A Safer Internet for All: Spreading Awareness on “Malvertising” Threats

By: Jae Kim, Kevin Ortez

Cal State LA

Introduction

In today's digital world, a simple click on a Google ad can lead to unexpected dangers. **"Malvertising"** – the use of online ads to spread malware – has become a significant threat to internet users worldwide.

Cybercriminals exploit Google's ad system by:
- Impersonating legitimate brands
- Manipulating Google's Click ID system
- Placing deceptive ads that appear trustworthy

These tactics often lead users to:
- Phishing websites
- Malware downloads
- Compromised personal information Despite Google's efforts, malvertising continues to grow in scale and sophistication.

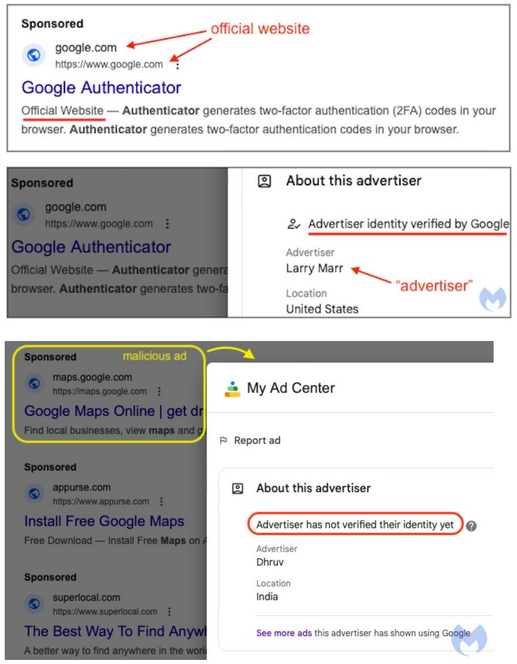
Our research explores:

1. Methods used by cybercriminals
2. The impact on users and businesses
3. Potential approaches to enhance online security

By understanding these threats, we aim to empower Google Searchers and propose more robust protective measures for a safer internet experience..

Objectives

- Explore methods used by cybercriminals to exploit Google's ad system
- Analyze the scale and impact of “malvertising” campaigns
- Propose potential approaches to mitigate these threats



Methods

“Malvertising” campaigns exploit vulnerabilities in Google's advertising system to bypass security measures and target users with malicious content. Scammers employ sophisticated techniques to evade detection, manipulate ad platforms, and differentiate between real users and security bots. Understanding these tactics is crucial for developing effective countermeasures. Our research methodology aims to dissect these malicious strategies:

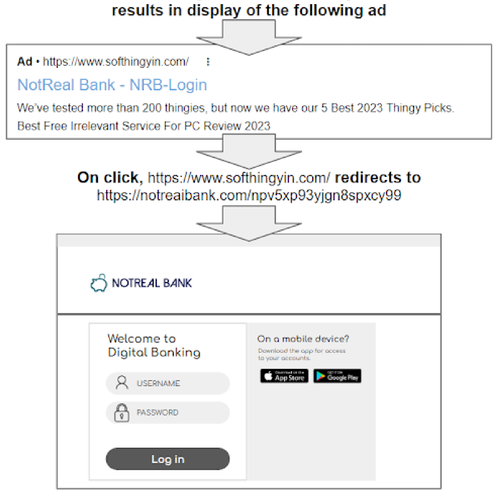
1. Data Collection:
   - Analyze Google's Click ID verification system
   - Study scammer tactics for bypassing ad review process

2. Threat Analysis:
   - Examine use of 302 redirect links
   - Investigate manipulation of Google's 'page.link' domain

3. User Impact Assessment:
   - Evaluate phishing website techniques
   - Identify types of sensitive information targeted

4. Advanced Evasion Techniques:
   - Analyze click-tracking services used by scammers
   - Study methods for differentiating between bots and real users

5. Redirect Behavior Mapping:
   - Track how Google Click IDs are dynamically redirected
   - Compare bot vs. real user experiences

