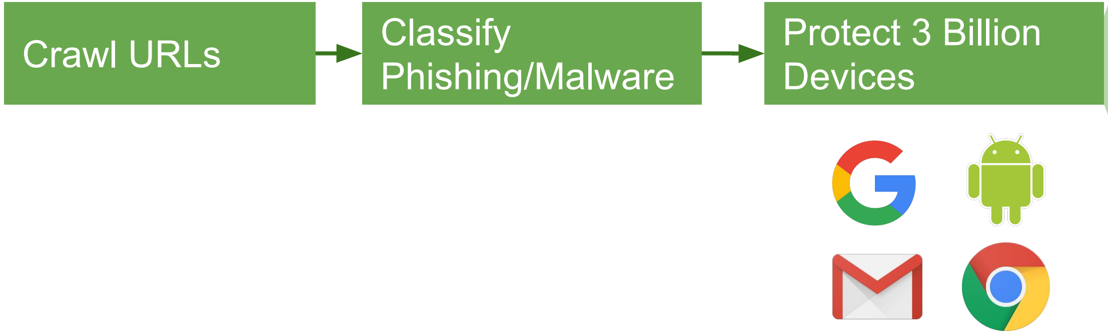
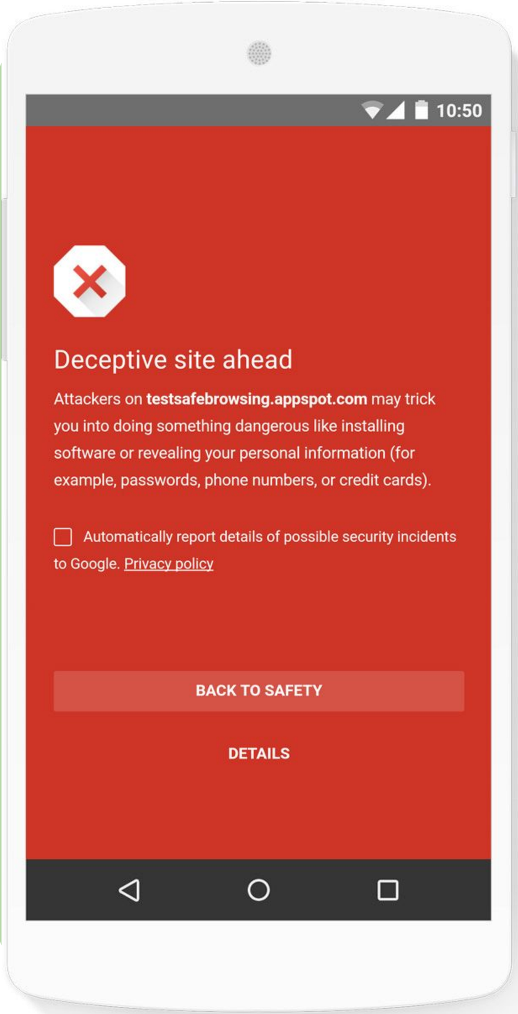
Google Safe Browsing

Goal: Make the world's information safely accessible

Google Safe Browsing



Crawl URLs → Classify Phishing/Malware → Protect 3 Billion Devices



Deceptive site ahead

Attackers on **testsafebrowsing.appspot.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

☐ Automatically report details of possible security incidents to Google. Privacy policy

Google Safe Browsing

3B+

Devices Protected

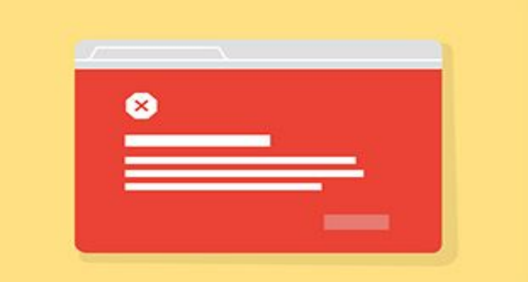
9M+

Warnings Shown in a day

5%

Click through rate on warnings

Google Safe Browsing

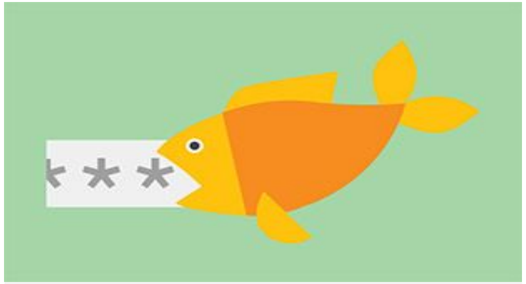


Malware

Software specifically designed to harm a device, the software it's running, or its users.

Unwanted Software

Disguised programs that actually make unexpected changes to a user's computer like switching homepage or other browser settings.



