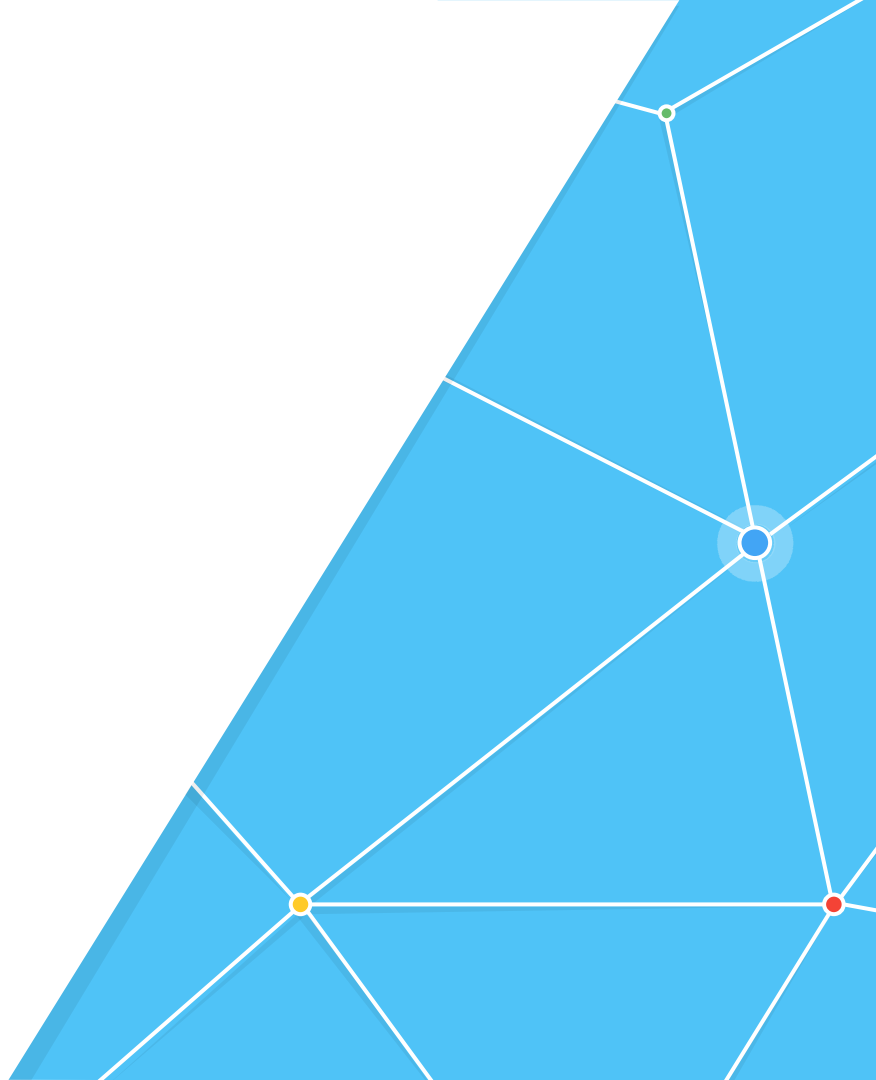


Research at 

# The Anatomy of Account-Takeover

Grzegorz Milka ([grzegorzmilka@google.com](mailto:grzegorzmilka@google.com))



# Online accounts are valuable targets



Financial data



Personal data



Contacts



Identity  
(impersonation)

# Data breaches are always there

SECURITY

**Dropbox data breach: 68 million user account details leaked**

TECHNOLOGY

***Yahoo Says 1 Billion User Accounts Were Hacked***

CHANGING FACE OF SECURITY

**LinkedIn Lost 167 Million Account Credentials in Data Breach**

# And so are targeted hijacks



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

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

## Key takeaway

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

# Password theft ecosystem



# The three avenues of password theft



Data breach



Malware (Keyloggers)



Phishing





# Commoditization of abuse





# The wares on sale

Register Purchase Blog API TOS FAQ Contact Leaked Sites

## LEAKEDSOURCE

There are currently 2,508,319,669 / 3,109,103,084 accounts in our database.

