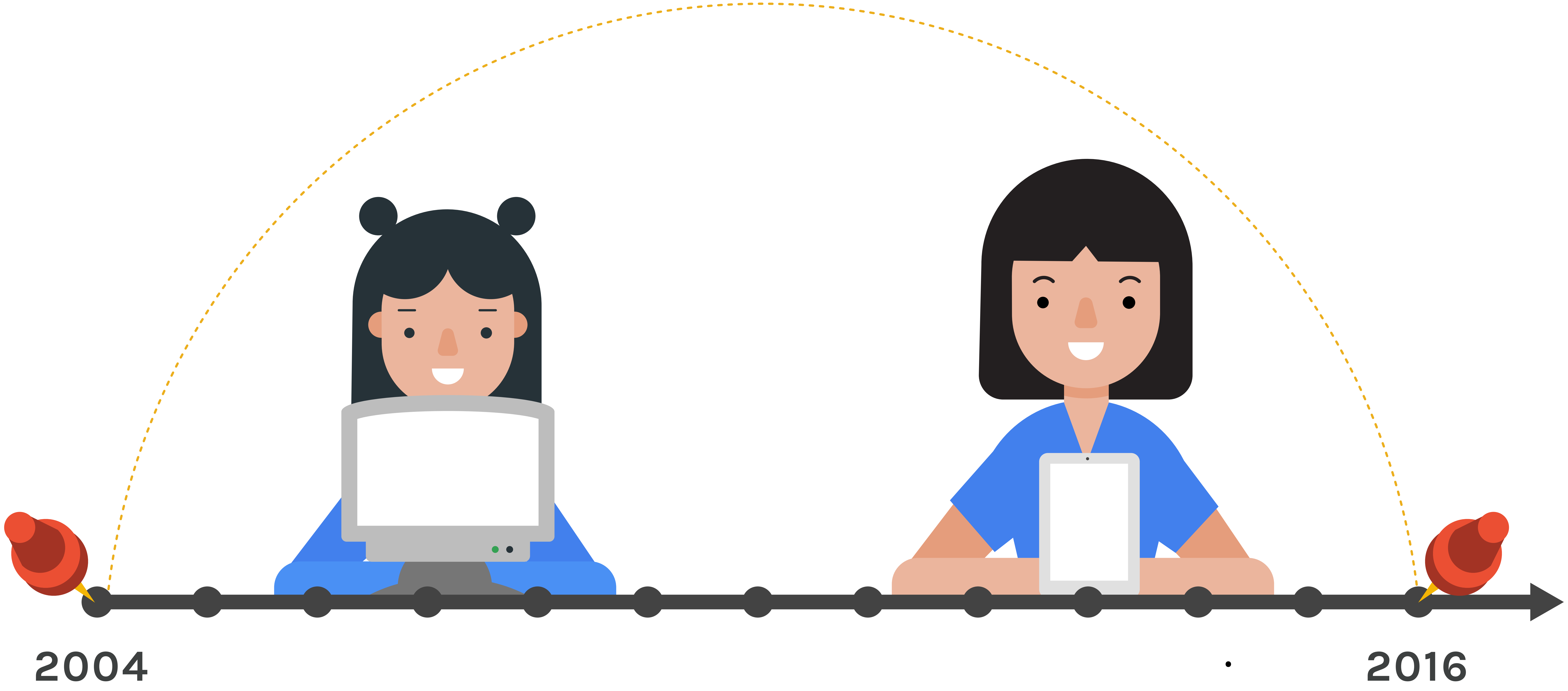
Lessons learned while PROTECTING GMAIL

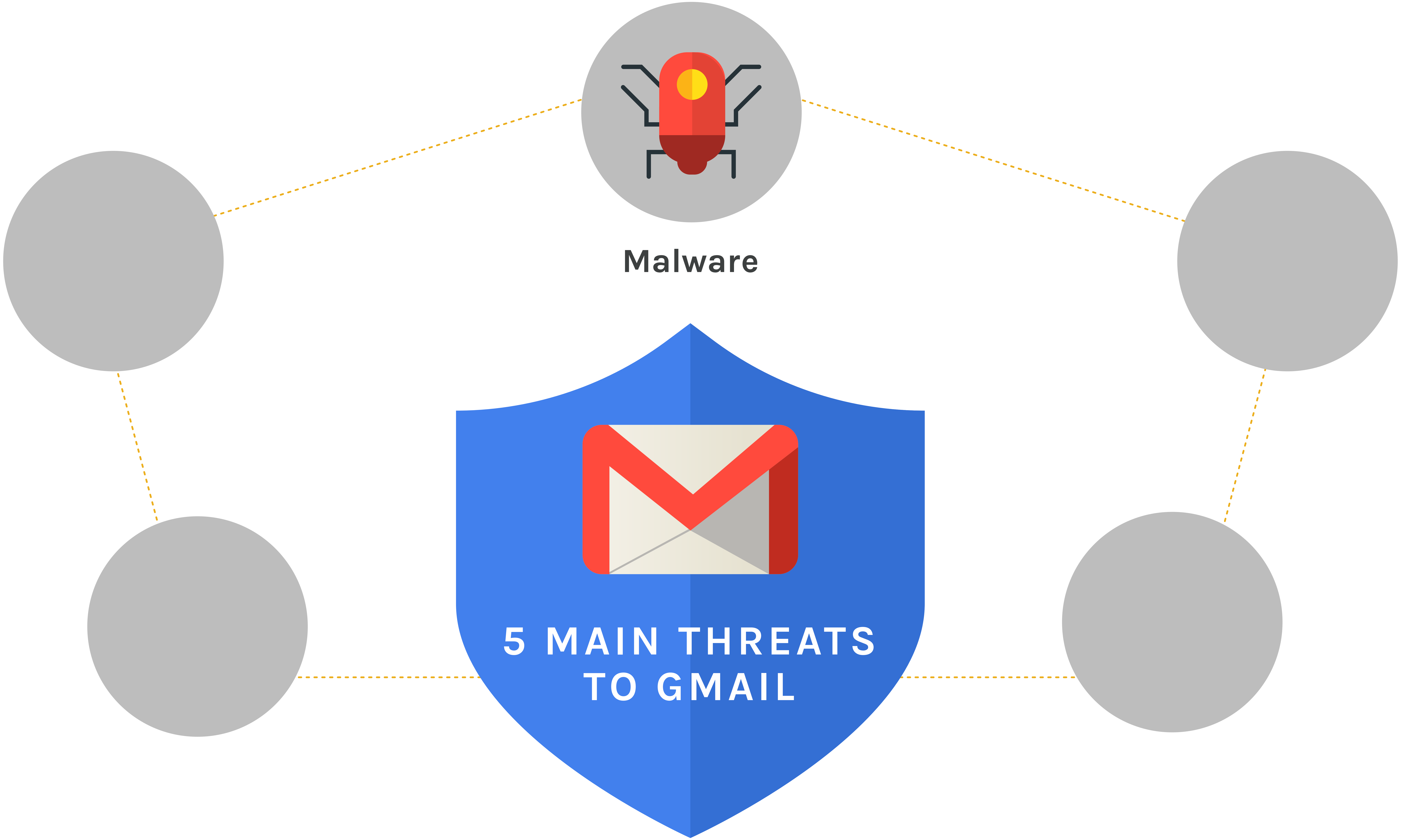
Elie Bursztein, Nicolas Lidzborski, & Vijay Eranti

