

**RSA®**Conference2019

San Francisco | March 4–8 | Moscone Center



SESSION ID: HT-R03

# Anatomy of Phishing Campaigns: A Gmail Perspective

**Nicolas Lidzborski**

Gmail & G Suite Security Engineering Lead

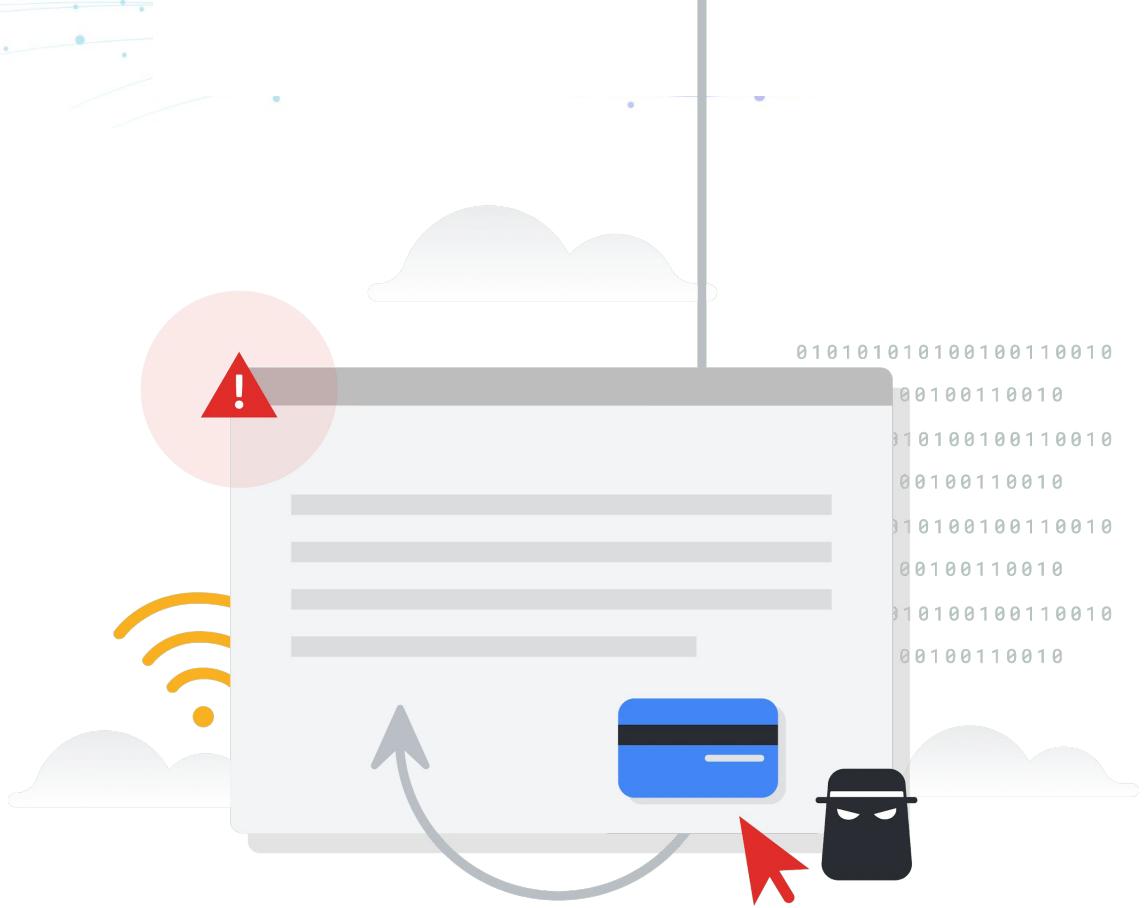
**Google**

**Ali Zand**

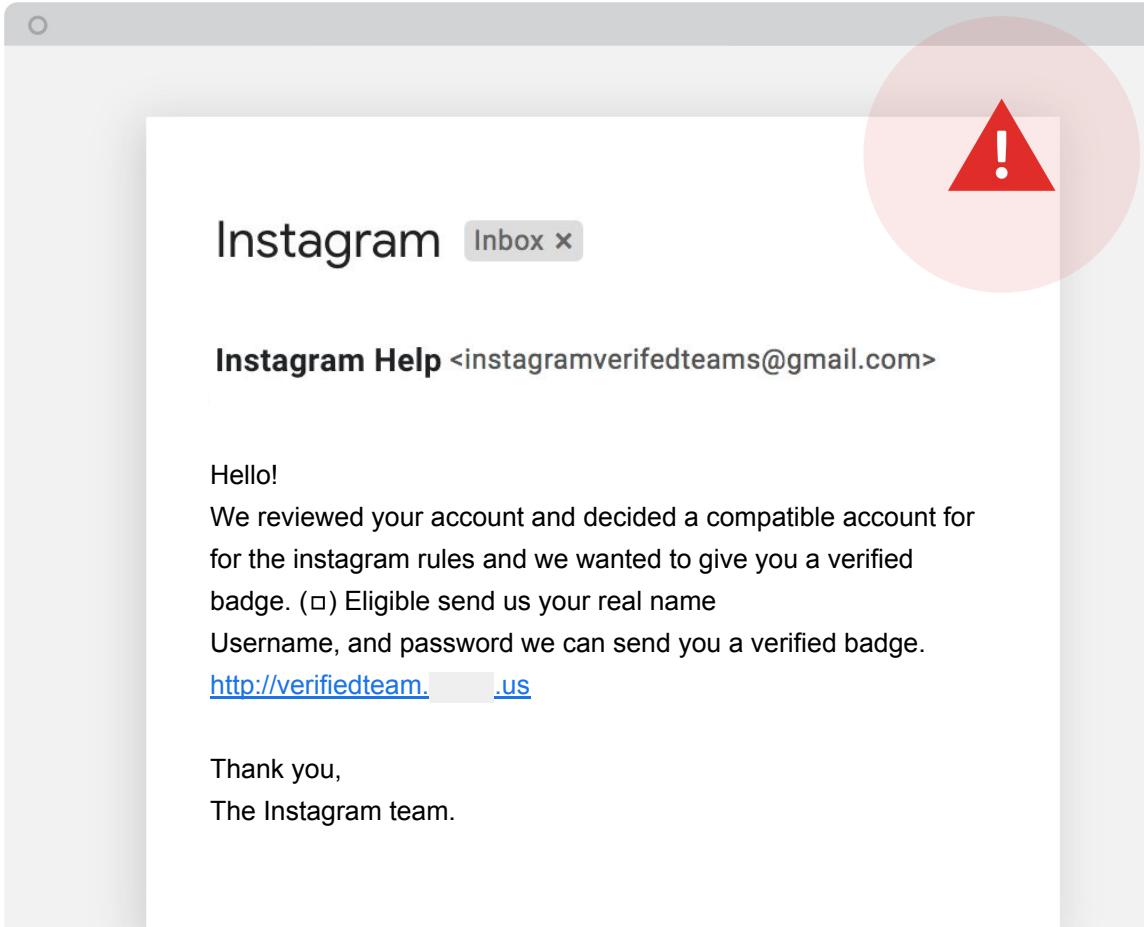
Google Anti-Abuse Research team

#RSAC

# Phishing 101



# Is phishing still a thing?



The image shows a screenshot of an email inbox from Instagram. The subject line is "Instagram". To the right of the subject line is a red circular icon containing a white exclamation mark, indicating a warning or alert. The message is from "Instagram Help <instagramverifiedteams@gmail.com>". The body of the message reads:

Hello!  
We reviewed your account and decided a compatible account for  
for the instagram rules and we wanted to give you a verified  
badge. (□) Eligible send us your real name  
Username, and password we can send you a verified badge.  
[http://verifiedteam.\\_\\_\\_\\_\\_us](http://verifiedteam._____us)

Thank you,  
The Instagram team.

**Phishing is  
actually  
prolific and  
effective!**





Gmail sees over 100M  
phishing emails per day!

ZDNet

MUST READ: Google CEO Sundar Pichai: 'Our mission is to protect your privacy'

## This phishing scam group built a list of 50,000 execs to target

CEO fraud group has a big list of potential victims; just hope you aren't on it.

By Steve Ranger | December 4, 2018 -- 14:36 GMT (06:36 PST) | Topic: Security

243 views | Dec 6, 2018, 08:01am

# Whaling Wars: A \$12 Billion Financial Dragnet Targeting CFOs

Dante Disparte Contributor ⓘ  
Crypto & Blockchain

Whaling Wars: A \$12 Billion Financial Dragnet Targeting CFOs

Cybersecurity

## Hackers Target 35,000 CFOs for Phishing Scam

A Nigerian gang's "business email compromise" scam aimed at finance execs shows how cybercriminals are becoming more sophisticated.

» Matthew Heller

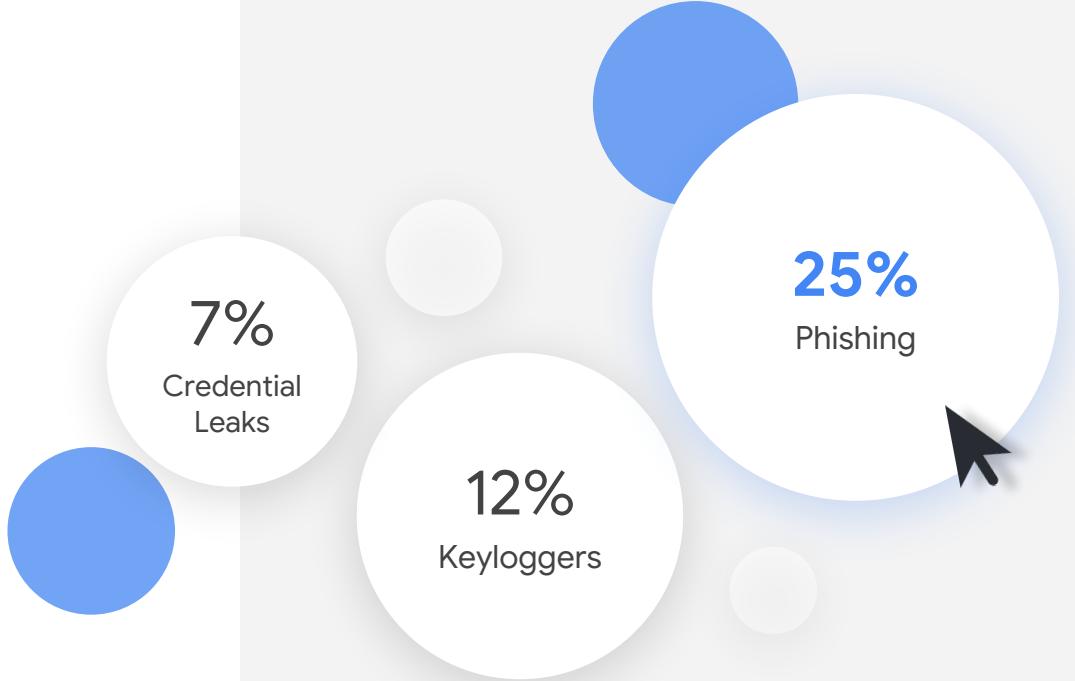
December 5, 2018 | CFO.com | US

SHARE [in Share](#) [G+ Share](#) [F Share 6](#) [Tweet](#)