[Click here to read this informative post.](#)

[Click here to subscribe and view your Raw data! As low as \\$0.76 a day!](#)

[Check for free to see if your email or account was hacked.](#)

Search Term

Email

Wildcard (Limit first 200 results) (What's wildcard?)

Data breach market

## HAWKEYE KEYLOGGER

Powered By iivissiaze HF

Option #1 Option #2 Option #3 Option #4

Options

- Add To Startup
- Melt File
- Confirm Exec.

Keystrokes

- Keylogs
- Clipboards
- Screenshots

Disablers

- Task Mgr.
- MsConfig
- CMD
- USB
- RegEdit
- P2P

Stealers

- Chrome
- Firefox
- Safari
- IE (All)
- Opera
- AIM
- Minecraft
- Nimbuzz
- Outlook
- FileZilla
- Steam
- SmartFTP
- Pidgin
- BTC
- PalTalk
- IDM
- JDownloader

Much More...

Clear History

- Chrome
- IE
- Firefox
- Steam
- Dely Exe.
- Sec

Status: Idle... 01/06/2015 22:45

Keyloggers

Welcome to Google Docs. Upload and Share Your Documents Securely  
Sign in with your email address to view or download attachment

Select your email provider

Gmail Sign in with Gmail

Email

Password

[Sign in to view attachment](#)

Stay signed in [Need help?](#)

Access your documents securely, no matter your location

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



17%\*  
reuse rate

\* internal estimate



Number of valid Google passwords  
found in data breaches:

**67 Million**



# Volume of credentials stolen in 2016\*



Data breaches

>3.3B



Keyloggers

>1M



Phishing

>12M

\*all services,  
lower bound



# 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:



You were in a breach



Had a keylogger



Were phished

\*lower bound





# Prevention

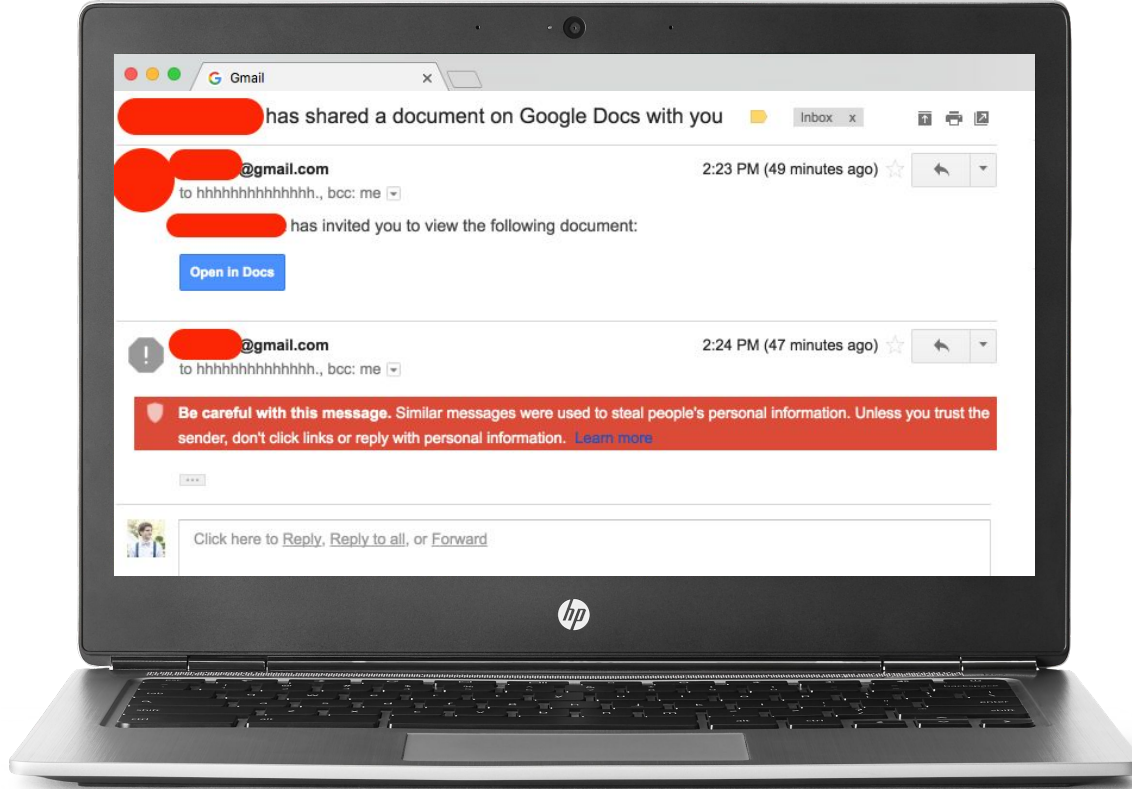
## Sign-in risk detection

### Challenges



## Key takeaway

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







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

**<10%**

2FA

Of active  
Google accounts

**~12%**

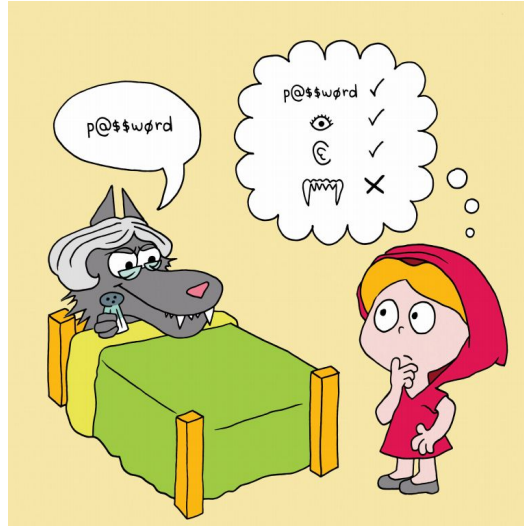
Password managers\*

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 .= "-----+ Begin +-----\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.