THE GMAIL SECURITY AND ANTI-ABUSE TEAM



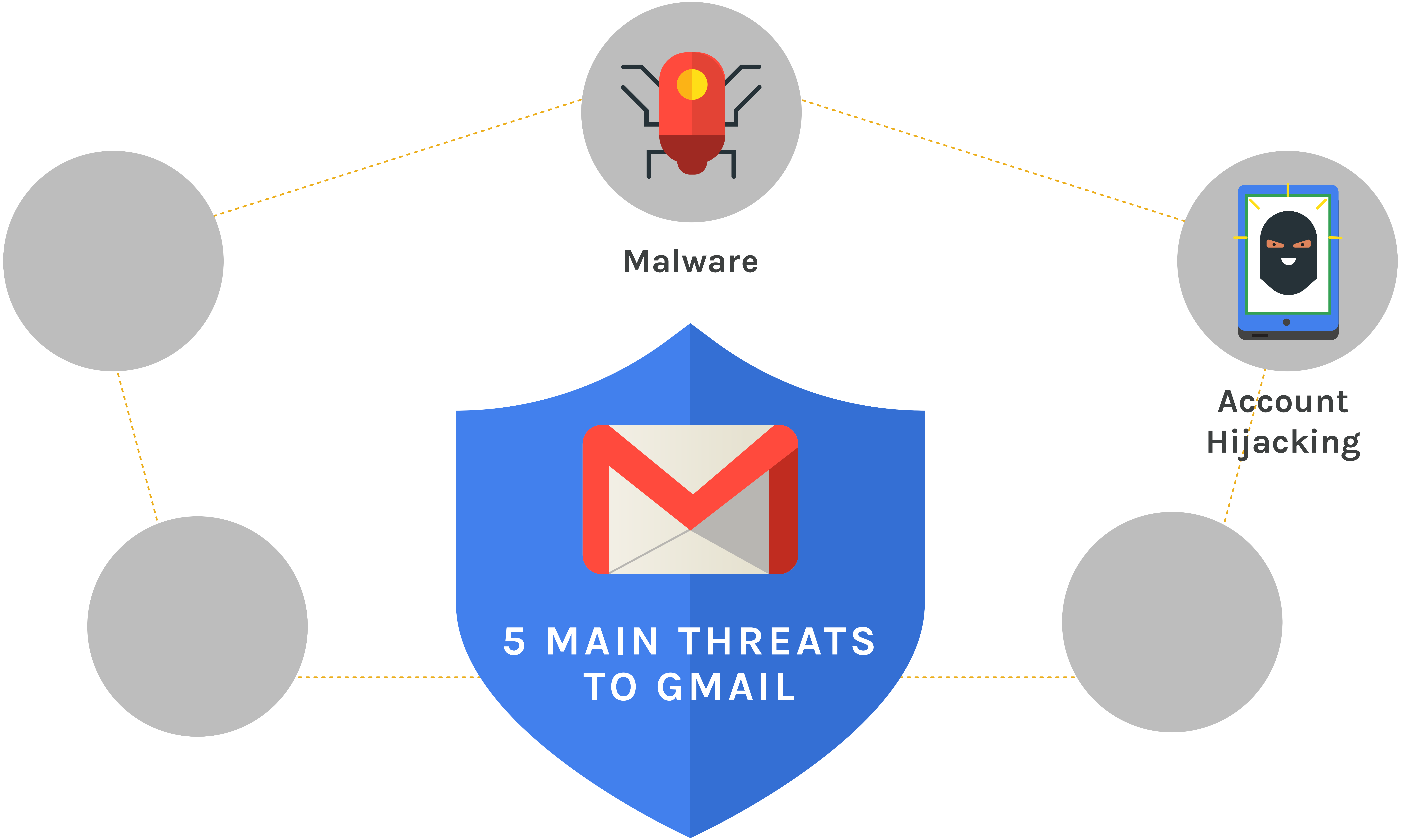
LESSONS WE’VE LEARNED WHILE

protecting Gmail users for over a decade



Malware

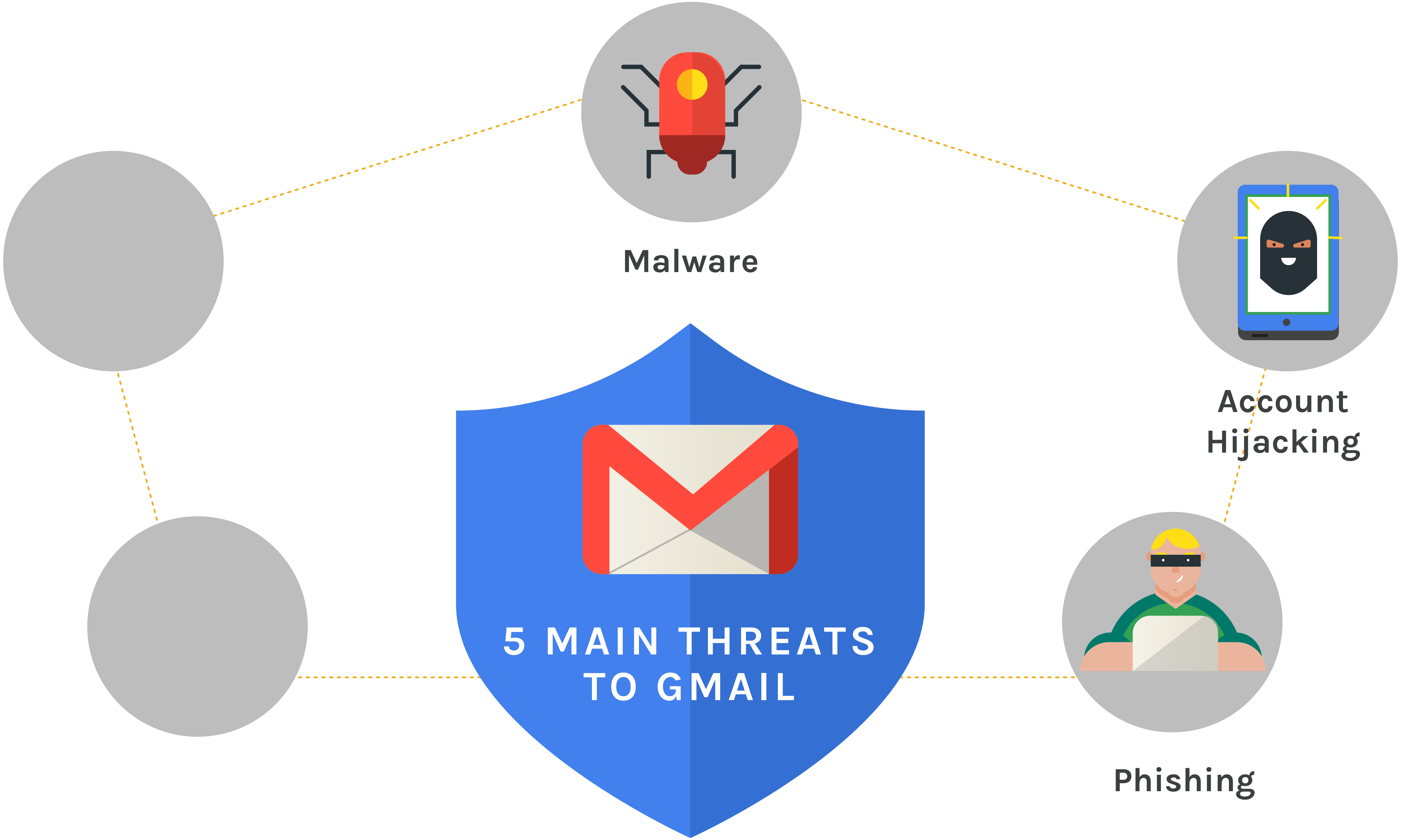
5 MAIN THREATS TO GMAIL



5 MAIN THREATS TO GMAIL

Malware

Account Hijacking

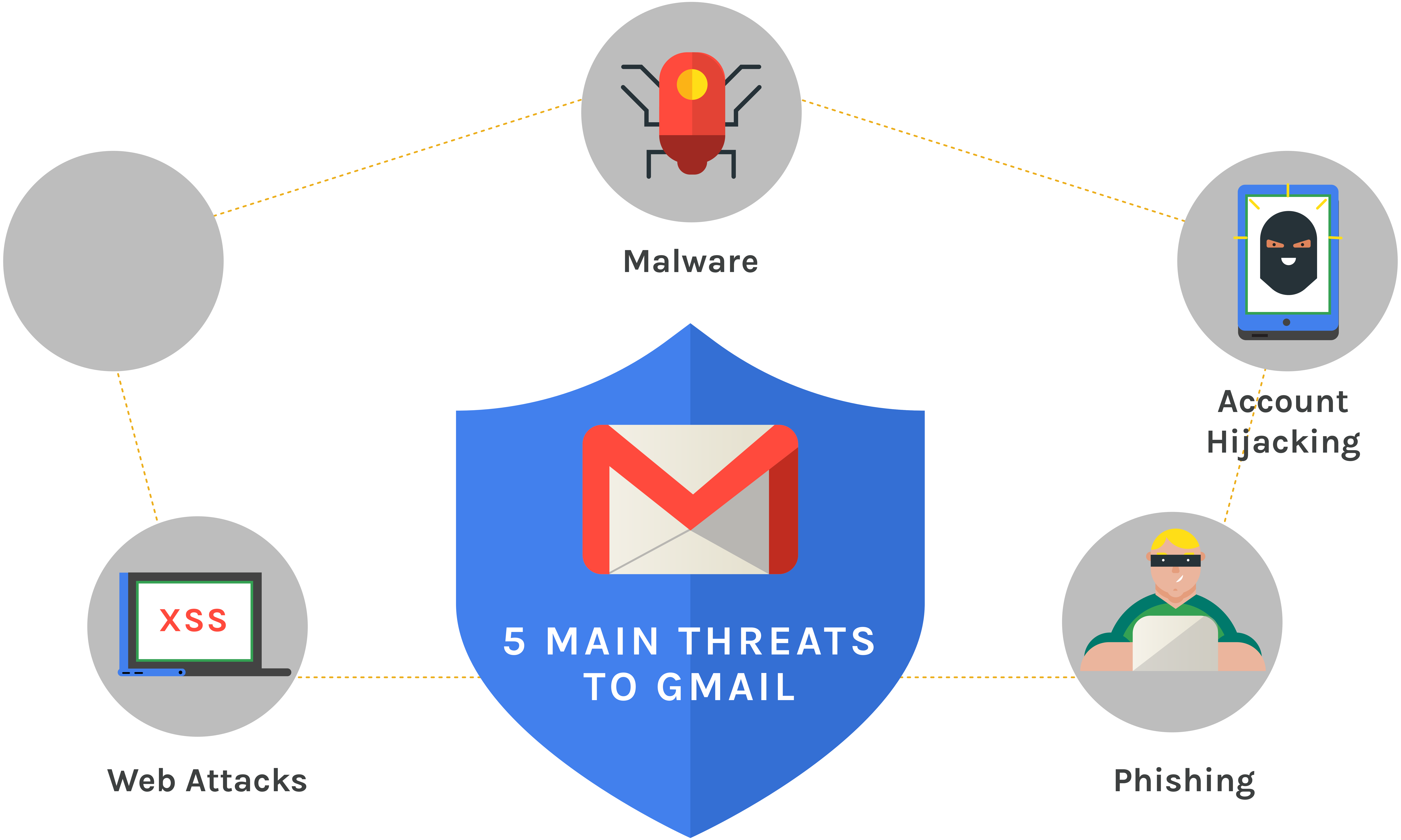


5 MAIN THREATS TO GMAIL

Malware

Account Hijacking

Phishing



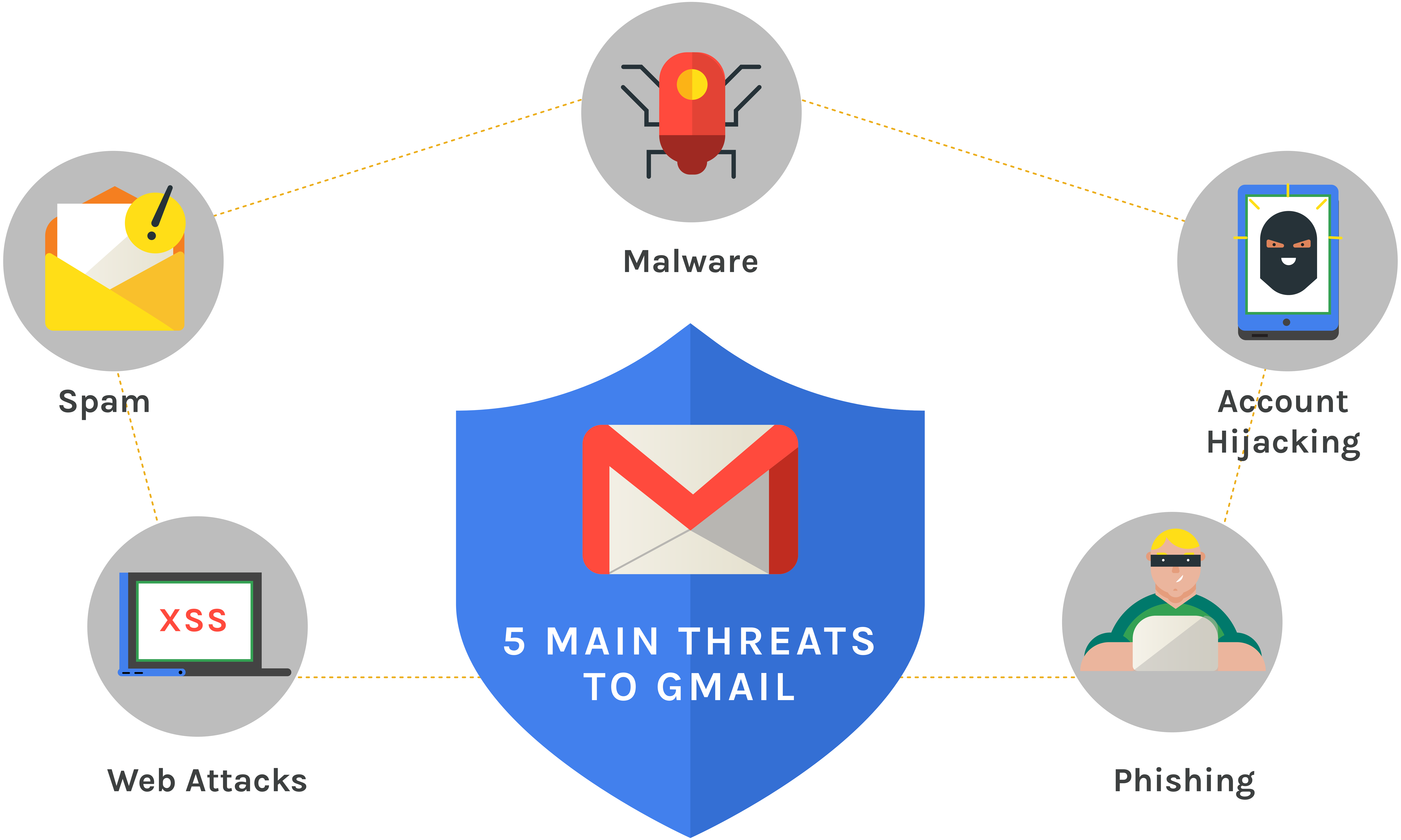
5 MAIN THREATS TO GMAIL

Malware

Account Hijacking

Phishing

Web Attacks



5 MAIN THREATS TO GMAIL

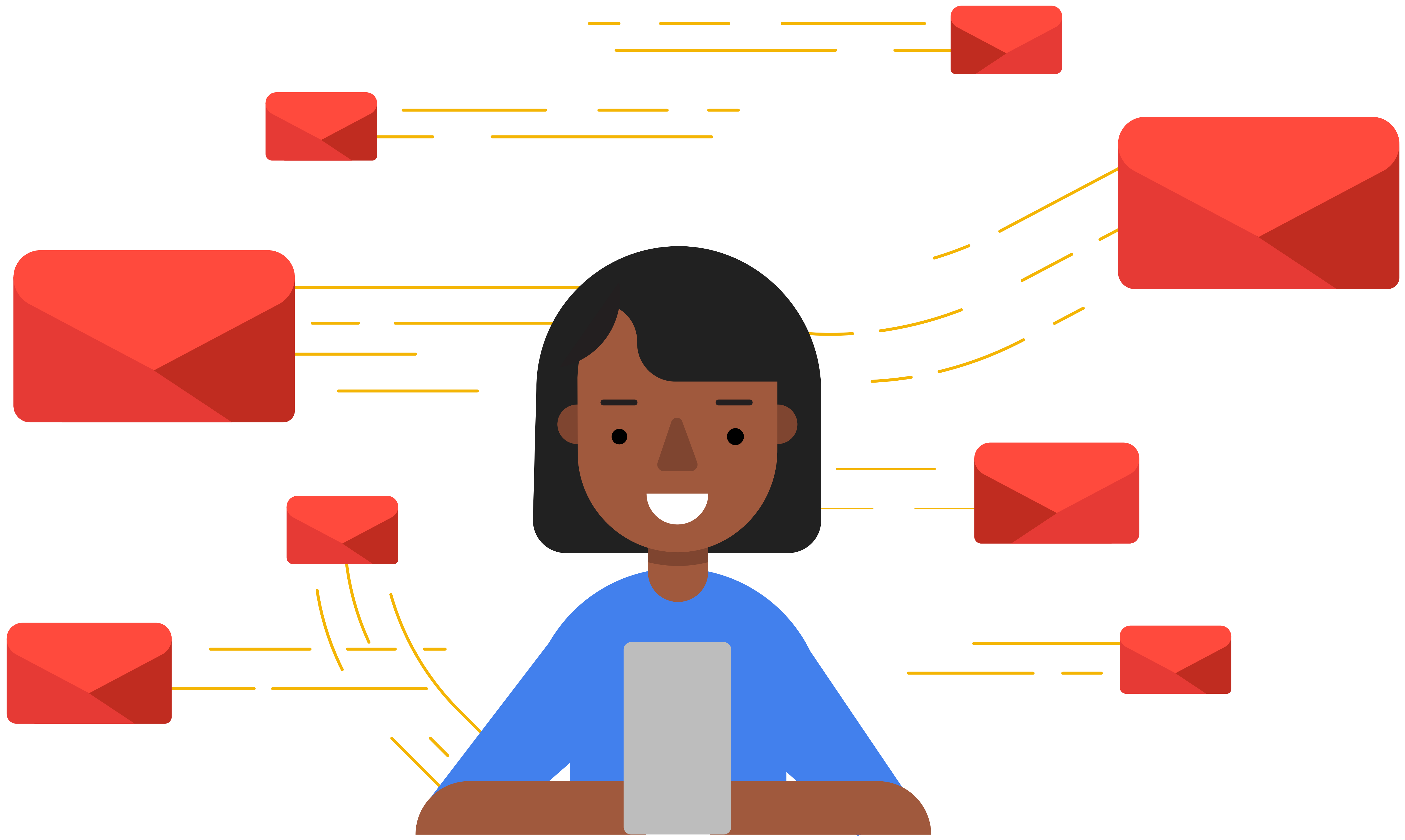
Malware

Spam

Account Hijacking

Web Attacks

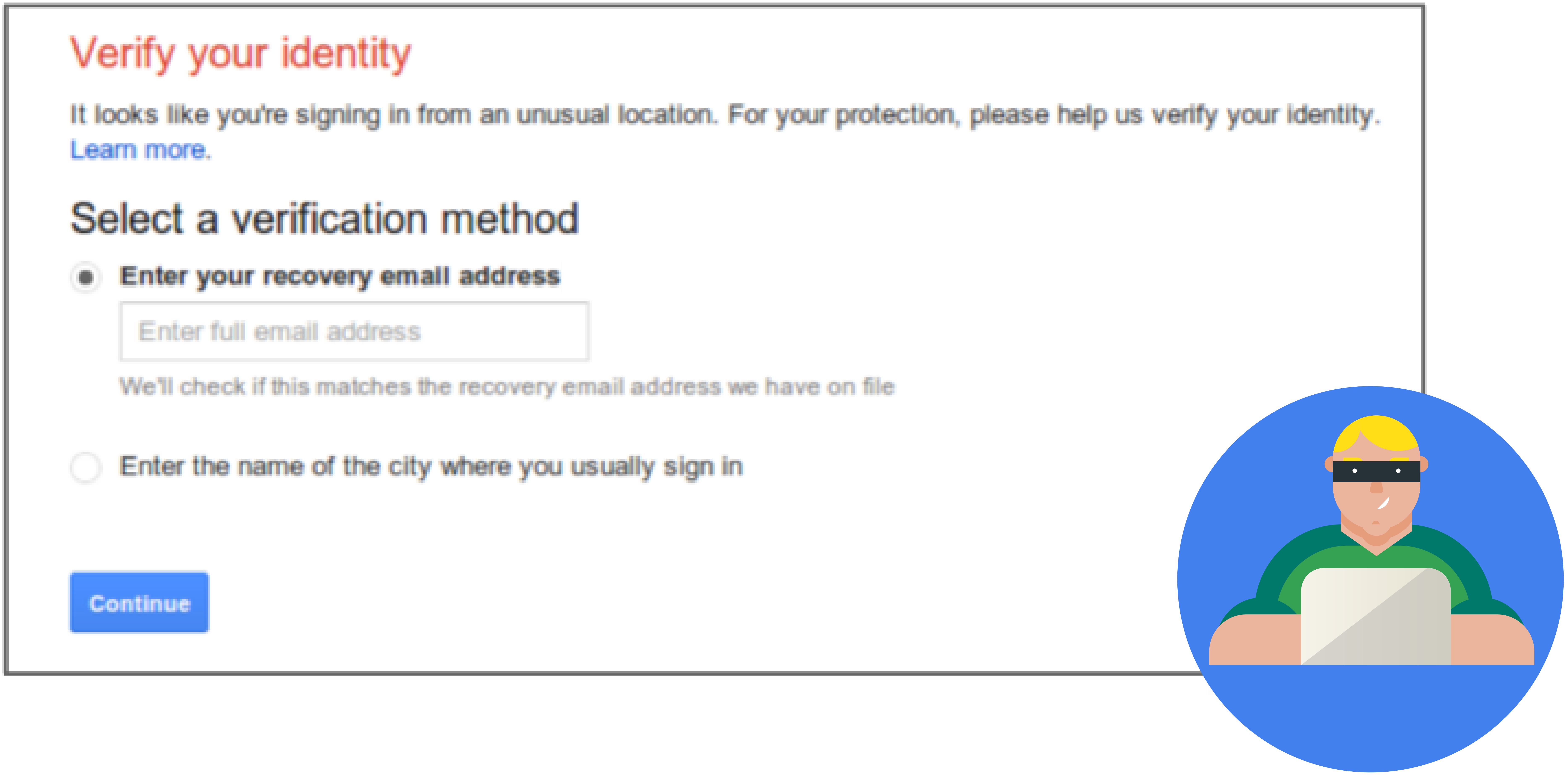
Phishing



900 MILLION+ USERS

hundreds of billions of messages per week

We launched login challenges In 2011



Verify your identity

It looks like you're signing in from an unusual location. For your protection, please help us verify your identity. Learn more.

Select a verification method

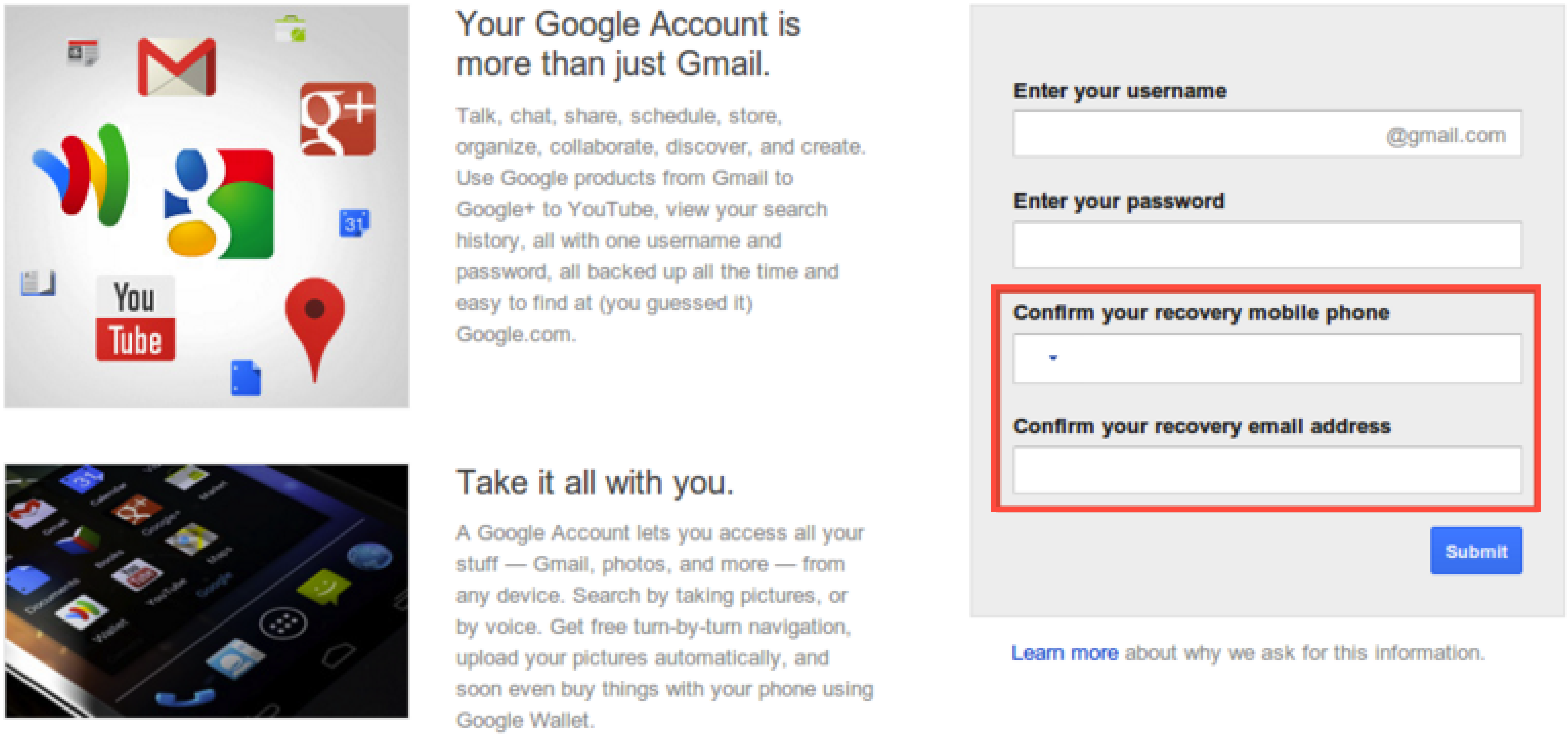
● **Enter your recovery email address**