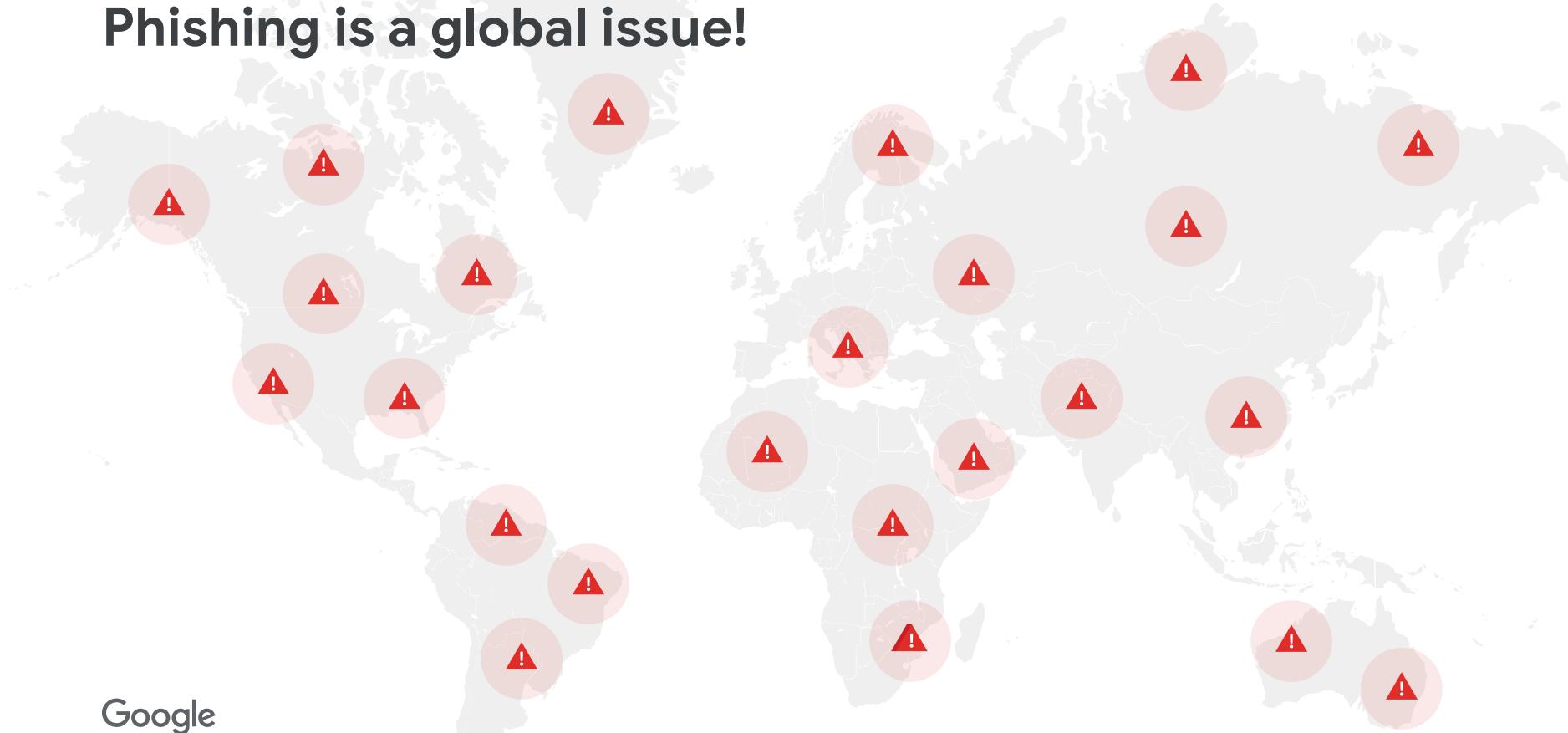
A group of Nigerian hackers included 35,000 CFOs in their list of targets for bogus requests to transfer money, highlighting the dangers of increasingly common "business email compromise" (BEC) scams.

Cyber threat detection firm Agari reported the group known as "London Blue" chose their targets from lists acquired from commercial data brokers, whose clients are usually marketers and sales teams.

# Successful Hijacking



# Phishing is a global issue!

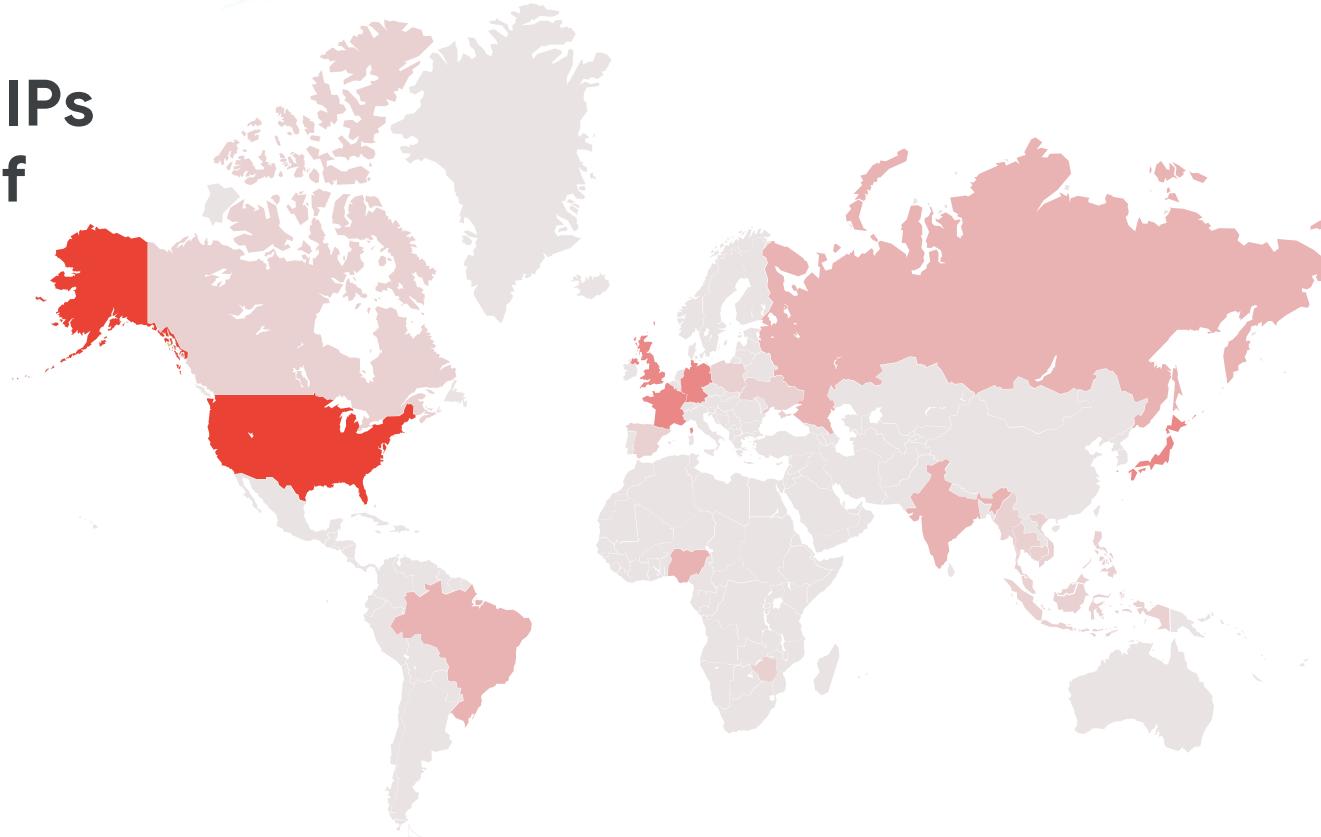




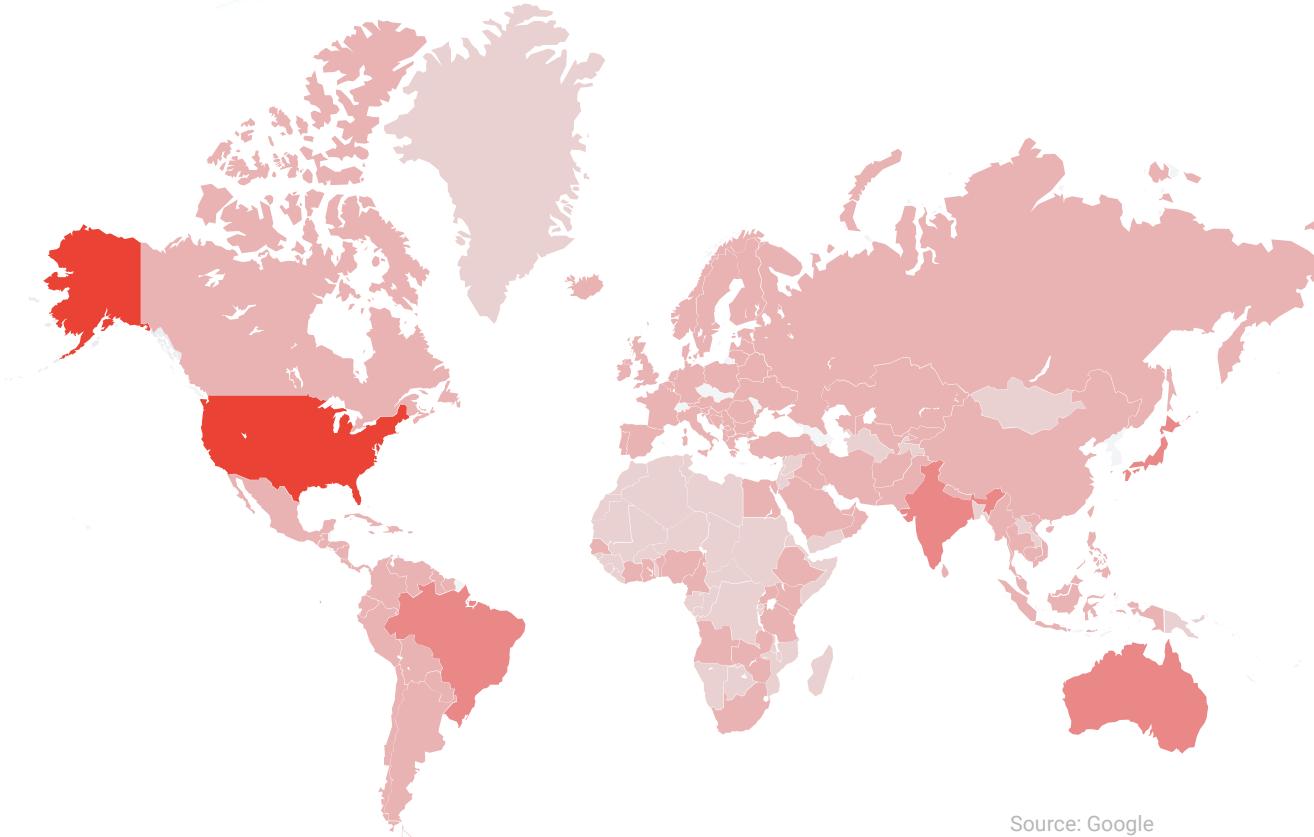
Google

RSA® Conference 2019

Attackers use IPs  
from variety of  
countries



Targets are  
everywhere



Source: Google

# Components of a phishing campaign

Target website



Email sending infrastructure



Target users



Credential exfiltration website



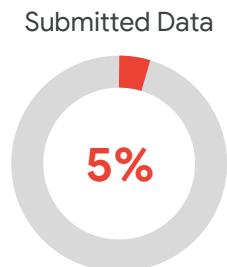
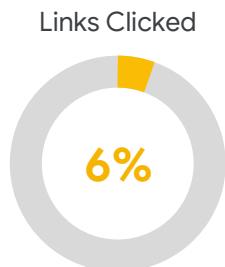
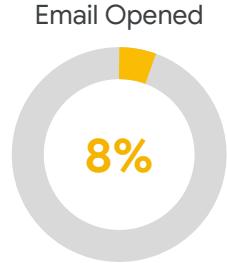
Email templates



People managing operation



# Open-source Phishing Campaign Engine



Source: [gophish dashboard](#)