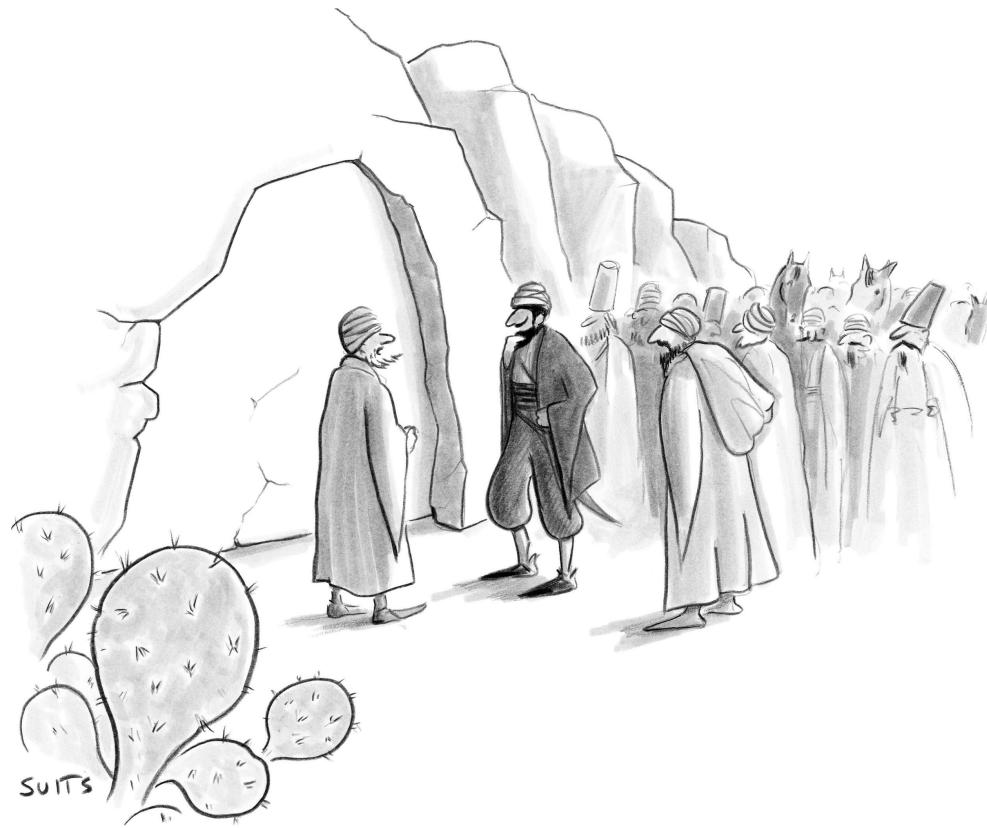
# 2 things that can go wrong





Hijacker gets in

“The burglar” by Eastlake  
Times (<https://goo.gl/yh4zyB>),  
CC BY 2.0



*“Try ‘Open underscore sesame.’”*

User is locked out

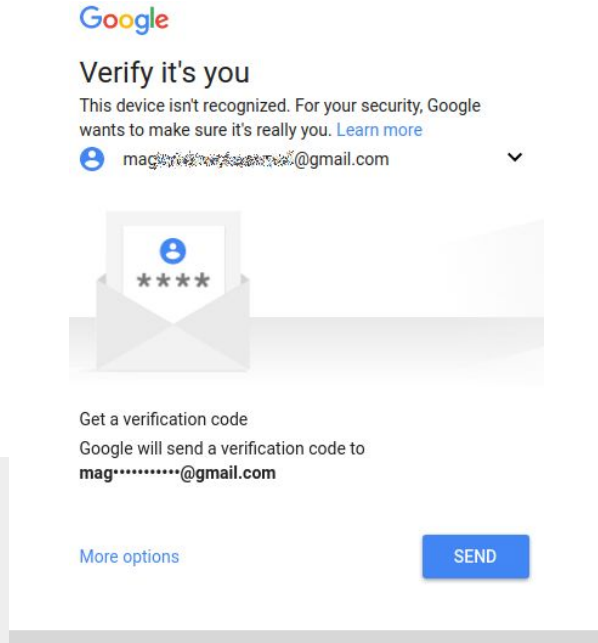


# Choose the challenge that minimizes damage





# Secondary e-mail verification

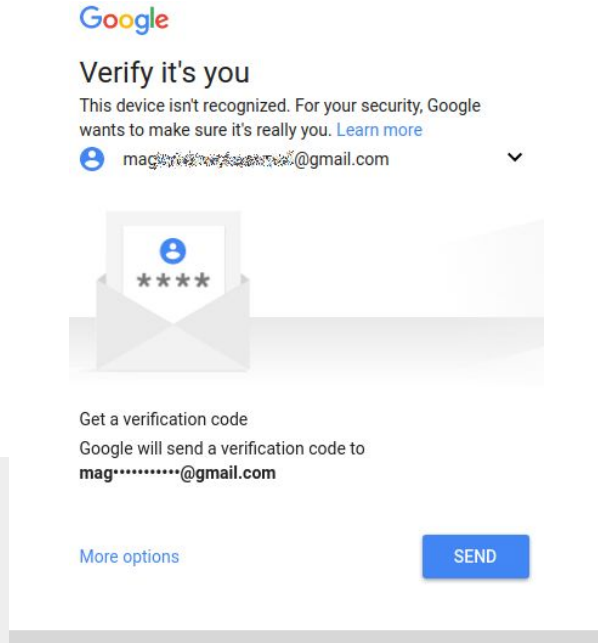


