Protecting Google Accounts Against Hijacking

Virginia Aguilar
Trust & Safety Account Security Manager

Every user is a potential target ...

...because online accounts are valuable ...

Information
(personal data, financial, credentials, contacts, etc)

Online Identity
(impersonation, account needed to get access to resources, etc)

...for different types of threat actors.

Cyber criminals

State-sponsored

Insider threats

(*)Icons made by smalllikeart, smashicons and freepik from www.flaticon.com

Three ways to access an account

Solving challenges
(e.g. password, 2SV,..)

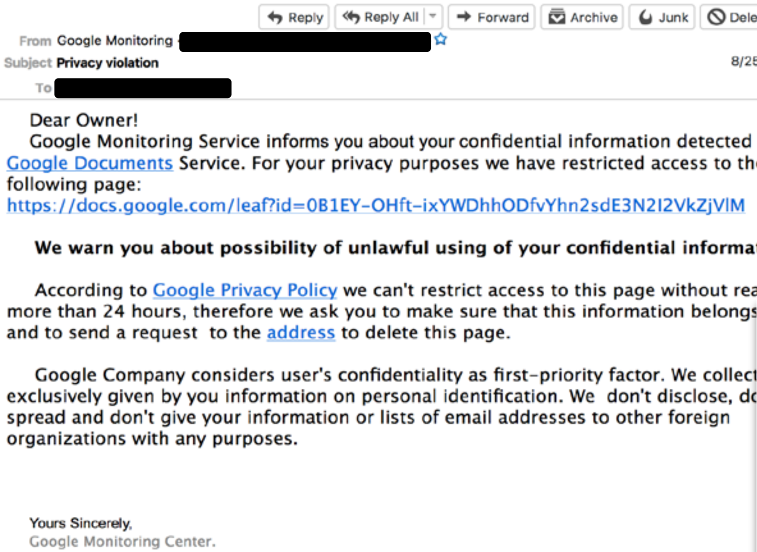
Access tokens
(steal or lure to grant access)

Compromise of devices
(access to user's endpoint)

(*)Icons made by monkik, freepik, smashicons and from www.flaticon.com

Evolution of the phishing sophistication

Phishing examples



From Google Monitoring [redacted]

Subject **Privacy violation** 8/25/10, 2:32 AM

To [redacted]

Dear Owner!

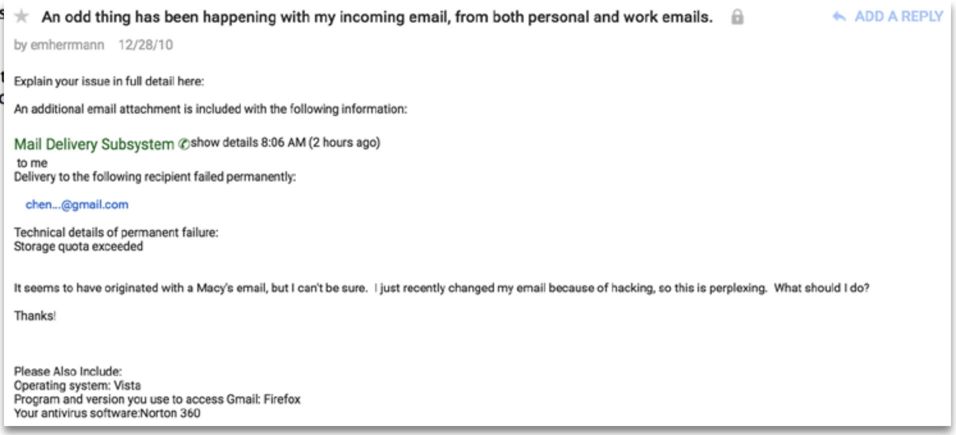
Google Monitoring Service informs you about your confidential information detected on Google Documents Service. For your privacy purposes we have restricted access to the following page:
https://docs.google.com/leaf?id=0B1EY-OHft-ixYWDhhODfvYhn2sdE3N2I2VkZjVlM

We warn you about possibility of unlawful using of your confidential information.

According to Google Privacy Policy we can't restrict access to this page without reasons for more than 24 hours, therefore we ask you to make sure that this information belongs and to send a request to the address to delete this page.

Google Company considers user's confidentiality as first-priority factor. We collect exclusively given by you information on personal identification. We don't disclose, do spread and don't give your information or lists of email addresses to other foreign organizations with any purposes.

Yours Sincerely,
Google Monitoring Center.



An odd thing has been happening with my incoming email, from both personal and work emails.

by emherrmann 12/28/10

Explain your issue in full detail here:

An additional email attachment is included with the following information:

Mail Delivery Subsystem show details 8:06 AM (2 hours ago)
to me
Delivery to the following recipient failed permanently:

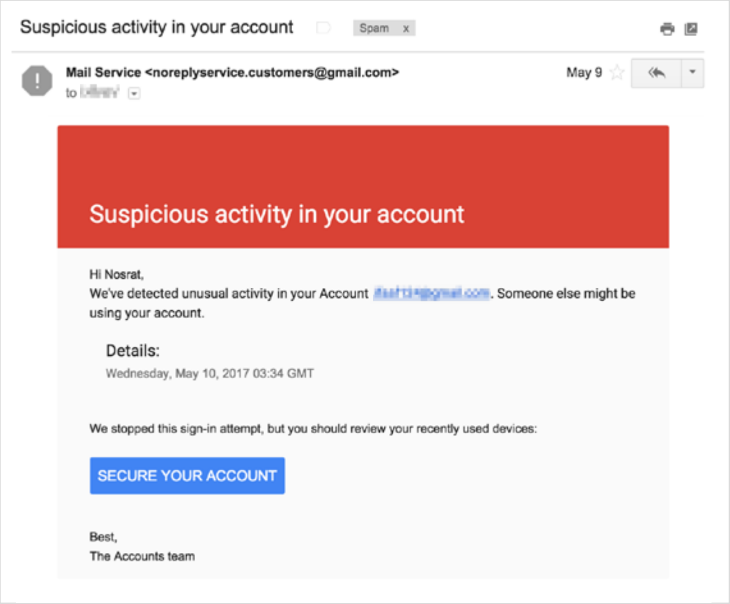
chen...@gmail.com

Technical details of permanent failure:
Storage quota exceeded

It seems to have originated with a Macy's email, but I can't be sure. I just recently changed my email because of hacking, so this is perplexing. What should I do?