Enter full email address

We'll check if this matches the recovery email address we have on file

○ Enter the name of the city where you usually sign in

Phishers updated their kits to ask for the challenge answers



Your Google Account is more than just Gmail.

Talk, chat, share, schedule, store, organize, collaborate, discover, and create. Use Google products from Gmail to Google+ to YouTube, view your search history, all with one username and password, all backed up all the time and easy to find at (you guessed it) Google.com.

Take it all with you.

A Google Account lets you access all your stuff — Gmail, photos, and more — from any device. Search by taking pictures, or by voice. Get free turn-by-turn navigation, upload your pictures automatically, and soon even buy things with your phone using Google Wallet.

Enter your username

@gmail.com

Enter your password

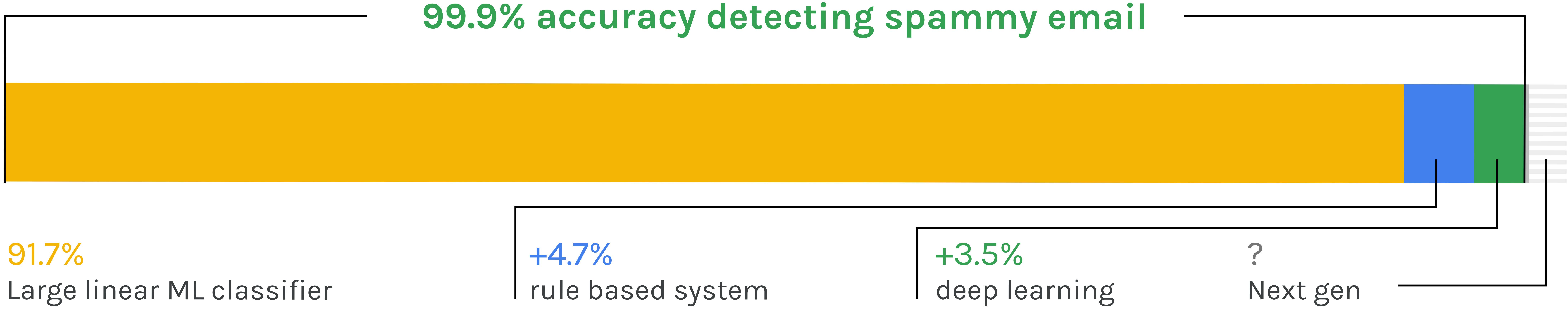
Confirm your recovery mobile phone

Confirm your recovery email address

Learn more about why we ask for this information.

