SUDLOW MARKETING

BOOTHS HALL, BOOTHS PARK, CHELFORD ROAD, KNUTSFORD, WA16 8GS
WWW.CARRIEANNSUDLOW.CO.UK

Guardian Doors Website Security & Technical Audit Findings – Impact on Google Ads Eligibility

This report outlines critical security and technical issues identified on your website. These findings are directly preventing your Google Ads account from being unsuspended and your advertising campaigns from running. Google maintains extremely strict policies regarding user safety and website security, and the current state of your site is in direct violation of these policies.

We strongly urge you to address these issues with immediate priority, as they pose not only a barrier to advertising but also significant risks to your website's users and overall brand reputation.

Executive Summary of Key Concerns

The primary and most severe findings are:

1. **Active Malware & Malicious Software Detections:** Two reputable cybersecurity firms (CyRadar and Fortinet) have flagged your site for containing malicious software. This is an immediate and critical red flag for Google Ads and is the most common reason for account suspension due to "Unacceptable Business Practices" or "Malicious Content."
2. **Significant HTTPS/HTTP Configuration Errors:** There are widespread issues with your website's security protocol (HTTPS) implementation. Crucially, 75 of your secure (HTTPS) pages are incorrectly telling search engines to index their insecure (HTTP) counterparts, and 74 pages are loaded over HTTP (unencrypted connections). Additionally, your homepage is not forcing users to the secure HTTPS version.
3. **Open TCP Ports & Discoverable Development Site:** The presence of multiple open TCP ports and a publicly accessible development environment (dev.guardiandoors.net) create serious security vulnerabilities.

These issues directly impact user trust, data security, and your site's credibility, which are non-negotiable requirements for advertising on Google Ads.

Detailed Findings and Impact on Google Ads

Below is a detailed explanation of the identified issues, their implications, and why they prevent your site from being approved for Google Ads.

A. Critical Security Threats (Immediate Google Ads Suspension Triggers)

- **Malware and Malicious Software Detected:**
    - **Finding:** CyRadar has flagged your site as Malicious, and Fortinet has identified Malware.
    - **Meaning:** This is the most severe issue. Your website appears to be hosting or distributing harmful software. This could be due to a compromised plugin, outdated software, or a direct attack.
    - **Impact on Google Ads:** Google has a zero-tolerance policy for websites containing malware or malicious software. This is a direct violation of their "Unacceptable Business Practices" and "Malicious Content" policies. Google's primary concern is protecting its users, and they will immediately suspend accounts linking to sites with these issues. Your account will remain suspended until these threats are entirely eradicated and verified.
- **Open TCP Ports (8 found - Medium Risk):**
    - **Finding:** Your server has 8 open TCP ports.
    - **Meaning:** Open ports can be entry points for attackers to gain unauthorised access to your server. While some ports need to be open for legitimate services (like web traffic on port 443/80), an excessive number or unnecessarily open ports indicate potential vulnerabilities.
    - **Impact on Google Ads:** While not a direct suspension trigger on its own, a site with known security vulnerabilities contributes to Google's assessment of it as an unsafe destination for users, reinforcing reasons for ad disapproval or account suspension.
- **Discoverable Development Site (dev.guardiandoors.net - Medium Risk):**
    - **Finding:** Your development environment (dev.guardiandoors.net) is publicly accessible.
    - **Meaning:** Development sites often contain outdated software, default credentials, or incomplete security measures. If an attacker gains access to your dev site, they could compromise sensitive data, upload malware, or use it as a springboard to attack your live site.
    - **Impact on Google Ads:** A publicly exposed and potentially insecure development environment signals a lack of robust security practices, which again, contributes to Google's view of your main site as a high-risk destination.

B. Major Technical & SEO Security Issues (Directly Impacting Google Ads & User Trust)

- **75 HTTPS pages have rel=canonical attributes pointing to HTTP pages.**
    - **Meaning:** You have secure (HTTPS) pages that are incorrectly telling search engines that their insecure (HTTP) versions are the preferred versions for indexing. This creates a contradictory signal for Google.
    - **Impact on Google Ads:** Google Ads requires landing pages to be secure (HTTPS) to ensure user safety. By canonicalizing HTTP, you are confusing search engines and potentially encouraging them to index the insecure versions of your pages. If Google's ad crawlers find the HTTP version indexed and advertised, or if the canonical tag overrides the HTTPS preference, your ads will be disapproved as the landing page will be deemed insecure.
    - **Solution:** All rel=canonical tags on HTTPS pages must point to the **HTTPS version** of that same page. For example, https://example.com/page should have a canonical tag referencing https://example.com/page, not http://example.com/page. This correction typically needs to be done within your website's CMS settings, theme, or plugin configurations.
- **74 pages are loaded over an insecure HTTP connection.**
    - **Meaning:** A significant number of your website pages are being served without encryption. This means any data transmitted between a user's browser and these pages (e.g., login details, form submissions) is sent in plain text and can be intercepted. Modern browsers will also display a "Not Secure" warning to users.
    - **Impact on Google Ads:** Google Ads strictly prohibits advertising for pages that are not secure. If your landing pages (or any pages linked from ads) load over HTTP, they will be flagged as insecure, leading to ad disapprovals. Users seeing "Not Secure" warnings are also highly unlikely to convert, leading to wasted ad spend.
    - **Solution:** Ensure all pages on your website are properly served over HTTPS. This often involves correctly configuring SSL/TLS certificates and ensuring all internal resources (images, scripts, CSS) are also loaded via HTTPS to avoid mixed content warnings.
- **53 HTTPS pages are linking to HTTP pages on your website.**
    - **Meaning:** Even if a user starts on a secure (HTTPS) page, if they click an internal link that points to an insecure (HTTP) page on your own domain, their browser connection becomes insecure. This creates a jarring experience and can trigger "Mixed Content" warnings in some browsers.
    - **Impact on Google Ads:** This issue directly undermines user trust and creates a poor, inconsistent user experience. Google Ads requires a seamless and secure user journey from click to conversion. Inconsistent security signals can lead to ad disapprovals, as Google wants to ensure users remain in a secure environment after clicking an ad.
    - **Solution:** All internal links on your website should use HTTPS URLs (e.g., https://example.com/page) or, ideally, relative URLs (e.g., /page). This requires auditing your content, menus, and internal linking structure to update all insecure references.