Thanks!

Please Also Include:
Operating system: Vista
Program and version you use to access Gmail: Firefox
Your antivirus software:Norton 360



Suspicious activity in your account

Mail Service <noreplyservice.customers@gmail.com> May 9

to [redacted]

Suspicious activity in your account

Hi Nosrat,

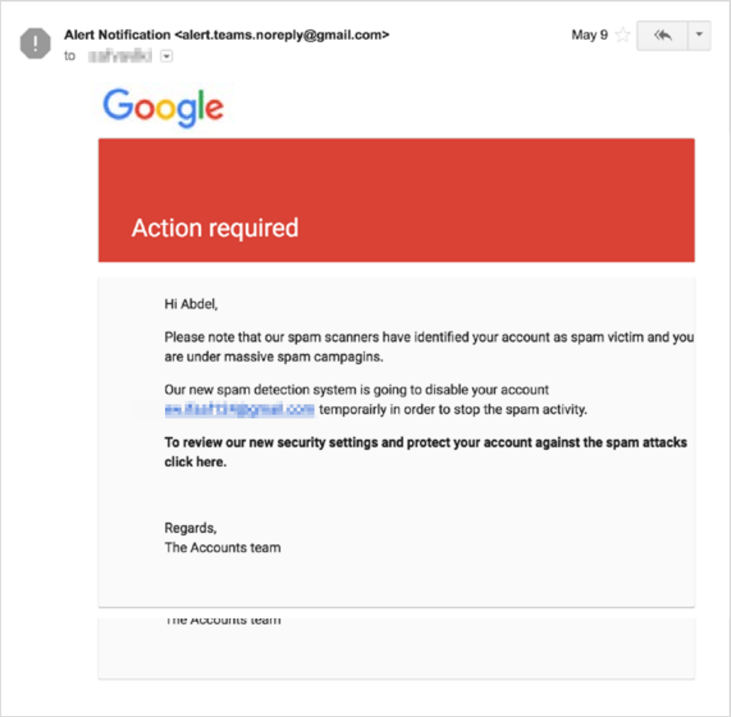
We've detected unusual activity in your Account [redacted]. Someone else might be using your account.

Details:

Wednesday, May 10, 2017 03:34 GMT

We stopped this sign-in attempt, but you should review your recently used devices:

Best,
The Accounts team



Alert Notification <alert.teams.noreply@gmail.com> May 9

to [redacted]

Action required

Hi Abdel,

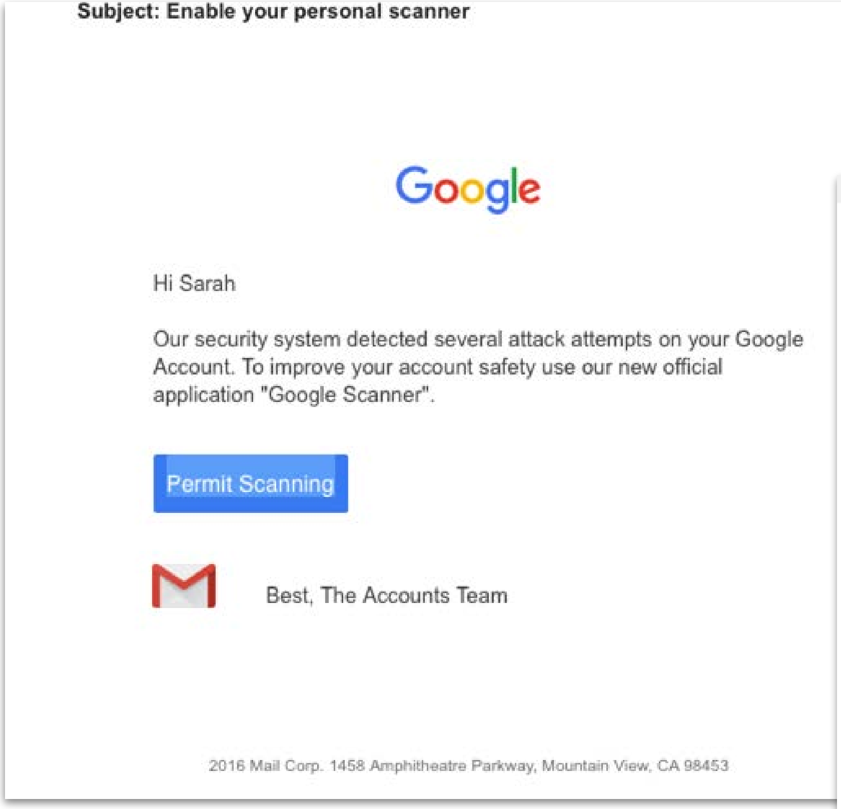
Please note that our spam scanners have identified your account as spam victim and you are under massive spam campagins.

Our new spam detection system is going to disable your account [redacted] temporairly in order to stop the spam activity.

To review our new security settings and protect your account against the spam attacks click here.