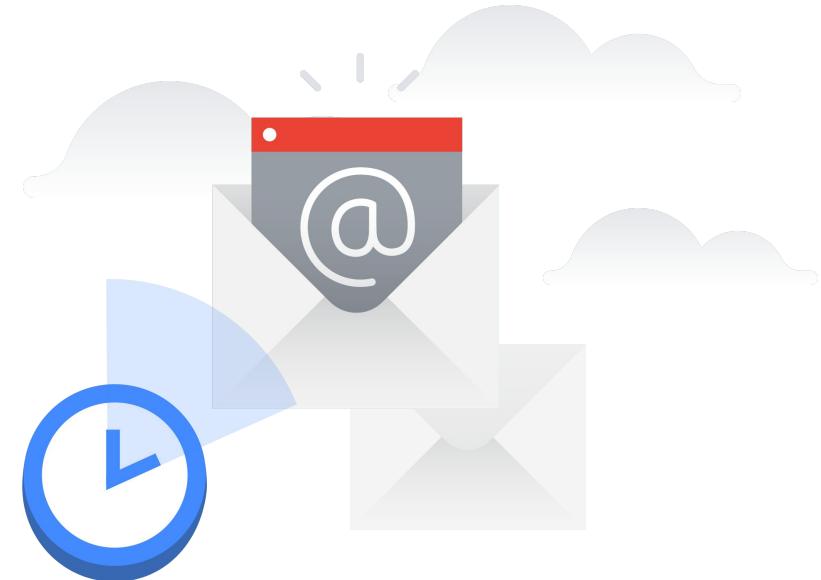
# Campaigns are small and short lived

250

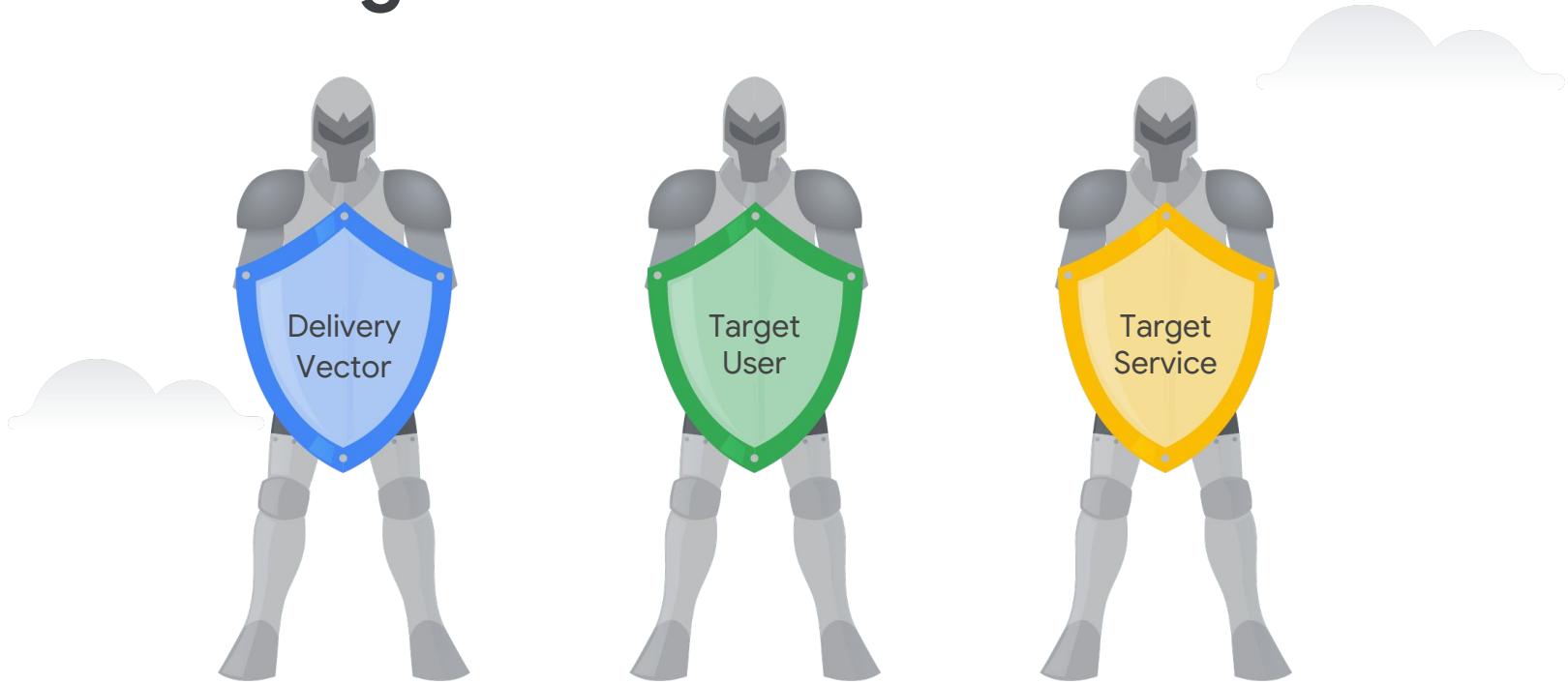
phishing emails  
per campaign

12

minutes campaign  
half life (median)



# The three guards



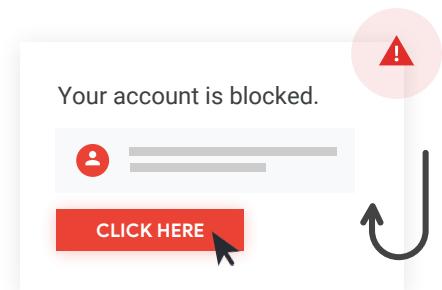
## Defeat the Delivery Vector

Email is accepted



## Defeat the User

User interacts with phishing email



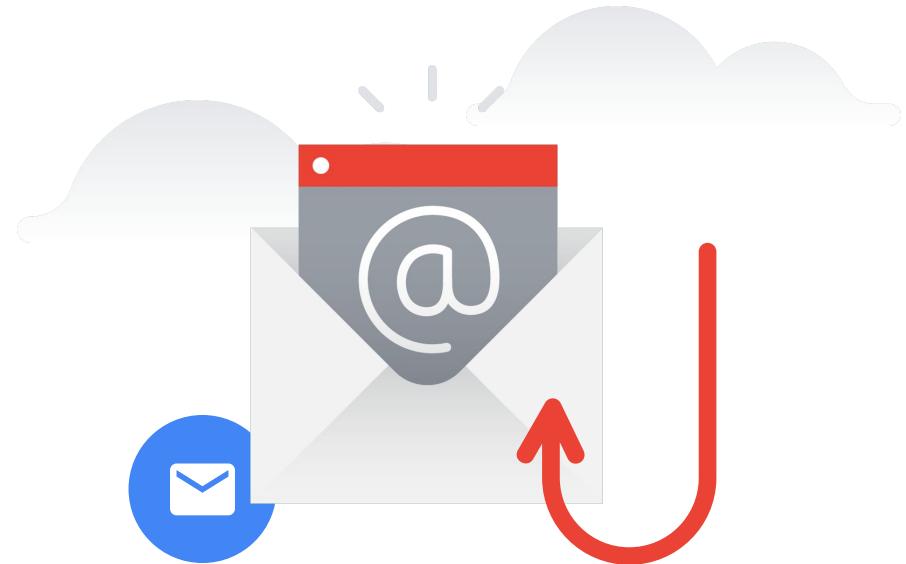
## Defeat the Target Service

Stolen authenticator logs in the phisher (ie. bank)



# Defeat the Delivery Vector

Email is accepted





# Anti-Phishing Infrastructure





Clustering



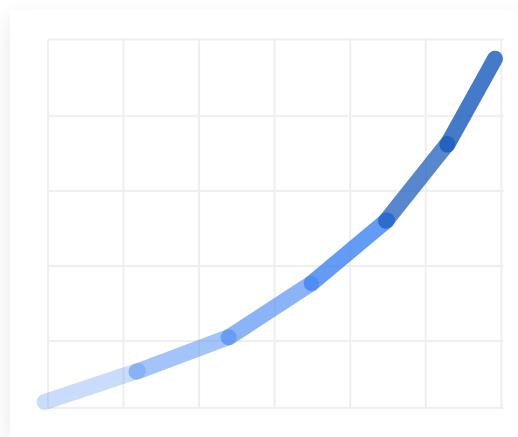
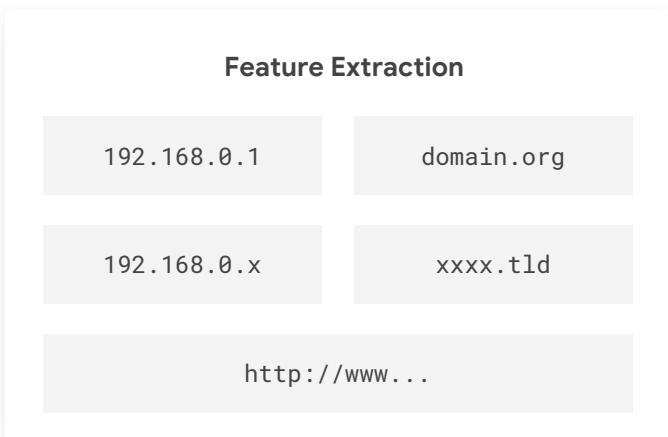
Reputation analysis