NEVER STOP IMPROVING YOUR DEFENSES

http://goo.gl/xMctOL



99.9% accuracy detecting spammy email

91.7%
Large linear ML classifier

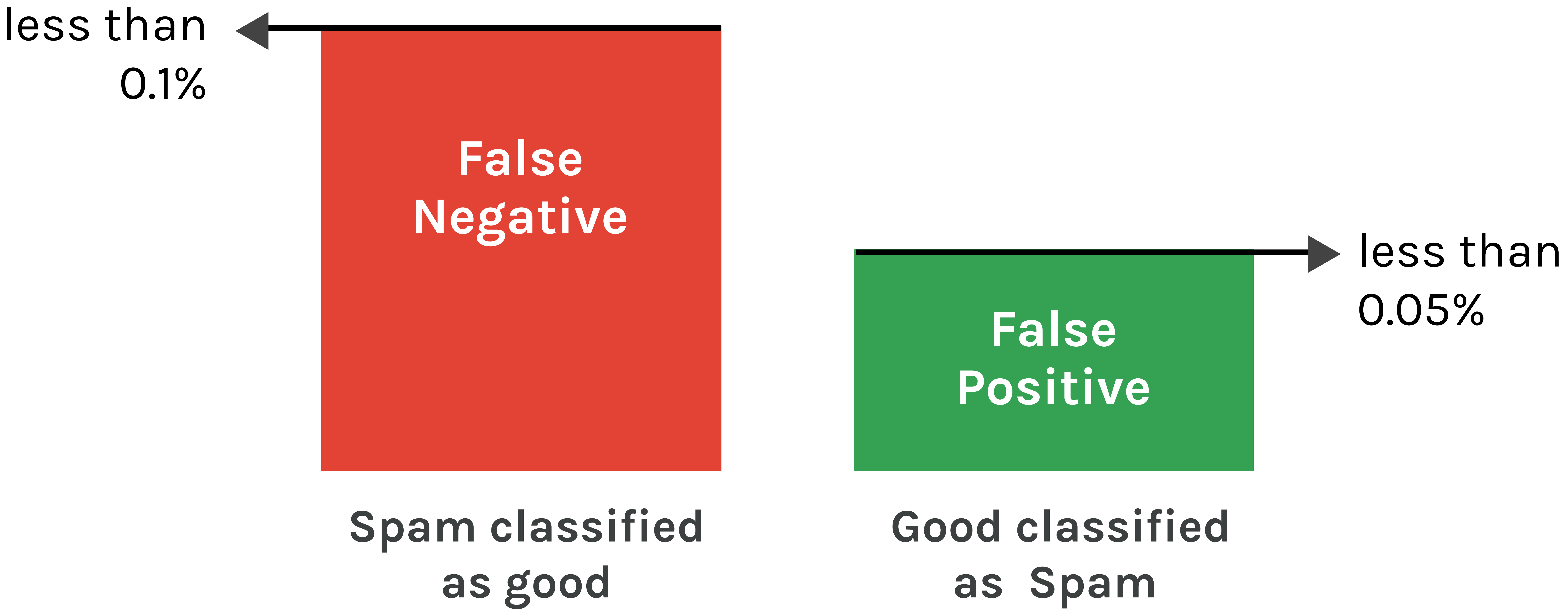
+4.7%
rule based system

+3.5%
deep learning

?
Next gen

THERE IS NO SILVER BULLET

http://goo.gl/0jgK96 *incremental coverage measurement



less than 0.1%

False Negative

Spam classified as good

False Positive

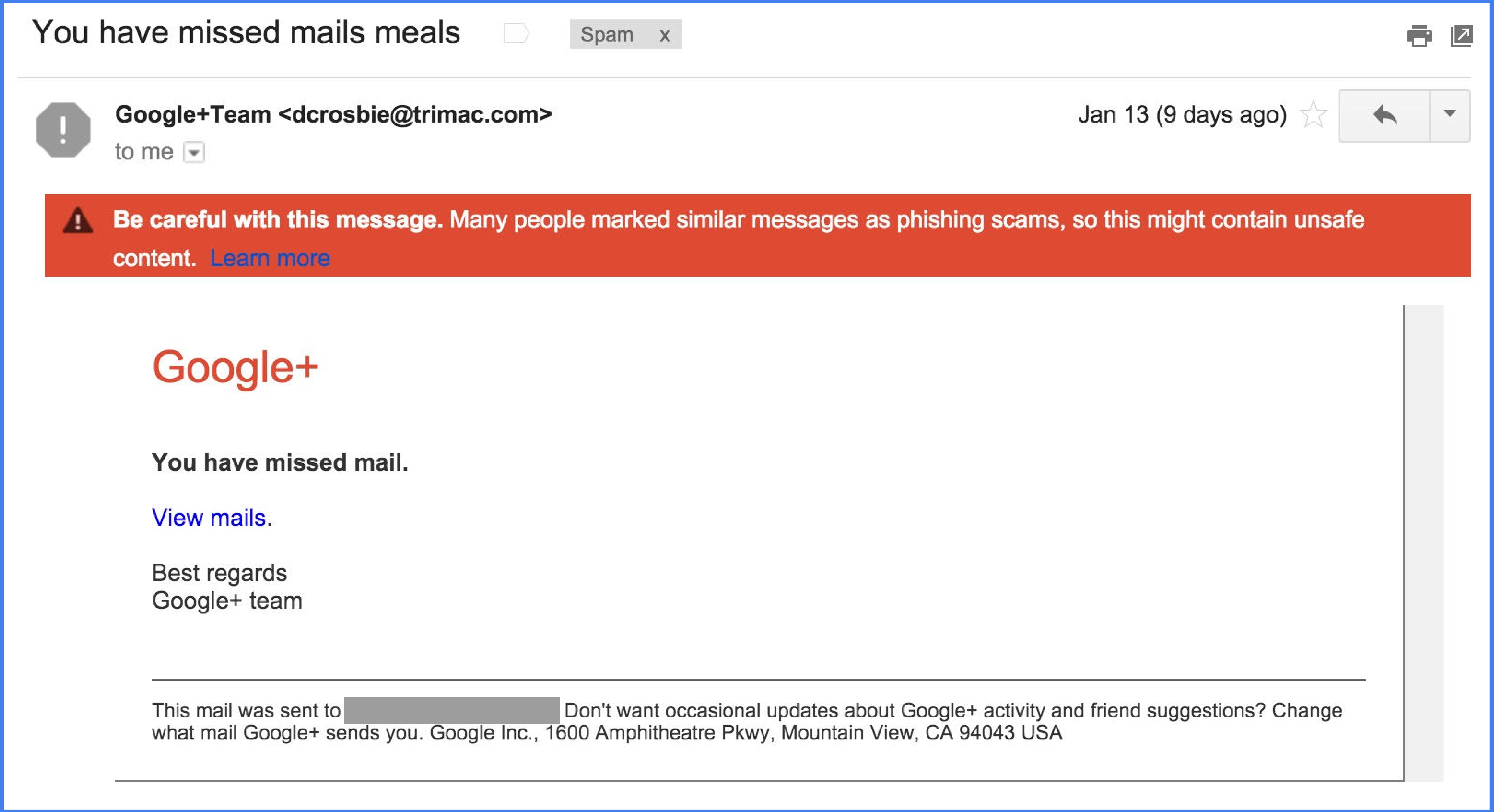
less than 0.05%

Good classified as Spam

TUNE YOUR CLASSIFIER

to match your product need

https://goo.gl/0jgK96



You have missed mails meals

Google+Team <dcrosbie@trimac.com>

to me

Jan 13 (9 days ago)

Be careful with this message. Many people marked similar messages as phishing scams, so this might contain unsafe content. Learn more

Google+

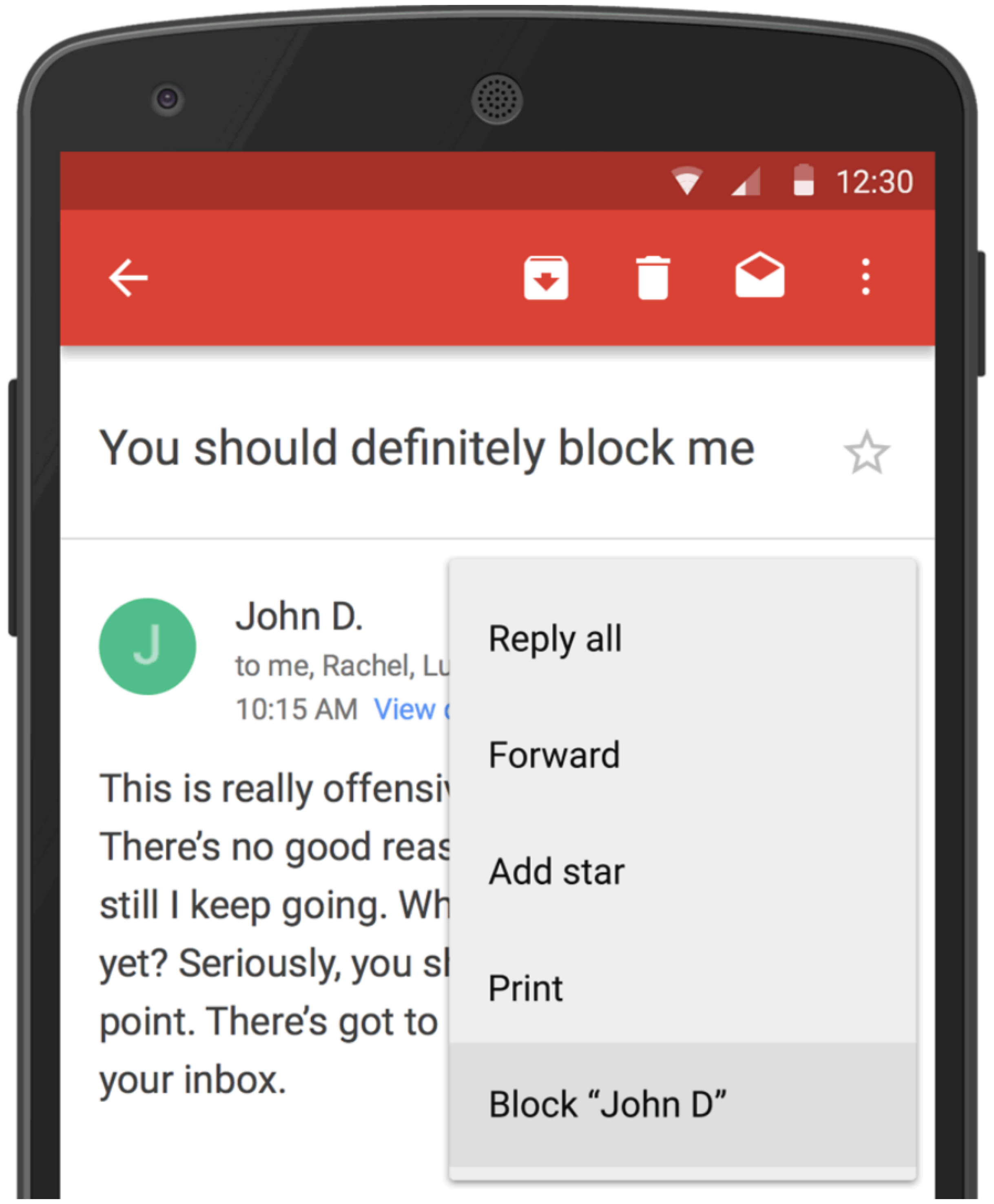
You have missed mail.

View mails.

Best regards
Google+ team

This mail was sent to [redacted] Don't want occasional updates about Google+ activity and friend suggestions? Change what mail Google+ sends you. Google Inc., 1600 Amphitheatre Pkwy, Mountain View, CA 94043 USA

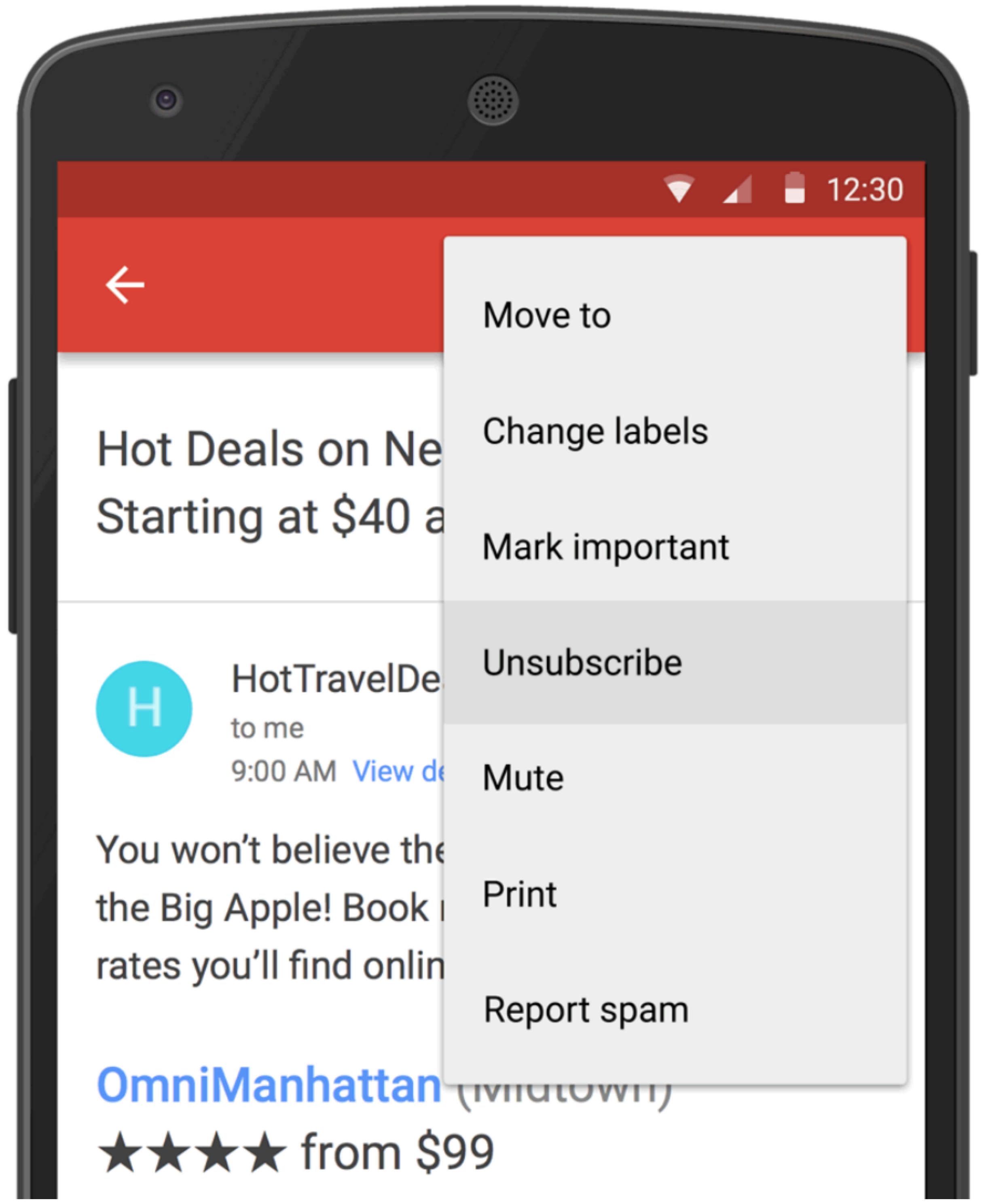
IMPLEMENT CATCH-UP MECHANISMS



You should definitely block me

John D.
to me, Rachel, Lu
10:15 AM View

This is really offensi
There's no good reas
still I keep going. Wh
yet? Seriously, you sl
point. There's got to
your inbox.