Regards,
The Accounts team

The Accounts team



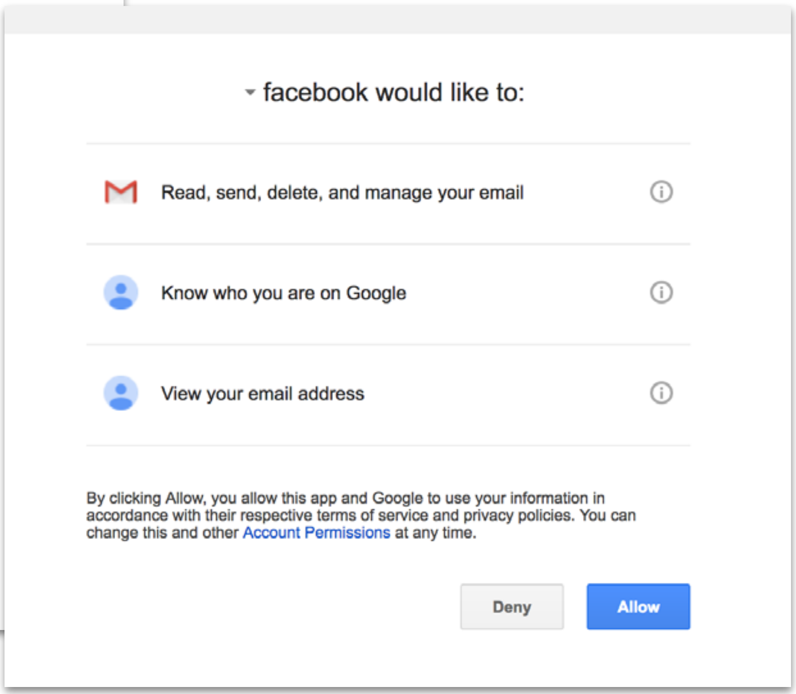
Subject: Enable your personal scanner

Hi Sarah

Our security system detected several attack attempts on your Google Account. To improve your account safety use our new official application "Google Scanner".

Best, The Accounts Team

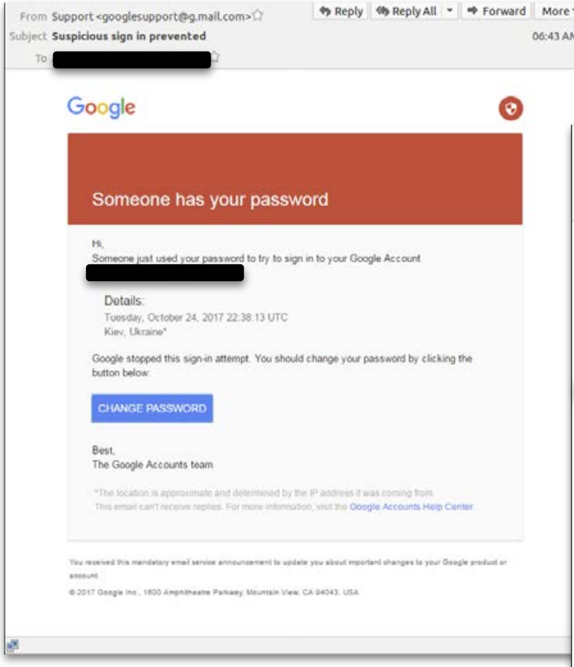
2016 Mail Corp. 1458 Amphitheatre Parkway, Mountain View, CA 98453



facebook would like to:

- Read, send, delete, and manage your email
- Know who you are on Google
- View your email address

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.



From Support <googlesupport@g.mail.com>

Subject **Suspicious sign in prevented**

06:43 AM

To [redacted]

Google

Someone has your password

Hi,
Someone just used your password to try to sign in to your Google Account [redacted]

Details:
Tuesday, October 24, 2017 22:38:13 UTC
Kiev, Ukraine*

Google stopped this sign-in attempt. You should change your password by clicking the button below:

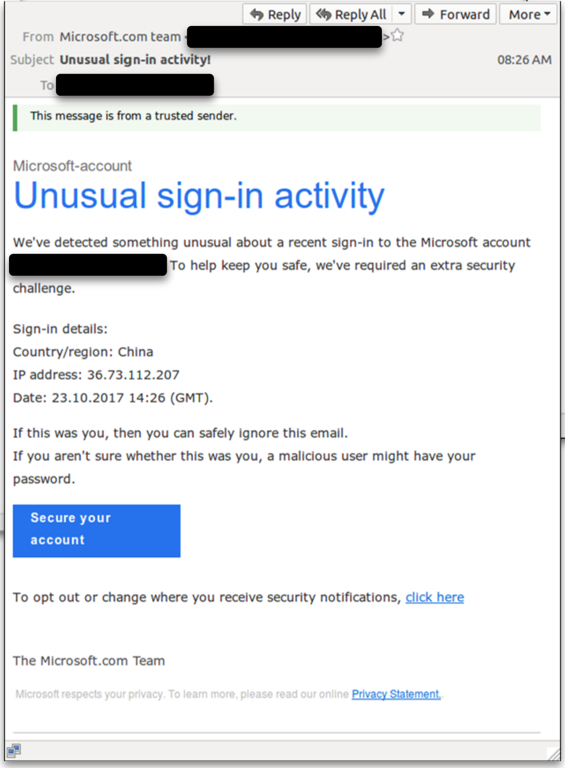
CHANGE PASSWORD

Best,
The Google Accounts team

*The location is approximate and determined by the IP address it was coming from.
This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2017 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA



From Microsoft.com team [redacted]>

Subject **Unusual sign-in activity!**

08:26 AM

To [redacted]

This message is from a trusted sender.

Microsoft-account

Unusual sign-in activity

We've detected something unusual about a recent sign-in to the Microsoft account [redacted] To help keep you safe, we've required an extra security challenge.

