RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: HT-R03

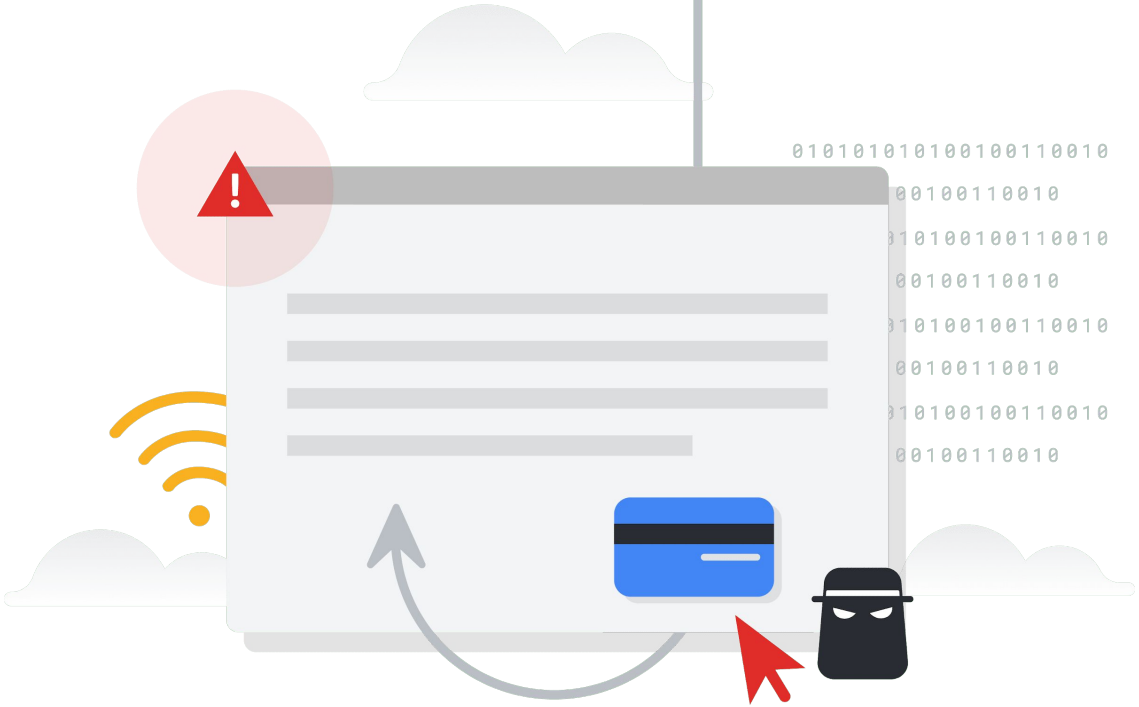
Anatomy of Phishing Campaigns: A Gmail Perspective

Nicolas Lidzborski
Gmail & G Suite Security Engineering Lead

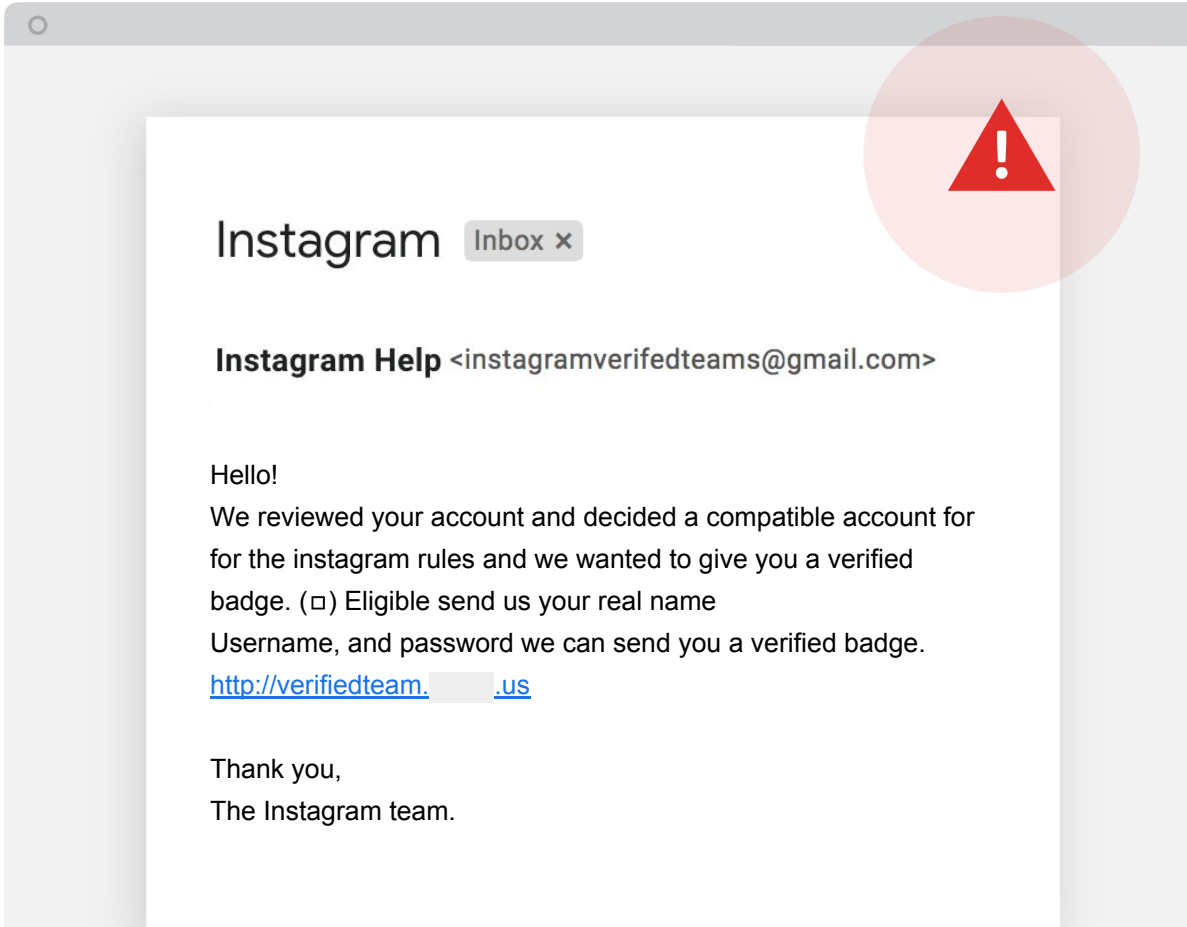
Ali Zand
Google Anti-Abuse Research team

Google

Phishing 101



Is phishing still a thing?



Phishing is actually prolific and effective!


Gmail sees over **100M**
phishing emails per day!

ZDNet MENU

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

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 Share Share 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.

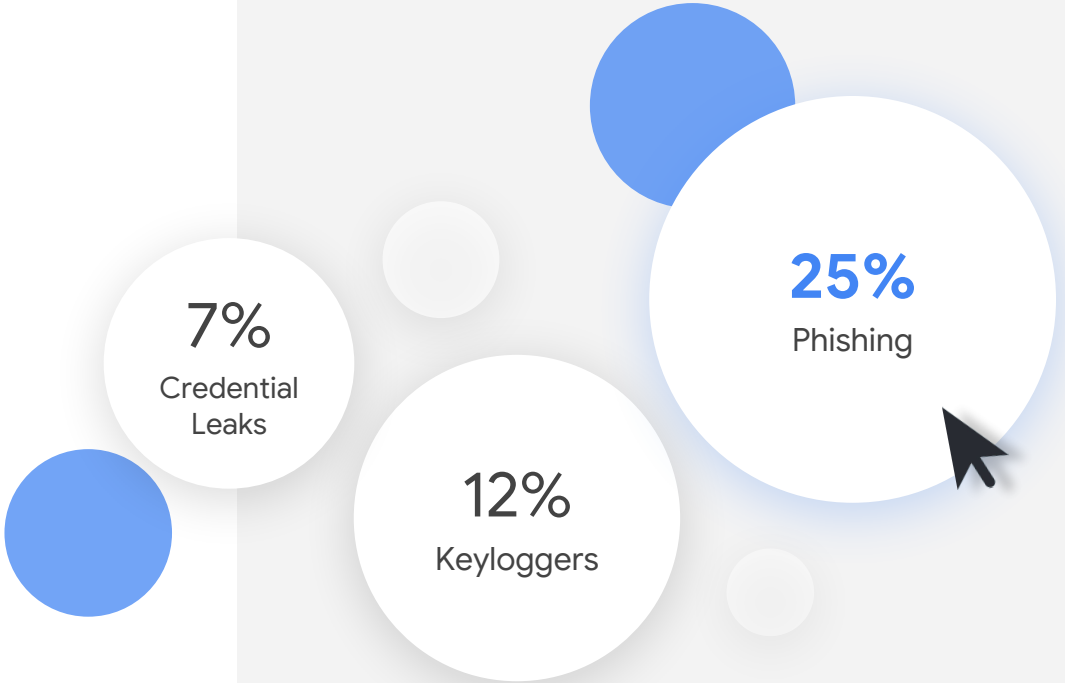
243 views | Dec 6, 2018, 08:01am

Whaling Wars: A $12 Billion Financial Dragnet Targeting CFOs

Dante Disparte Contributor

Crypto & Blockchain

Successful Hijacking

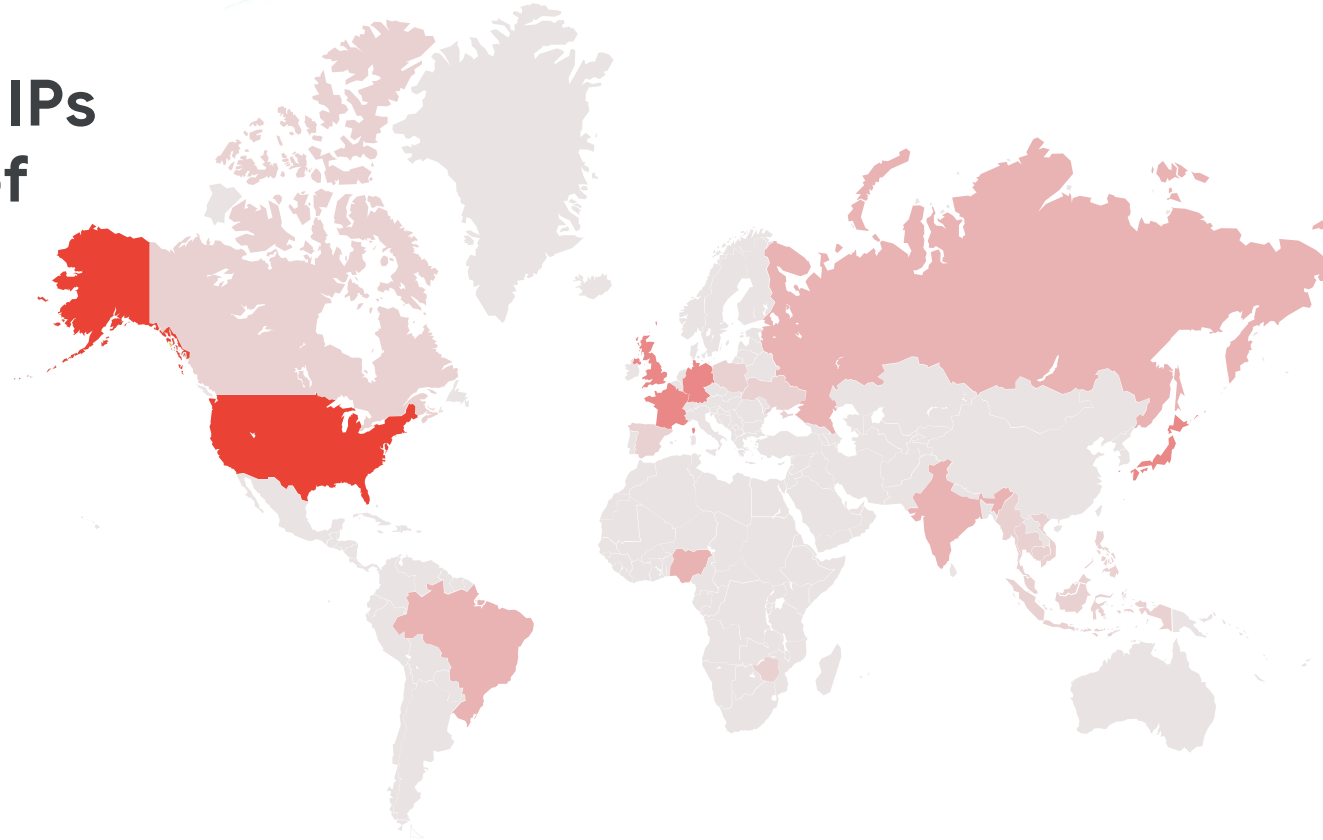


Source: Data breaches, phishing, or malware?: Understanding the risks of stolen credentials

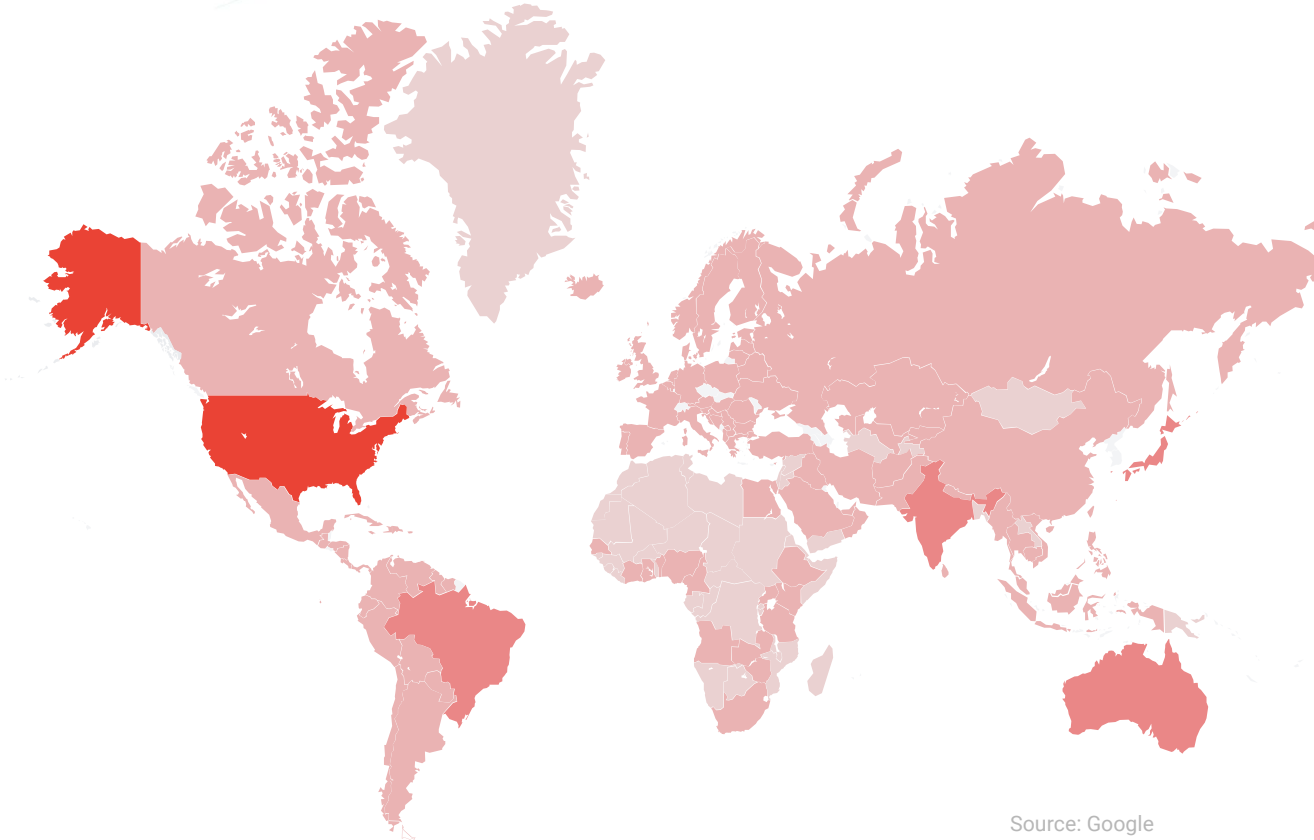
Google

Phishing is a global issue!