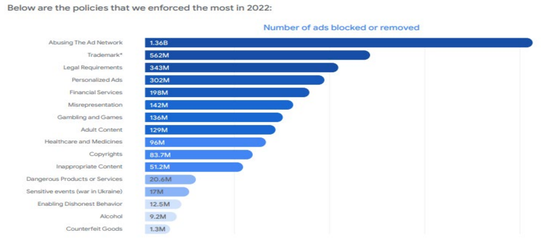


Results

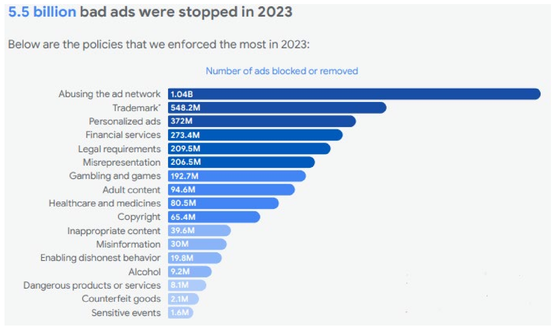
Google's efforts to combat “malvertising” have shown both progress and ongoing challenges:

Google's 2022 Ad Safety Report:
- 5.2 billion ads removed
- 4.3 billion ads restricted
- 6.7 million advertiser accounts suspended
- 1.36 billion ads blocked for abuse
- 143 thousand publishers’ advertisements blocked

These figures highlight the massive scale of Google's efforts to maintain ad safety. The removal of 5.2 billion ads represents a significant increase from previous years, indicating either improved detection methods or a rise in malicious advertising attempts.



Google’s 2023 Ad Safety Report:
- 5.5 billion ads removed
- 6.9 billion ads restricted
- 12.7 million advertiser accounts suspended
- 395 thousand publishers’ advertisements blocked



Sentinel One 2023 study:
- Rise in malware infections from ads spoofing legitimate software
- Spread of infostealer trojans (IcedID, Redline Stealer)
- Malicious ads appearing in sponsored content at top of search results

Despite Google's efforts, the Sentinel One study reveals that sophisticated “malvertising” campaigns continue to evolve and exploit vulnerabilities. The appearance of malicious ads in top sponsored content is particularly concerning, as these positions are often viewed as more trustworthy by users.

Conclusion

Scams are becoming increasingly sophisticated, posing significant challenges to both users and security systems. The data highlights that despite Google's efforts to combat malvertising, harmful ads continue to infiltrate the platform, putting users at risk of malware infections and phishing attacks. It is evident that Google's current security measures are insufficient to fully protect users from these evolving threats. Therefore, it is crucial for users to adopt precautionary measures, such as verifying the legitimacy of advertisers and using browser extensions like Malwarebytes Browser Guard or URL scanners to validate the authenticity of websites before engaging with them. Moreover, as the landscape of online threats continues to evolve, Google must adapt its security protocols to address these emerging attack vectors effectively. Developing a program that continuously validates URLs before redirects occur could offer real-time protection that goes beyond the capabilities of current web-crawling bots, ultimately ensuring a more robust defense against fraudulent schemes.

Suggestions

- Avoid clicking on Sponsored Ads on Google. Instead, type in the expected URL
- Check Advertiser Verification status / location
- Implement trusted browser extensions such as 'Malwarebytes Browser Guard' or 'Malware & URL Scanner' to verify website authenticity, block suspicious redirects, and protect against malicious practices
- Browse responsibly!

References

“TRENDING: Google Ads as Phishing Hooks -Understanding the Threat and Protecting Your Brand - Allure security.” *Allure security - Online Brand Protection*, 20 Apr. 2023, allure security.com/trending-google-ads-as-phishing-hooks-understanding-the-threat-and-protecting-your-brand/.

SlowMist. “Unraveling the Sophisticated Phishing Scheme behind Fake Google Ads.” *Medium*, Medium, 5 Mar. 2024, slowmist.medium.com/unraveling-the-sophisticated-phishing-scheme-behind-fake-google-ads-259893841d21.

Naprys, Ernestas. “Scammers Bypassing Google Ad Checks to Impersonate Real Brands.” *Cybernews*, cybernews.com/security/scammers-bypassing-google-impersonate-brands/.

Using Google Search to Find Software Can Be Risky – Krebs on Security. 25 Jan. 2024, krebsonsecurity.com/2024/01/using-google-search-to-find-software-can-be-risky/.

Google. *2022 Google Ad Safety Report*. https://services.google.com/fh/files/misc/2022_google_ads_safety_report.pdf

Google. *2023 Google Ad Safety Report*. https://services.google.com/fh/files/misc/ads_safety_report_2023.pdf

Acknowledgements

We thank Cal State LA for promoting and supporting this research.

We would also like to thank the Computer Science and Cybersecurity Professors and Staff here on Campus that gave us the baseline tools and knowledge to garner our curiosity in the subject.