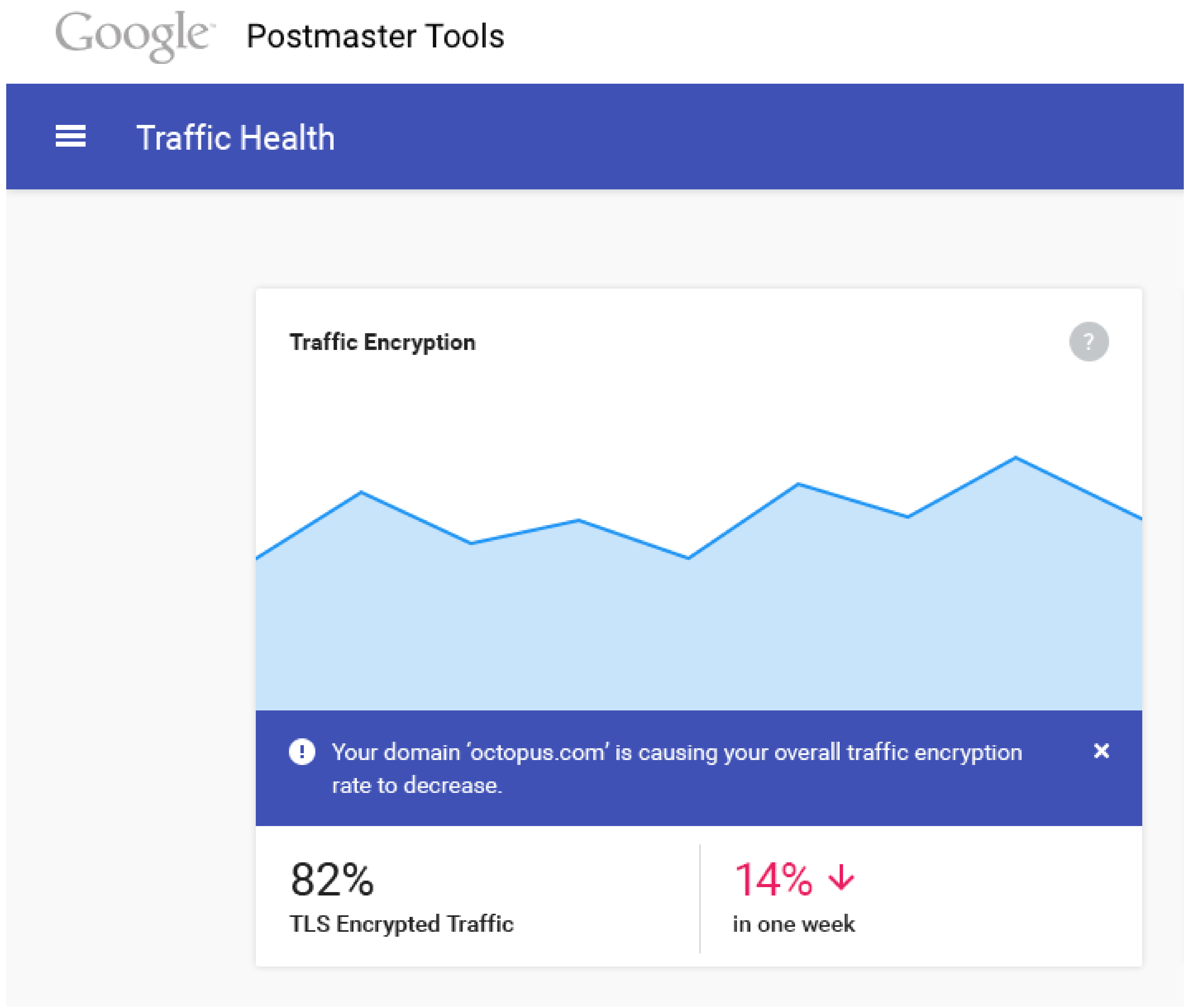


Hot Deals on Ne
Starting at $40 a

HotTravelDe
to me
9:00 AM View de

You won't believe the
the Big Apple! Book
rates you'll find onlin

OmniManhattan (Midtown)
★★★★ from $99



Google Postmaster Tools

Traffic Health

Traffic Encryption

Your domain 'octopus.com' is causing your overall traffic encryption rate to decrease.