Attackers use IPs from variety of countries



Targets are everywhere

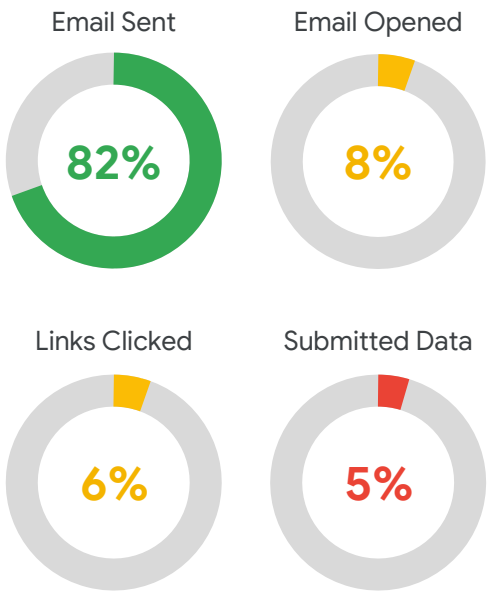


Source: Google

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

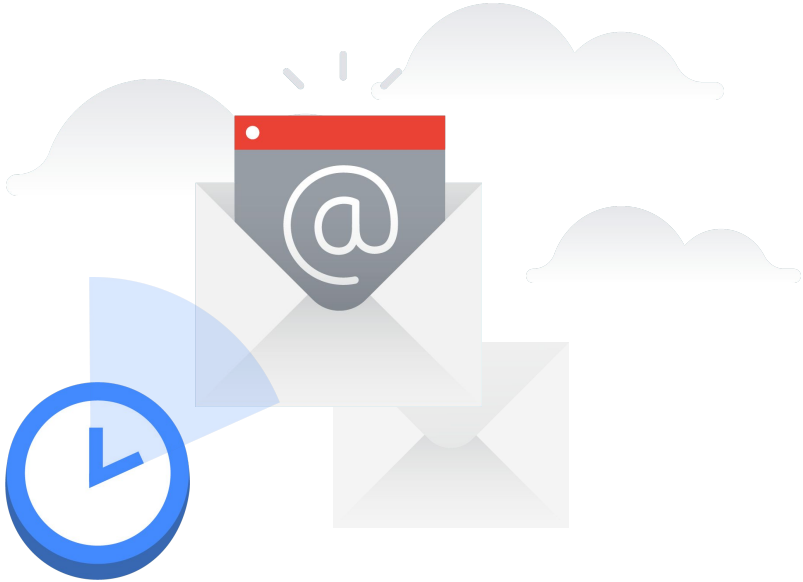


Source: gophish dashboard

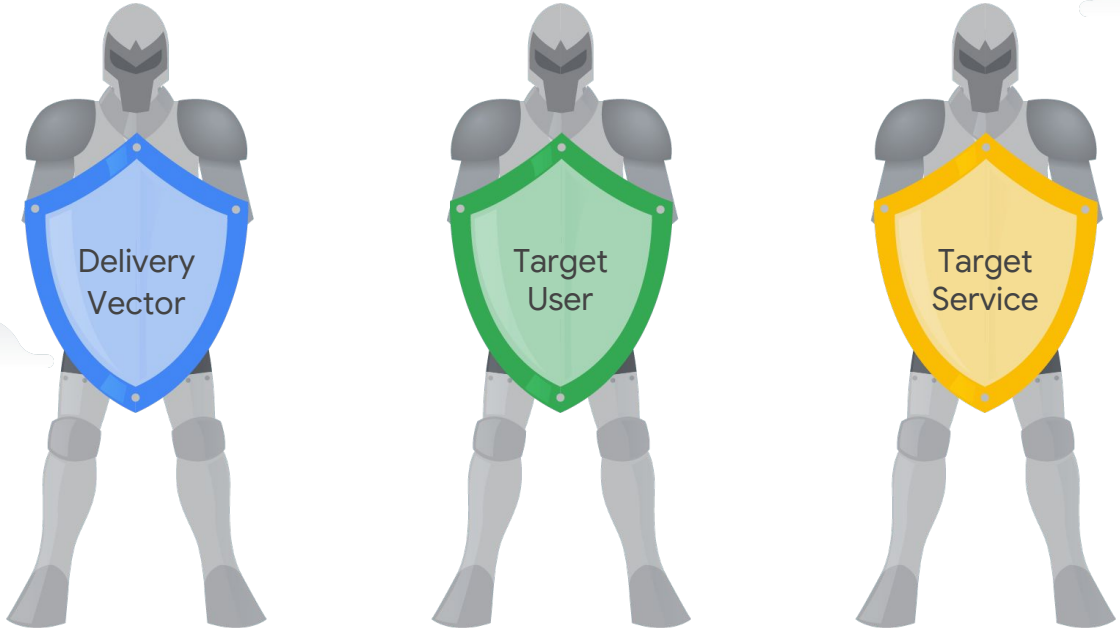
Campaigns are small and short lived

250 phishing emails per campaign

12 minutes campaign half life (median)



The three guards

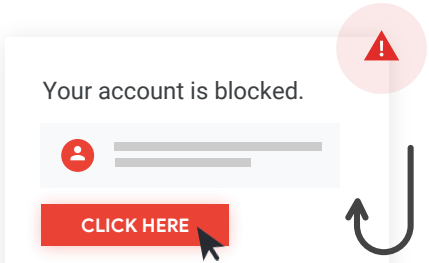


Defeat the Delivery Vector

Email is accepted

Defeat the User

User interacts with phishing email



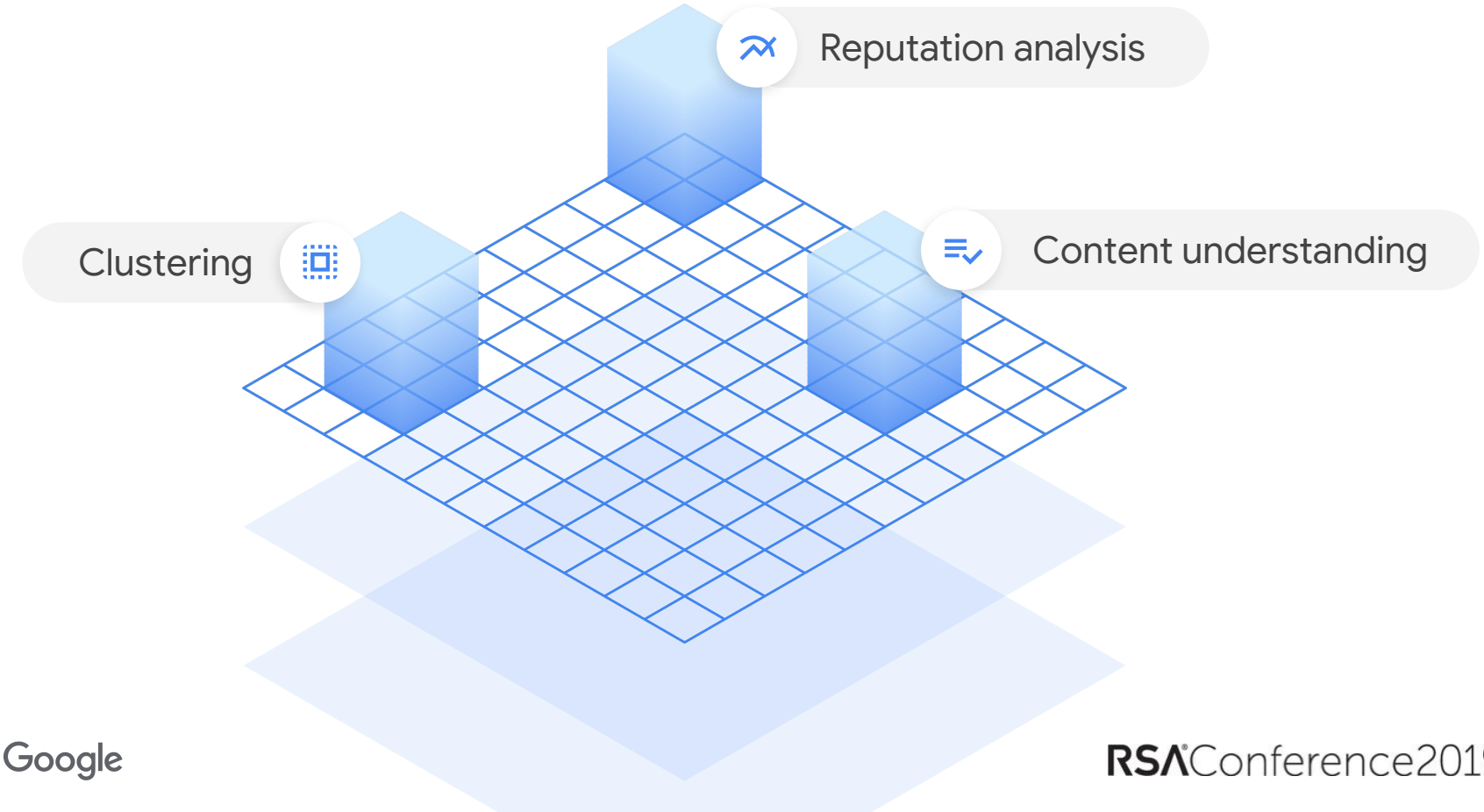
Defeat the Target Service

Stolen authenticator logs in the phisher (ie. bank)

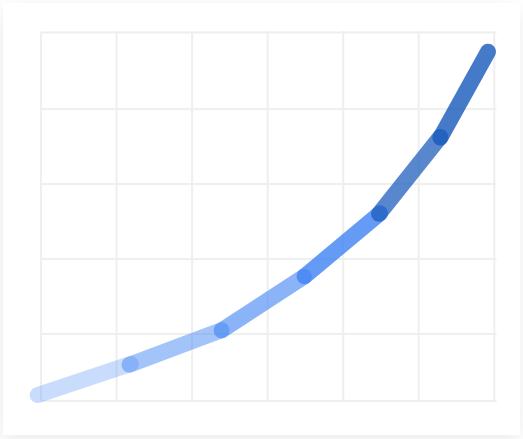
Defeat the Delivery Vector

Email is accepted

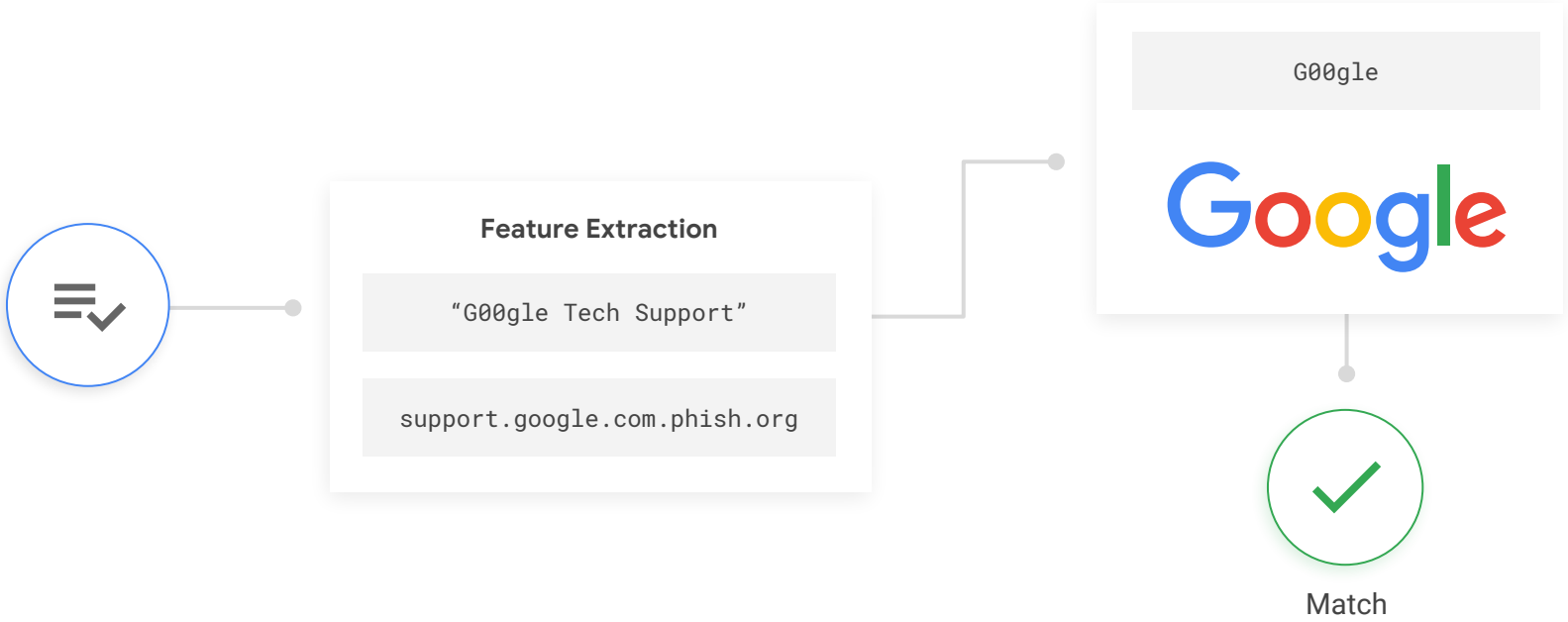
Anti-Phishing Infrastructure


Reputation analysis
Clustering
Content understanding

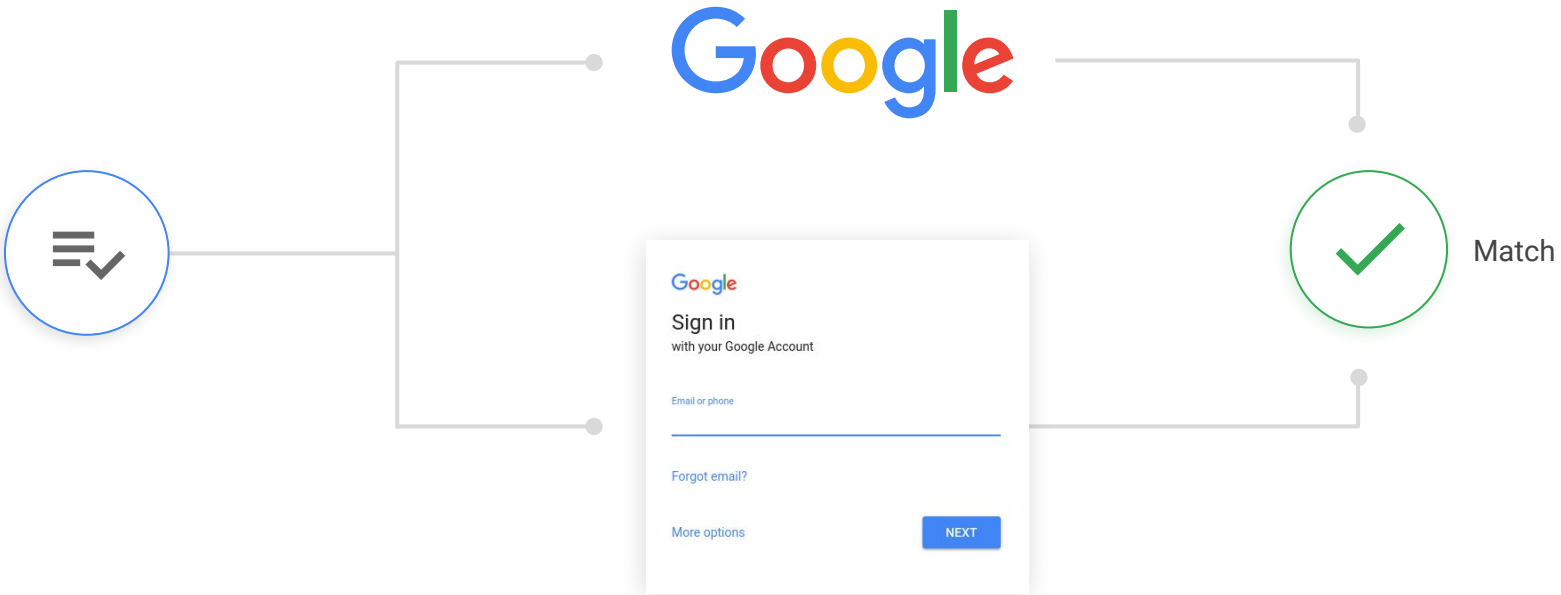
Feature reputation



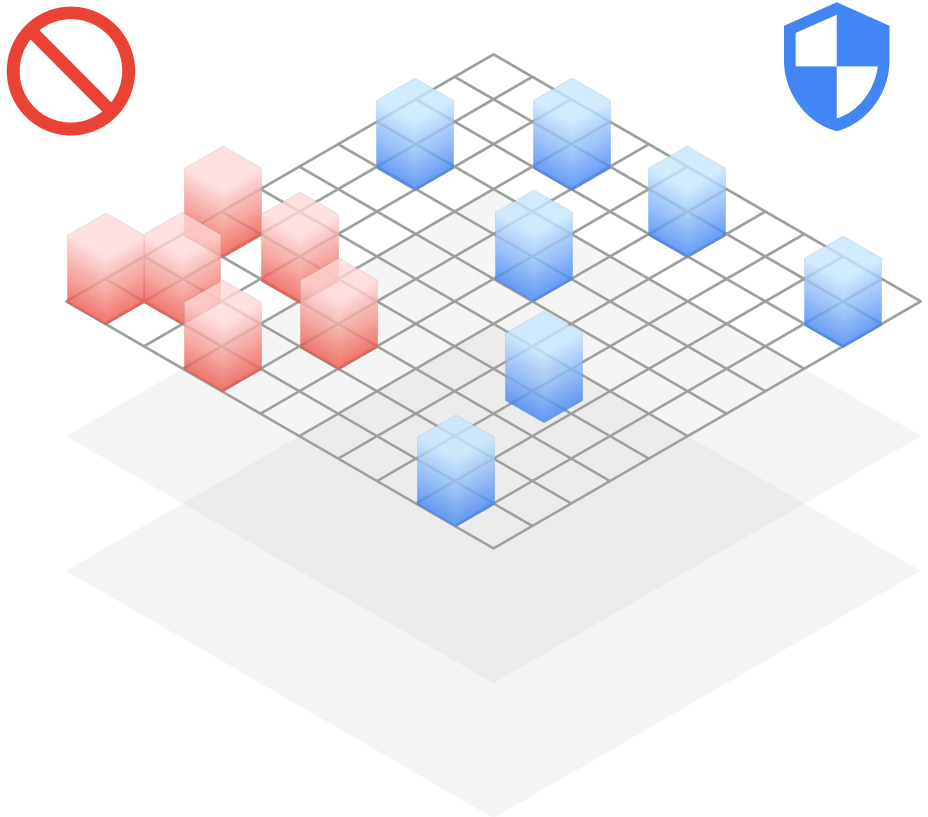
Name / domain spoofing



Visual similarity



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 112.2o7.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?