10%  
Of users

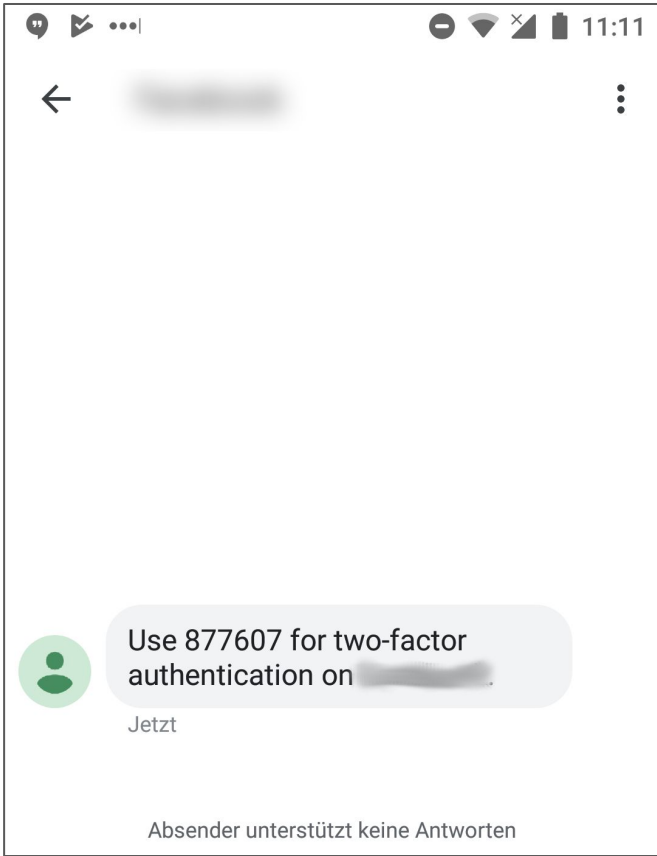
have problems passing this challenge



# Secondary e-mail verification



Vulnerable to password reuse



# 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.

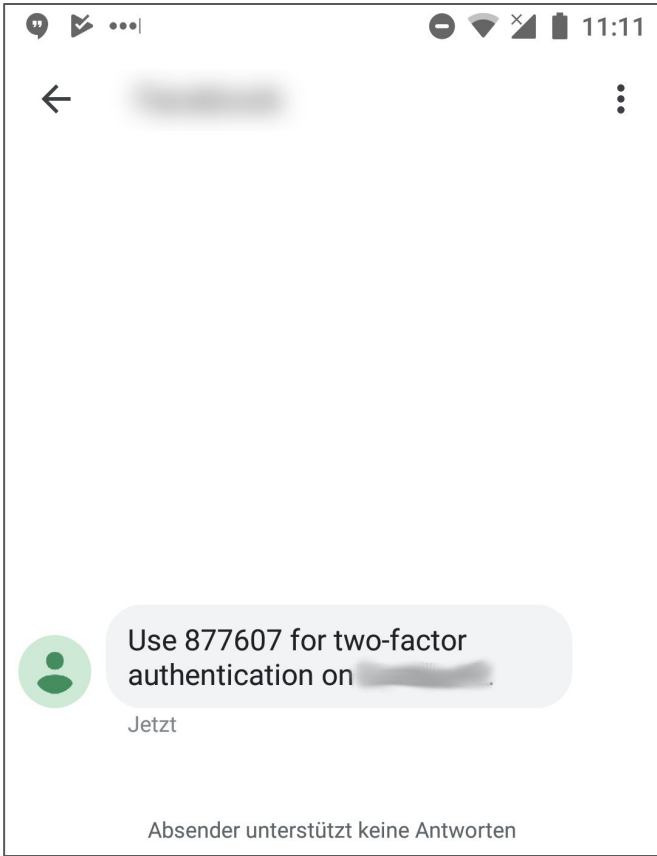


## I was hacked

Posted Aug 23, 2017 by [John Biggs](#) (@johnbiggs)