Content understanding

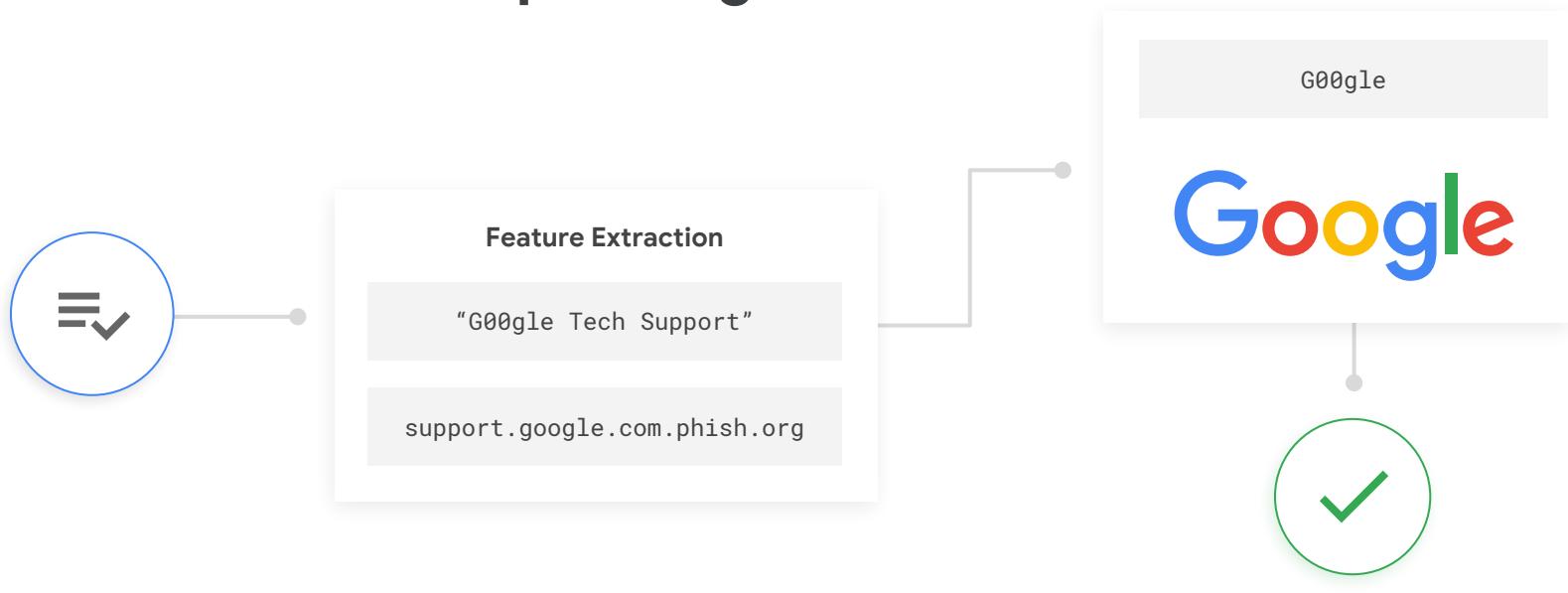


# Feature reputation



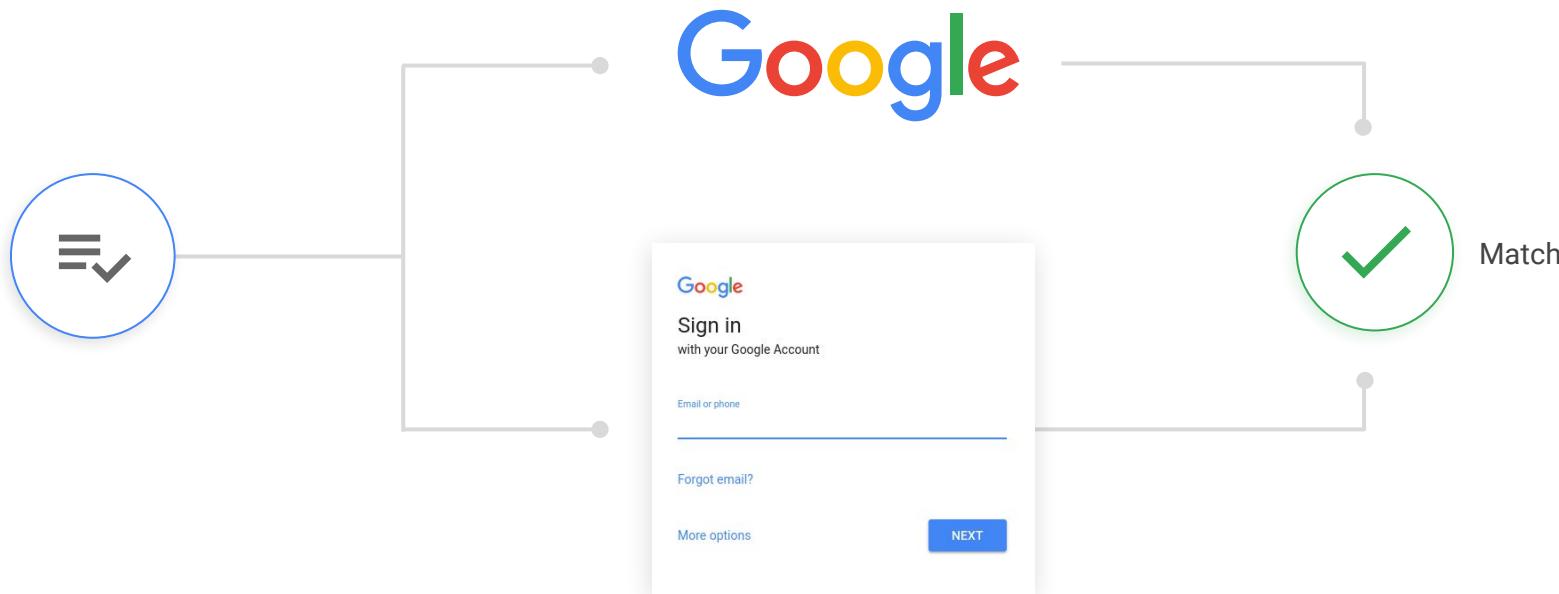


# Name / domain spoofing





# Visual similarity

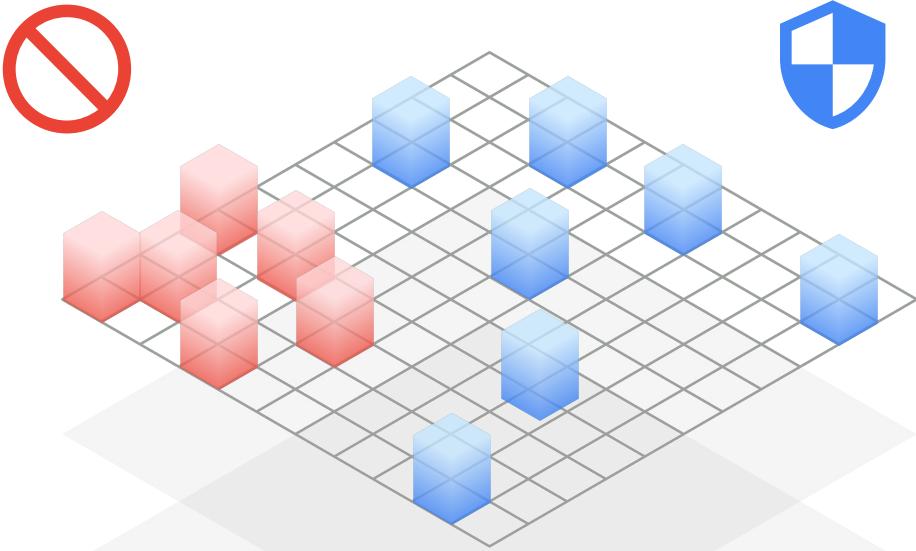


Google

RSA®Conference2019



# Harnessing AI to keep the bad out





# How to defeat ML?



## Evasion

Make attack  
a moving target





# Evasion: simple cloaking by IP subnet and domains

```
deny from paypal.com
deny from 112.207.com
deny from firefox.com
deny from apple.com
deny from zeustracker.abuse.ch
deny from virustotal.com
deny from adminus.net
deny from aegislab.com
deny from alienvault.com
deny from antiy.net
deny from avast.com
deny from team-cymru.org
deny from eset.com
deny from fireeye.com
deny from microsoft.com
deny from kernelmode.info
deny from malwaredomainlist.com
```



# Evasion: block by user agent

```
if(in_array($_SERVER['REMOTE_ADDR'], $bannedIP)) {  
    header('HTTP/1.0 404 Not Found');  
    exit();  
}  
  
if(strpos($_SERVER['HTTP_USER_AGENT'], 'google') or  
strpos($_SERVER['HTTP_USER_AGENT'], 'msnbot') or  
strpos($_SERVER['HTTP_USER_AGENT'], 'Yahoo! Slurp') or  
strpos($_SERVER['HTTP_USER_AGENT'], 'YahooSeeker') or  
strpos($_SERVER['HTTP_USER_AGENT'], 'Googlebot') or  
strpos($_SERVER['HTTP_USER_AGENT'], 'bingbot') or  
strpos($_SERVER['HTTP_USER_AGENT'], 'crawler') or  
strpos($_SERVER['HTTP_USER_AGENT'], 'PycURL') or  
strpos($_SERVER['HTTP_USER_AGENT'], 'facebookexternalhit')  
!== false) { header('HTTP/1.0 404 Not Found'); exit; }
```



# How to defeat ML?



## Evasion

Make attack  
a moving target



## Deception

Make ML and user  
see different things





# Deception: Human Perception vs Machine

Someone has your password

Hi Giorgi,  
Someone just used your password to try to sign in to your Google Account  
[redacted]@gmail.com.

Details:  
Tuesday, December 19, 2017 [redacted]  
United States (Las Vegas)\*

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

Someone has your password

Hi Giorgi,  
Someone just used your password to try to sign in to your Google Account  
[redacted]@gmail.com.

Details:  
Tuesday, December 19, 2017 [redacted]  
United States (Las Vegas)\*

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



# How to defeat ML?



## Evasion

Make attack  
a moving target



## Deception

Make ML and user  
see different things



## Confusion

Trick the user to provide  
ML with misleading data





# Confusion: fake affinity via reply

*To cancel the termination  
request reply to this mail.*

Google

The screenshot shows a Gmail inbox with a single message highlighted. The subject of the message is "Request To Terminate Your Google™". The message is labeled as "Final Notice" and is directed to the user's account. A warning banner indicates that the message is in spam because it is similar to messages identified as spam in the past. Below the message, there is a greeting to the "Gmail™ Customer" and a redacted email address. The main body of the email contains instructions for canceling the termination request by replying to the message. It also states that all files in the inbox will be deleted and access to the account will be denied if no reply is received within three working days. If the user wishes to terminate their email address, they are encouraged to sign up for a new one. Finally, it provides contact information for further help.

Request To Terminate Your Google™

Final Notice

to me

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

Dear Gmail™ Customer,

@gmail.com

You submitted a request to terminate your Gmail mail account and the process has started by our Gmail™ Team, Please give us 3 working days to close your mail account.

To cancel the termination request reply to this mail.

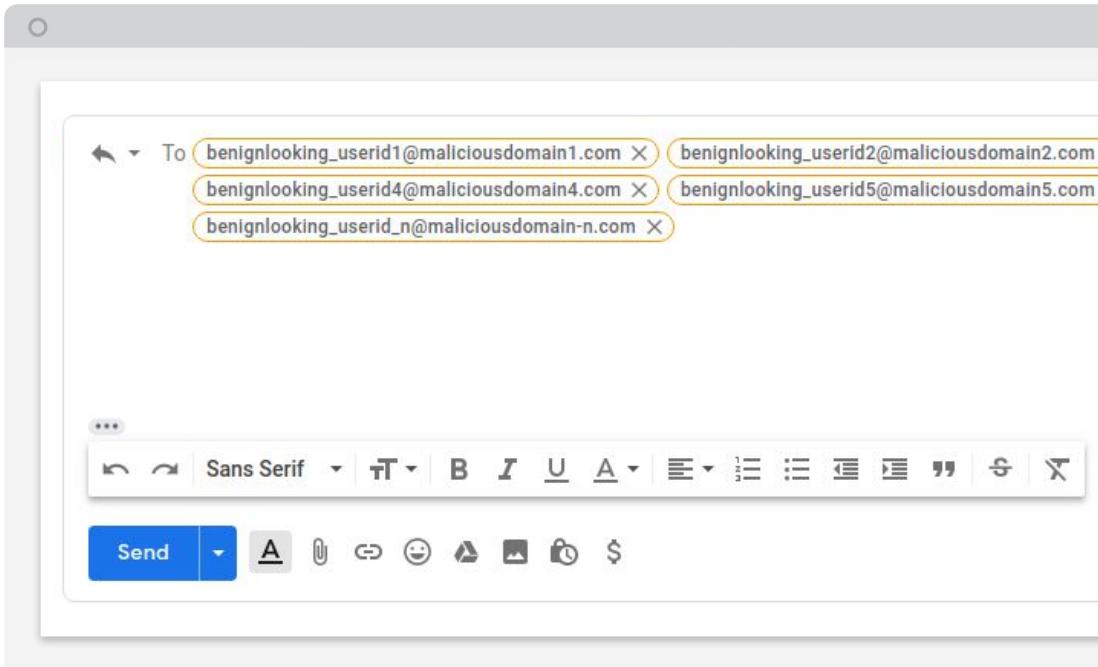
All files on your Gmail mail including (Inbox, Sent, Spam, Trash, Draft) will be deleted and access to your Gmail™ mail account will be Denied.

If you wish to Terminate your Email Address, you can Sign Up for a new Gmail™ account.

For further help please contact by replying to this mail.