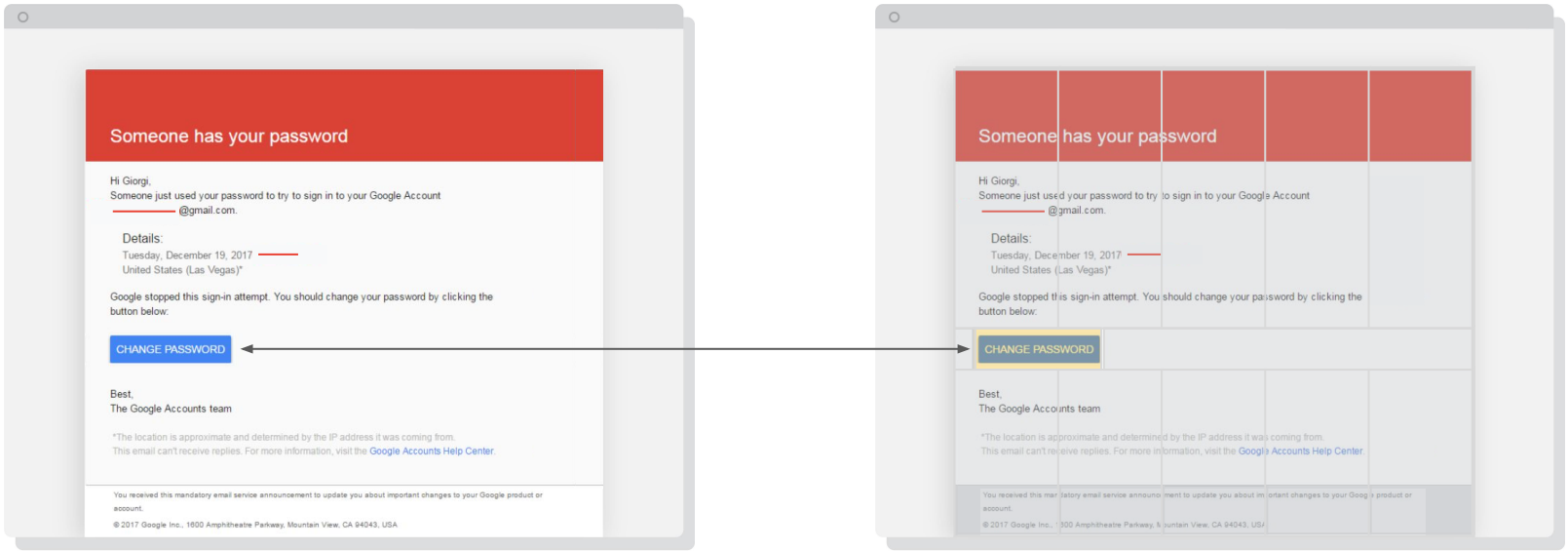
Evasion

Make attack
a moving target

Deception

Make ML and user
see different things

Deception: Human Perception vs Machine



How to defeat ML?

Evasion

Make attack
a moving target

Deception

Make ML and user
see different things

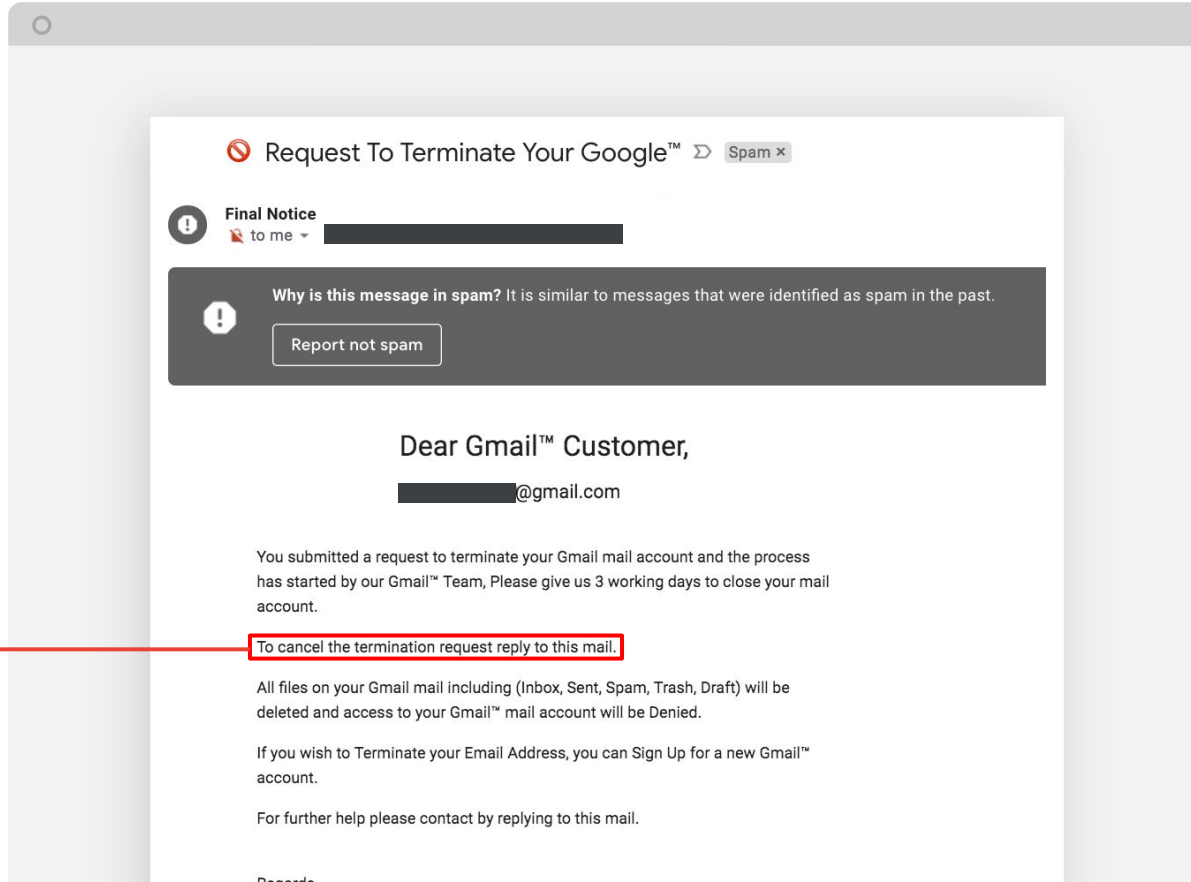
Confusion

Trick the user to provide
ML with misleading data

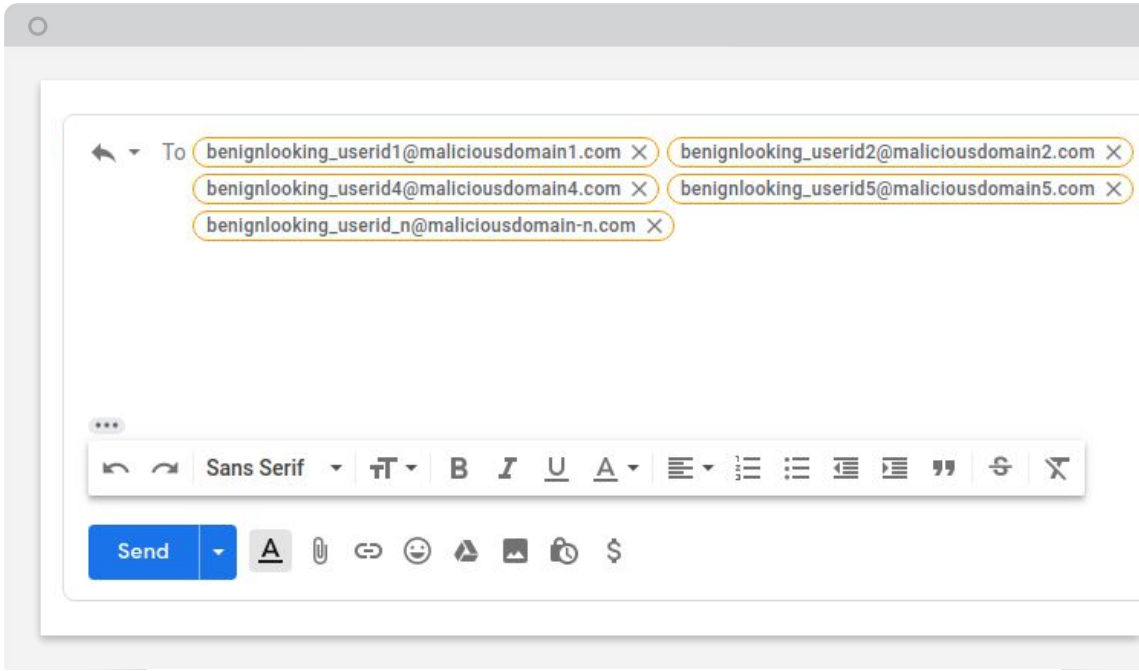
Confusion: fake affinity via reply

To cancel the termination request reply to this mail.

Google



Confusion: fake affinity via reply



How to defeat ML?

Evasion

Make attack
a moving target

Deception

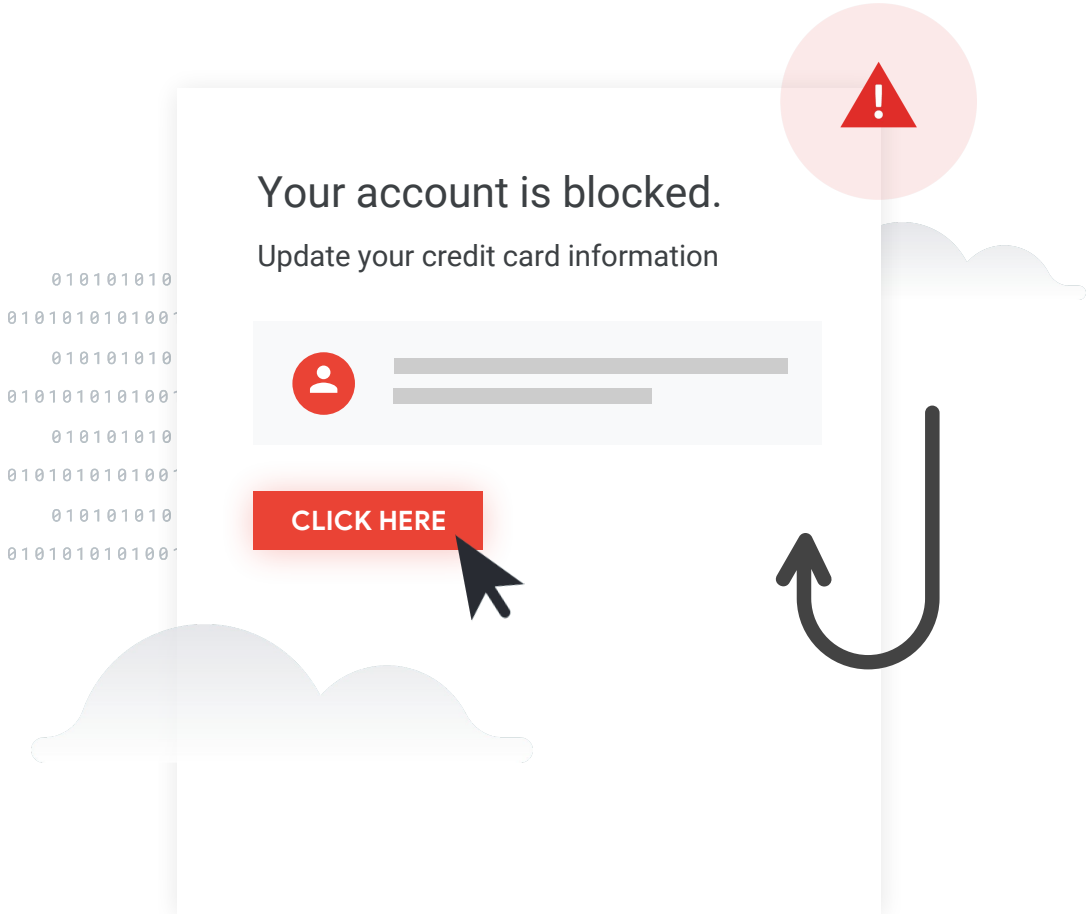
Make ML and user
see different things

Confusion

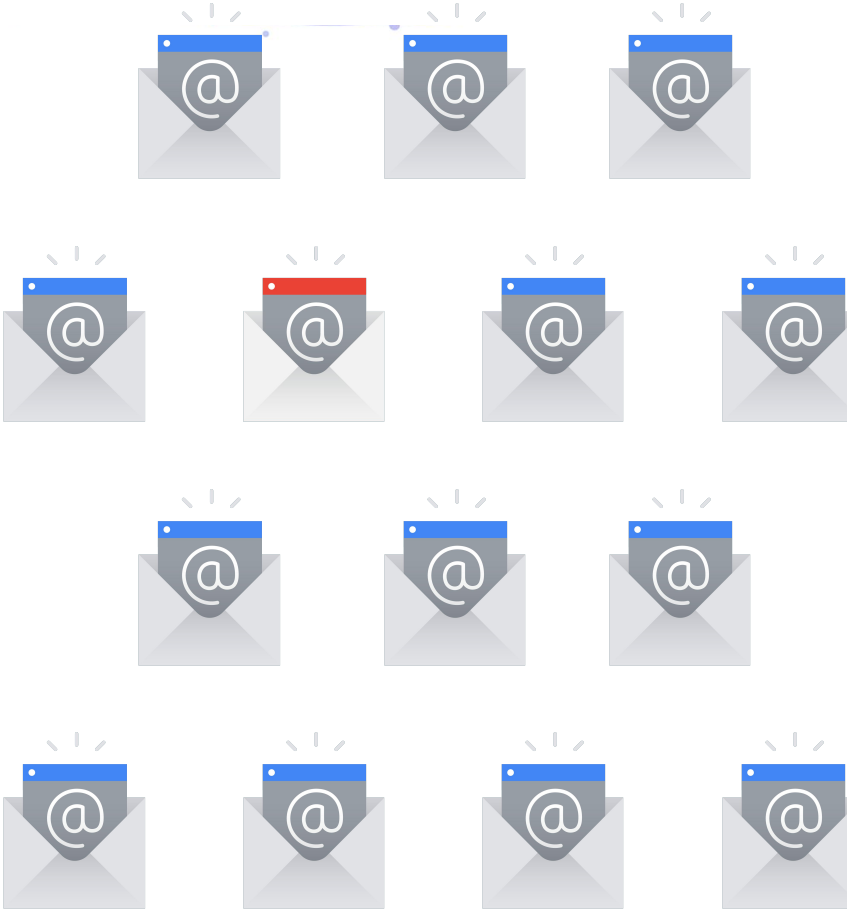
Trick the user to provide
ML with misleading data