Sign-in details:
Country/region: China
IP address: 36.73.112.207
Date: 23.10.2017 14:26 (GMT).

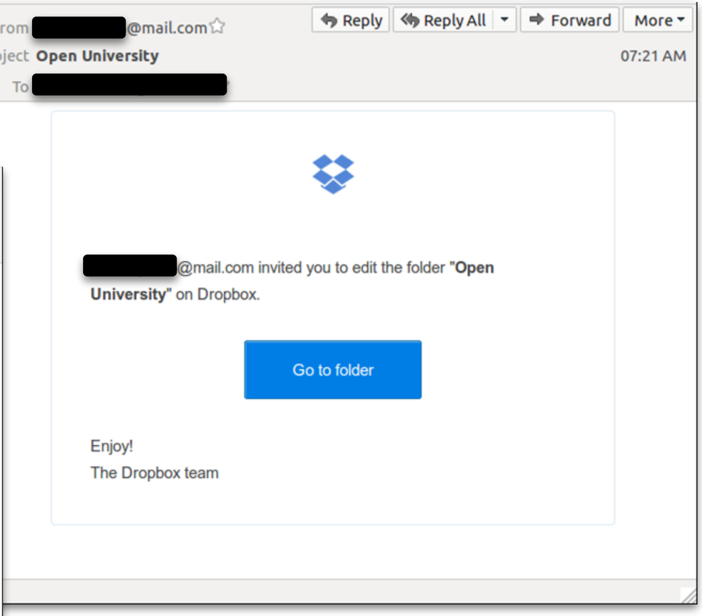
If this was you, then you can safely ignore this email.
If you aren't sure whether this was you, a malicious user might have your password.

Secure your account

To opt out or change where you receive security notifications, click here

The Microsoft.com Team

Microsoft respects your privacy. To learn more, please read our online Privacy Statement.



From [redacted]@mail.com

Subject **Open University**

07:21 AM

To [redacted]

[redacted]@mail.com invited you to edit the folder **"Open University"** on Dropbox.

Go to folder

Enjoy!
The Dropbox team

And what are we doing about it?

2 things that can go wrong

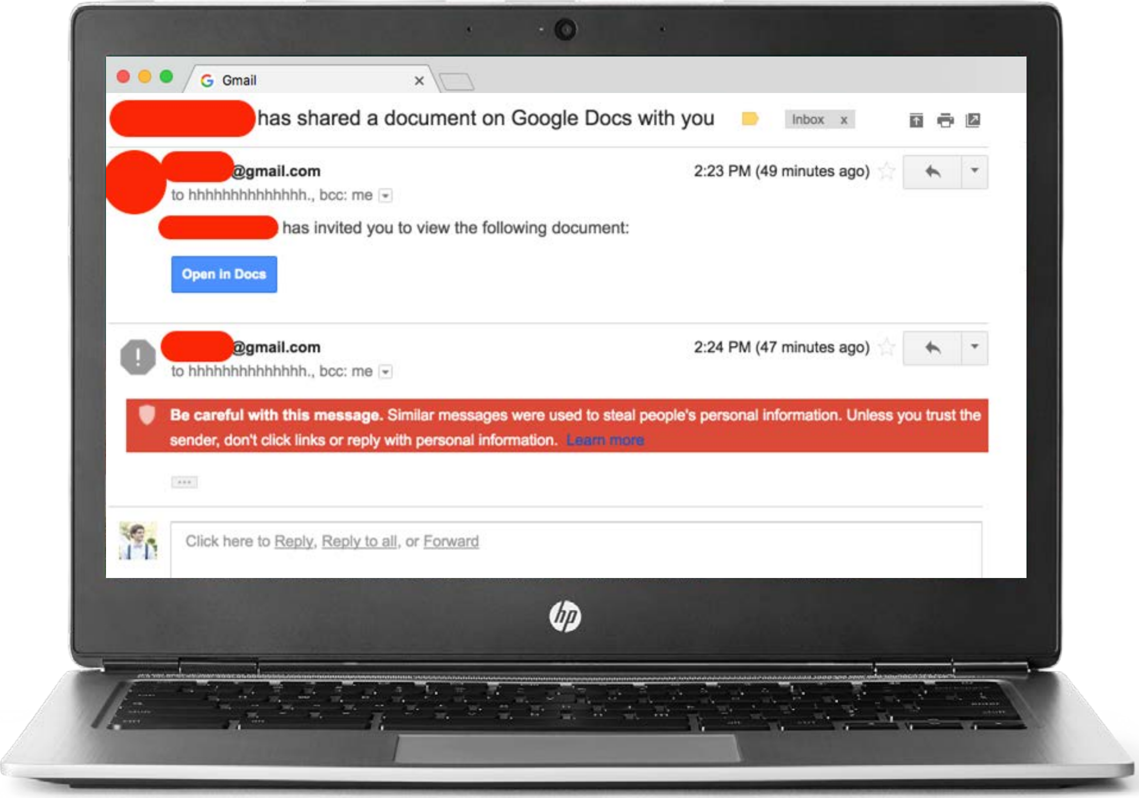
Hijacker gets in

User is locked out

Prevention

Sign-in risk detection

Challenges



[redacted] has shared a document on Google Docs with you

[redacted]@gmail.com 2:23 PM (49 minutes ago)

to hhhhhhhhhhhhhh., bcc: me

[redacted] has invited you to view the following document:

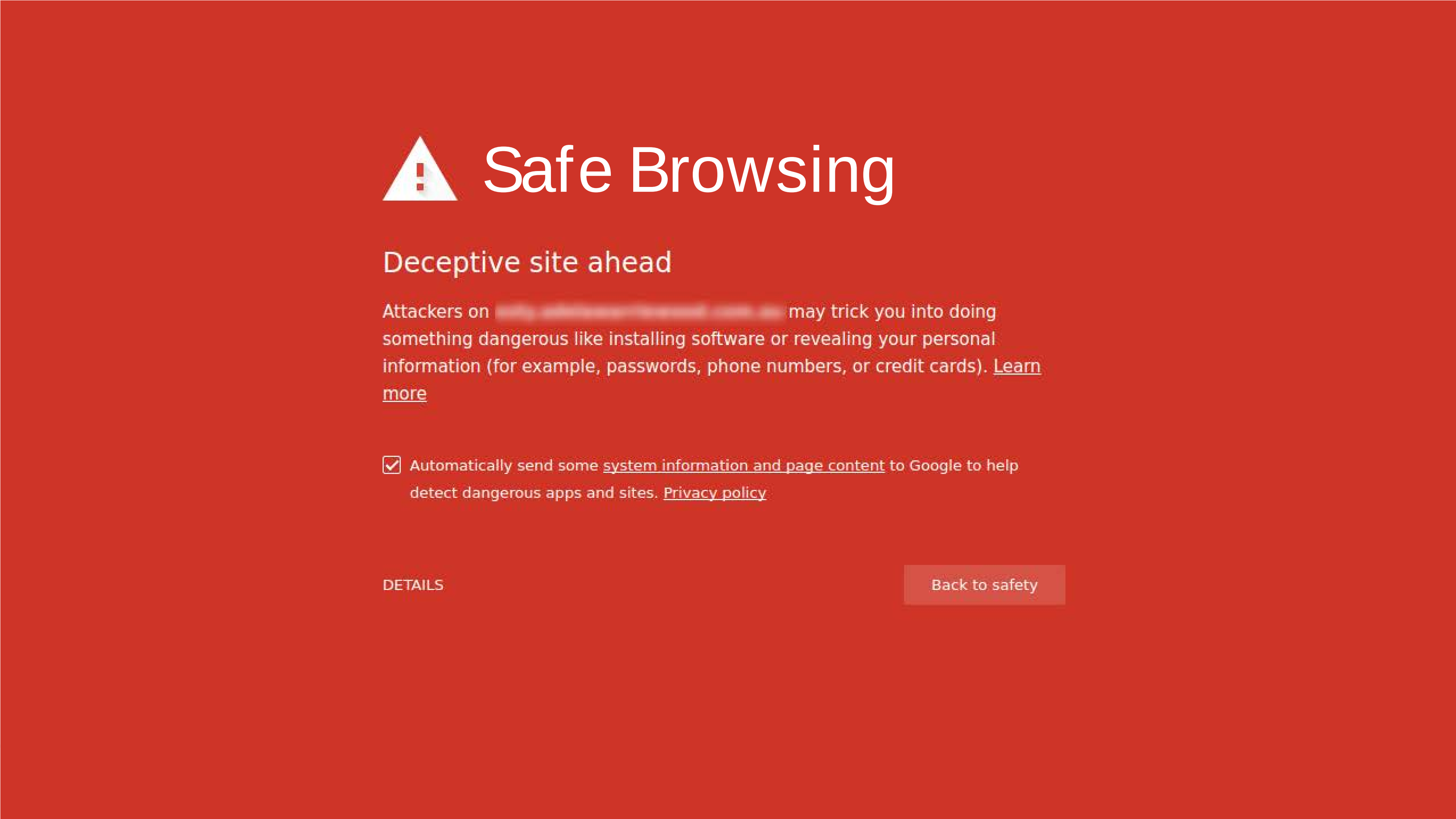
[redacted]@gmail.com 2:24 PM (47 minutes ago)

to hhhhhhhhhhhhhh., bcc: me

Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more

Click here to Reply, Reply to all, or Forward

Safe Browsing



Deceptive site ahead

Attackers on [redacted] may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

☑ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

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

Prevention

Sign-in risk detection

Challenges

Dimensionality of risk

How surprised we are to see you login like that?

Unusual location, device, time

How suspicious does the login look?

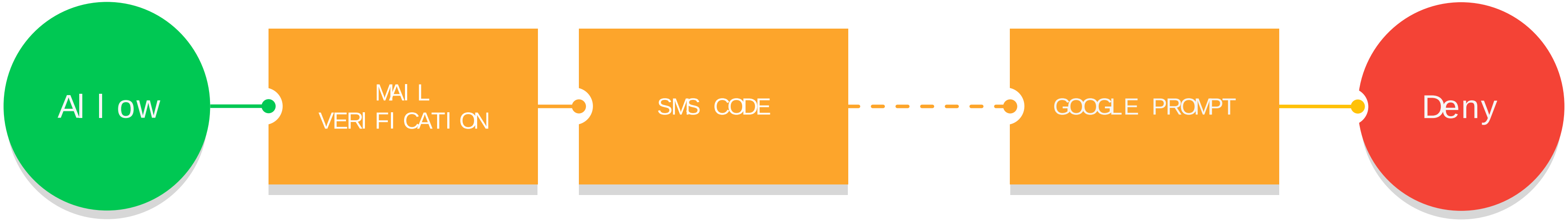
- Similarity to known hijacking patterns
- Is user at risk?