Social Engineering

Tricks users into performing an action that they normally would not if they knew the true identity of the attacker

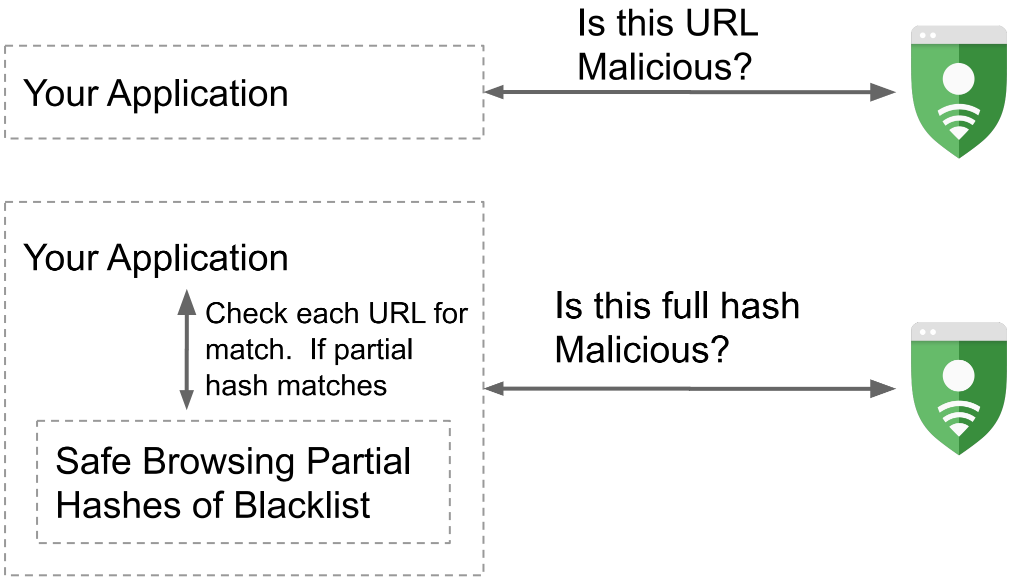
Why is this hard?

Challenges

- Cloaking (agent types, times, geo, IPs)
- Delivery channels (email, messaging, texts, ads)
- Balance of accuracy and recall false positives to create the best outcome for both webmasters and users

How to get involved

Access Our Data
Safe Browsing Lookup/Update APIs



Your Application

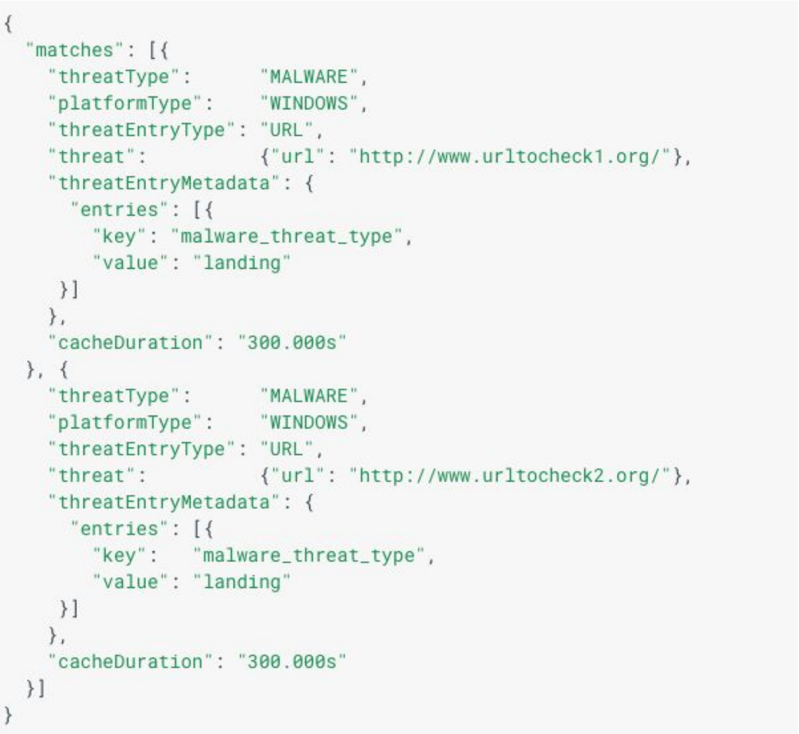
Is this URL Malicious?

Your Application

Check each URL for match. If partial hash matches

Safe Browsing Partial Hashes of Blacklist

Is this full hash Malicious?



```
{
  "matches": [{
    "threatType":      "MALWARE",
    "platformType":    "WINDOWS",
    "threatEntryType": "URL",
    "threat":          {"url": "http://www.urltocheck1.org/"},
    "threatEntryMetadata": {
      "entries": [{
        "key": "malware_threat_type",
        "value": "landing"
      }]
    },
    "cacheDuration": "300.000s"
  }, {
    "threatType":      "MALWARE",
    "platformType":    "WINDOWS",
    "threatEntryType": "URL",
    "threat":          {"url": "http://www.urltocheck2.org/"},
    "threatEntryMetadata": {
      "entries": [{
        "key":   "malware_threat_type",
        "value": "landing"
      }]
    },
    "cacheDuration": "300.000s"
  }]
}
```

Limit of 10k Queries/day

Submit Data
Safe Browsing Submission API

Single Incident Reports: https://safebrowsing.google.com/safebrowsing/report_phish/

Programmatic Access for Submitters with more than 1k URLs/month

```
threat_report: {
    threat_entry_type: "URL",
    threat_entry: {url: "http://testsafebrowsing.appspot.com/s/phishing.html"}
},
client_info: {
    client_id: “initialTest”,
    client_version: “1”
}
```

Summary

Safe Browsing Protects Devices and Infrastructures from Phishing, Malware, and UwS

A combination of multiple approaches is the only way to succeed

ML helps us cover our defense-in-depth strategy.

You can let us know about phishing via the Submission API and you can access our verdicts via the Lookup/Update APIs