# Confusion: fake affinity via reply





# How to defeat ML?



## Evasion

Make attack  
a moving target



## Deception

Make ML and user  
see different things



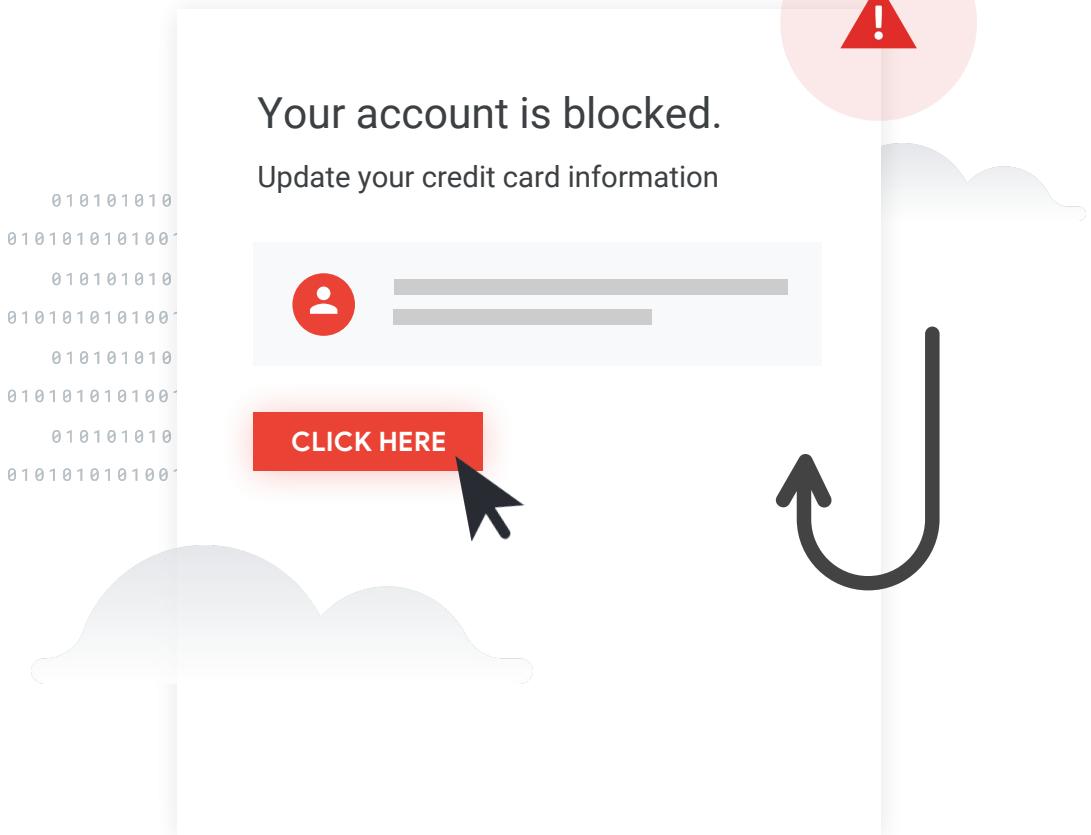
## Confusion

Trick the user to provide  
ML with misleading data



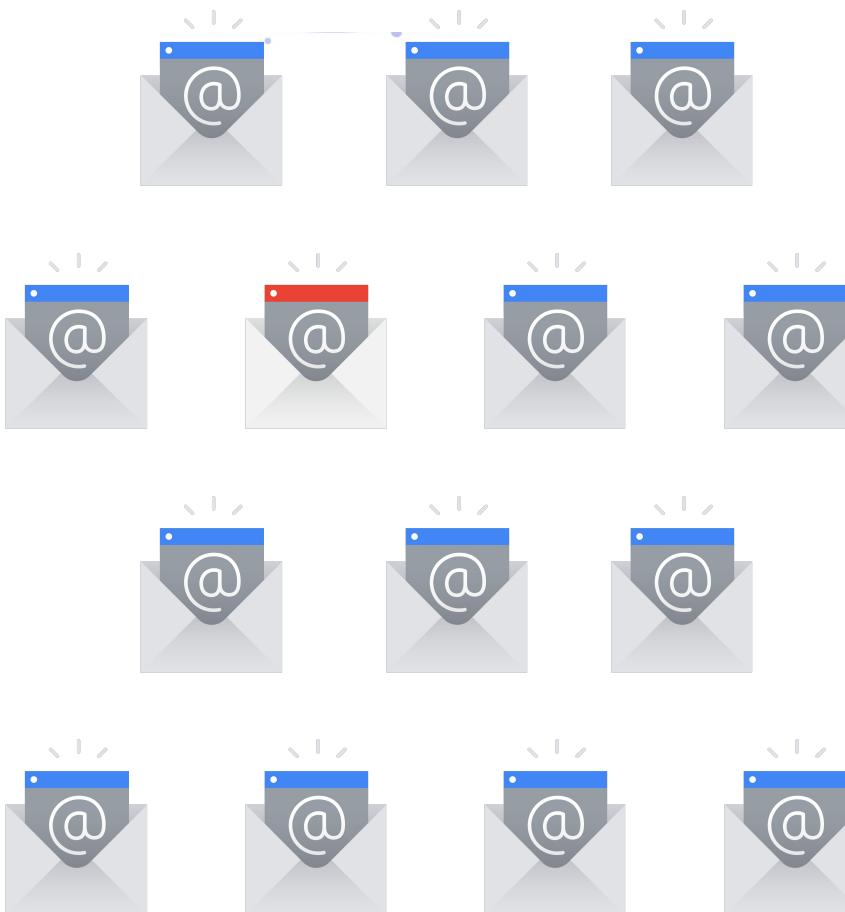
# Defeat the User

User interacts with phishing email





**Attention is a  
limited capacity  
resource**

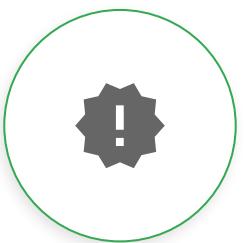




## How to fool users?



**Habits**  
Safe and Familiar



**Pressure**  
Embarrassment and Fear

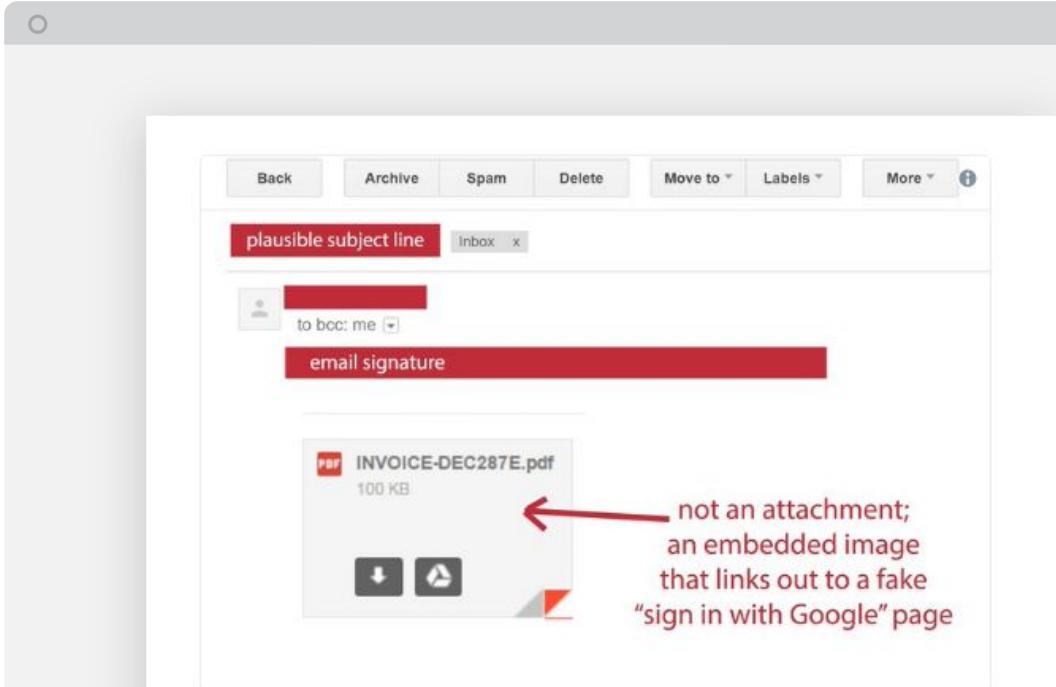


**Vanishing Reward**  
Limited opportunity



## Familiar user interface

Google



Source: Twitter @tomscott



# Technical support reaching out

Google

**Contact Gmail Klantenservice Team ontlast alle technische fouten van uw mailbox**

Absolut, na alle praktische functies van de Gmail-service, kunt u tijdens het gebruik van uw mailbox technische en niet-technische problemen tegenkomen. Wanneer u problemen ondervindt bij het gebruik van deze e-mailservice, moet u op zoek naar een betrouwbare oplossing, zodat alle problemen binnen een fractie van een tijd zijn opgelost. Om dit te doen, moet u contact opnemen met een expert van Gmail Klantenservice Nederland team. Wij, bij het technische ondersteuningsteam, bieden een oplossing voor elke kleine maar ook complexe situatie van uw mailbox en uw e-mailaccount bevindt zich nog steeds in een solide situatie. Er kunnen enkele technische en niet-technische problemen zijn en sommige staan hieronder vermeld:

**Onverwachte fouten van Google Mail/Gmail:**

- Fout bij e-mailbijlage.
- Problemen bij scannen of bestanden.
- Problemen met accounthacken.
- Kan geen back-up van de gegevens maken.
- Kan een account niet herstellen.
- Account ten onrechte verwijderd.
- Andere gerelateerde problemen.

U kunt enkele problemen tegenkomen die niet in deze lijst staan, geen zorgen; technisch team heeft de oplossing voor allerlei problemen. Alle technische fouten eindigen nu als u met een expert spreekt.

**Consistente technische ondersteuning van Gmail is nu mogelijk in slechts een paar klikken**

Het maakt niet uit of u een situatie waar u mee geconfronteerd wordt tijdens het openen van deze mailbox klein of ingewikkeld is; allerlei zorgen worden snel gemaakt. Als u onze expert vraagt, helpt hij u uw postvak in een robuuste staat te krijgen en krijgt u een verbeterde toegangservaring. Je kunt terug naar je werk en alles wordt gemakkelijk en de druk van je hoofd wordt vrijgegeven wanneer je contact opneemt met ons **Gmail ondersteuning Nederland**. Alle technische en niet-technische storingen komen ten einde wanneer u de aanwijzingen van onze technische assistentie-experts begint te volgen. Wat als u niet de steun van ons team heeft, het leidt zeker tot het verspillen van uw kostbare tijd. Hier is een lijst met oplossingen die u een volledig idee geven over de hulp die ons team van experts biedt.

Technische assistentie aangeboden door Gmail-experts:

- Hulp bij het maken van een sterk wachtwoord.
- Hulp bij het creeren van beveiliging in uw mailbox.
- Begeleiding om uw mailbox in een beveiligde toestand te houden.
- Directe hulp voor gehackte accounts.
- Help om een verandering in het thema aan te brengen.
- Hulp bij het ordenen van uw mailboxmails.
- Richtingen om een bepaald contact te blokkeren.
- Help om de ongewenste e-mails weg te houden.
- Extra beveiling van uw mailbox.
- Andere gerelateerde oplossingen.

Als je al deze bovengenoemde oplossingen hebt gelezen, dan heb je vast wel het idee van de oplossingen die haalbaar zijn door ons technische team. Het is echter een kleine afbeelding hier; u krijgt de complete oplossingen van ons team van experts.

**Is het belangrijk om met het technische team te praten?**

Ja! Het is goed als u een expert vraagt om een vraag op te lossen die u tegenkomt met uw e-mailaccount. Een van de belangrijkste redenen om verbinding te maken met de technische ondersteuning van Gmail, is dat je onmiddellijk hulp krijgt en de duurzame oplossingen van onze experts. Alle verontrustende situaties komen tot een stilstand en u zult in de toekomst niet dezelfde situatie vinden. Als u ons **Gmail klantenservice telefoonnummer** bewaart, krijgt u de onmiddellijke hulp van experts.

**Waarom contact opnemen met het Gmail ondersteuningsteam?**

Er zijn een aantal redenen om contact op te nemen met het Gmail ondersteuningsteam; hier zijn enkele redenen die je het belang zullen bepalen.

- 24/7 Telefonische ondersteuning door helpdesk nummer
- Alle kleine en complexe problemen worden opgelost in één enkele oproep.
- Volledige beschikbaarheid voor alle gebruikers.
- Hulp op afstand.

Houd ons Gmail helpdesk telefoon bij de hand om contact op te nemen met ons technische team van experts.



# Using embarrassment or fear

Google

Thanks from X-rated

Inbox ×

X-rated <team@xrated.com>



THANKS FOR SHARING

X-rated now has automated video sharing to your social media account

Thanks X-rated

Decline Sharing

No need to share your videos to your friends and family ever again because  
this new revolutionary sharing feature does it for you! Automatically!



# Credential leaks for sextortion

Google

Hi, stranger!

I know the **password123**, this is your password, and I sent you this message from your account.

If you have already changed your password, my malware will be intercepts it every time.

You may not know me, and you are most likely wondering why you are receiving this email, right?

In fact, I posted a malicious program on adults (pornography) of some websites, and you know that you visited these websites to enjoy (you know what I mean).

While you were watching video clips, my trojan started working as a RDP (remote desktop) with a keylogger that gave me access to your screen as well as a webcam.

Immediately after this, my program gathered all your contacts from messenger, social networks, and also by e-mail.

What I've done?  
I made a double screen video.  
The first part shows the video you watched (you have good taste, yes ... but strange for me and other normal people), and the second part shows the recording of your webcam.

What should you do?



# Service interruption...

Google

The image shows a digital communication interface. At the top, there's a decorative header with blue and purple abstract patterns and icons. Below it, a large red circular button on the right contains a white exclamation mark. To its left is a white rectangular area containing an email message. The message starts with "Dear Customer," followed by "Thank you for choosing XXXXXX." It continues with an explanation about server upgrading and account details. Below this, it says "For more details please log in to your XXXXXX Control Panel:" followed by a URL. At the bottom, it concludes with "Sincerely," and the name "Sebastian Gonzalez" along with his title "XXXXXX Head of Customer Service".

Dear Customer,

Thank you for choosing XXXXXX.

We are currently upgrading our server to give you the best of our service. We require you to upgrade your account details to avoid service being interrupted. A separate confirmation e-mail will be sent with your contract terms and conditions once your upgrade has been successfully processed.

For more details please log in to your XXXXXX Control Panel:

<http://cp.xxxxxxxx.com.nevs.net.au>

Sincerely,

Sebastian Gonzalez  
XXXXXX Head of Customer Service



... with ironic  
anti-phishing  
training

Security Update  
Webmail Login

Email Address  
Password

Log In      Forgot Password?

Remember this info  
 Use SSL

SUSPICIOUS EMAIL  
Learn to quickly identify and report

SEE HOW >

Need webmail for your business? Learn more about Hosted Email from [RingCentral](#)

Privacy Statement | Website Terms

Google



Entice you with  
the promise of  
a prize...

Google

The screenshot shows a mobile browser displaying the Interac e-Transfer website. At the top, there's a black header bar with the Interac e-Transfer logo on the left and language options (FRANÇAIS, ?, =) on the right. Below the header, the main content area has a light gray background. A large downward arrow icon is followed by the text "Deposit Your Money". Underneath, it shows a transfer amount of "\$32,75 CAD" and the "From" information as "Bell mobility". There are two buttons below this section: "View Transfer Details" with a magnifying glass icon and "Select Your Financial Institution" with a search icon. The "Select Your Financial Institution" section contains a grid of logos for various Canadian banks and financial institutions, including BMO, CIBC, Desjardins, HSBC, RBC, and Meridian.



**...and ask nicely  
for your bank  
credentials**

Google

Your Online Banking session has expired. If you wish to continue using Online Banking, please log in again.

