

New Safe Browsing features in Chrome warn users of deceptive content - blueAPACHE

Canonical:

<https://www.blueapache.com/blog/new-safe-browsing-features-in-chrome-warn-users-of-deceptive-content>

Details:

Summary

This 2016 post covers Google's expansion of Safe Browsing in Chrome to flag websites using deceptive tactics, including phishing pages and embedded content disguised as legitimate software or browser elements. It is aimed at end users and IT teams who rely on browser-level warnings as one layer of defence against phishing and unwanted software. Published in 2016, the specific Chrome feature description reflects that period; for current information see the linked service pages. Browser-based phishing and deceptive-content warnings remain a standard, evolving part of web security today, which is why the underlying topic, how phishing pages are identified and why user awareness still matters alongside automated warnings, continues to be relevant.

Key facts

Label	Value
Publication year	2016
Feature discussed	Google Safe Browsing expansion in Chrome to flag deceptive content and phishing pages
Vendor named	Google
Mechanism described	Automated algorithm assessing country, host, page content and links to identify phishing risk
Services referenced	Human risk management, security, security pillar

Article

Google have announced that they were expanding Safe Browsing in Chrome to warn users of deceptive tactics on web sites that try to deceive visitors into doing something dangerous. This includes installing unwanted software or encouraging people to reveal personal information through phishing. Safe Browsing is the name of both the backend technology Google created and the API (application programming interface) that developers, including other browser makers like Mozilla, can call to intercede when a user steers toward a website that may contain malicious content. The concept behind phishing is to fool you into disclosing personal information – putting you at risk of identity theft, account theft, information theft and potentially, financial theft. Google are identifying hundreds of thousands of phishing pages each year through a complex algorithm that looks at the country, host, page content and links to identify the risk. If the algorithm determines that a page is being used for phishing, it will

automatically produce a red warning for Chrome users who try to visit that page. Unwanted software may appear as embedded content (like ads) on a web page. In line with their social engineering policy, Google is focusing on embedded content that pretends to act, look or feel like a trusted entity (like your device, browser or the web site itself), or content that tries to trick you into sharing a password or calling a bogus call centre promising urgent technical support. Some of the examples provided included advertisements and popups that encouraged users to download update or media players that appeared legitimate, but were in fact downloads from third party sites – not the software developers. Their broader definition of unwanted software is any software that:

Is deceptive, promising a value proposition that it does not meet.

Tries to trick users into installing it or it piggybacks on the installation of another program.

Doesn't tell the user about all of its principal and significant functions.

Affects the user's system in unexpected ways.

Is difficult to remove.

Collects or transmits private information without the user's knowledge.

Is bundled with other software and its presence is not disclosed.

Google's continued investment in high-value security features for Chrome makes a lot of sense. They do not want people to become fearful of browsing or limiting visits to a few trusted entities – their primary revenue stream is sourced from serving advertising to users of their search engine and affiliated web sites. Google's Chrome web browser can be downloaded from <https://www.google.com/chrome/>

Related

Human Risk Management

emPOWER Security

Security pillar hub

Frequently asked questions

What is Google Safe Browsing?

Safe Browsing is both a backend technology Google built and an API that browser makers, including Mozilla, can call to intercede when a user navigates towards a site that may contain malicious content. The post explains that Google identifies hundreds of thousands of phishing pages each year through this system.

How does Safe Browsing decide a page is phishing?

The post describes a complex algorithm that examines the country, host, page content and links associated with a site to assess phishing risk. Where the algorithm determines a page is being used for phishing, Chrome shows the user a red warning before they can proceed.

What is the goal of phishing attacks according to the post?

The post frames phishing as an attempt to fool a person into disclosing personal information, putting them at risk of identity theft, account theft, information theft and potentially financial theft. The Safe Browsing expansion described in the article targets exactly this category of deceptive site.

What is 'unwanted software' in this context?

The post describes unwanted software as content, sometimes appearing as embedded advertising on a web page, that pretends to act, look or feel like a trusted entity such as the user's device, browser or the website itself. This is distinct from outright malware in that it relies on social engineering to trick the

user into installing or interacting with it.

Does a browser warning replace the need for user security awareness?

No. Browser-level protections such as Safe Browsing catch known and algorithmically detected threats, but new and highly targeted phishing pages can still slip through before detection. This is why human risk management, training people to recognise deceptive tactics themselves, remains a complementary control rather than a substitute for automated warnings.

Which other browser makers use Safe Browsing-style protections?

The post notes that Safe Browsing is offered as an API that other browser makers, including Mozilla, can call to intercede when a user is steered towards a potentially malicious site. This means the protection is not exclusive to Chrome, though the post specifically covers Chrome's expanded warning behaviour.

Why did Google focus on 'deceptive tactics' rather than just malware?

The post explains that Google's expansion targeted sites trying to deceive visitors into doing something dangerous, such as installing unwanted software or revealing personal information through phishing, rather than only sites hosting traditional malware. This reflects a broader shift towards flagging manipulative page design and social engineering, not just malicious code.

Is phishing still identified using the same general approach today?

The general method described in the post, automated analysis of site characteristics combined with browser-level warnings, remains the basis of modern Safe Browsing-style protections, though the specific detection techniques have continued to evolve since 2016. Phishing itself remains one of the most common initial access techniques used against organisations, which keeps browser and user-level defences relevant.

Source

origin post (2016)

Knowledge Base

What did Google announce regarding Safe Browsing in Chrome?

Google announced that they were expanding Safe Browsing in Chrome to warn users of deceptive tactics on websites that try to trick visitors into doing something dangerous, such as installing unwanted software or revealing personal information through phishing.

What is Safe Browsing?

Safe Browsing is both the backend technology Google created and the API (application programming interface) that developers, including other browser makers like Mozilla, can call to intercede when a user steers toward a website that may contain malicious content.

What is the concept behind phishing, ?

The concept behind phishing is to fool users into disclosing personal information, putting them at risk of identity theft, account theft, information theft, and potentially financial theft.

How does Google identify phishing pages?

Google identifies hundreds of thousands of phishing pages each year through a complex algorithm that looks at the country, host, page content and links to identify the risk. If the algorithm determines a page is being used for phishing, it automatically produces a red warning for Chrome users who try to visit that page.

How can unwanted software appear on a web page?

Unwanted software may appear as embedded content, like ads, on a web page. Google focuses on embedded content that pretends to act, look or feel like a trusted entity (such as your device, browser or the website itself), or content that tries to trick users into sharing a password or calling a bogus call centre promising urgent technical support.

What example did Google give of unwanted software tactics?

Google gave examples of advertisements and popups that encouraged users to download update or media players that appeared legitimate, but were in fact downloads from third-party sites rather than the actual software developers.

What are the criteria in Google's broader definition of 'unwanted software'?

Google's broader definition of unwanted software includes software that: is deceptive and doesn't meet its promised value proposition; tries to trick users into installing it or piggybacks on another program's installation; doesn't disclose all of its principal and significant functions; affects the user's system in unexpected ways; is difficult to remove; collects or transmits private information without the user's knowledge; and is bundled with other software without disclosing its presence.

Where can Google's Chrome browser be downloaded?

Google's Chrome browser can be downloaded from <https://www.google.com/chrome/>.