Defeat the User

User interacts with phishing email



Attention is a limited capacity resource



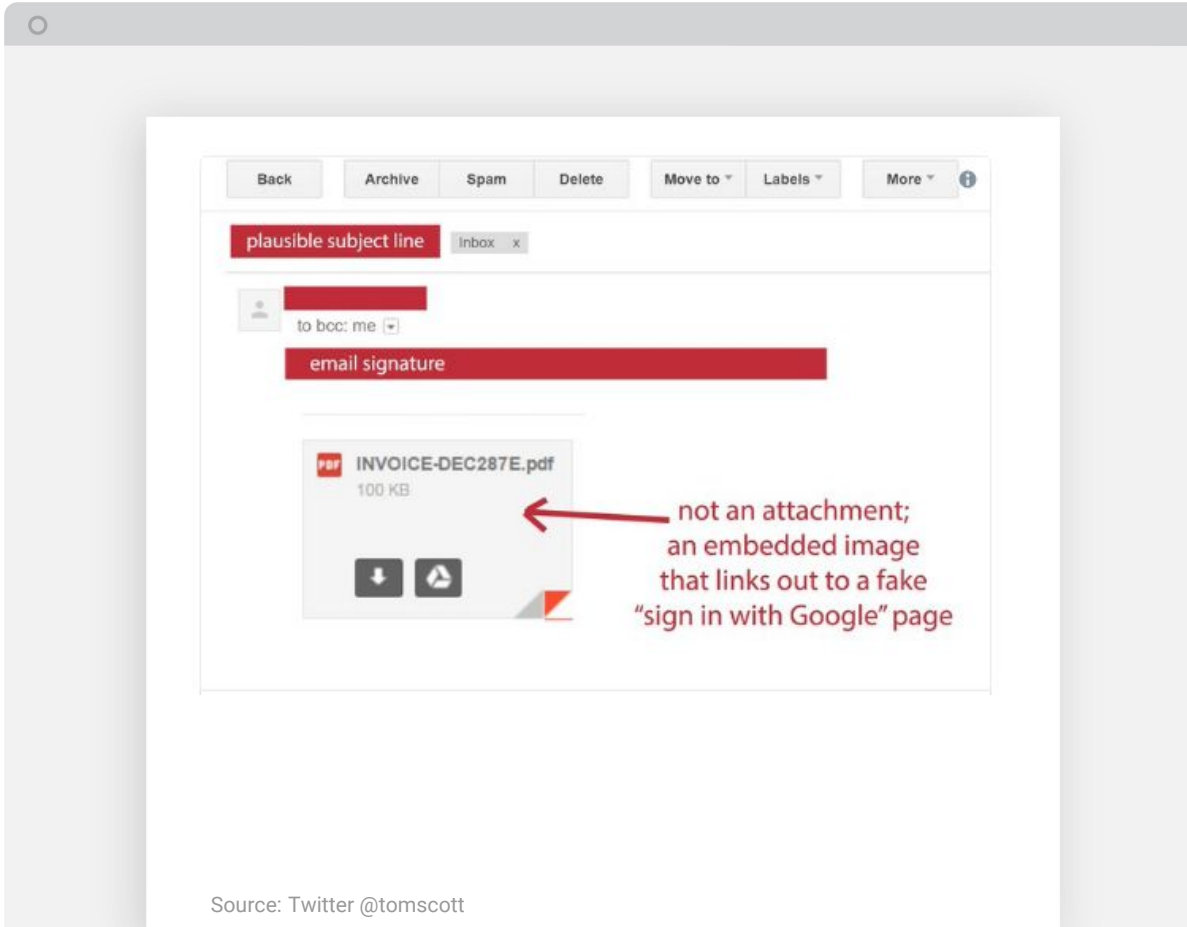
How to fool users?

Habits
Safe and Familiar

Pressure
Embarrassment and Fear

Vanishing Reward
Limited opportunity

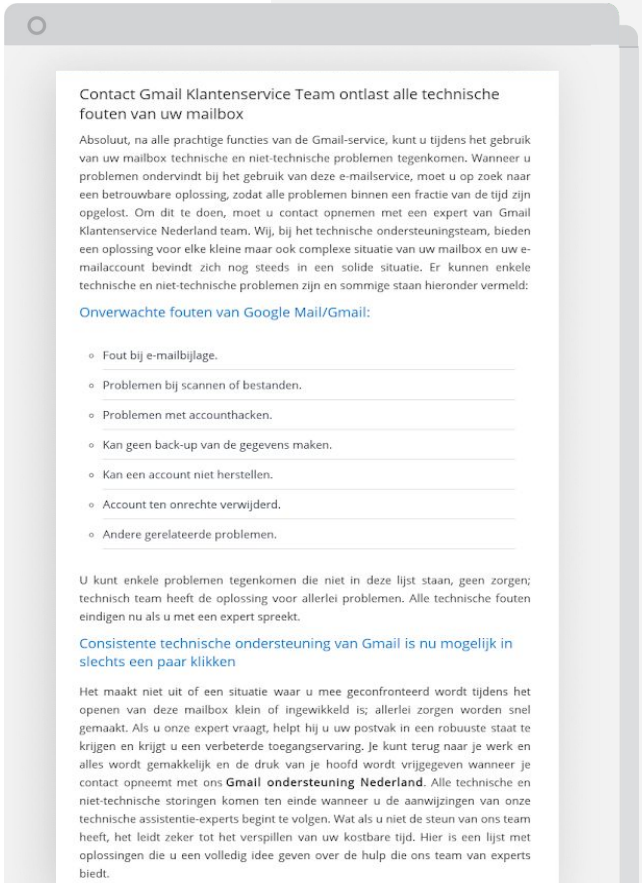
Familiar user interface



Source: Twitter @tomscott

Google

Technical support reaching out



Contact Gmail Klantenservice Team ontlast alle technische fouten van uw mailbox

Absoluut, na alle prachtige 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 de 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 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 creëren 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 beveiliging 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?

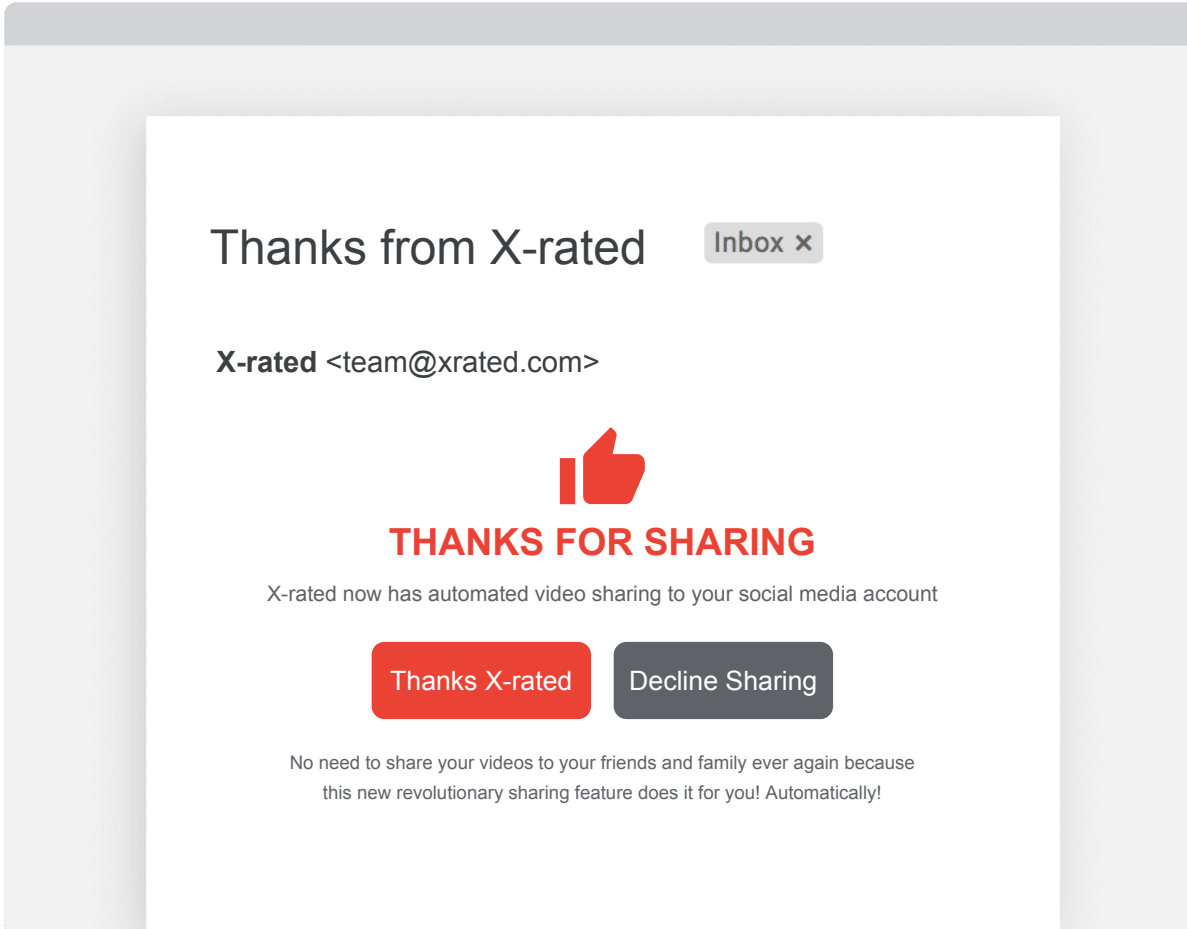
Er zijn een aantal redenen om contact op te nemen met het Gmail-ondersteuningsteam; hier zijn enkele redenen die je het belang zullen bepalen.

- 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.

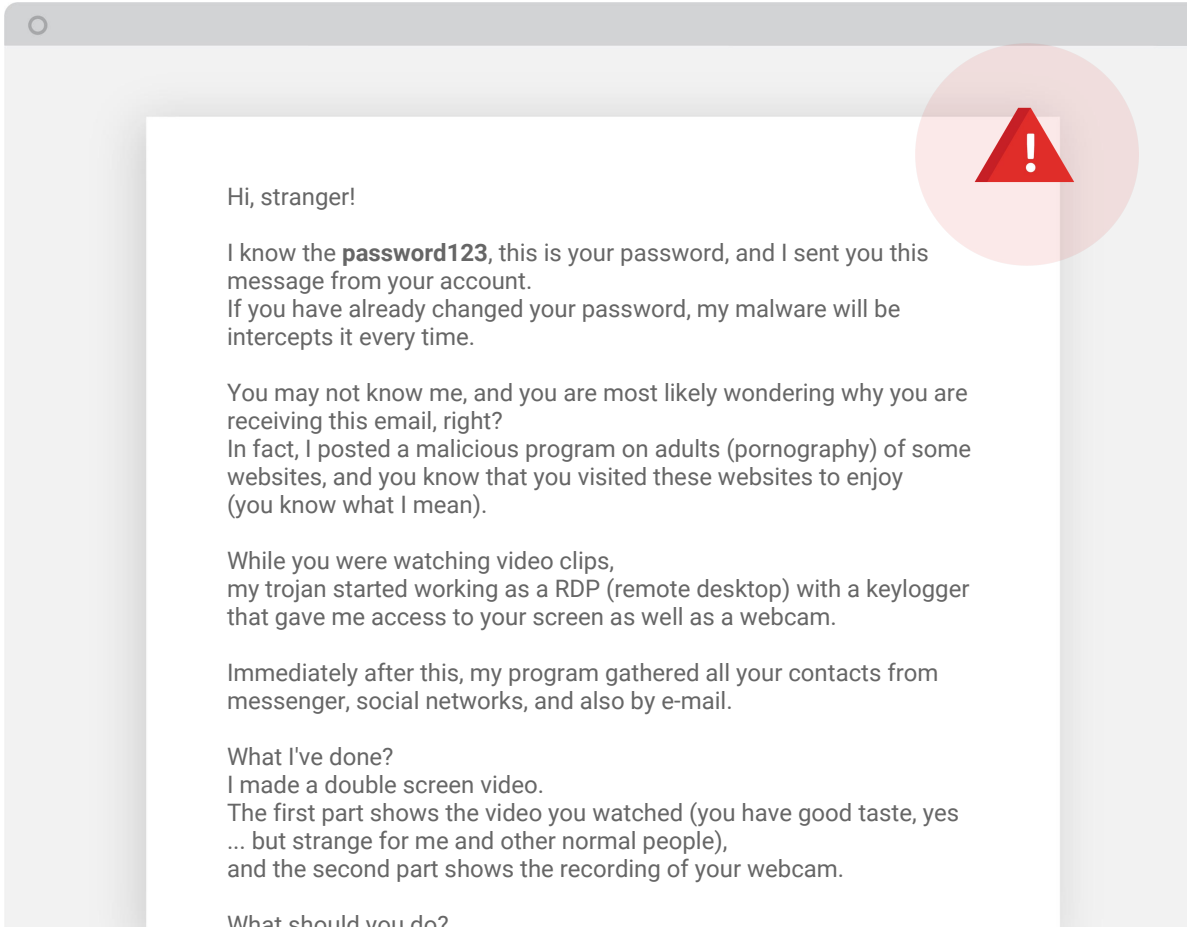
Houd ons Gmail helpdesk telefoon bij de hand om contact op te nemen met ons technische team van experts.