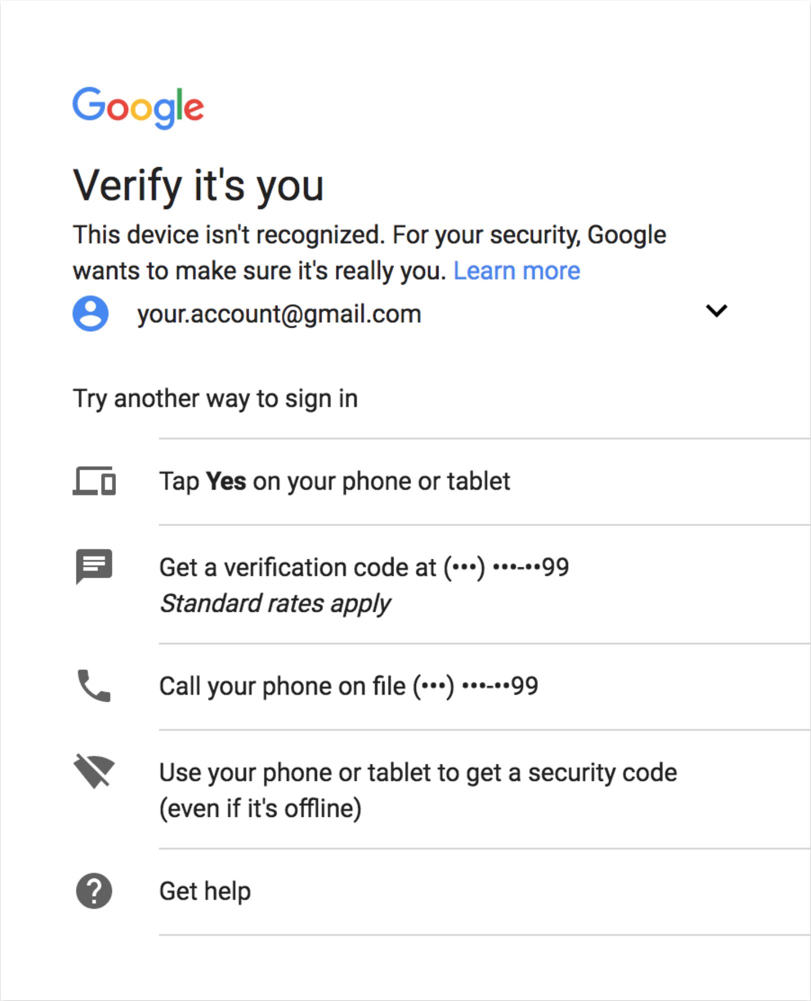
Prevention

Sign-in risk detection

Challenges

Choose the challenge that minimizes damage





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

Try another way to sign in

Tap **Yes** on your phone or tablet

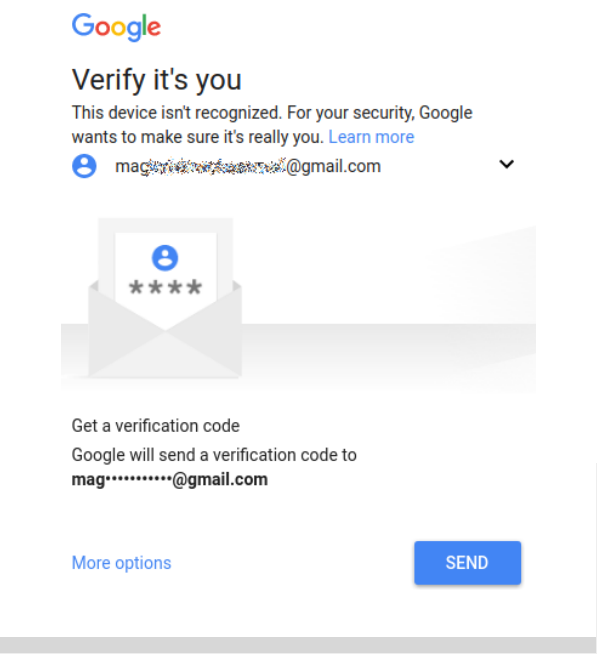
Get a verification code at (•••) •••-••99
Standard rates apply