- **The home page has no server-side 301 redirect from HTTP to HTTPS.**
  - **Meaning:** If a user types http://yourwebsite.com or clicks an old link using HTTP, they will land on the insecure HTTP version of your homepage instead of being automatically redirected to the secure HTTPS version.
  - **Impact on Google Ads:** This is a fundamental security and SEO flaw. It creates duplicate content issues for search engines (both HTTP and HTTPS versions of your homepage exist) and exposes users to an insecure connection upon first arrival. Google Ads demands that all traffic be routed to a secure destination, and the absence of this redirect is a clear violation.
  - **Solution:** Implement a permanent (301) server-side redirect from HTTP to HTTPS for your entire domain, ensuring that any request to http://yourwebsite.com is automatically redirected to https://www.yourwebsite.com. This is typically configured in your web server's settings (e.g., .htaccess for Apache or Nginx configuration).

C. Other Important Security & Technical Issues (Affecting Site Health & Trust)

- **Multiple Cookie Issues (Low Risk):**
  - **Meaning:** While specified as low risk, multiple cookie issues can relate to how cookies are handled (e.g., missing Secure flags, HttpOnly flags, or SameSite attributes). This could potentially expose session cookies to client-side scripts or cross-site requests.
  - **Impact on Google Ads:** While not a direct suspension cause, poor cookie security can contribute to an overall impression of an insecure site, impacting user privacy and potentially leading to future vulnerabilities.
- **Invalid robots.txt file:**
  - **Meaning:** The robots.txt file guides search engine crawlers on which parts of your site they can or cannot access. An invalid file can either prevent important pages from being indexed (harming SEO) or allow sensitive pages to be indexed that you intended to block (security/privacy risk).
  - **Impact on Google Ads:** An invalid robots.txt can hinder Google's ability to properly crawl and understand your site's content and structure, which is essential for ad quality and targeting.
- **Content-Security-Policy (CSP) header is missing.**
  - **Meaning:** Your website lacks a Content Security Policy header. CSP is a crucial security layer that helps prevent various attacks like Cross-Site Scripting (XSS) and data injection by specifying which dynamic resources (scripts, images, styles) are allowed to load.
  - **Impact on Google Ads:** The absence of a CSP makes your website more vulnerable to common web attacks, directly impacting its overall security posture and Google's assessment of its safety for users.
- **2 Pages with Canonical Command Chains.**
  - **Meaning:** You have pages (e.g., Page A) that canonicalize to another page (Page B), which then itself canonicalizes to a third page (Page C). This creates a "chain" (A → B → C) of canonical instructions.

- **Impact on Google Ads:** While less critical for suspension than malware or HTTPS issues, these chains can confuse search engines, waste crawl budget, and potentially dilute SEO value. Google prefers direct canonical signals for optimal performance.
- **Solution:** All canonical tags should point directly to the ultimate canonical version of the page (e.g., A → C and B → C).

Conclusion and Next Steps

The overarching theme of these findings is a significant lack of robust security measures and correct technical configuration on your website. Google Ads prioritises user safety above all else, and any indication of malware, insecure connections, or confusing signals regarding site security will result in account suspension and ad disapproval.

To reinstate your Google Ads account and begin advertising, you **must** address all of the critical and major issues outlined above. We recommend the following immediate actions:

1. **Eliminate Malware:** This is paramount. Engage a professional cybersecurity firm or your hosting provider immediately to scan, identify, and thoroughly remove all malicious software from your website.
2. **Implement Server-Side 301 Redirects:** Ensure all HTTP versions of your pages (especially the homepage) are permanently redirected to their HTTPS counterparts. This is a server-level configuration.
3. **Correct Canonical Tags:** Review all 75 HTTPS pages that are canonicalizing to HTTP and update their canonical tags to point to the correct HTTPS URLs.
4. **Update All Internal Links:** Audit your website content, navigation, and internal links to ensure all internal references are to HTTPS URLs.
5. **Secure Development Environment:** Remove public access to dev.guardiandoors.net or implement strong access controls (e.g., IP whitelisting, password protection).
6. **Review Open Ports:** Consult with your hosting provider or a network administrator to identify and close any unnecessary open TCP ports.
7. **Implement Content Security Policy (CSP):** Add a robust Content-Security-Policy header to enhance your site's defence against XSS and data injection attacks.
8. **Address Cookie Issues:** Review and correct any identified cookie vulnerabilities to enhance user privacy and security.
9. **Validate robots.txt:** Ensure your robots.txt file is correctly formatted and is not inadvertently blocking important pages or allowing unintended indexing.
10. **Fix Canonical Chains:** Update canonical tags on any pages involved in chains to point directly to the final canonical URL.

Once these fundamental issues are resolved, we can assist with a re-evaluation of your site's security and prepare the necessary appeals to Google Ads for account reinstatement. Please understand that until these critical security deficiencies are rectified, no advertising can proceed.