Google

Using embarrassment or fear

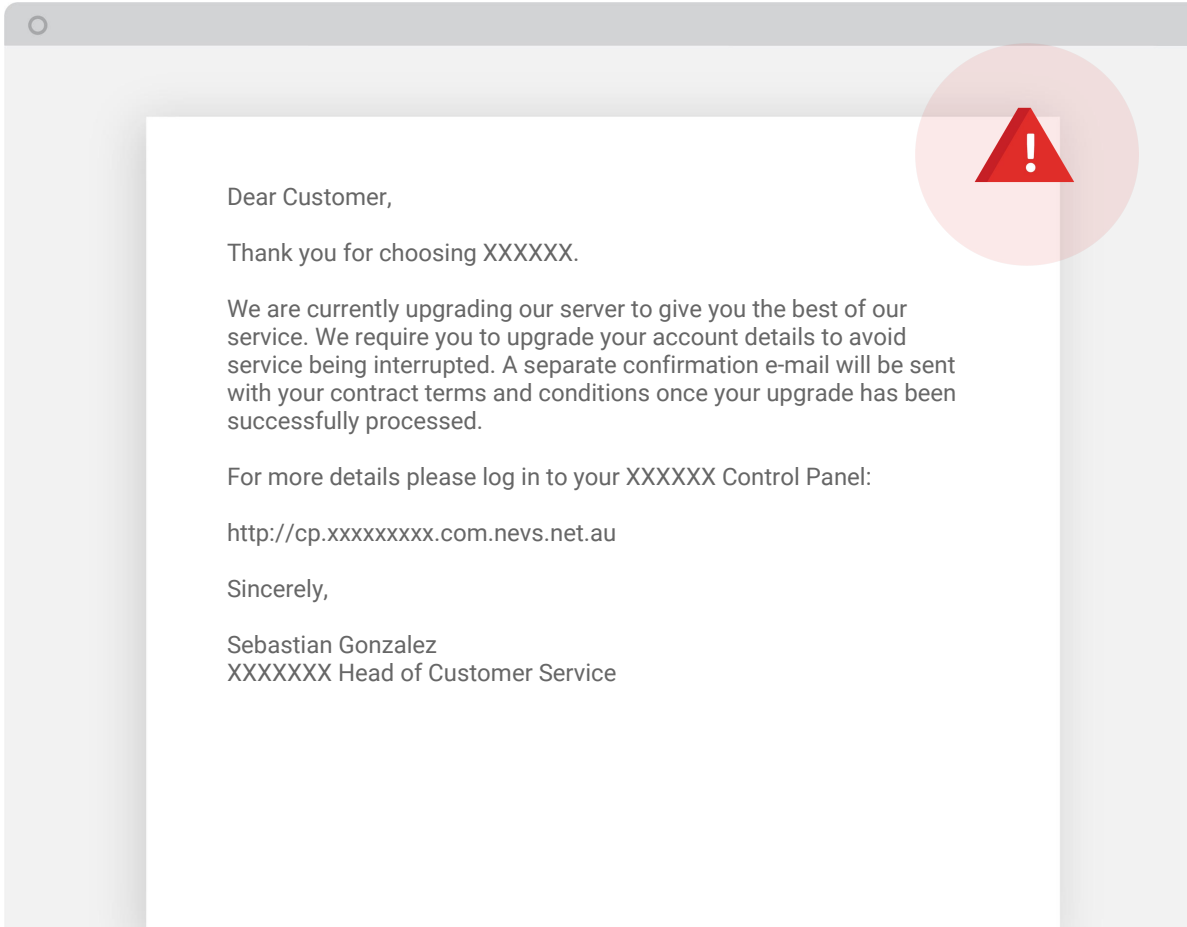


Credential leaks for sextortion



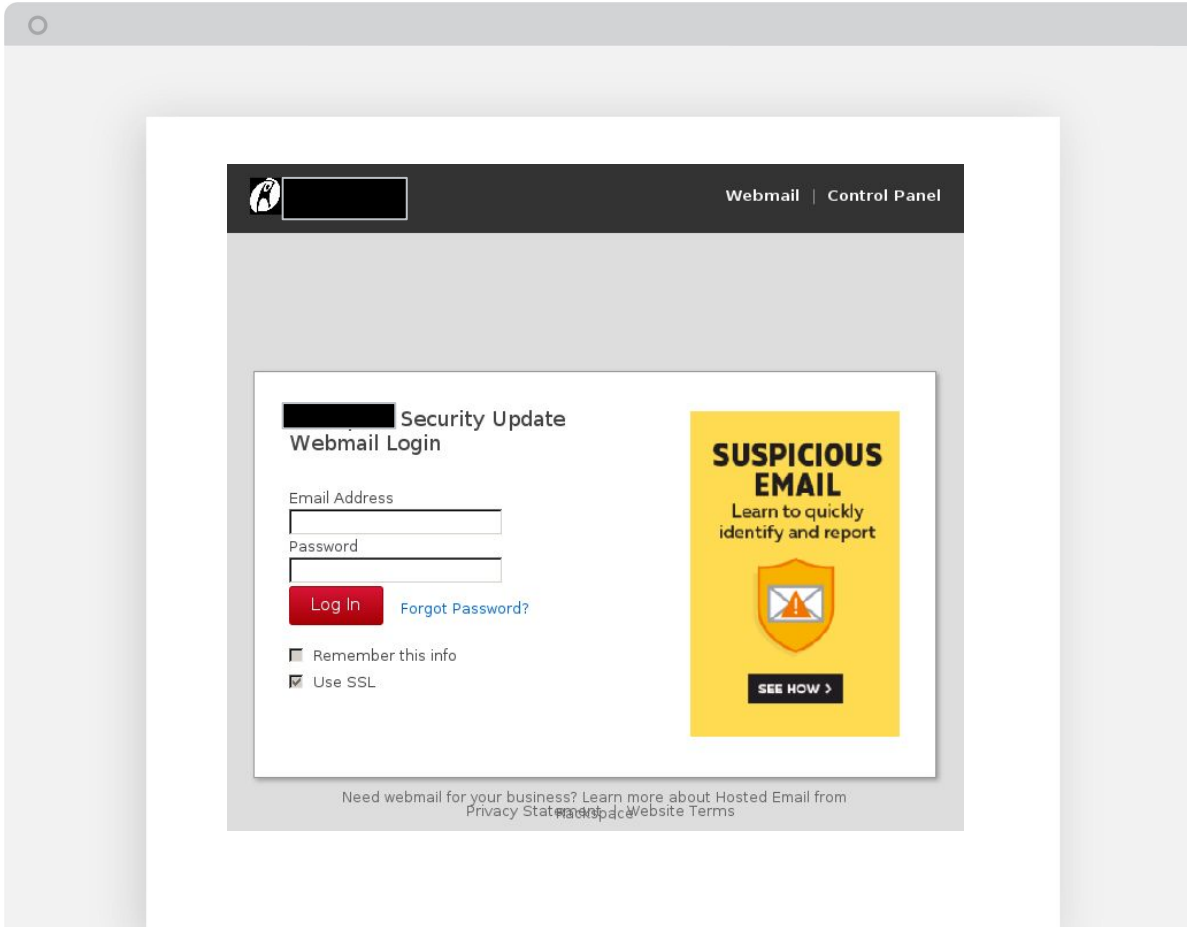
Google

Service interruption...



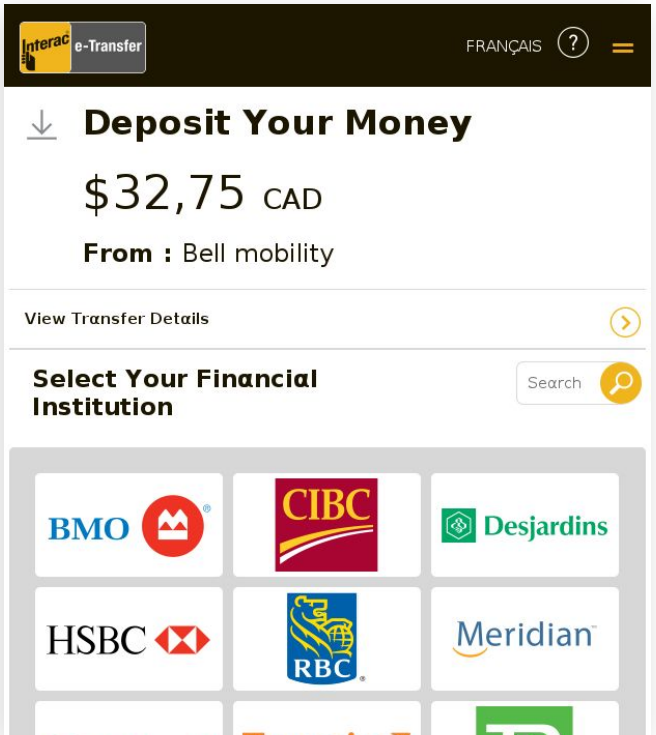
Google

… with ironic anti-phishing training

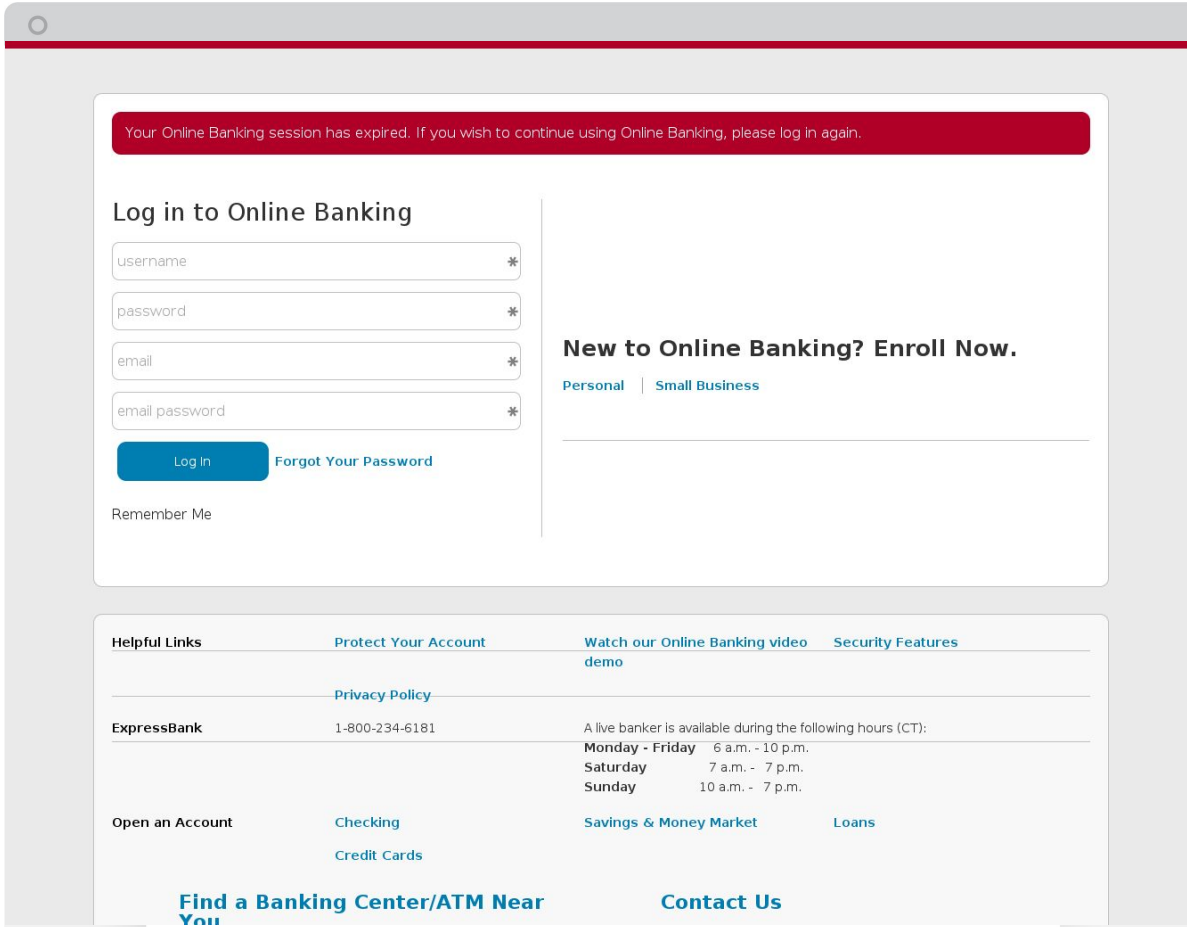


Google

Entice you with the promise of a prize...

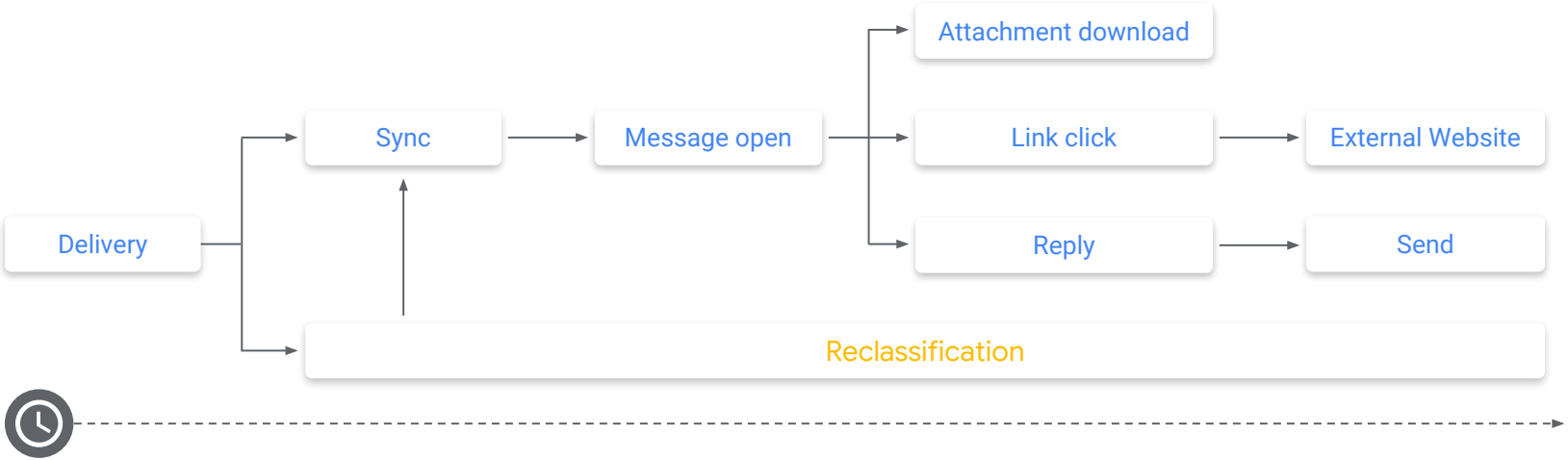


...and ask nicely for your bank credentials

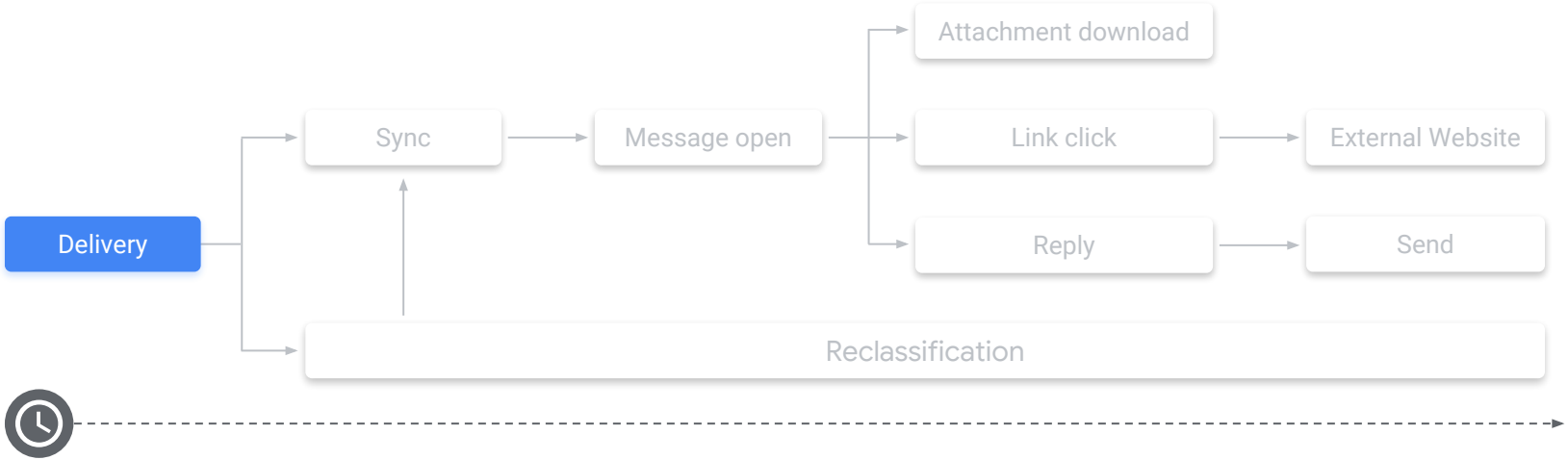


Google

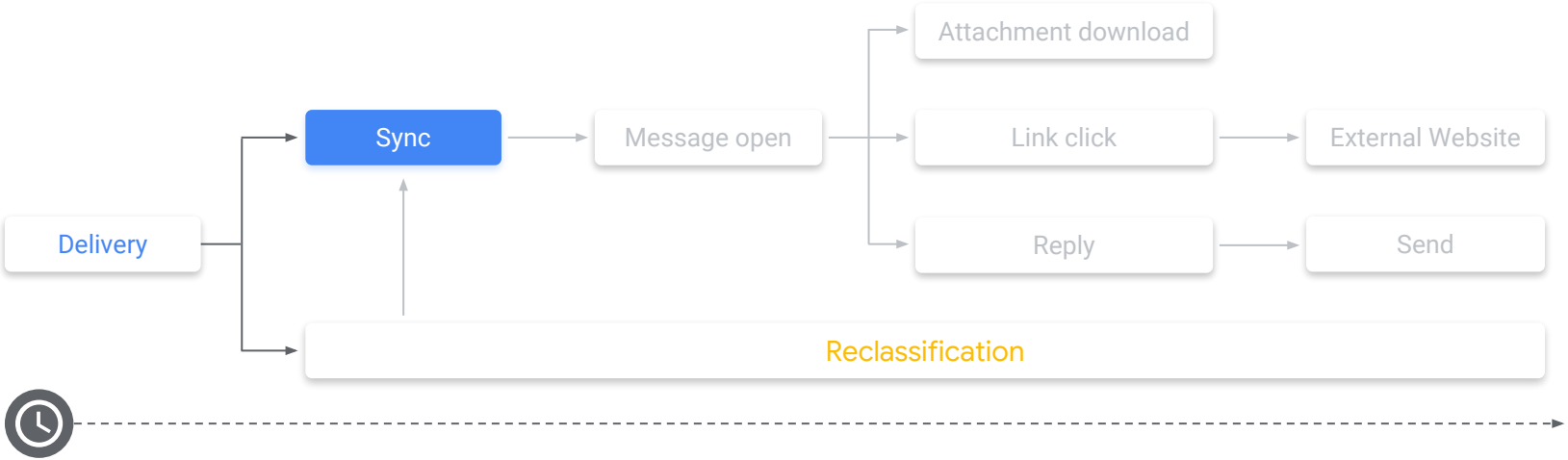
The life of a message



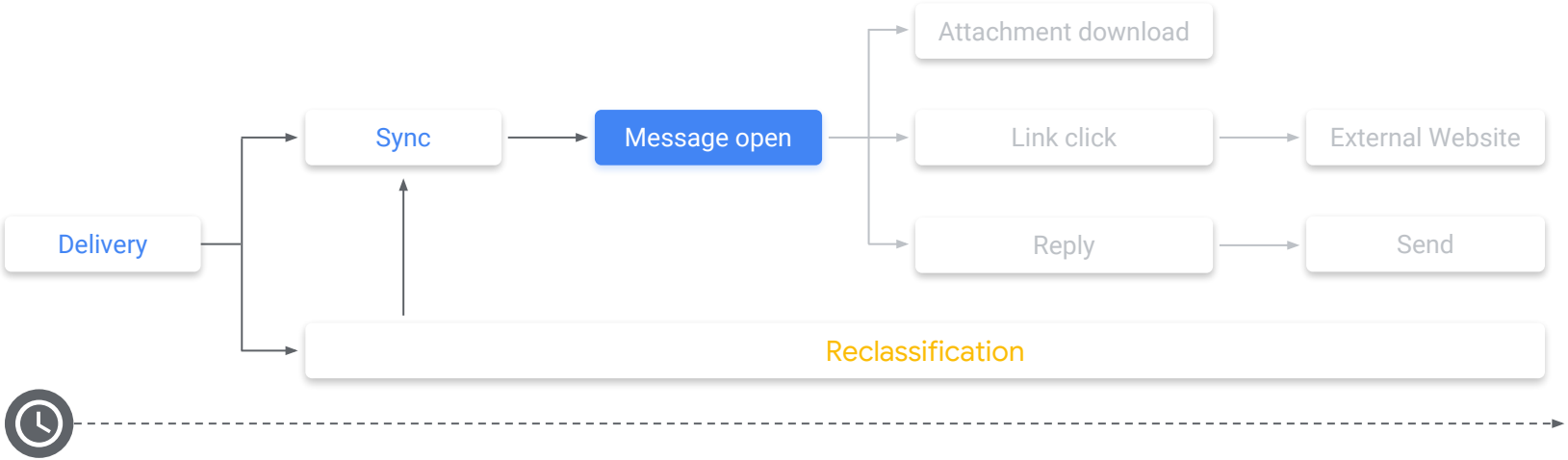
Delivery


Attachment download
Sync
Message open
Link click
External Website
Delivery
Reply
Send
Reclassification