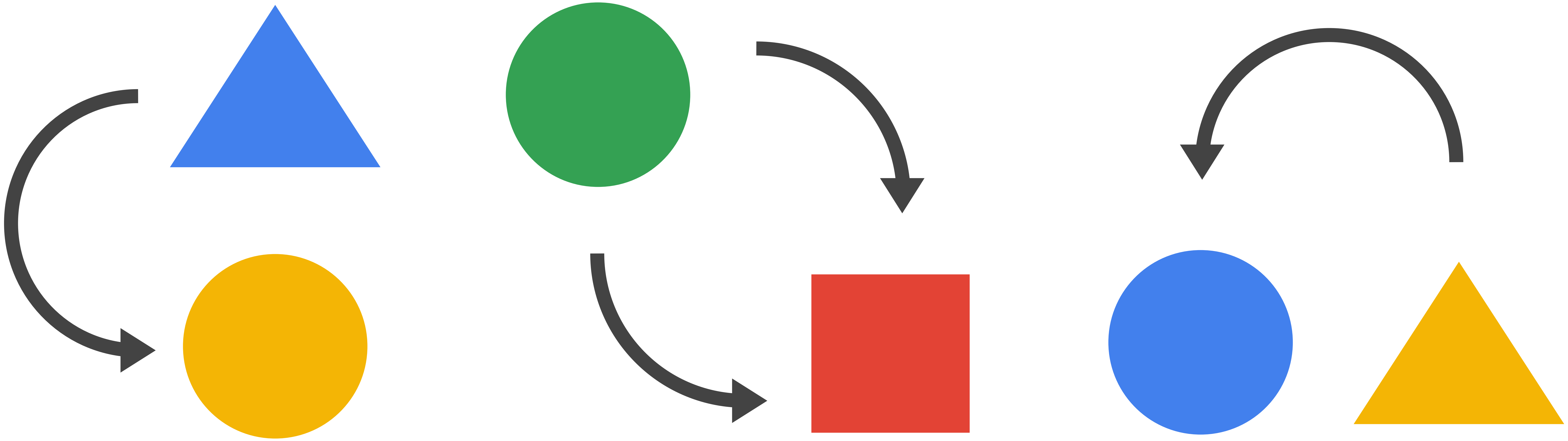
82%
TLS Encrypted Traffic

14% ↓
in one week

EMPOWER USERS

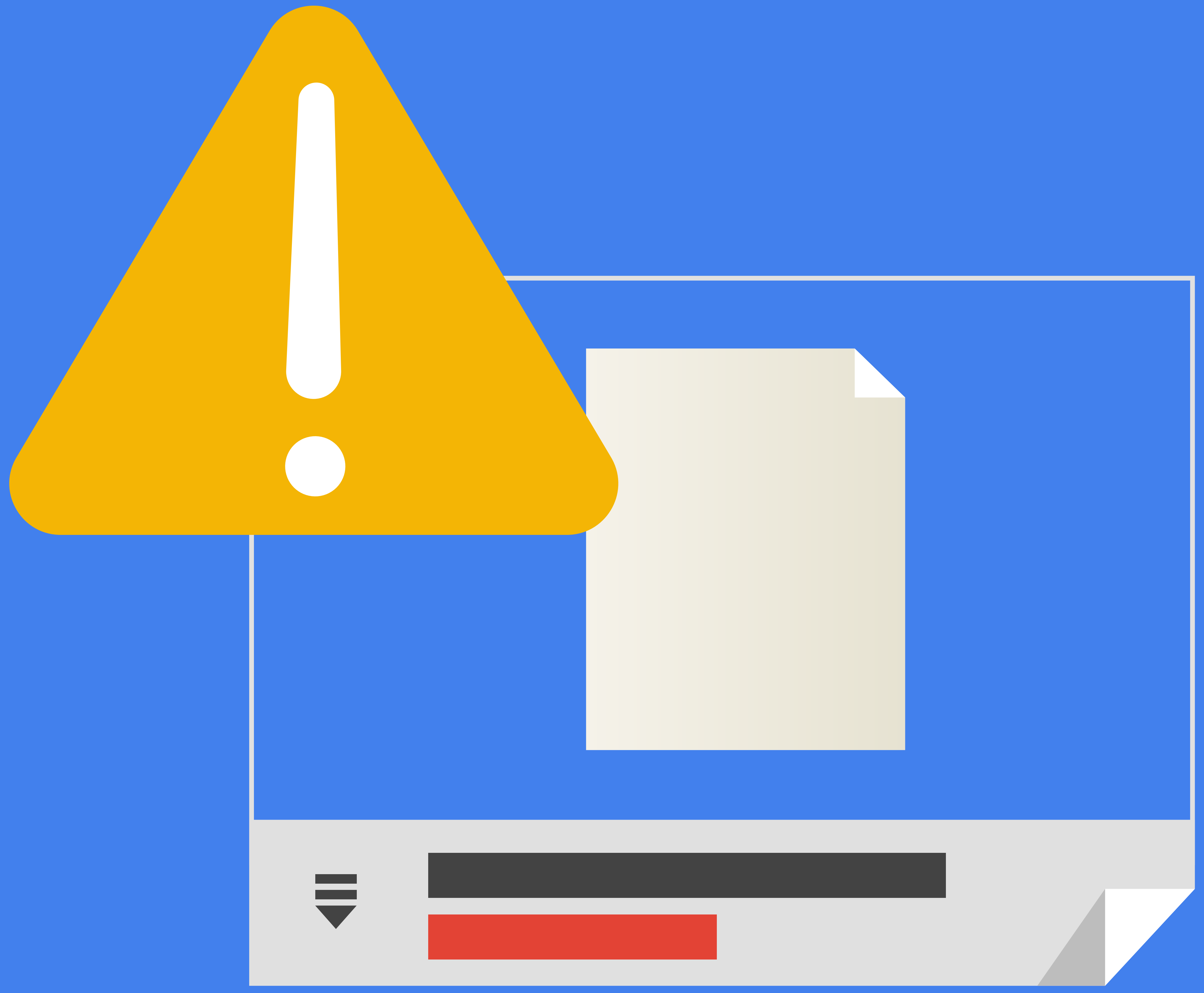
to take action through meaningful UI

https://goo.gl/gqk6Bn & https://goo.gl/sL5VWC

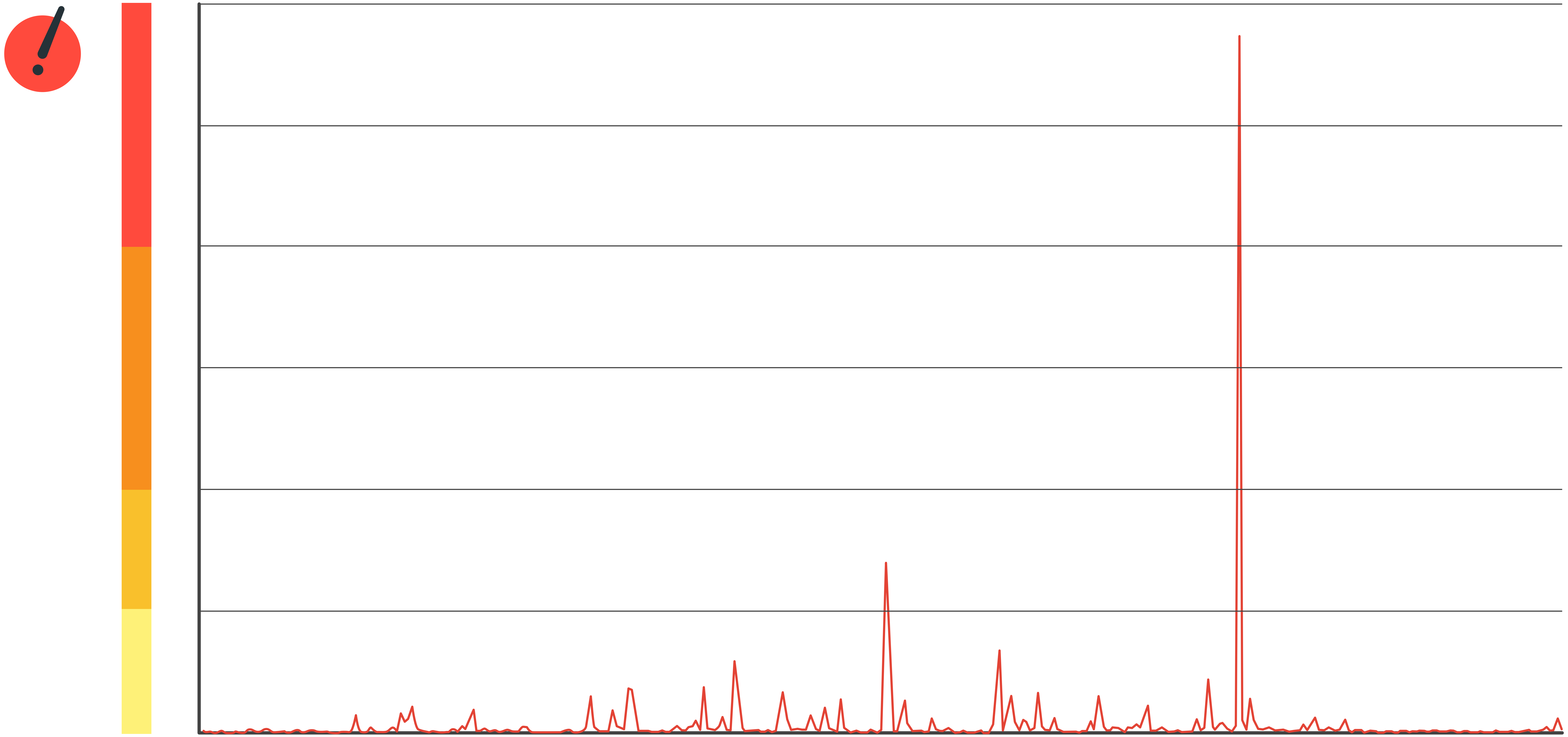


USE OVERWHELMING FORCE

Deploy many countermeasures at once

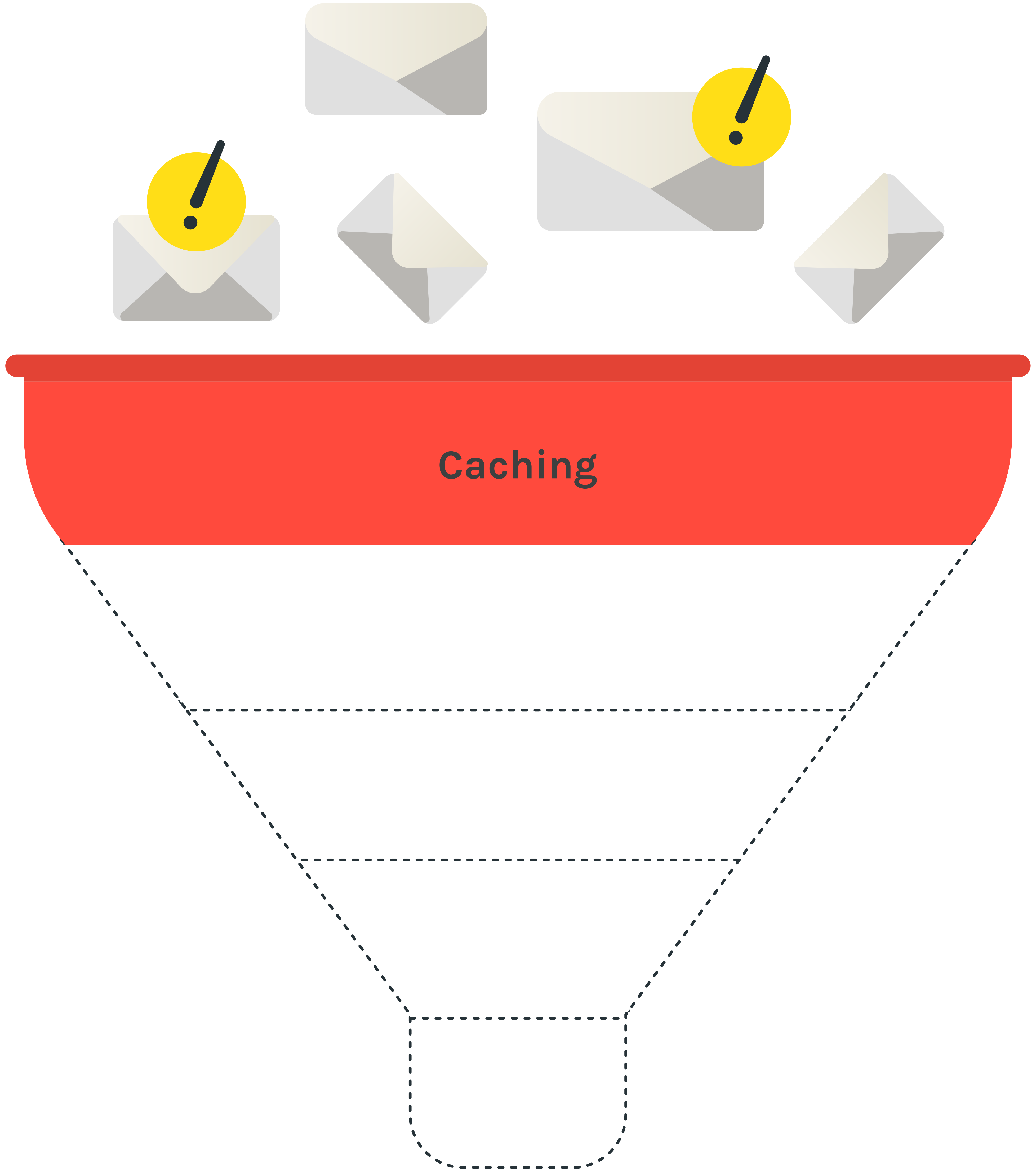


EMAIL ATTACHMENT



ATTACKS COME IN BURSTS

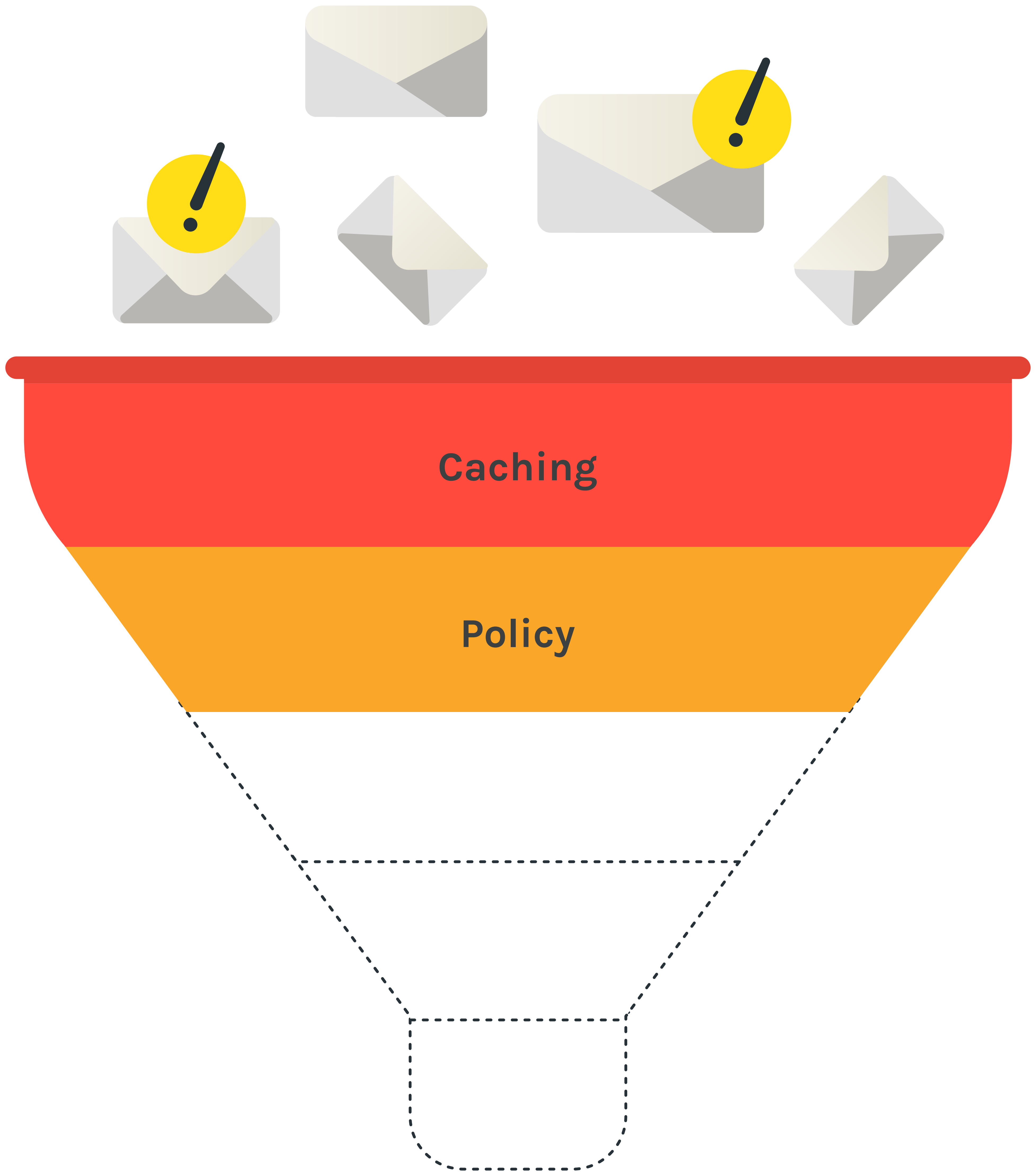
plan for it



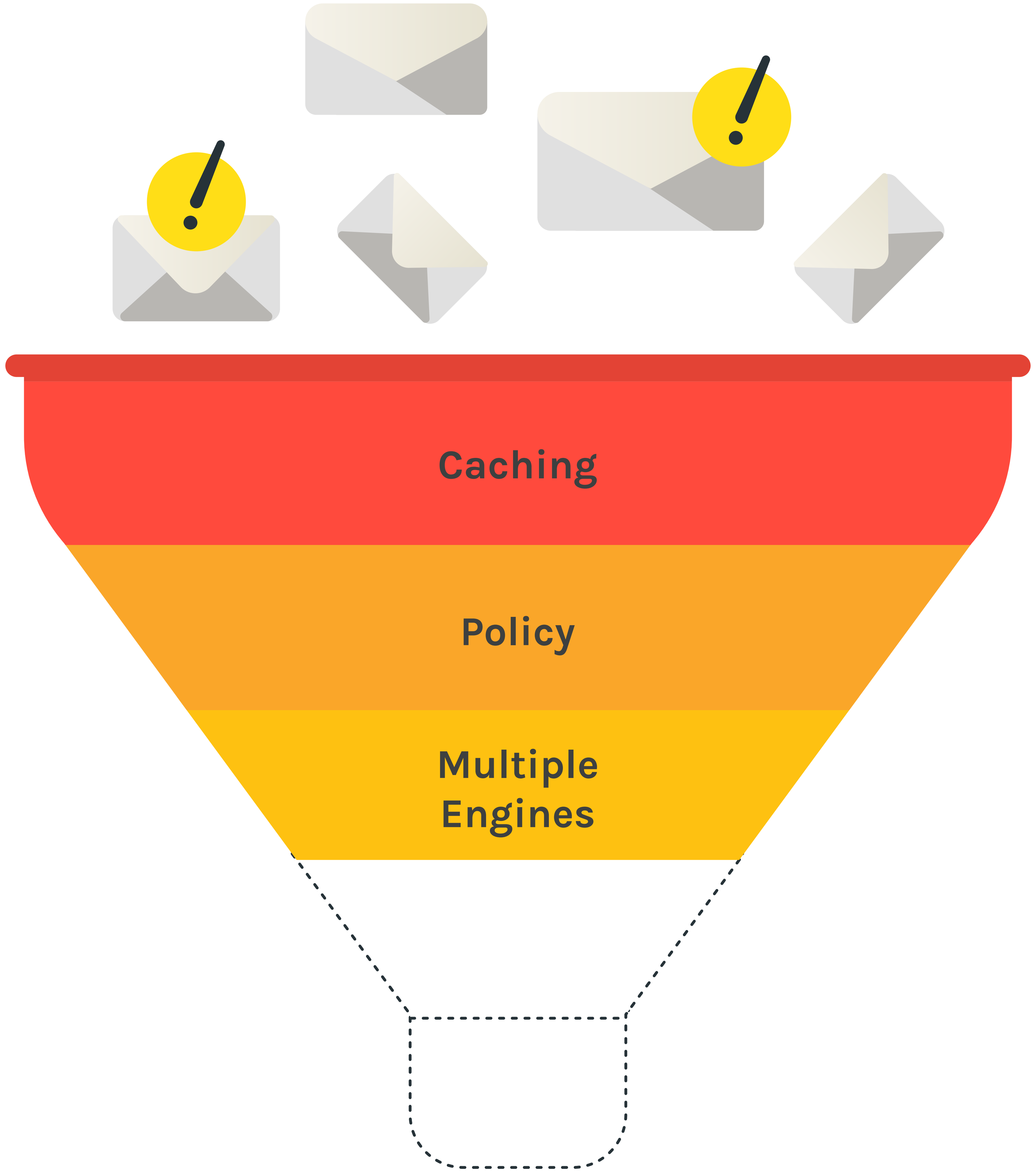
DON’T PROCESS TWICE

Whitelisting and blacklisting allows up to 50% reduction in computation

BE SECURE BY DESIGN



Gmail does not allow
executable attachments



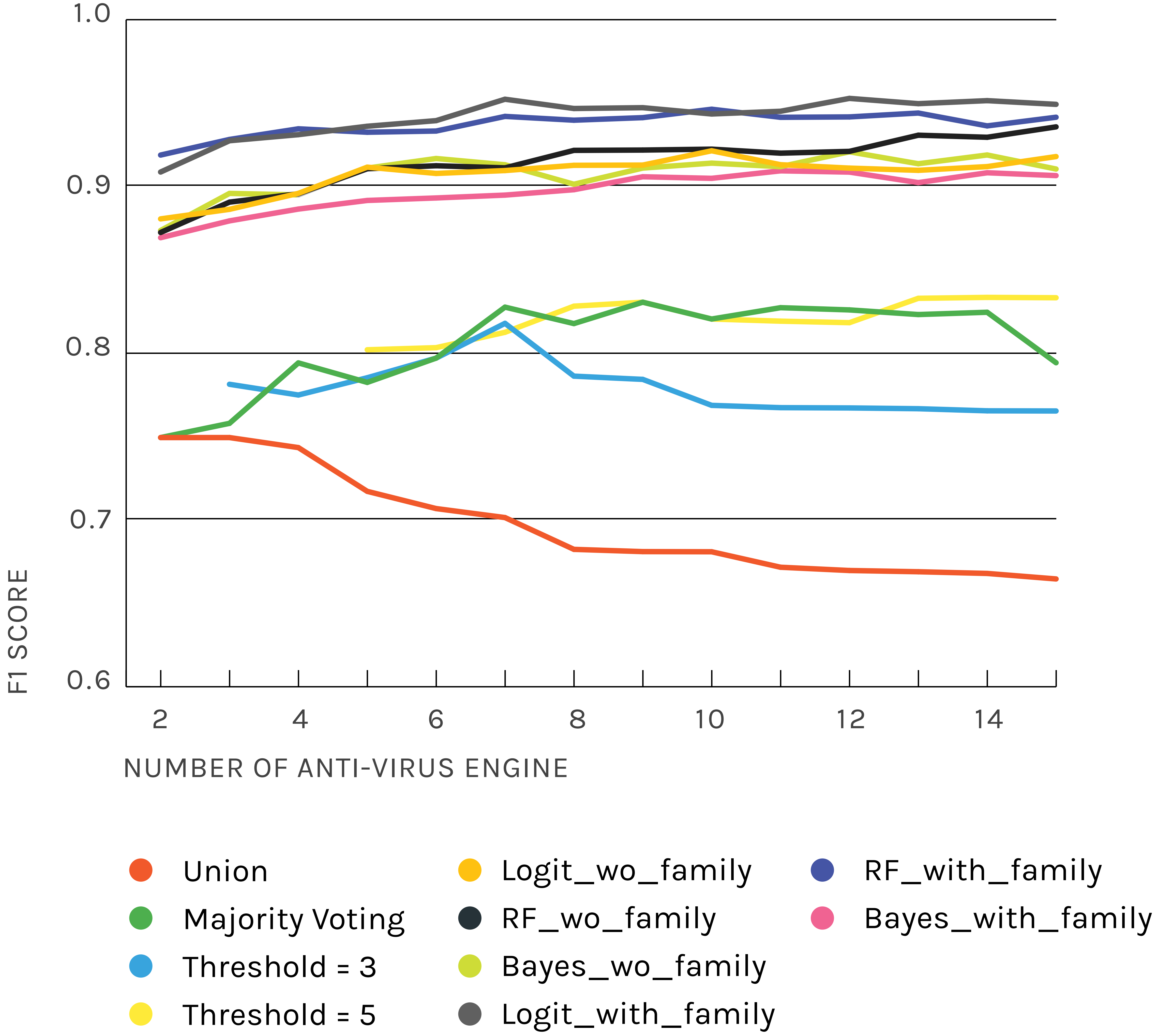
Caching

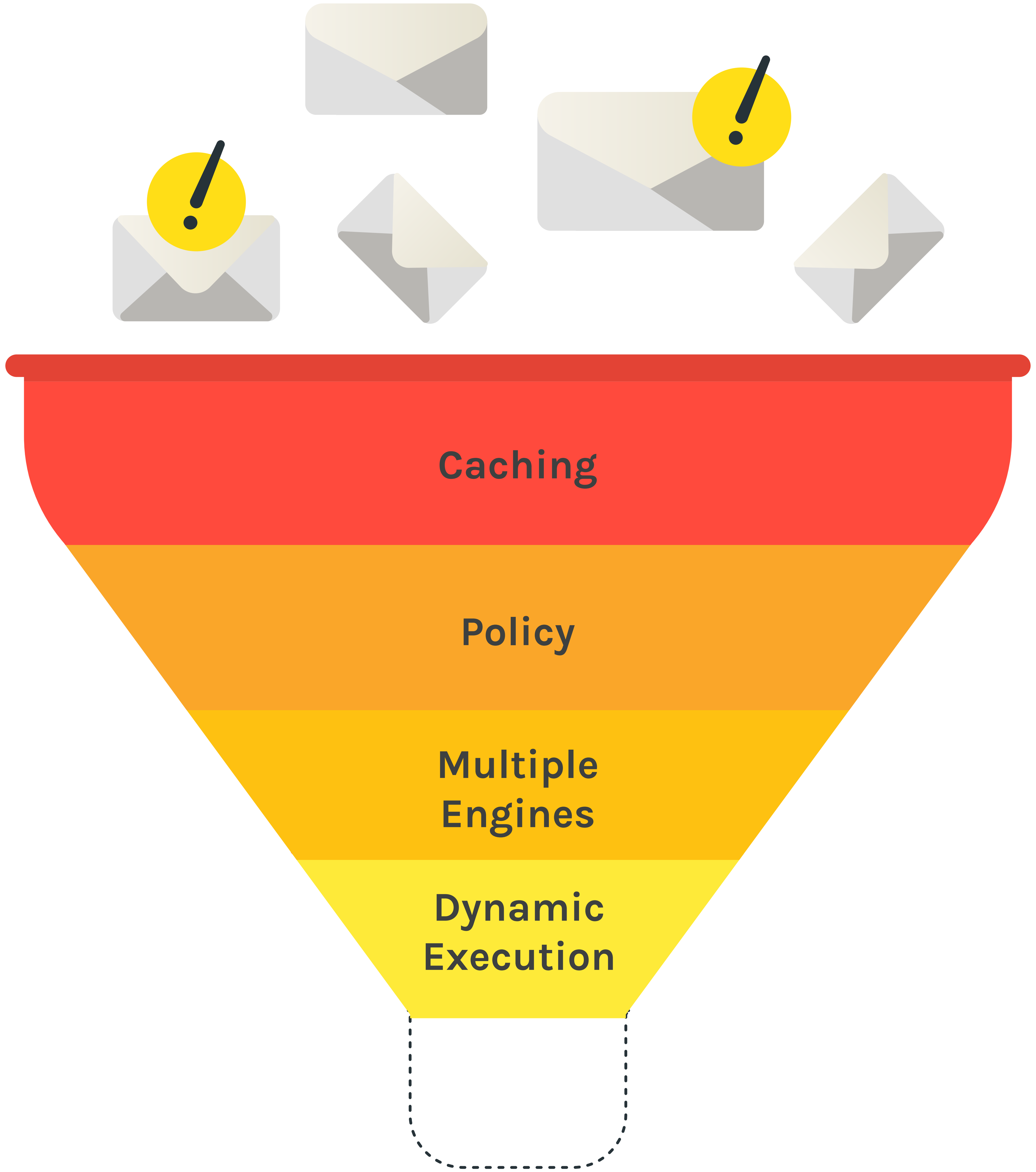
Policy

Multiple Engines

USE ENSEMBLE LEARNING

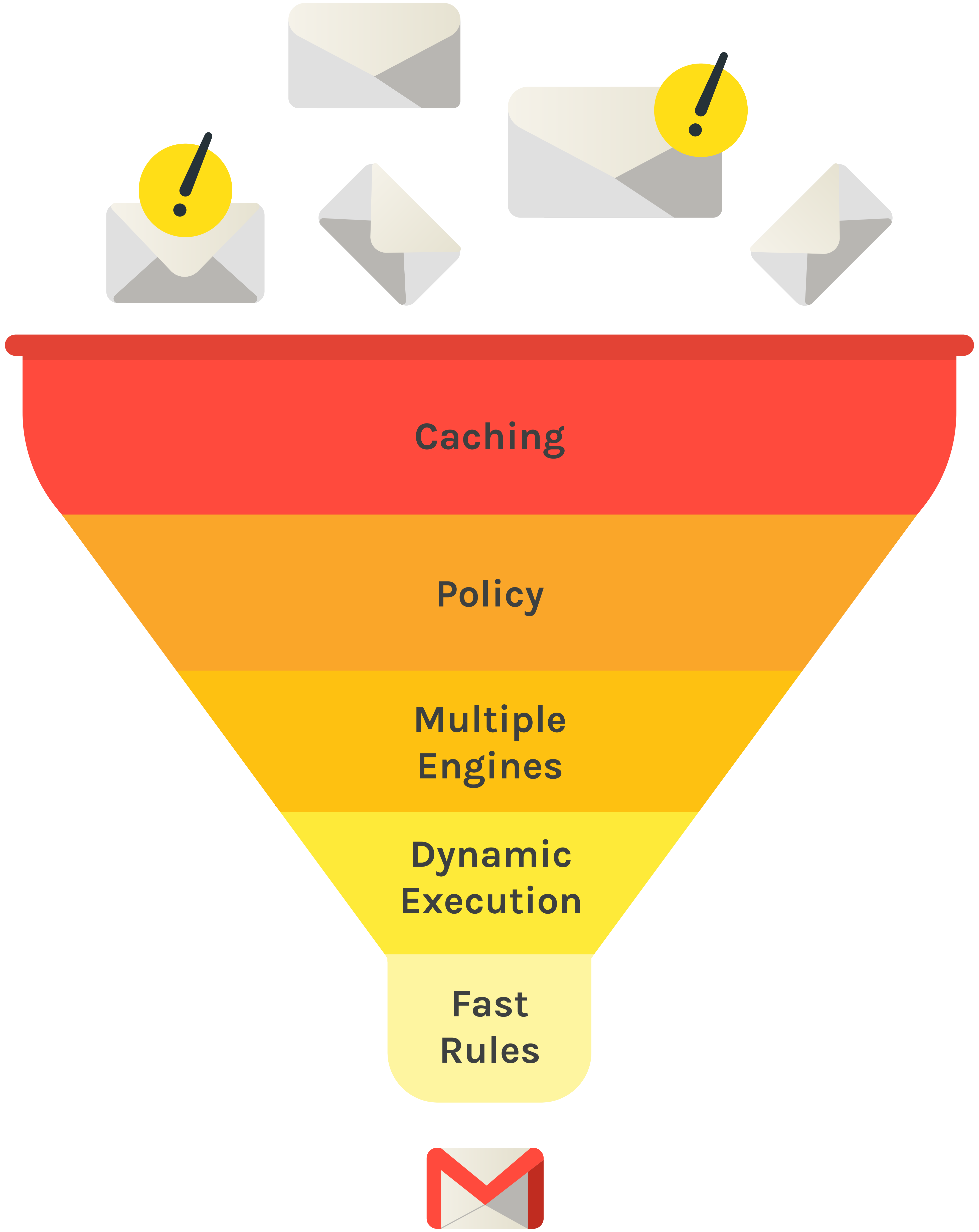