### Log in to Online Banking

username \*

password \*

email \*

email password \*

[Log In](#) [Forgot Your Password](#)

Remember Me

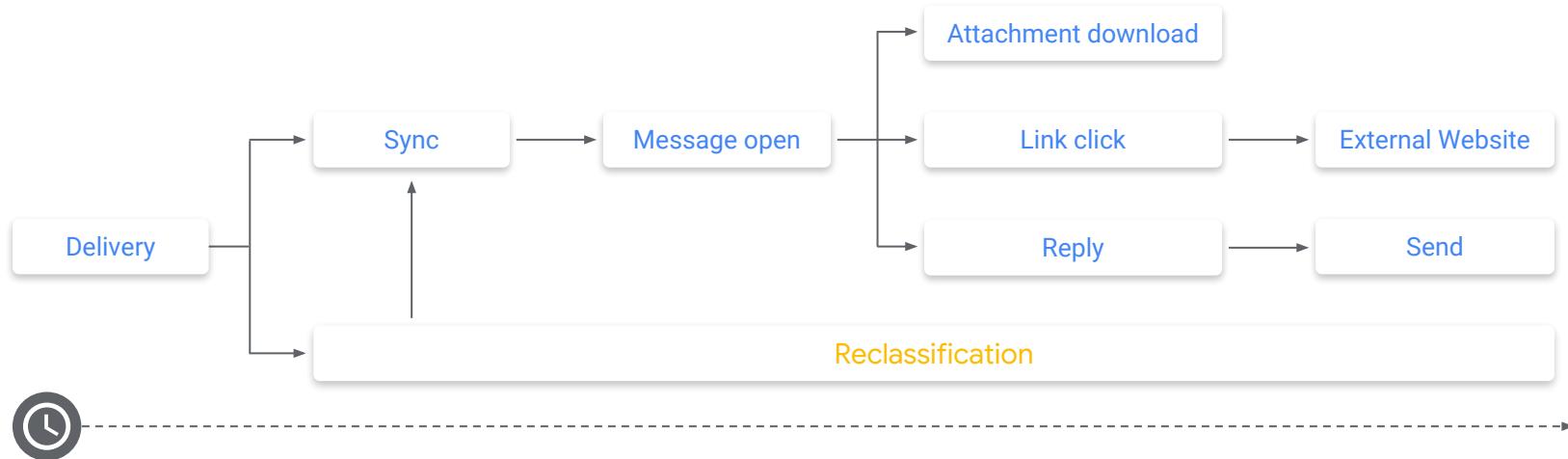
New to Online Banking? Enroll Now.

[Personal](#) | [Small Business](#)

<b>Helpful Links</b>	<a href="#">Protect Your Account</a>	<a href="#">Watch our Online Banking video</a>	<a href="#">Security Features demo</a>
<hr/>			
<a href="#">Privacy Policy</a>			
<b>ExpressBank</b>	1-800-234-6181		A live banker is available during the following hours (CT):
			<b>Monday - Friday</b> 6 a.m. - 10 p.m.
			<b>Saturday</b> 7 a.m. - 7 p.m.
			<b>Sunday</b> 10 a.m. - 7 p.m.
<b>Open an Account</b>	<a href="#">Checking</a>	<a href="#">Savings &amp; Money Market</a>	<a href="#">Loans</a>
	<a href="#">Credit Cards</a>		
<a href="#">Find a Banking Center/ATM Near You</a>		<a href="#">Contact Us</a>	

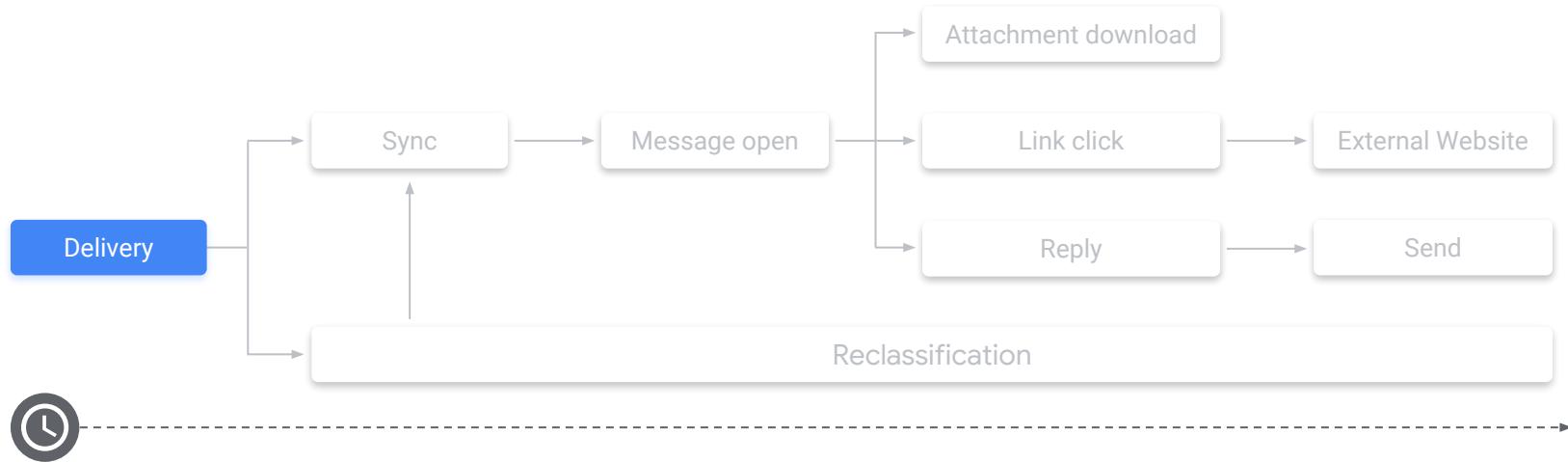


# The life of a message



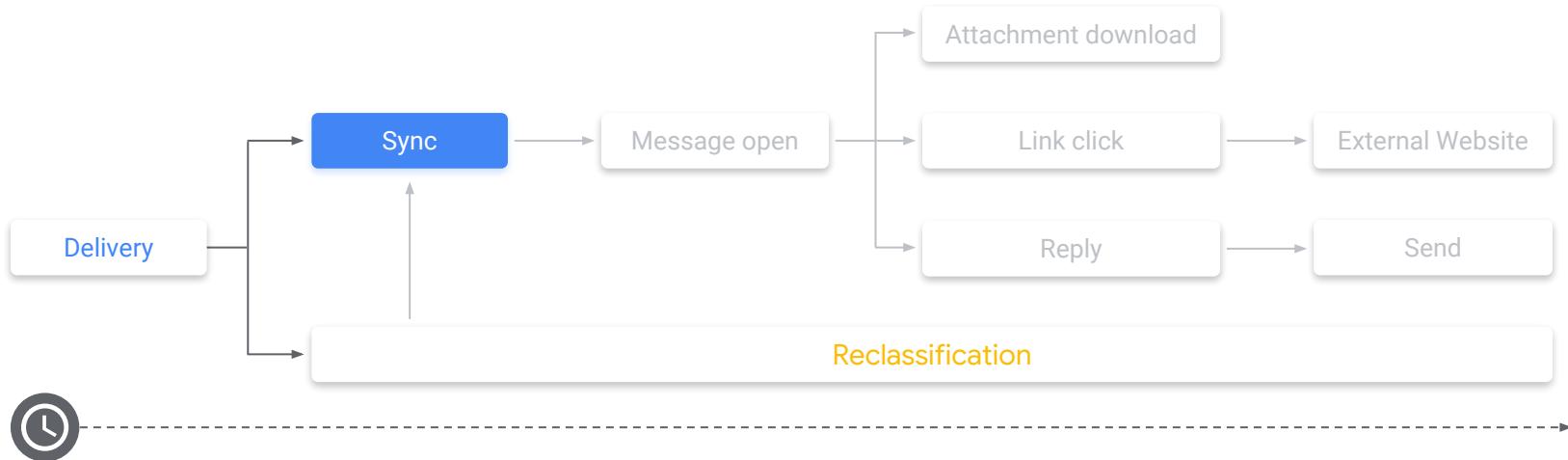


# Delivery



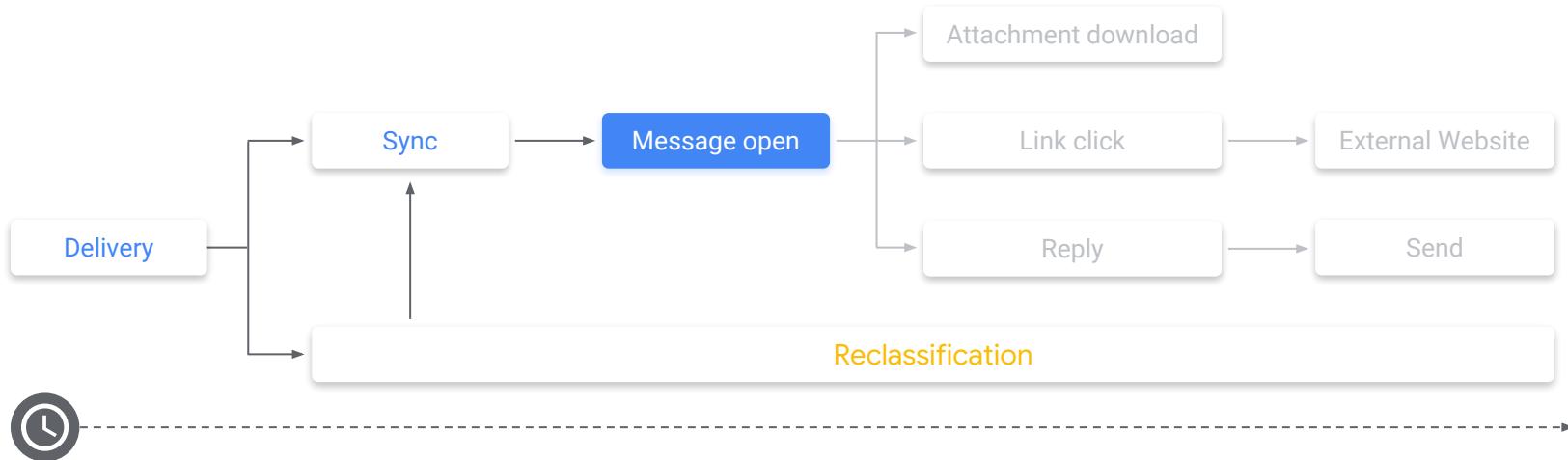


# Sync



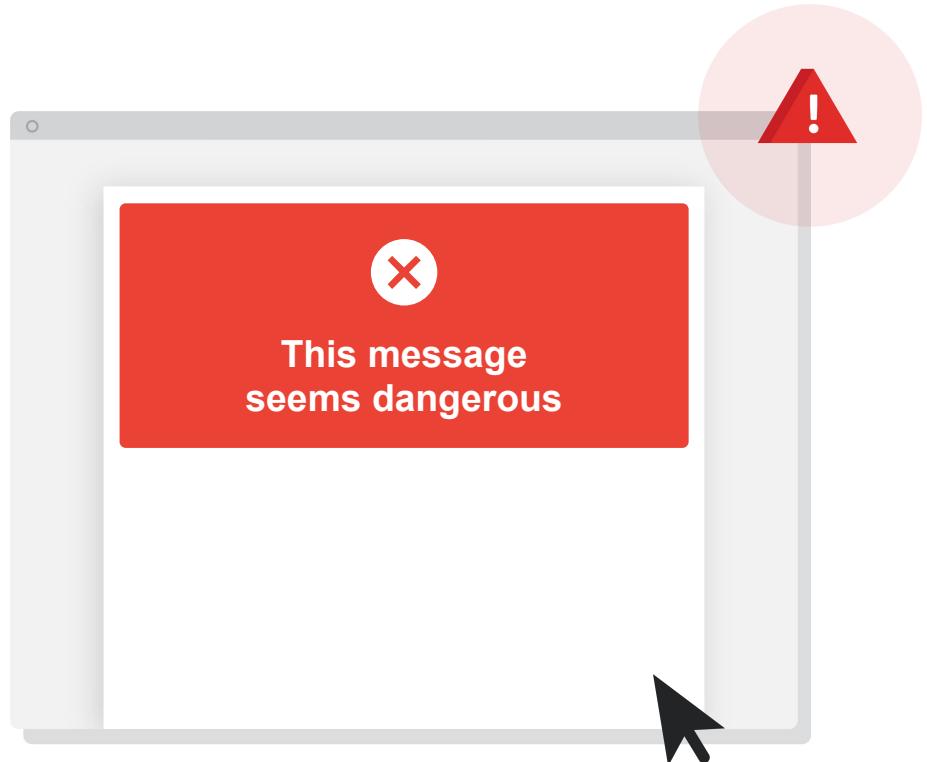


# Message open





# Big and obvious warning banners





# Message open: warning banners

Re: Security Banner Design Inbox ×

Charlie Samuel <csamuel@frdesign.cx>



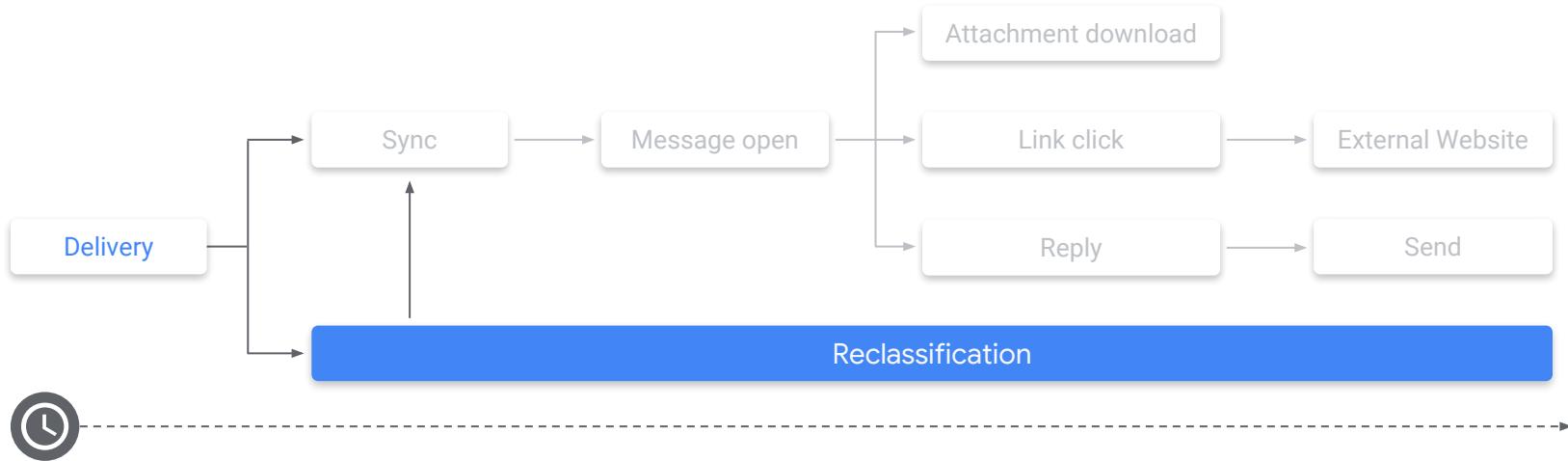
**This message seems dangerous**

The sender's account may have been compromised. Avoid clicking links, downloading attachments, or replying with personal information. If you Know the sender, consider alerting them (but avoid replying to this email).