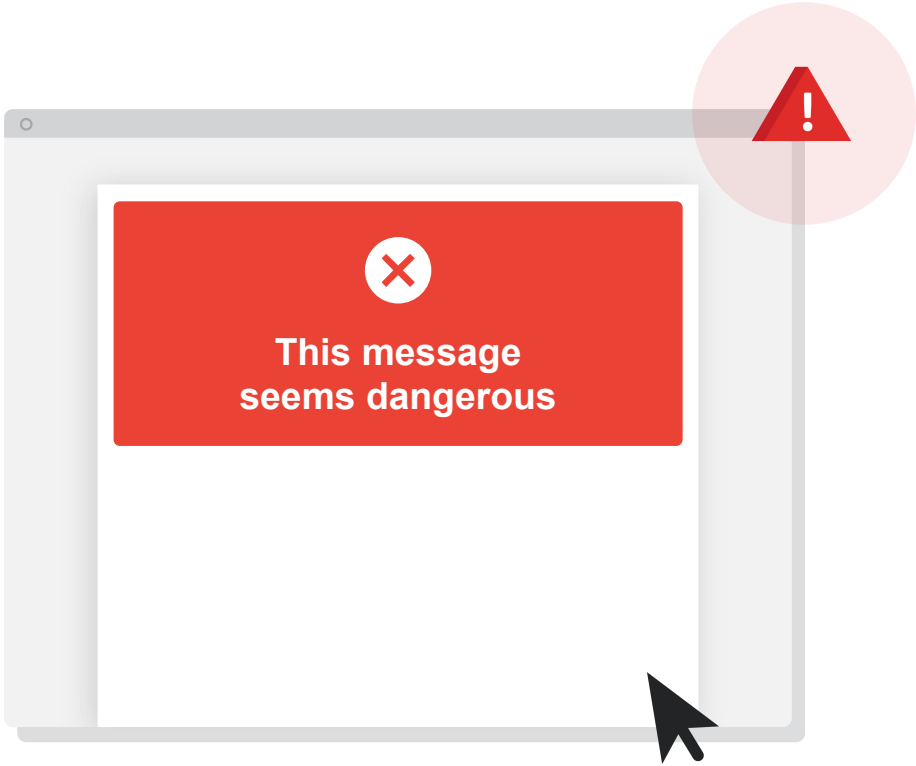
Sync


Attachment download
Sync
Message open
Link click
External Website
Delivery
Reply
Send
Reclassification

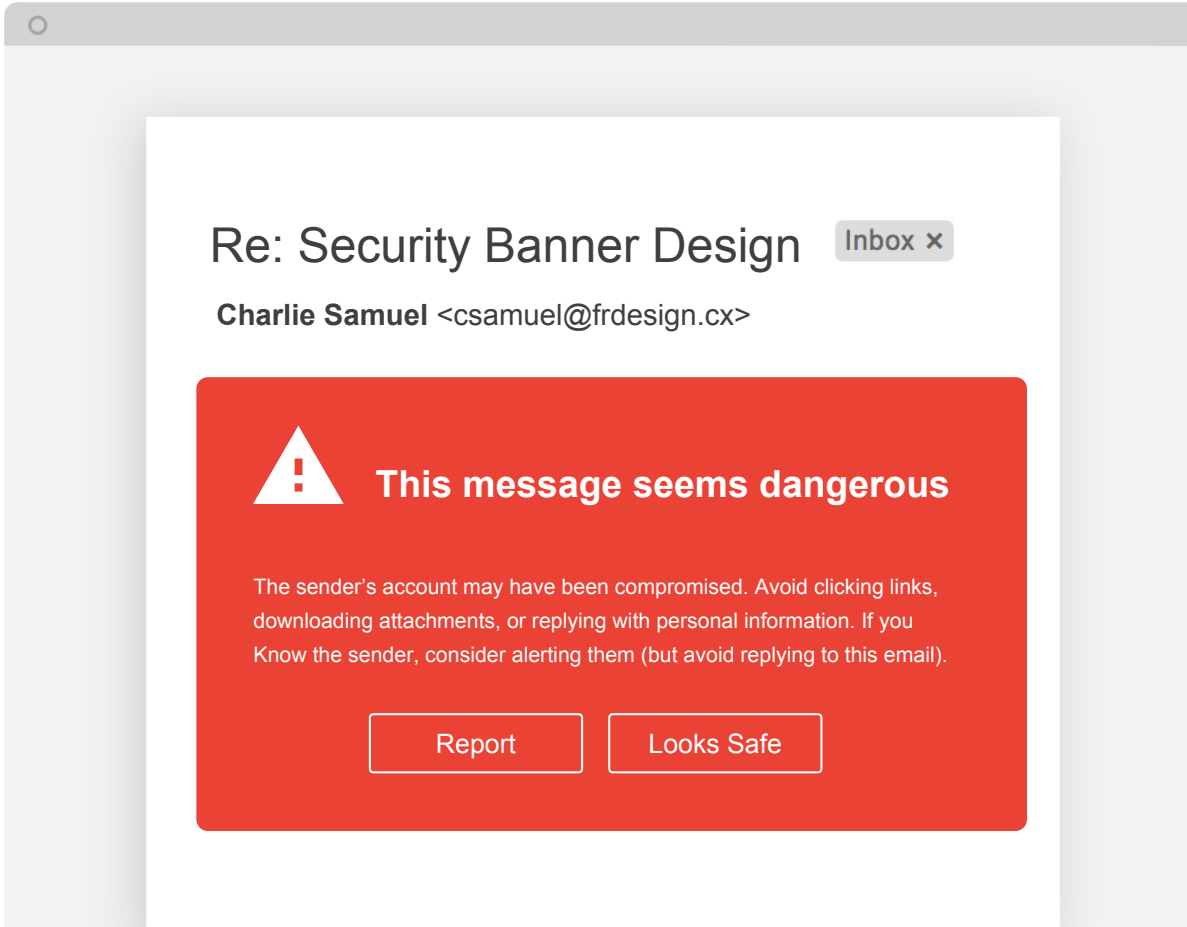
Message open



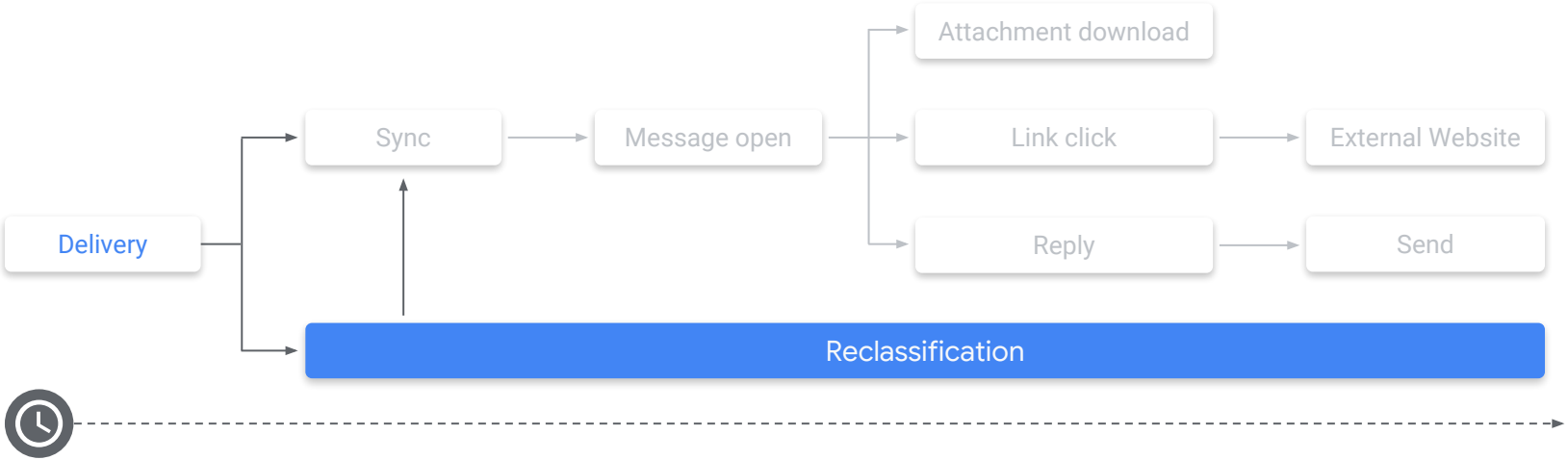
Big and obvious warning banners



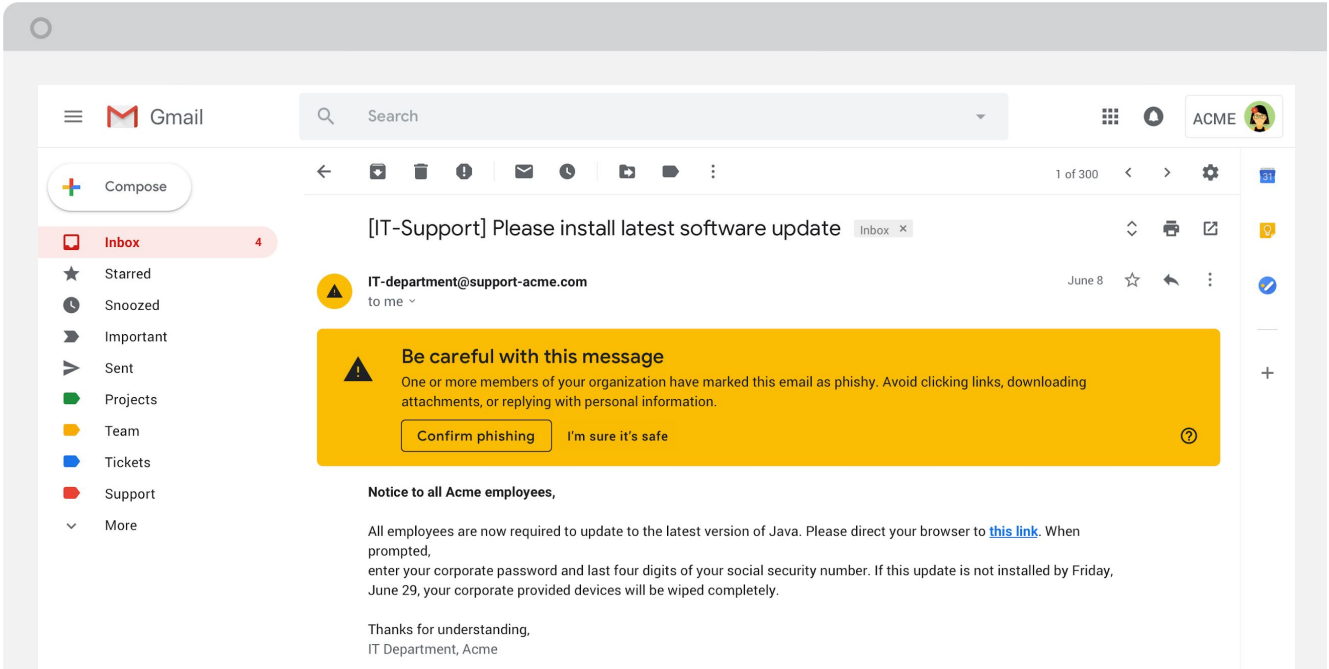
Message open: warning banners



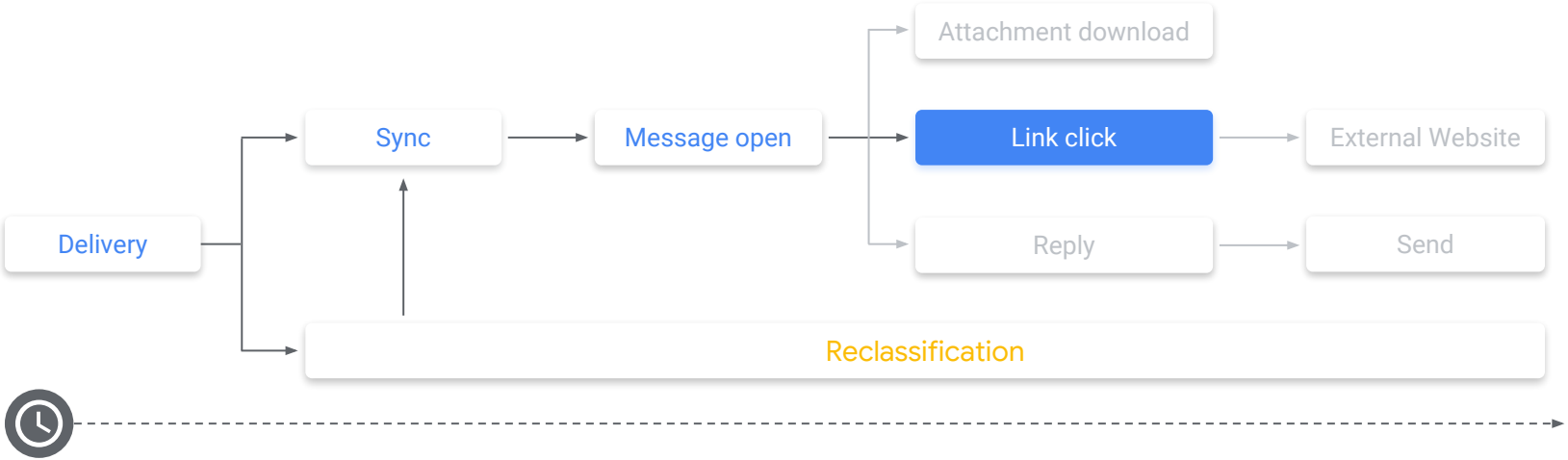
Reclassification



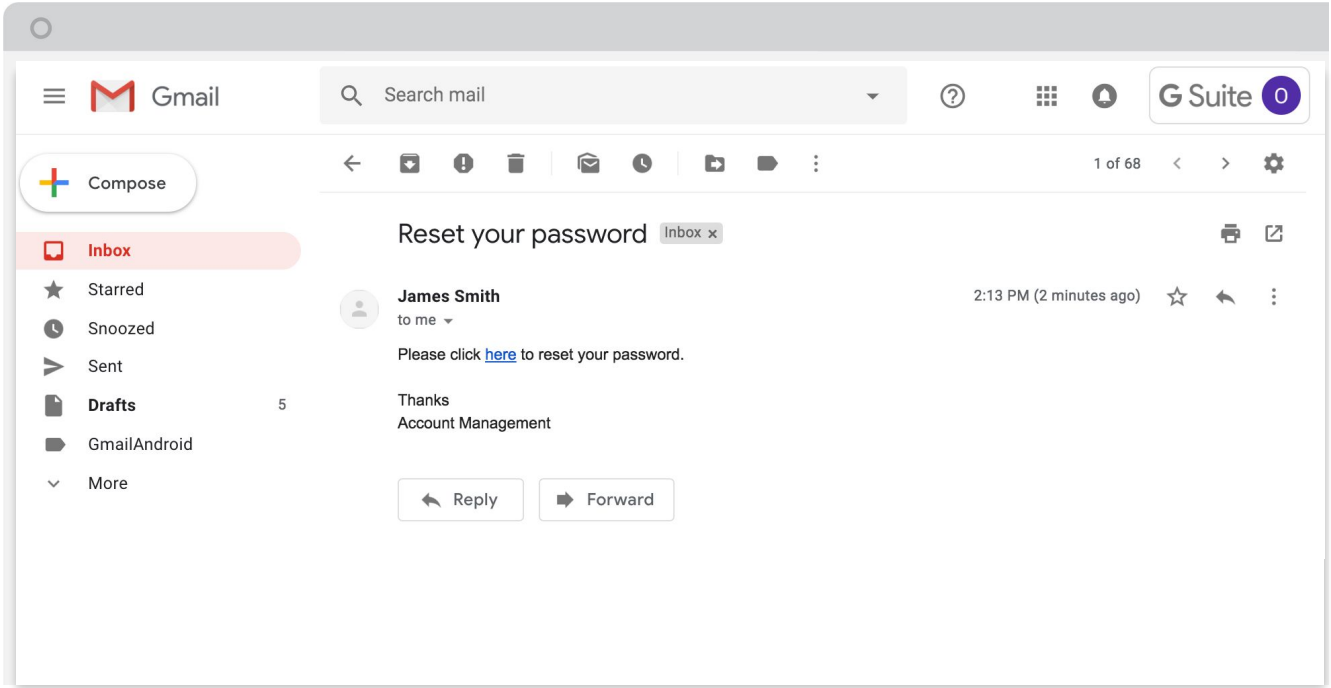
Phishing locality: co-worker warning via outbreak banners