multiple anti-viruses are combined



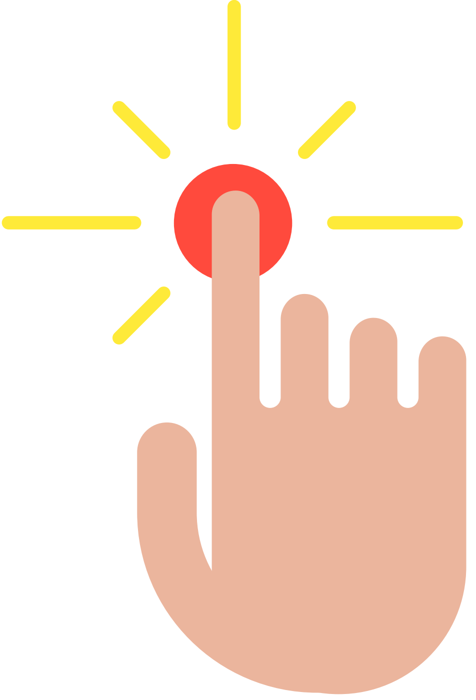


USE DYNAMIC EXECUTION

to catch undetected malwares (very rare)



IMPLEMENT EMERGENCY BLOCKING SYSTEMS



Unpredictable attacks and bugs happen.
Get as ready as possible for it

INBOUND

62%

Messages from other providers to Gmail are encrypted

OUTBOUND

82%

Messages from Gmail to other providers are encrypted

ENCRYPT EVERYTHING

in transit and at rest

https://goo.gl/iv2tIa * Gmail always tries to encrypt email communication. Encryption failures are due to other providers not supporting encryption

Manual and Unsafe Escaping

```
{template .page}
<a href="{$profile.blogUrl |sanitizeUrl}">
```

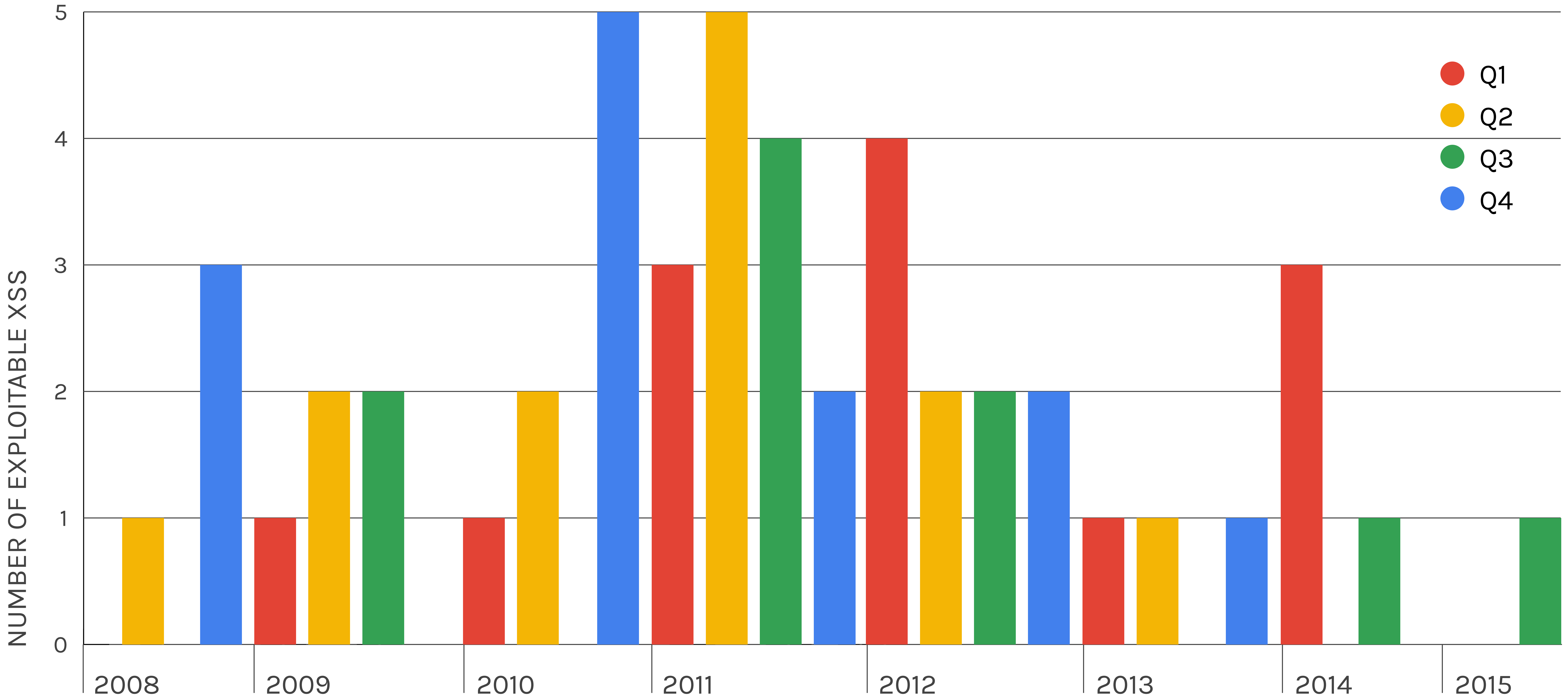
VS

Closure Templates Strict Autoescaping

```
{template .page autoescape="strict"}
<a href="{$profile.blogUrl}">
```