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

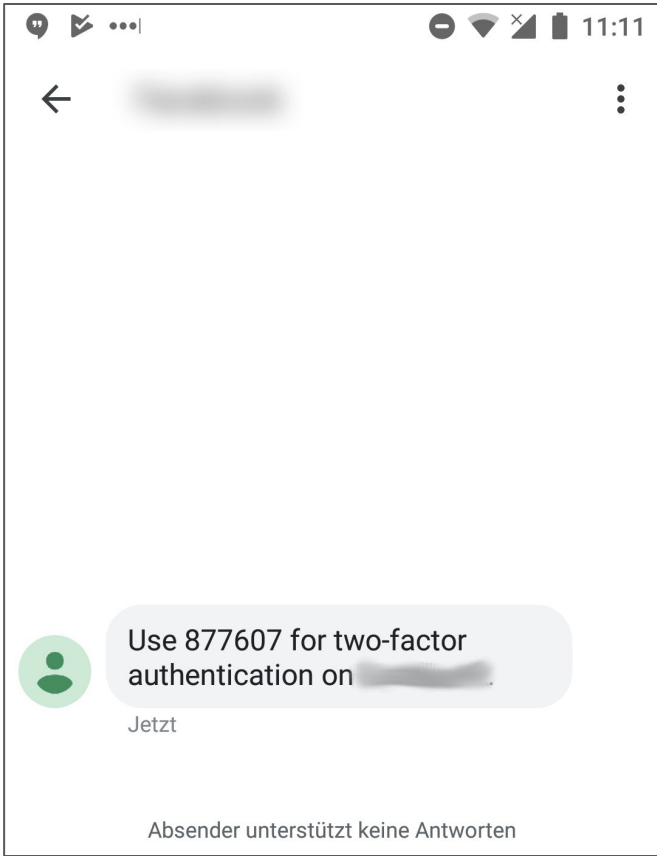


# SMS code

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.

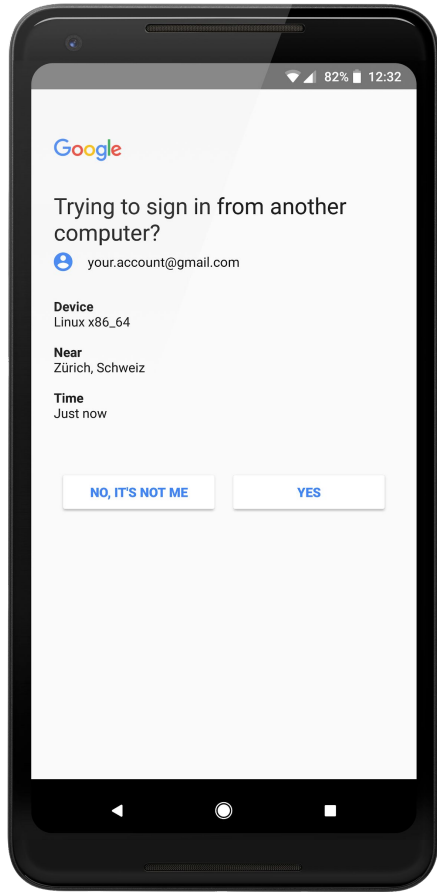




# SMS code

“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

Google



## Suspicious activity in your account

Hi Grzegorz,

Someone recently signed into your Google account [redacted] 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

\*The location is approximate and determined by the IP address it was coming from.

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

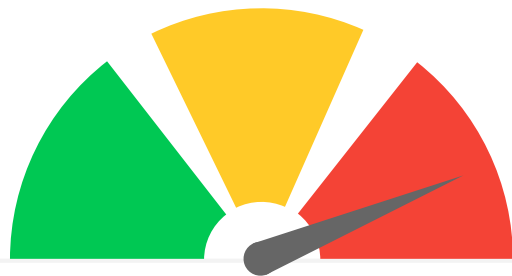
```
20:54:24 | LOGIN (new) |  
20:55:51 | MAIL_DELETE | 1 (new device notifn.)  
21:01:30 | EXPORT_CONTACTS |
```





# Finding the hijacker in-session

```
20:54:24 | LOGIN (new) |  
20:55:51 | MAIL_DELETE | 1 (new device notifn.)  
21:01:30 | EXPORT_CONTACTS |  
21:06:45 | MAIL_SEND | with phishing links  
21:07:50 | MAIL_FILTER | "hacked"->Trash  
21:08:07 | LOGOUT |
```







## Key takeaway

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