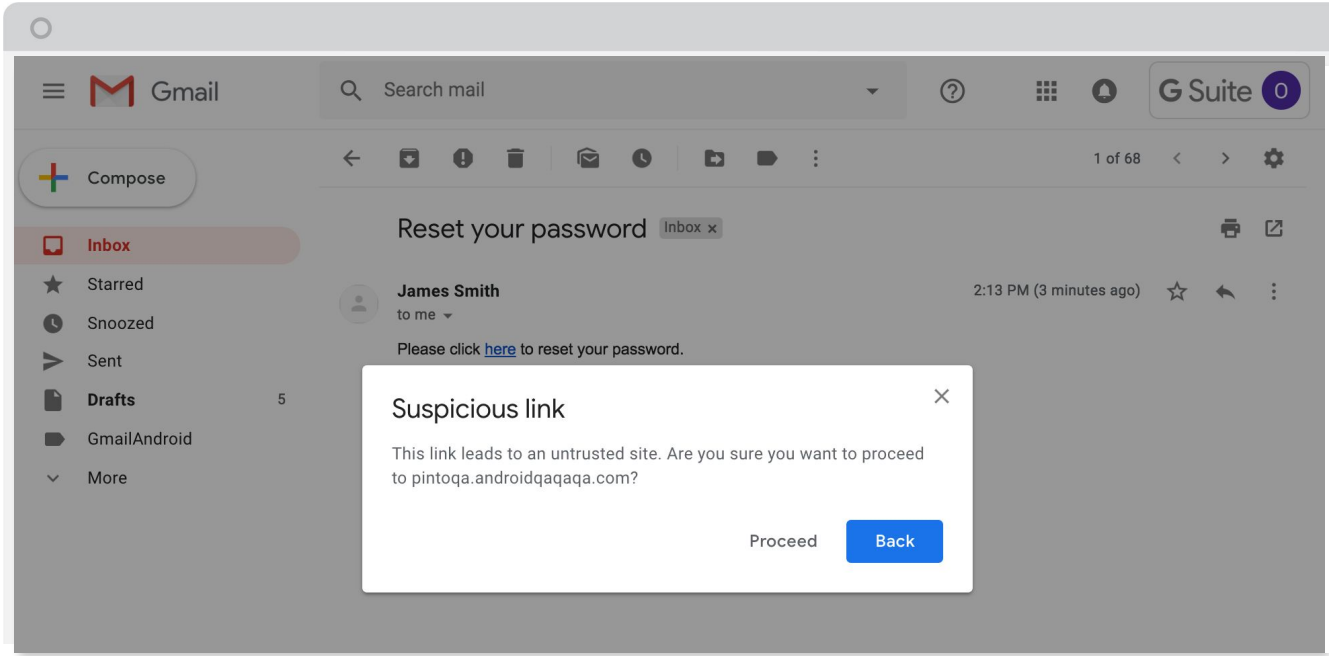
Link click


Attachment download
Sync
Message open
Link click
External Website
Delivery
Reply
Send
Reclassification

Suspicious Link Warning

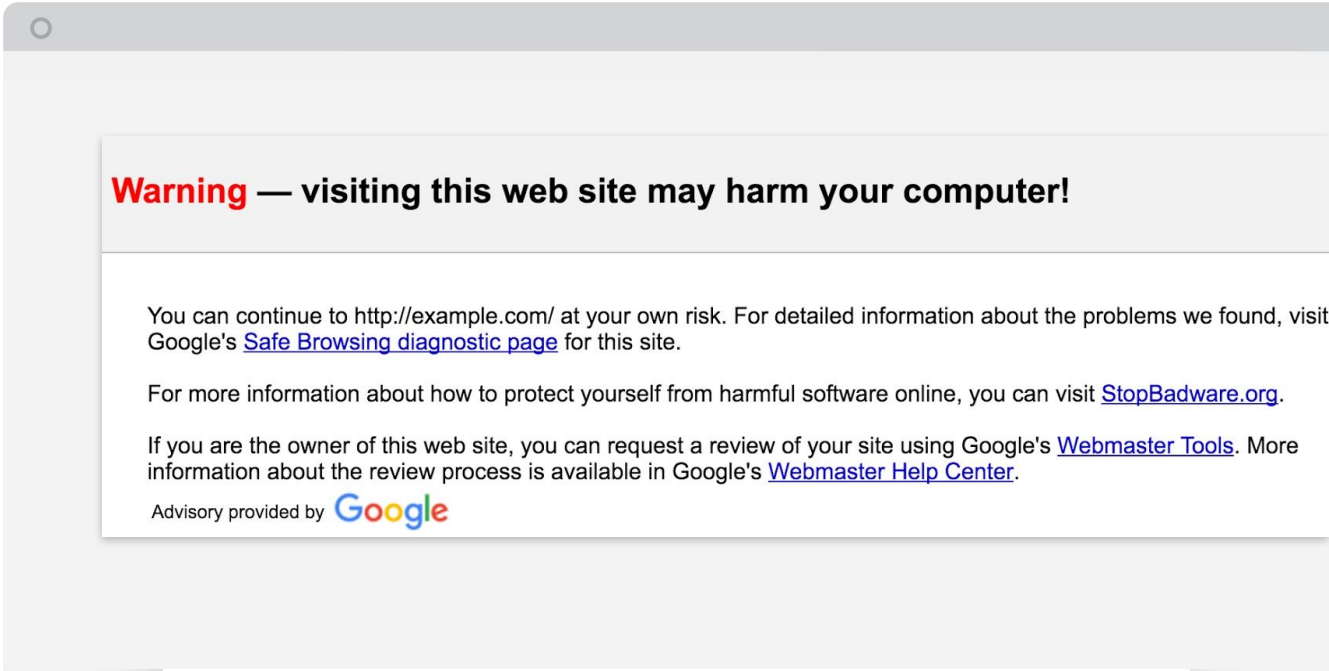


Suspicious Link Warning

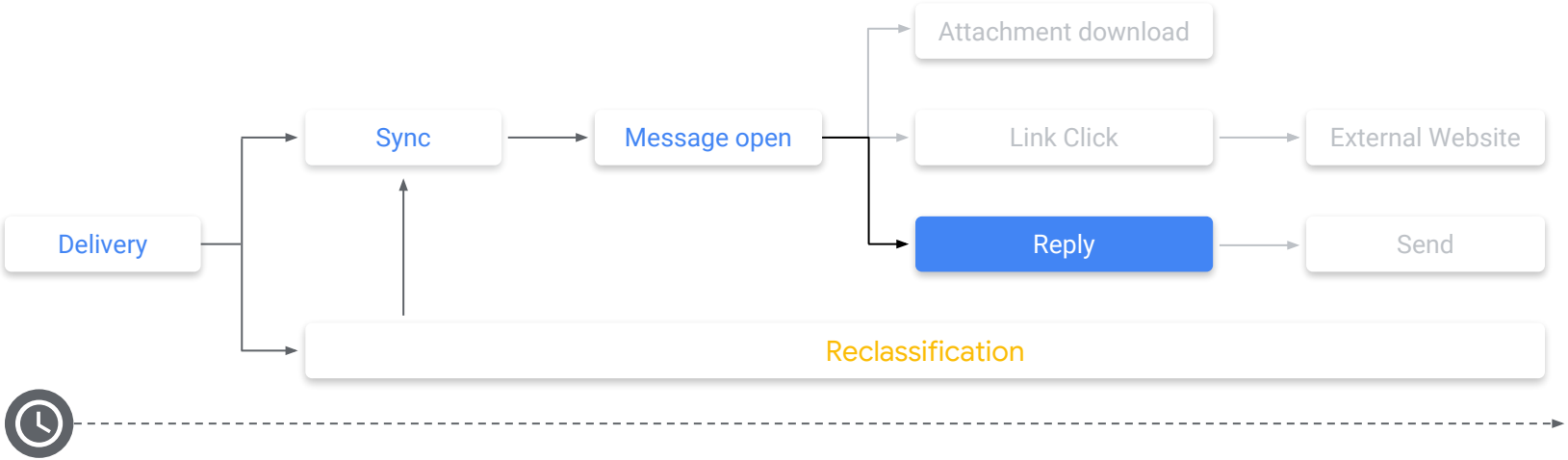


Real Time Check

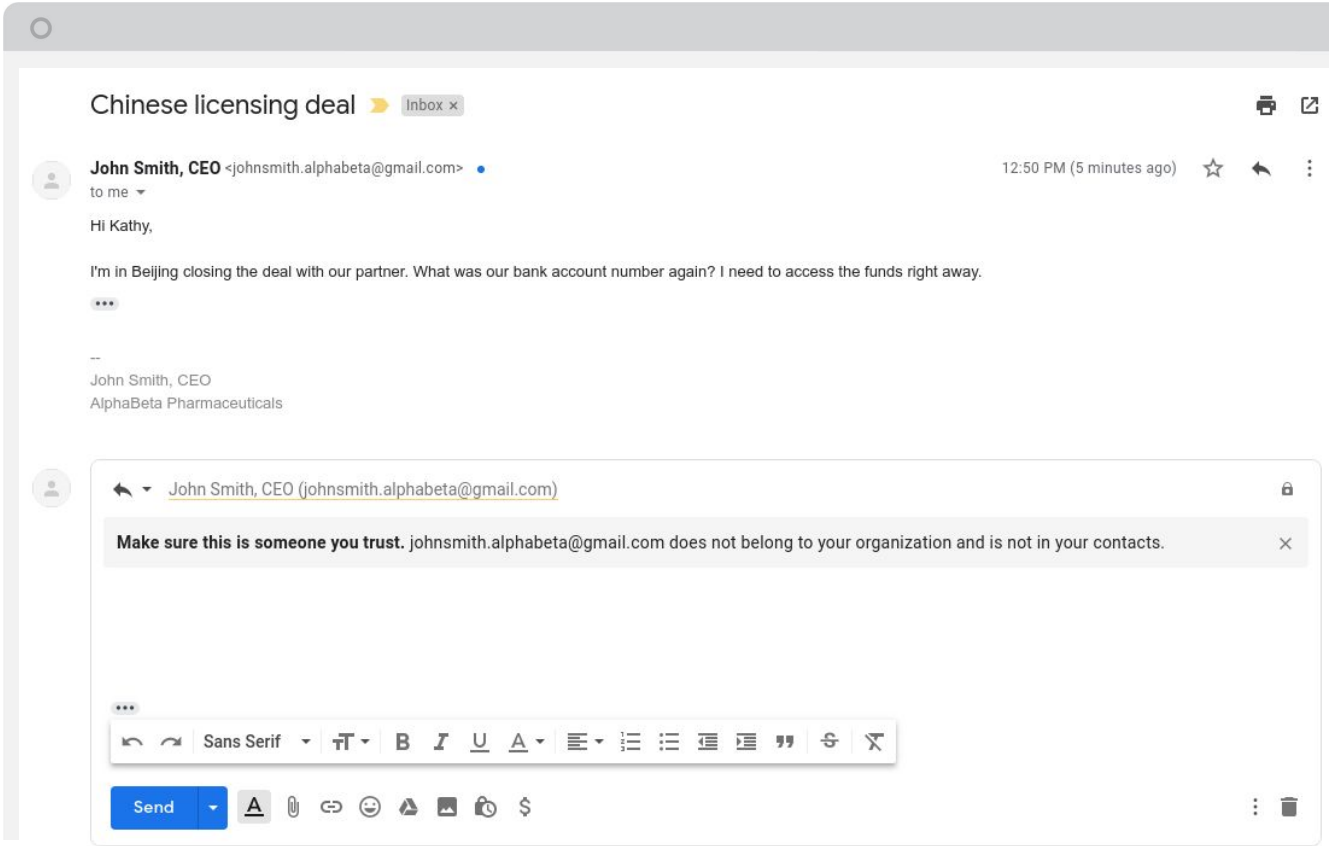
Google Safe Browsing



Reply

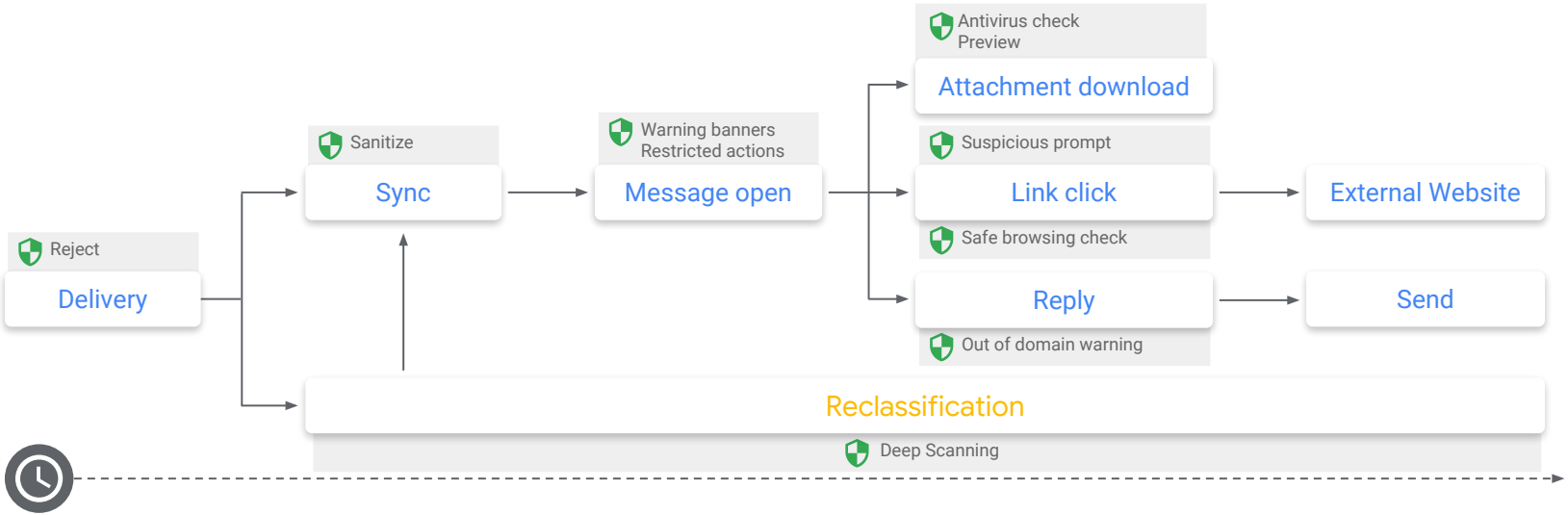

Attachment download
Sync
Message open
Link Click
External Website
Delivery
Reply
Send
Reclassification