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

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

Get help

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

mag[redacted]@gmail.com

Get a verification code

Google will send a verification code to **mag••••••••••@gmail.com**

More options

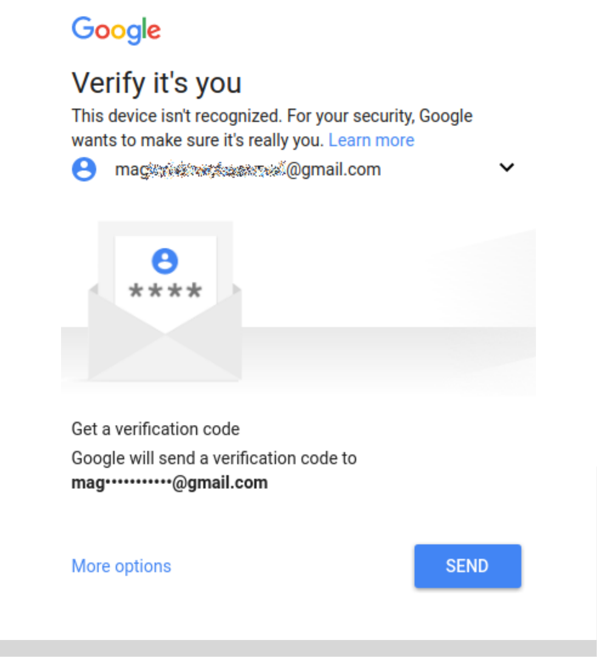
SEND

10%

Of users

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

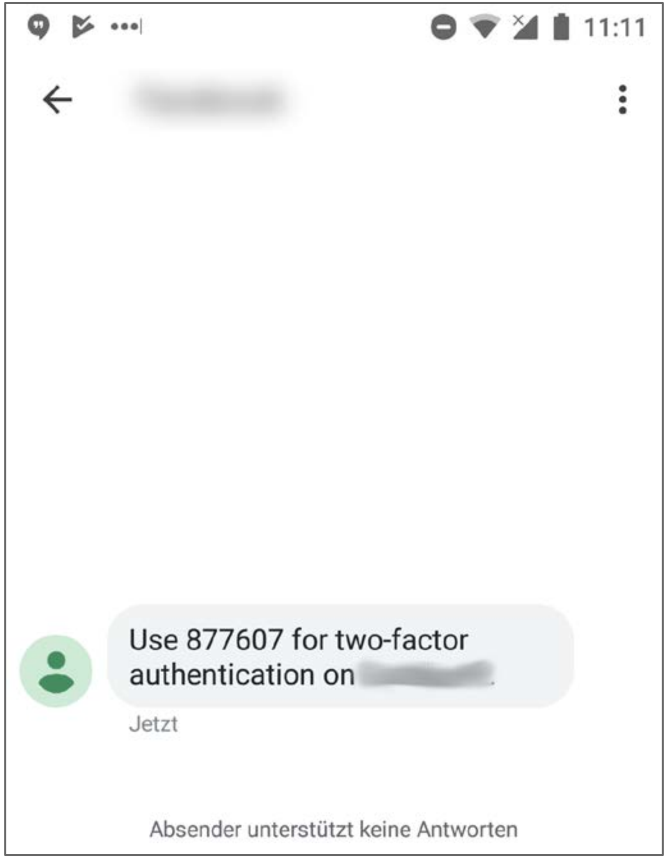
mag[redacted]@gmail.com

Get a verification code

Google will send a verification code to **mag•••••••••••@gmail.com**

Vulnerable to phishing and password reuse

SMS code



[redacted]

Use 877607 for two-factor authentication on [redacted].

Jetzt

Absender unterstützt keine Antworten

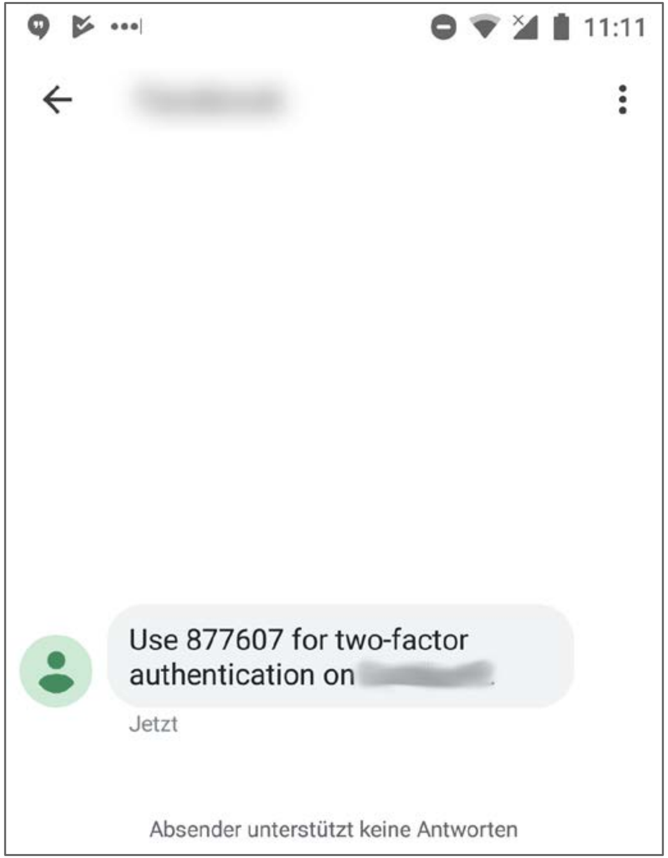
Vulnerable to phishing...

18% of observed phishing kits collect phone data.

...and other methods

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

SMS code



[redacted]

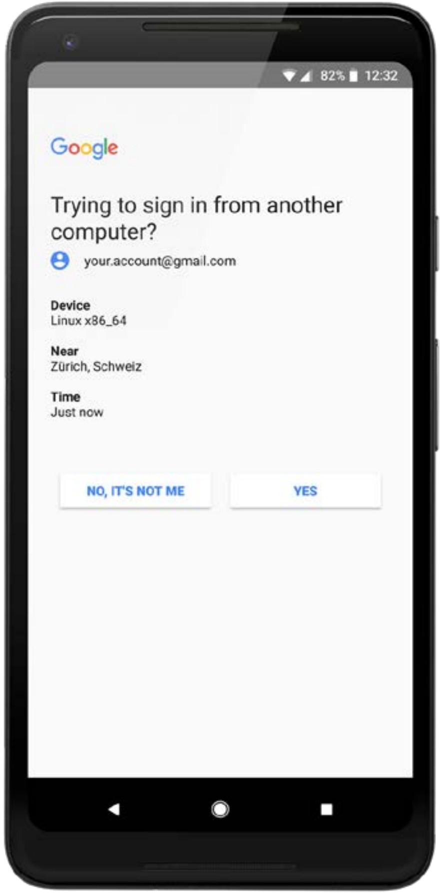
Use 877607 for two-factor authentication on [redacted].