Report Looks Safe



# Reclassification



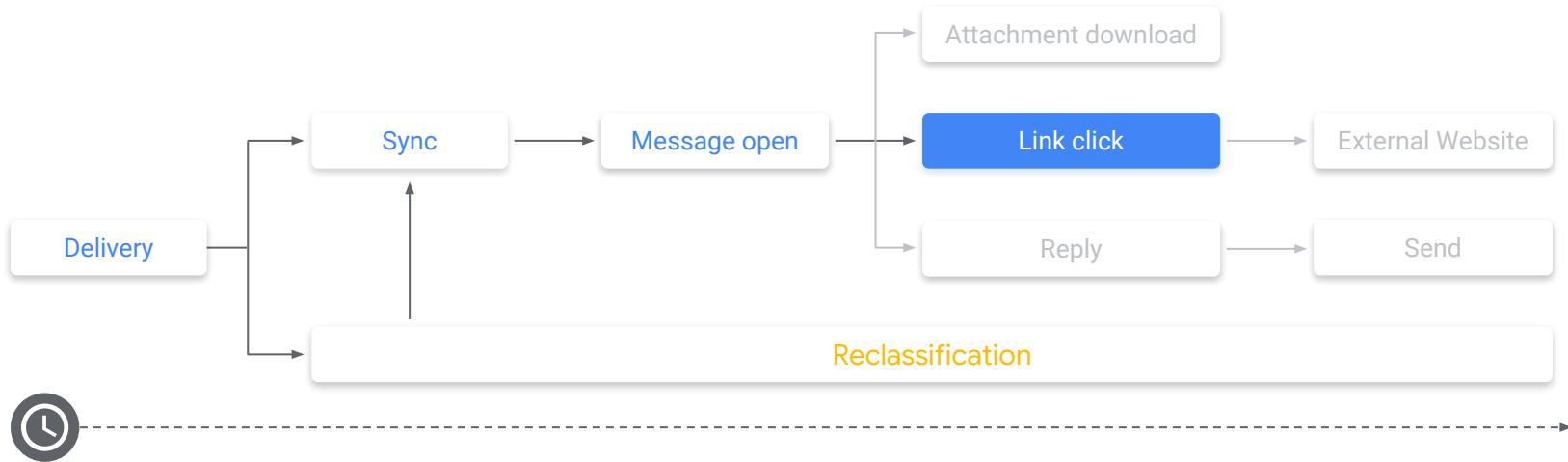


# Phishing locality: co-worker warning via outbreak banners

The screenshot shows a Gmail inbox interface. On the left, there's a sidebar with navigation links: Compose, Inbox (which is highlighted in red), Starred, Snoozed, Important, Sent, Projects, Team, Tickets, Support, and More. The main area displays an email from "IT-support@support-acme.com" with the subject "[IT-Support] Please install latest software update". A yellow warning banner is overlaid on the email content, containing the text "Be careful with this message" and "One or more members of your organization have marked this email as phishy. Avoid clicking links, downloading attachments, or replying with personal information." It includes two buttons: "Confirm phishing" and "I'm sure it's safe". Below the banner, the email body continues with "Notice to all Acme employees," and instructions about updating Java. At the bottom, it says "Thanks for understanding, IT Department, Acme". The top right corner of the screen shows the "ACME" logo.



# Link click





# Suspicious Link Warning

The screenshot shows a Gmail inbox interface. On the left, a sidebar lists 'Inbox' (highlighted with a red bar), 'Starred', 'Snoozed', 'Sent', 'Drafts' (with 5 items), 'Gmail/Android', and 'More'. The main area displays an email from 'James Smith' to the user, received at 2:13 PM (2 minutes ago). The subject is 'Reset your password'. The message body contains the text: 'Please click [here](#) to reset your password.' Below the message are 'Reply' and 'Forward' buttons.



# Suspicious Link Warning

The screenshot shows a Gmail inbox with the following details:

- Inbox:** Reset your password (from James Smith, 2:13 PM (3 minutes ago))  
Message preview: Please click [here](#) to reset your password.
- Left sidebar:** Starred, Snoozed, Sent, Drafts (5), GmailAndroid, More
- Bottom right modal:** Suspicious link  
Text: This link leads to an untrusted site. Are you sure you want to proceed to pintoqa.androidqaqaqa.com?  
Buttons: Proceed (gray), Back (blue)



# Real Time Check



Google Safe Browsing

**Warning — visiting this web site may harm your computer!**

You can continue to <http://example.com/> at your own risk. For detailed information about the problems we found, visit Google's [Safe Browsing diagnostic page](#) for this site.

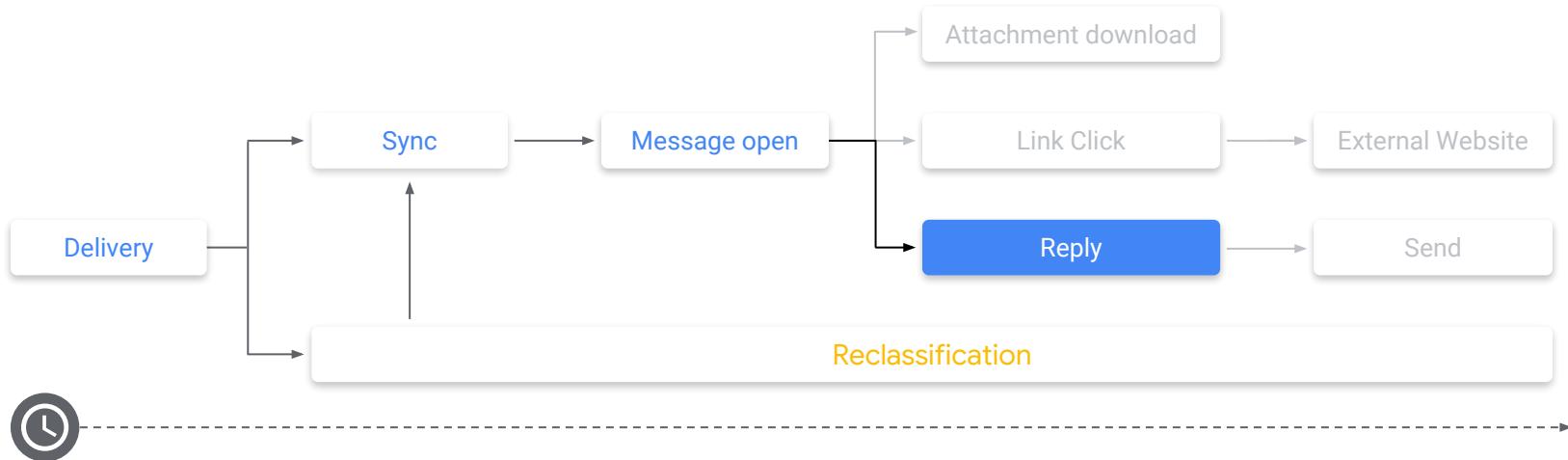
For more information about how to protect yourself from harmful software online, you can visit [StopBadware.org](#).

If you are the owner of this web site, you can request a review of your site using Google's [Webmaster Tools](#). More information about the review process is available in Google's [Webmaster Help Center](#).

Advisory provided by



# Reply





# Out of Domain Warning

The screenshot shows an email in the inbox titled "Chinese licensing deal". The sender is "John Smith, CEO <johnsmith.alphabeta@gmail.com>". The recipient is "to me". The timestamp is "12:50 PM (5 minutes ago)". The body of the email reads:

Hi Kathy,  
I'm in Beijing closing the deal with our partner. What was our bank account number again? I need to access the funds right away.

---

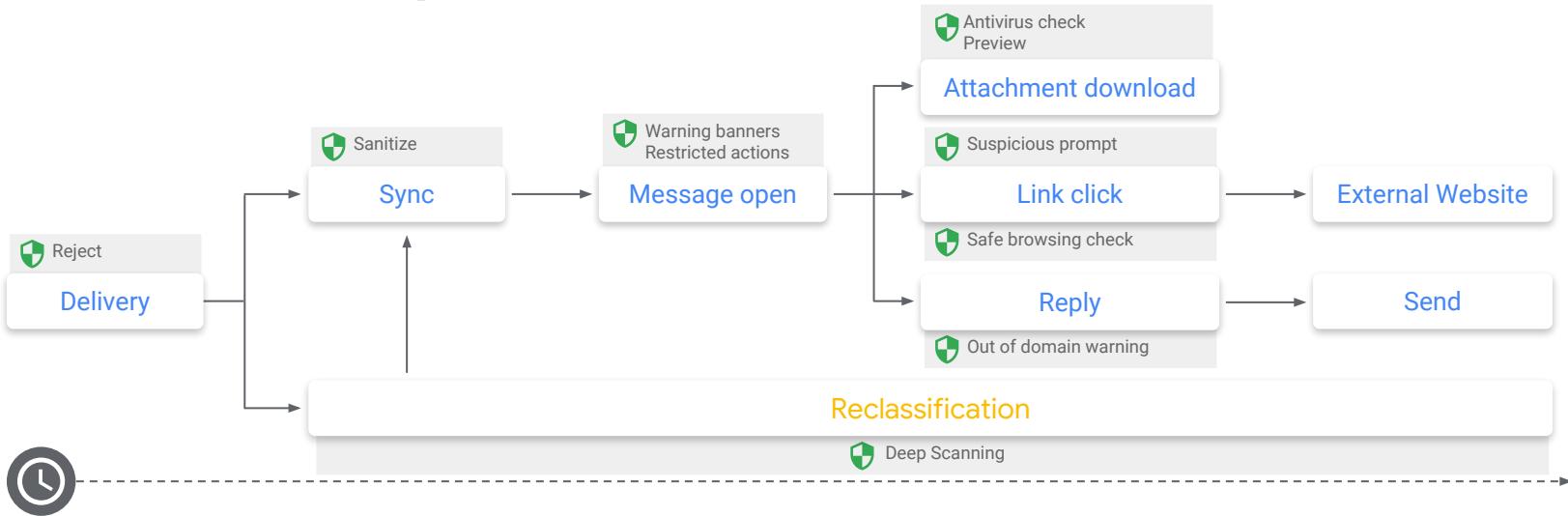
John Smith, CEO  
AlphaBeta Pharmaceuticals

A tooltip message "Make sure this is someone you trust. johnsmith.alphabeta@gmail.com does not belong to your organization and is not in your contacts." appears over the recipient field.

The bottom of the screen shows the standard Gmail compose interface with a toolbar containing icons for font style, size, bold, italic, underline, alignment, and other editing tools. A "Send" button is visible at the bottom left.



# Defense in depth





# Look ahead for malicious remote content

Links and external images Additional settings to prevent email phishing due to links and external images. [?](#)

Locally applied

Disable all settings

Enable all settings

This provides your domain with the strongest level of safety.  
All settings under "Customize settings" below will be enabled.  
**Future settings will be automatically enabled.**

Customize settings

Future recommended settings will be automatically enabled.

Identify links behind shortened URLs  
Allow discovery of hidden malicious links behind shortened URLs.

Scan linked images  
Allow scanning of images referenced by links to find hidden malicious content.