https://goo.gl/1tLf3w

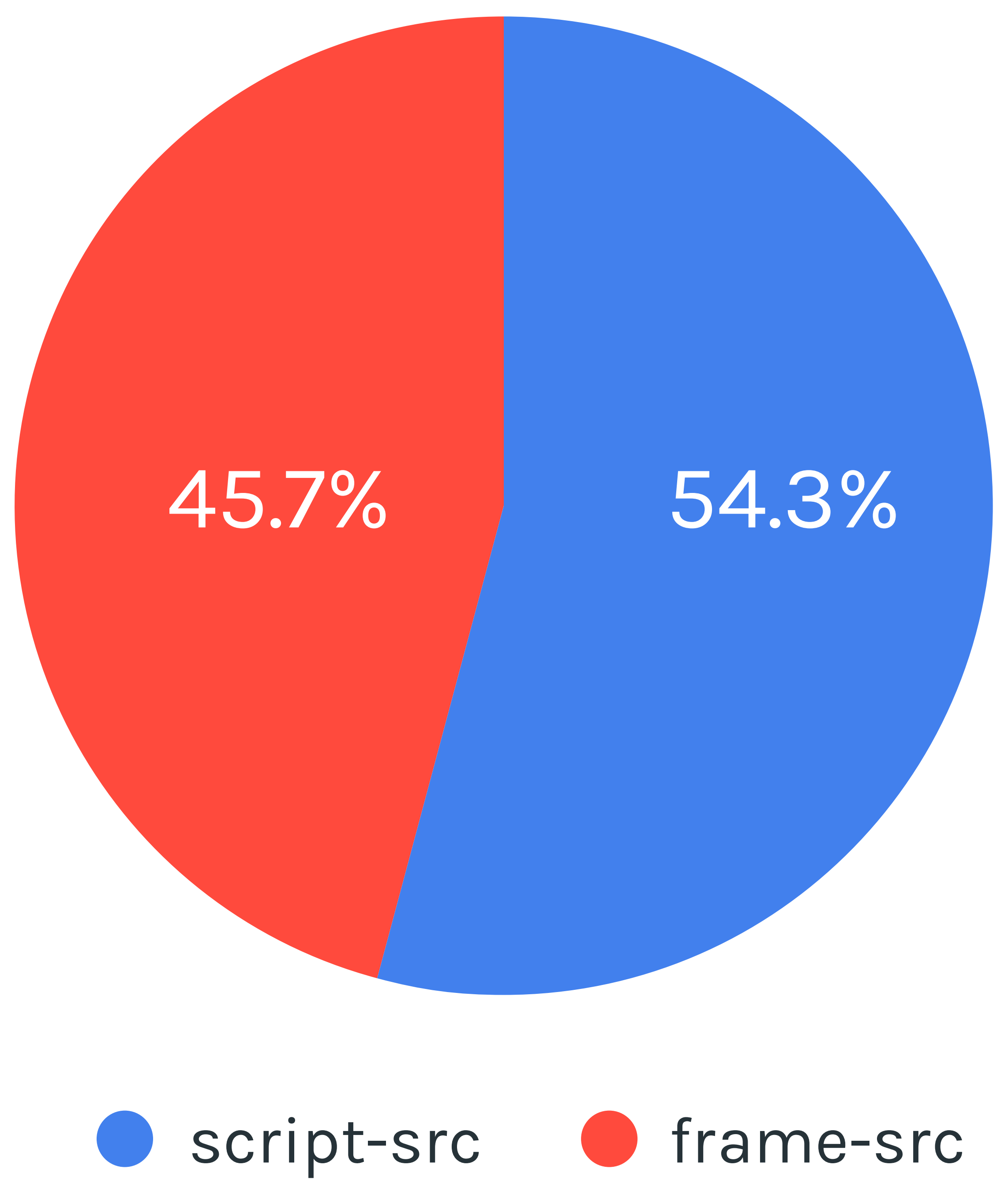
Number of XSS affecting Gmail webmail fixed per quarter



BE METRICS DRIVEN

PREVENT BUGS THROUGH GOOD SOFTWARE DESIGN

CSP violations for Google Inbox just before launch

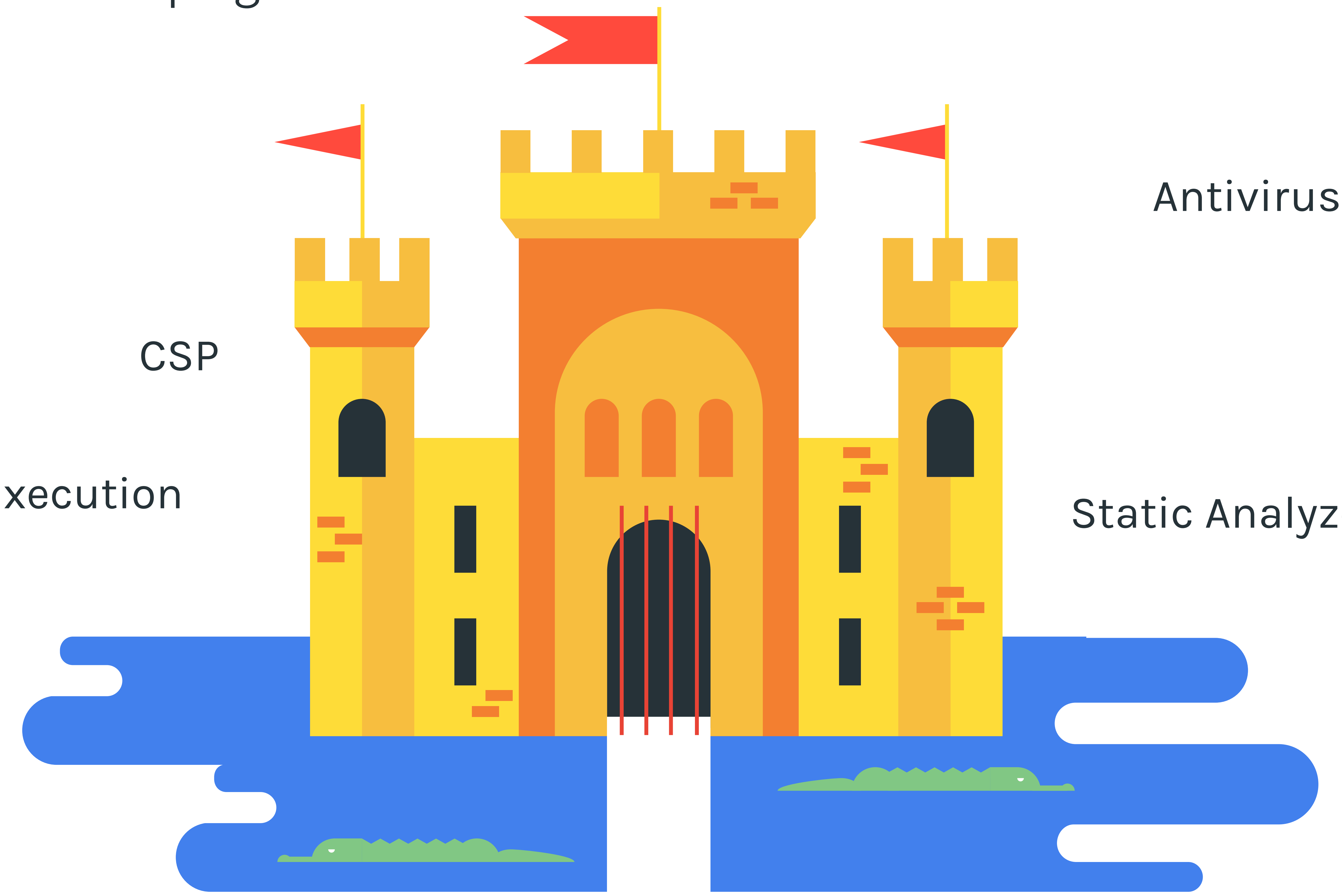


CSP blocks a lot of bad stuff

Smart labels potential XSS

```
<! <img src="><img src=x onerror=alert(1)// ">
```

CSP helped us identify potential XSS



Deep Learning

Encryption

Auto-escaping

Linear Classifiers

Fuzzing

Antivirus

DDOS prevention

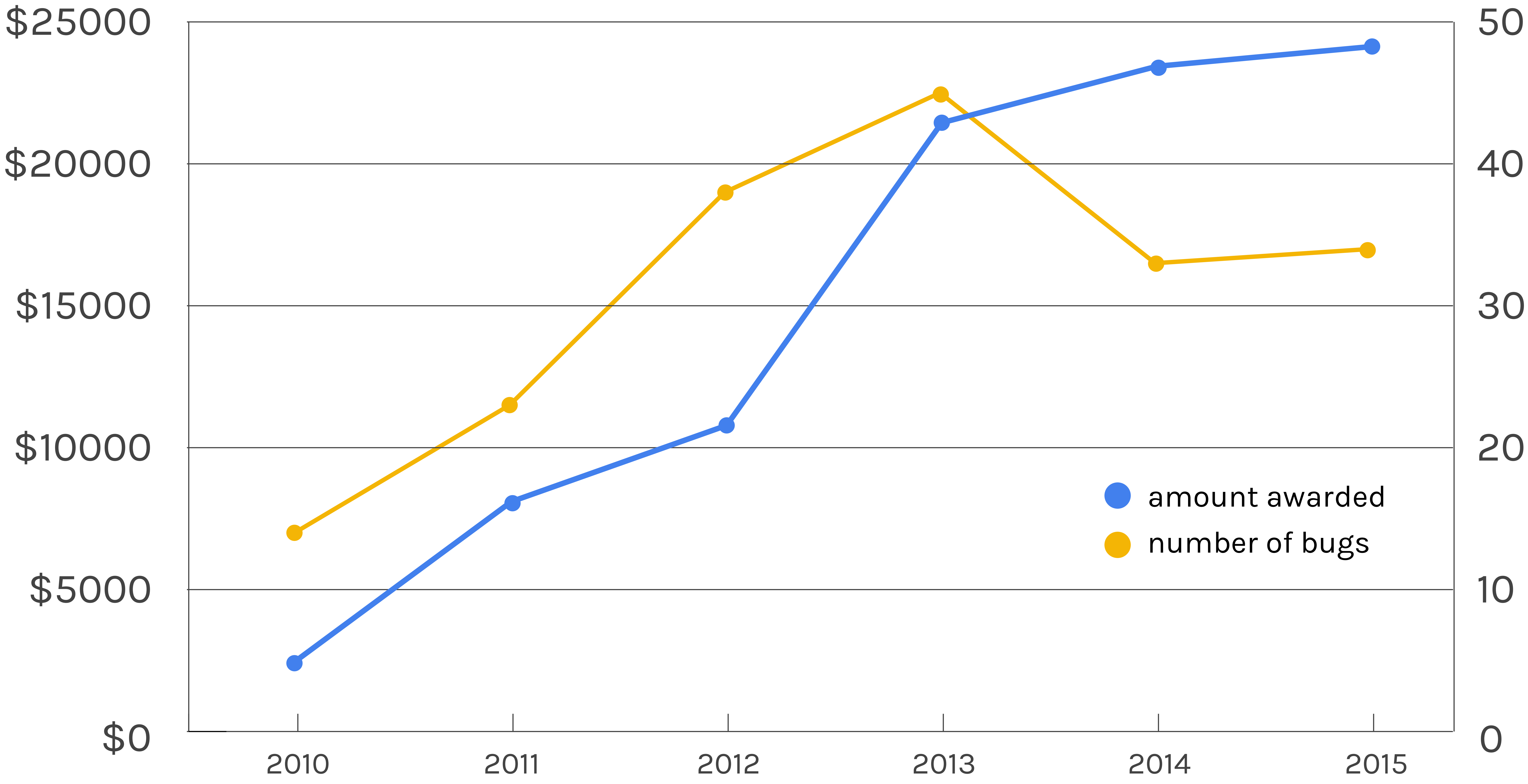
Security audits

CSP

Dynamic Execution

Static Analyzers

IMPLEMENT DEFENSE IN DEPTH



PAY FOR BUGS

it's worth it

KEY CHALLENGES IN 2016

Dynamic rendering
CSS, Javascript. E.g Media Queries

Hacked site
Good sites used in phishing attacks

Email security standards
Yet to be fully adopted

Advanced phishing attacks
e.g spear phishing

KEY TAKEAWAYS

Combine detection technologies in each layer
There is no silver bullet so diversification is key to lasting security.

Defense in depth
Add multiple layers of security because sooner or later an attacker will break one.

Have a strong team that keeps running
It takes all your efforts to keep the product clean. No rest for the brave.

Thank you!