Jetzt

Absender unterstützt keine Antworten

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

Trying to sign in from another computer?

your.account@gmail.com

Device
Linux x86_64

Near
Zürich, Schweiz

Time
Just now

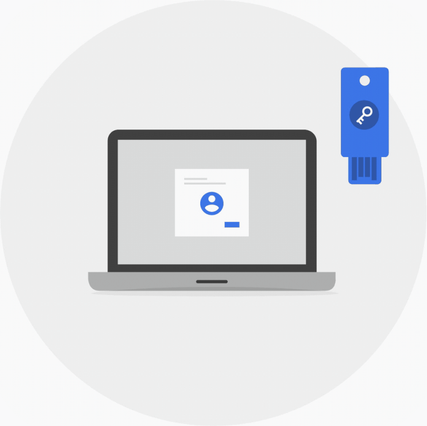
Google Prompt

Nothing stops the user from just clicking “Yes”

More flexible

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

Advanced Protection Program



Strongest phishing defenses via physical Security Key

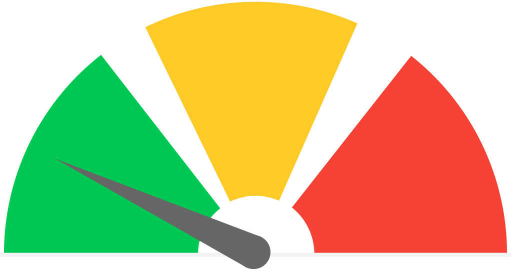
Protect sensitive data from accidental sharing

Enhanced in-product security features

In-session detection

Finding the hijacker in-session

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

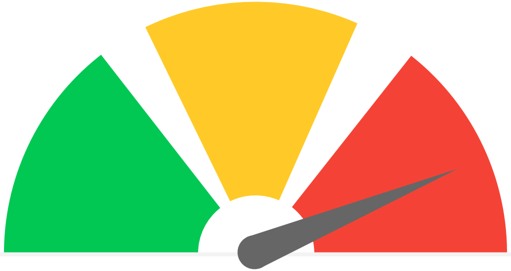


Finding the hijacker in-session

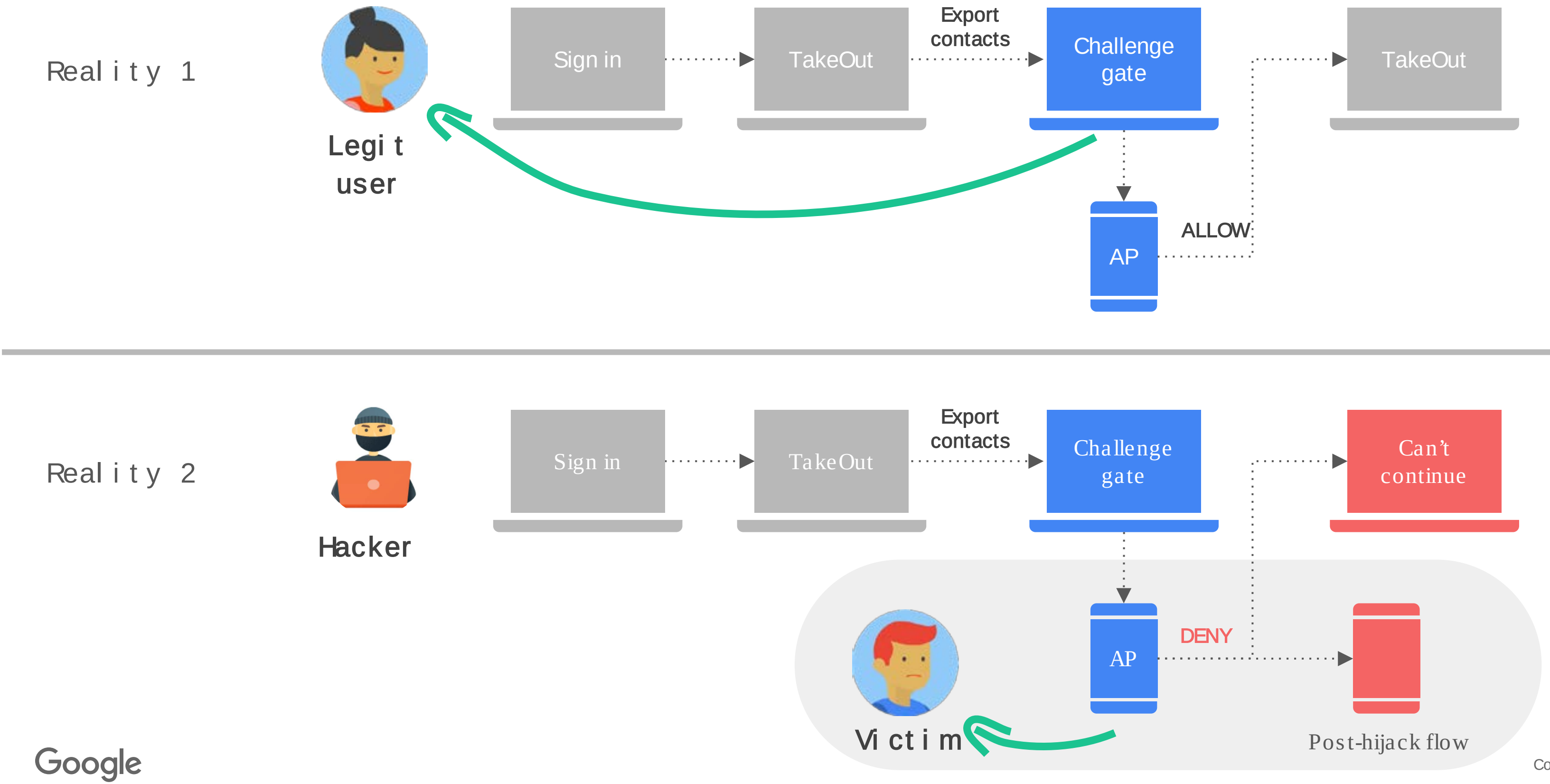
```
20:54:24 | LOGIN (new)      |
20:55:51 | MAIL_DELETE      | 1 (new device notifn.)
21:01:30 | EXPORT_CONTACTS  |
```

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             |
```



Building resilience



Reality 1

Legit user

Sign in

TakeOut

Export contacts

Challenge gate

AP

ALLOW

TakeOut

Reality 2

Hacker

Sign in

TakeOut

Export contacts

Challenge gate

AP

DENY

Can't continue

Victim

Post-hijack flow

Key takeaway

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

<eof>