Out of Domain Warning

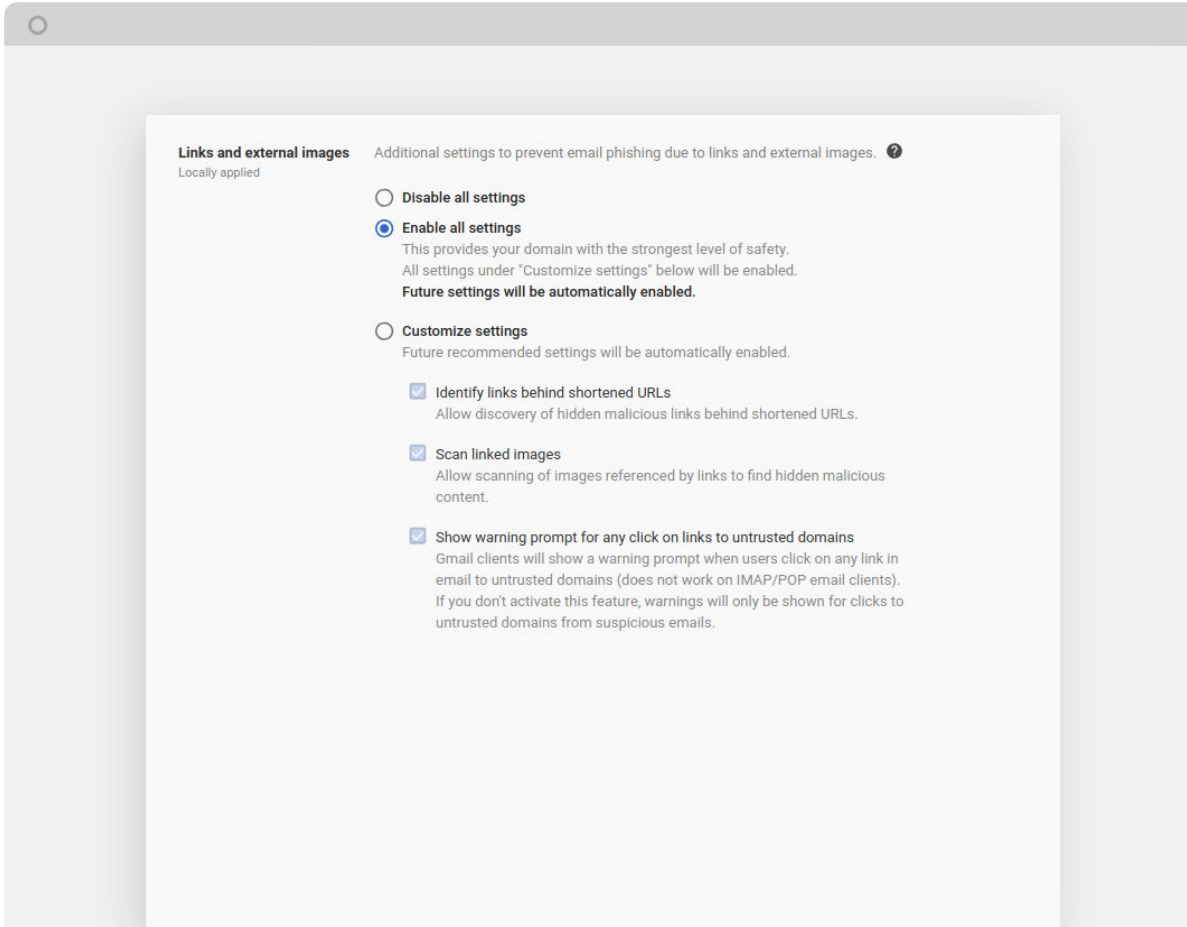


Google

Defense in depth

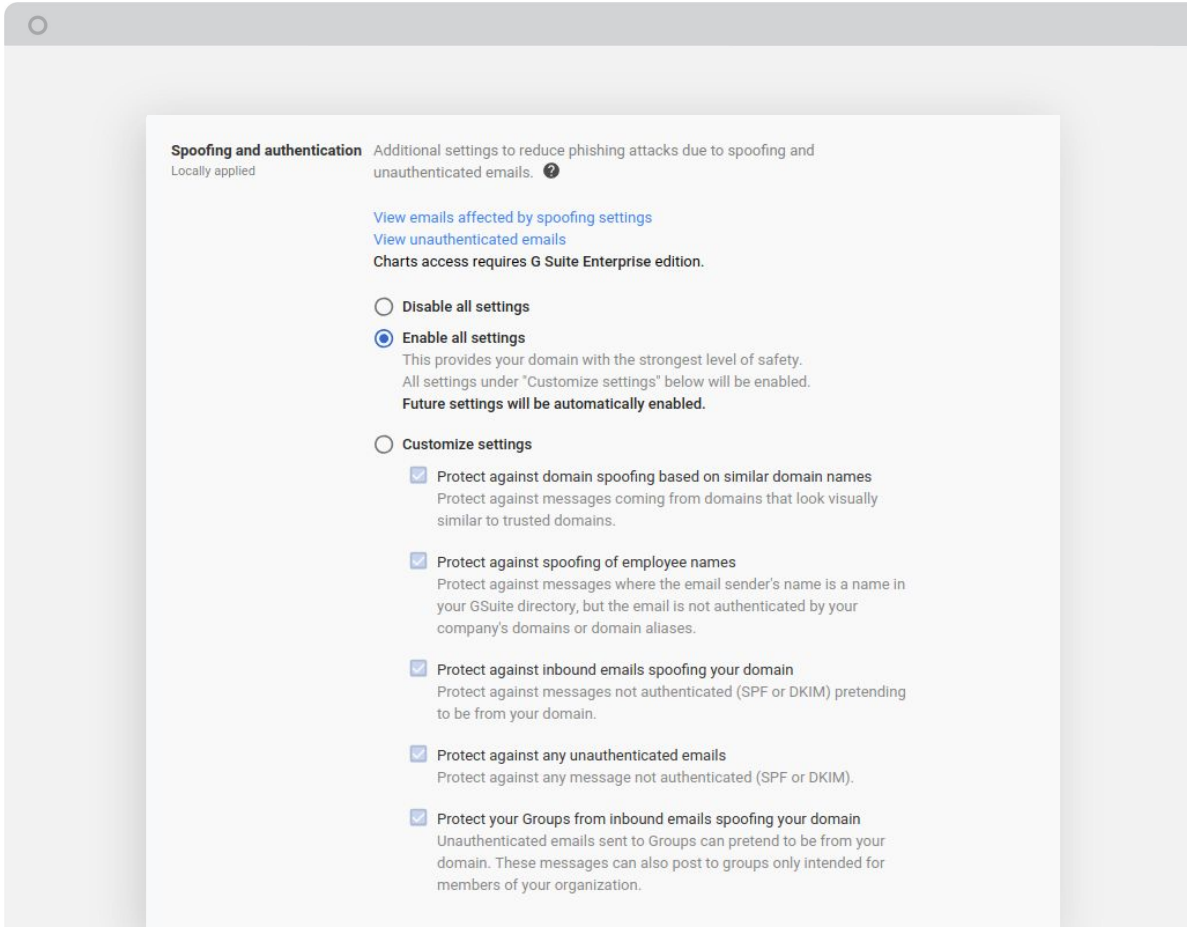


Look ahead for malicious remote content



Google

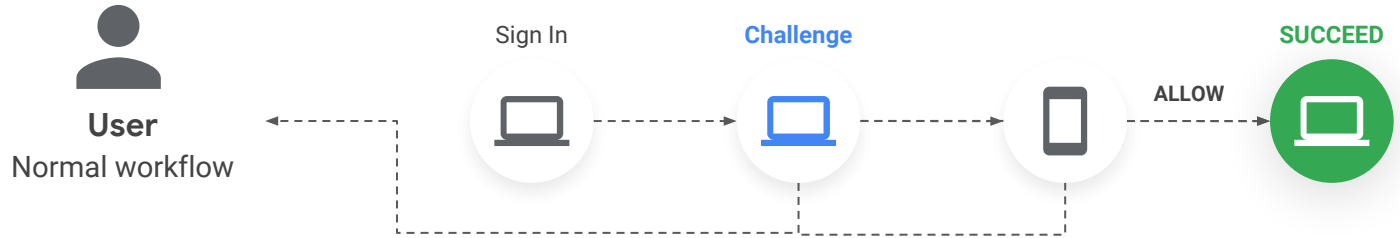
Protect against domain and employee spoofing

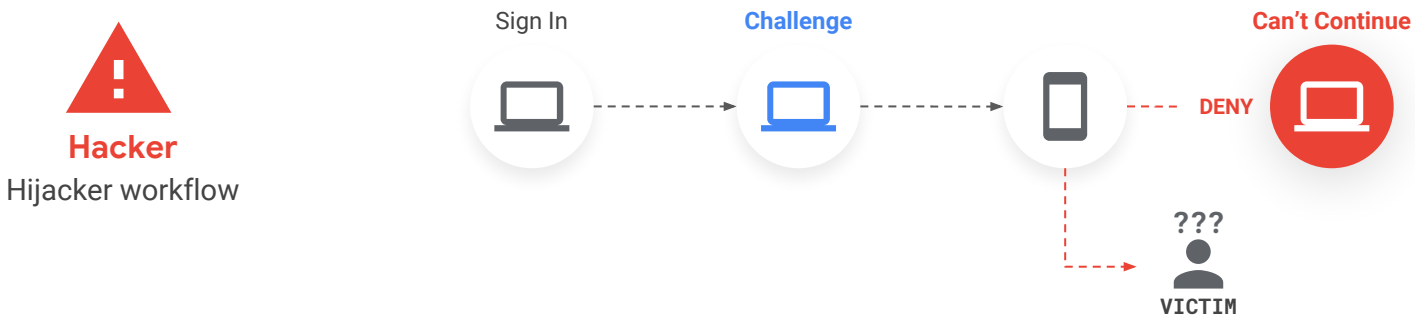


Google

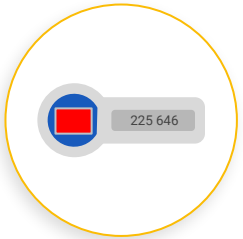
Defeat the Target Service

Phisher using the stolen authenticator


User
Normal workflow
Sign In
Challenge
ALLOW
SUCCEED


Hacker
Hijacker workflow
Sign In
Challenge
DENY
Can't Continue
???
VICTIM

Attackers are adapting



Phisable 2FA

Mobile Platforms

Monitor for unusual activity

Use second factor

Use phishing resistant authentication

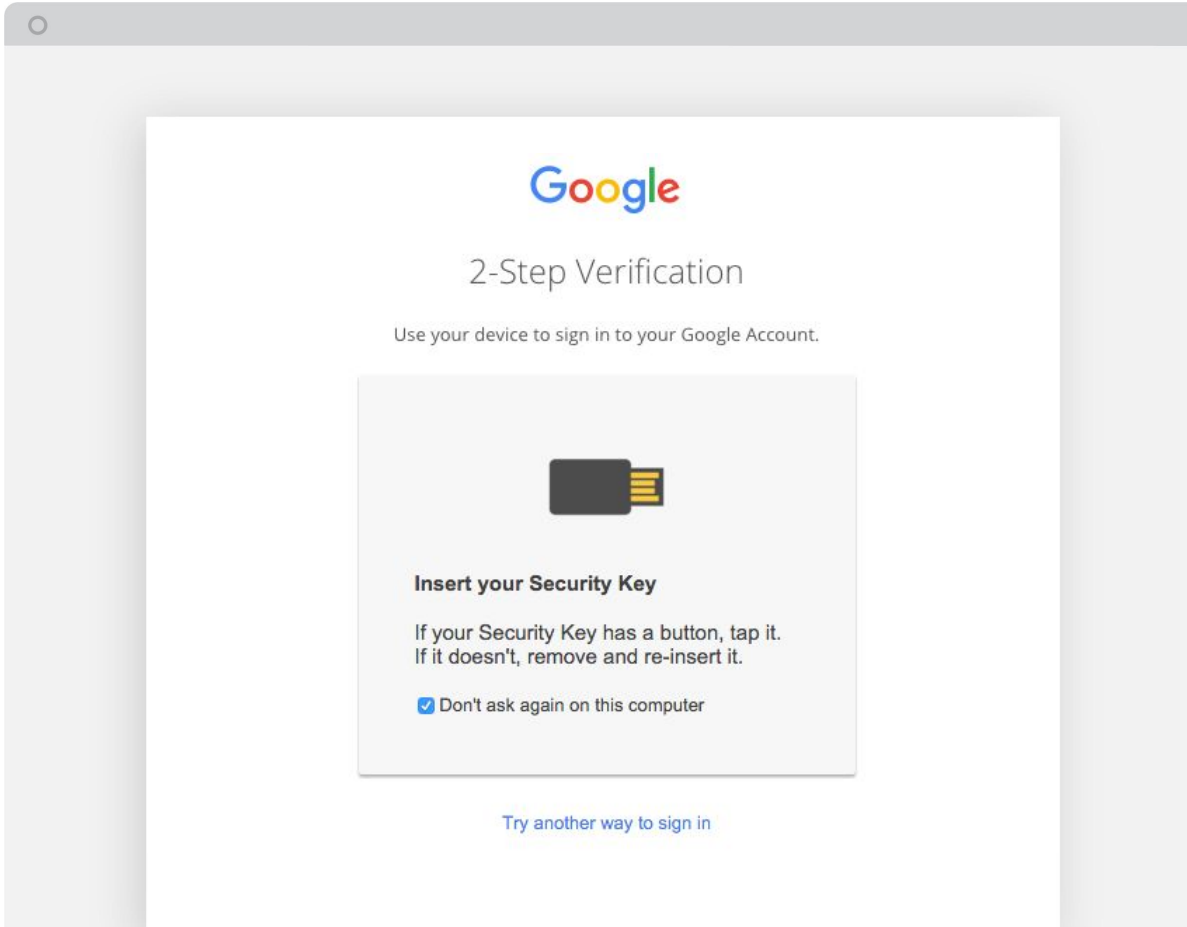
Faking user geolocation/
browser configuration

Phish for second factor

Use a different attack method

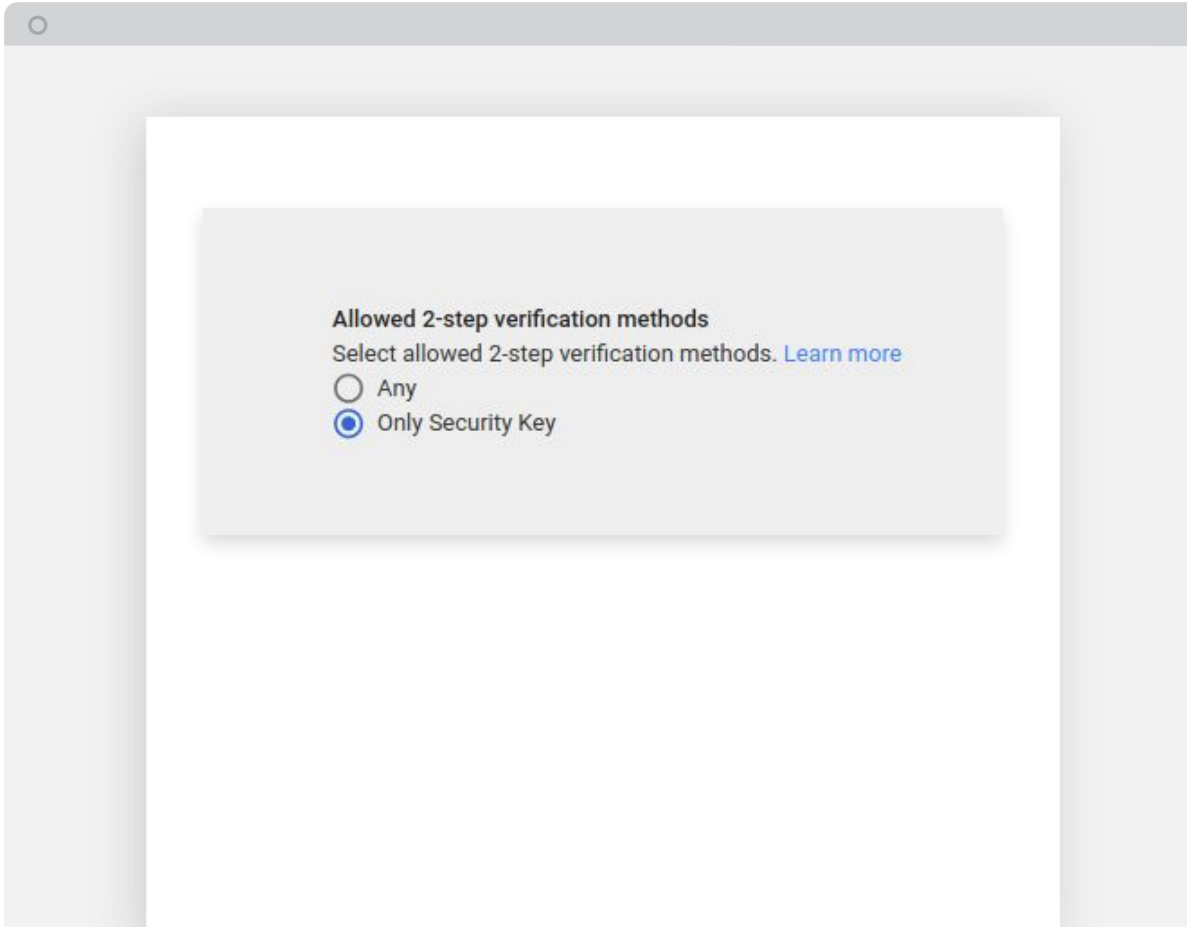
Raising the bar

FIDO U2F tokens



Google

Make it mandatory and phishing resistant for employees



Google

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