Show warning prompt for any click on links to untrusted domains  
Gmail clients will show a warning prompt when users click on any link in email to untrusted domains (does not work on IMAP/POP email clients).  
If you don't activate this feature, warnings will only be shown for clicks to untrusted domains from suspicious emails.



# Protect against domain and employee spoofing

Google

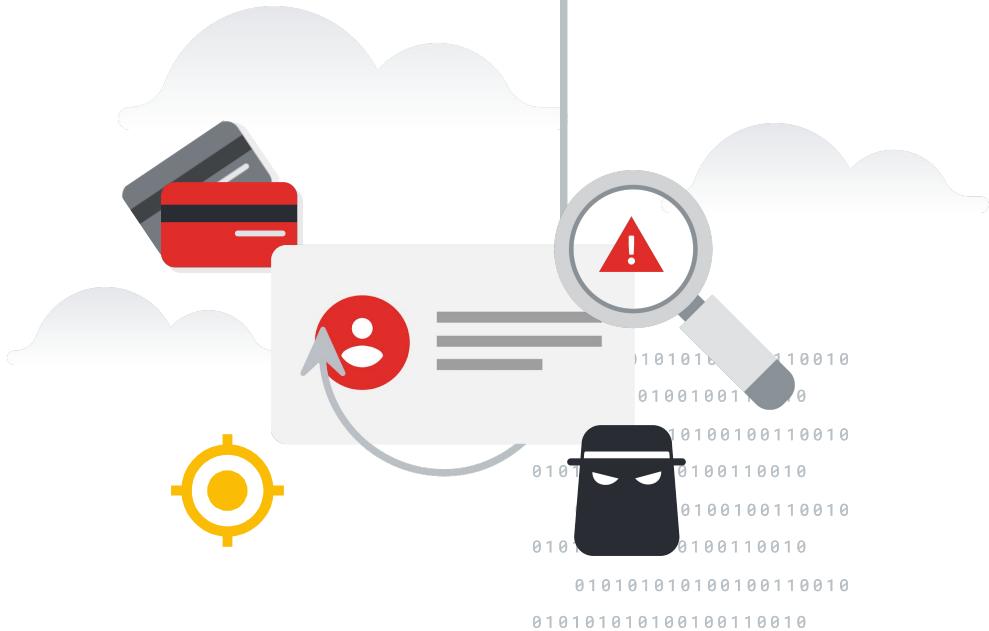
The screenshot shows a web interface for managing security settings. At the top, there's a header with the title "Spoofing and authentication" and a note "Locally applied". Below this, there are three main options: "Disable all settings" (radio button), "Enable all settings" (radio button, selected), and "Customize settings". Under "Customize settings", five checkboxes are listed, all of which are checked:

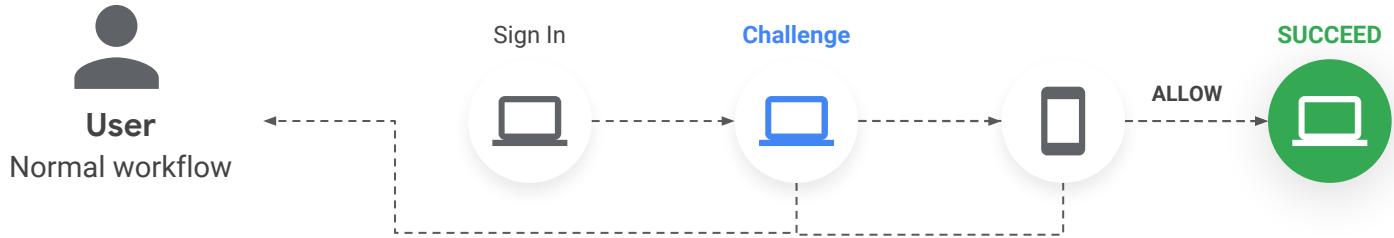
- Protect against domain spoofing based on similar domain names
- Protect against spoofing of employee names
- Protect against inbound emails spoofing your domain
- Protect against any unauthenticated emails
- Protect your Groups from inbound emails spoofing your domain

Each checked item has a descriptive subtitle below it.

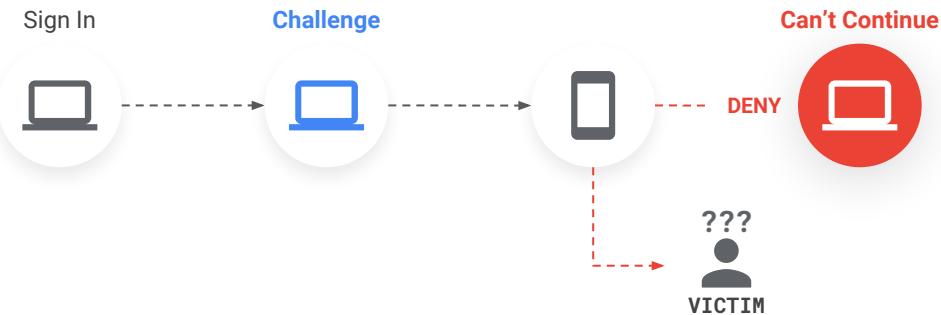
# Defeat the Target Service

# Phisher using the stolen authenticator



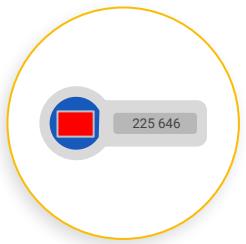


Hacker  
Hijacker workflow





# Attackers are adapting



Phisable 2FA



Mobile Platforms



Monitor for unusual activity



Use second factor



Use phishing resistant authentication

Faking user geolocation/  
browser configuration



Phish for second factor



Use a different attack method



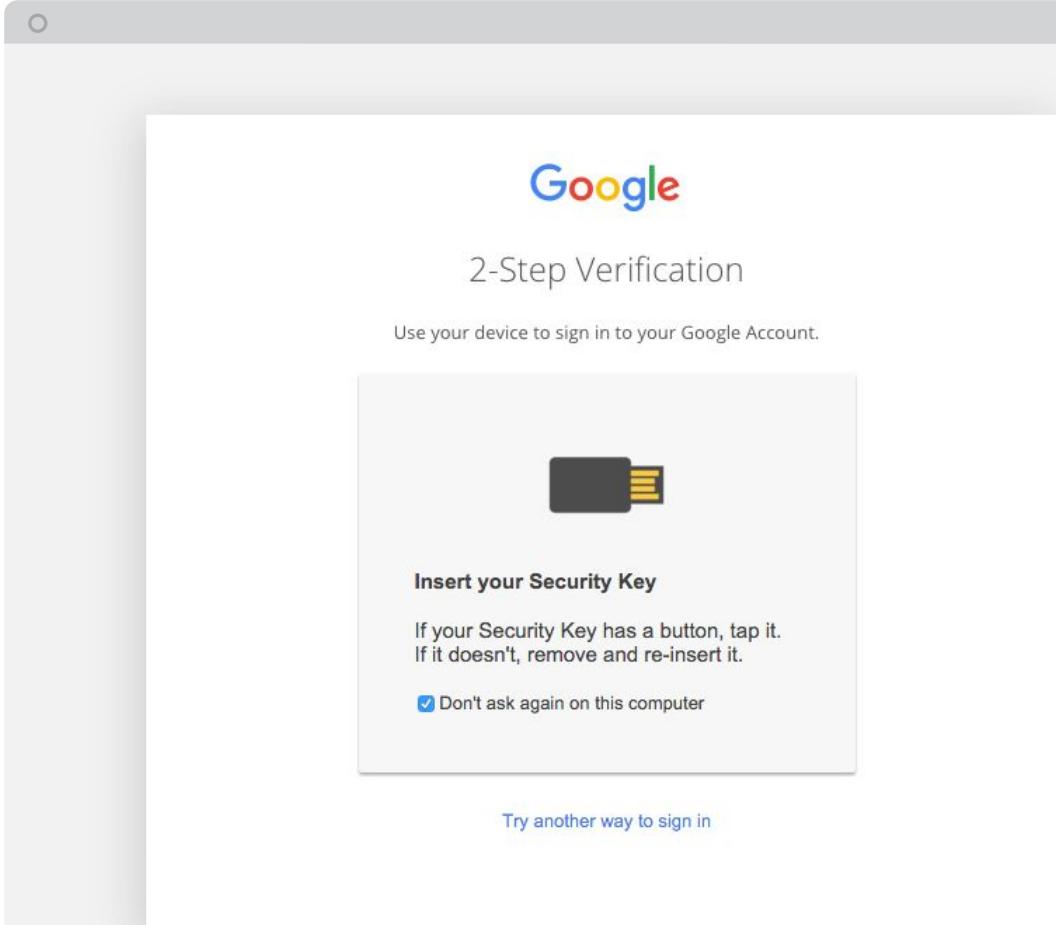


# Raising the bar



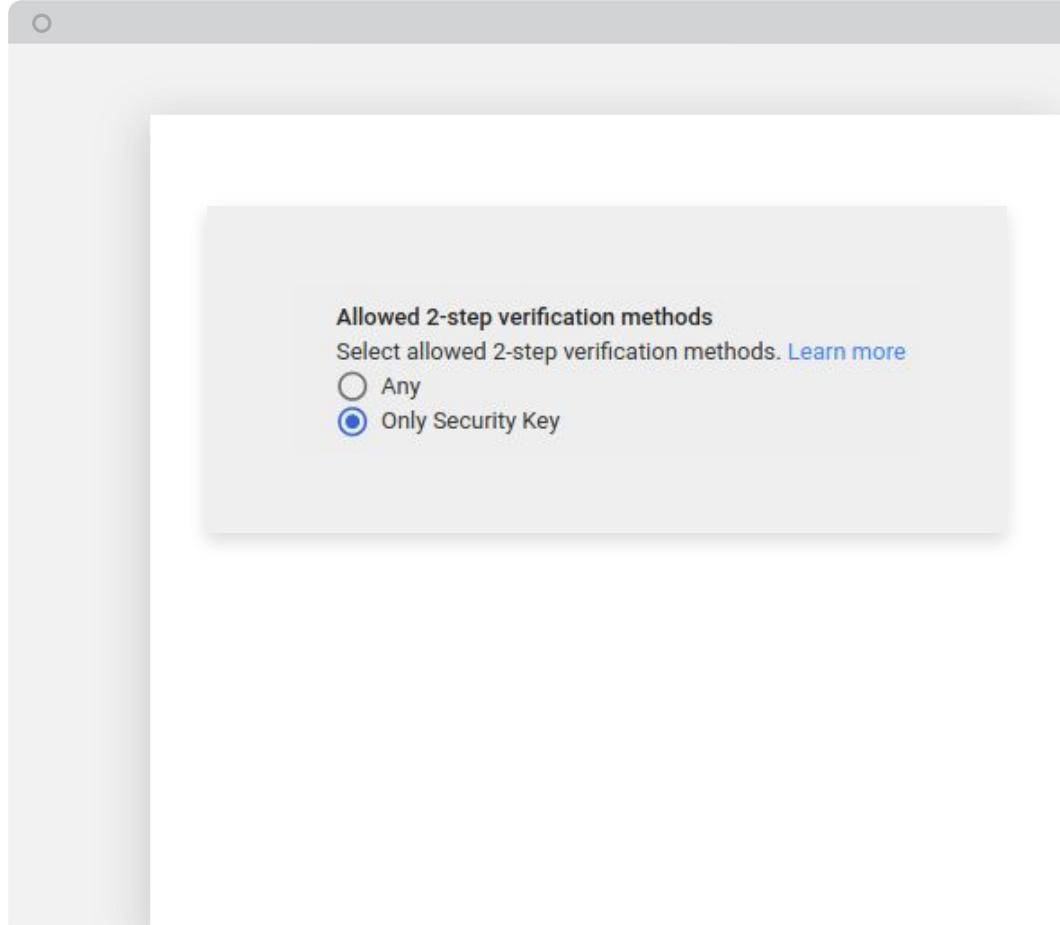
# FIDO U2F tokens

Google





**Make it  
mandatory  
and phishing  
resistant for  
employees**





## Apply what you learned today



Build defenses  
in depth



Use phishing resistant  
solutions



Apply domain  
specific defenses



Monitor unusual  
activity on accounts

# Takeaways: next week

- Ensure your outgoing emails are all strongly authenticated (DKIM, DMARC).
- Use a password manager and 2FA.

# Takeaways: over the next 3 months

- Start plan for phishing resistant 2FA solutions for all employees.
- Enable advanced security options for incoming emails.

# Takeaways: over the next 6 months

- Investigate Brand Indicators for Message Identification (BIMI).
- Investigate FIDO2 for service auth.



# Questions?

<https://safety.google> | <https://cloud.google.com/security>



# Thanks.

<https://safety.google> | <https://cloud.google.com/security>