

Is anmedplus.by a scam? TrustSniffer's high-risk assessment: 0/100

anmedplus.by

Verdict

0

OUT OF 100

CRITICAL RISK

anmedplus.by shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Assessed 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

Russian-language site for IOOO "АНМЕДПЛЮС", a wholesale distributor of medical and orthopedic products since 2008. Contains product categories, item listings, contact information (address in Minsk, phones, email) and notes that the site is not an online store.

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

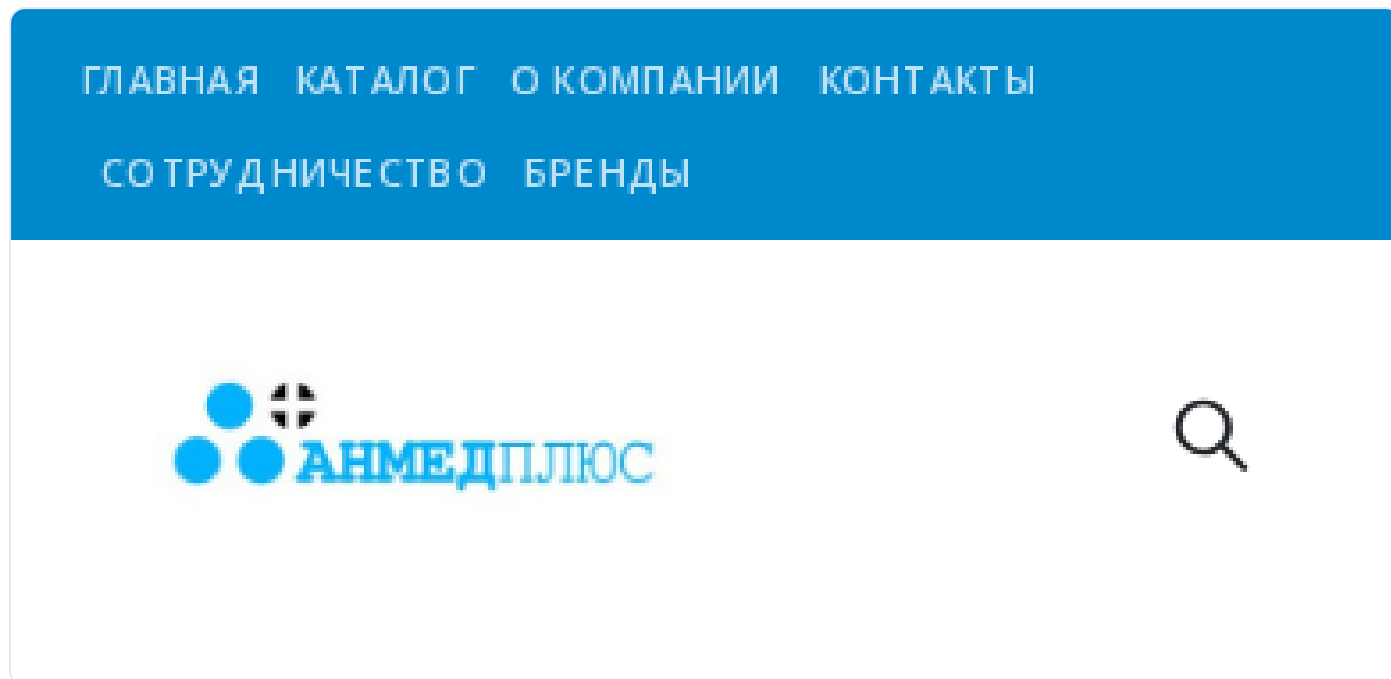
At a glance

The checks that decide most of this verdict.

Malware engines	4 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	17 years old Registered history	CLEAR
Web archive	Archived since 2010 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

https://anmedplus.by/



What anmedplus.by served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2010.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Fortinet flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website is a Russian-language corporate catalog for ИООО «АНМЕДПЛЮС», presenting itself as a wholesale distributor of medical equipment, orthopedic products, rehabilitation goods, and related supplies. Its apparent business model is catalogue-led wholesale distribution, with visitors directed toward company contact channels rather than an online checkout.

Scam/Impersonation Risk

The principal concern is a **confirmed blacklist status**, supported by four malicious and three suspicious external detections, including a Tier-1 security-vendor flag. This is a direct contradiction to treating the site as suitable for sensitive interaction, even though the visible pages present a coherent medical-products catalogue and the page analysis found no brand impersonation or conflicting legal-entity names. Browser testing also recorded one hidden form and substantial DOM changes after interaction; these observations do not independently prove malicious intent, but they reinforce the need to keep credentials and financial activity away from the site. The available evidence therefore supports a clearly cautionary assessment for sensitive actions.

EVIDENCE

- External reputation telemetry recorded 4 malicious and 3 suspicious detections from 12 evaluated results, with the domain listed by 2 blacklist sources.
- The homepage sandbox recorded 1 hidden form and a maximum post-interaction DOM difference of 1940.
- The domain registration record shows creation on 2009-07-02 and an age of 17.15 years, with expiry on 2027-07-15.
- Archive records show first observation on 2010-07-04 and last observation on 2025-03-18, covering 16 years of tracked history with sparse archival coverage.

Regulatory Verification Notes

The About and homepage content identifies ИООО «АНМЕДПЛЮС» as a wholesale distributor of medical and orthopedic products and states that the business has operated since 2008. That apparent commercial identity is consistent across the supplied site content, but independent identity verification remains incomplete. The pages do not present a licensing authority or license number; for a distributor of medical equipment and registered products, this is a material disclosure point requiring external confirmation rather than an automatic conclusion of fraud. No matching third-party broker record was identified. The valid transport certificate and identified hosting environment are technical attributes only and do not establish licensing or legal standing.

EVIDENCE

- The homepage and company-information content name ИООО «АНМЕДПЛЮС» and describe wholesale distribution of medical equipment, orthopedic products, and rehabilitation goods.
- The registration record lists Active Technologies LLC as registrar and ИООО «Анмедплюс» as the registrant organization.
- The site is hosted on AS6697, BELPAK-AS - Republican Unitary Telecommunication Enterprise Beltelecom, BY.
- TLS uses issuer YR2 with DV validation and is valid to 2026-10-17T23:46:08+00:00.

What to Verify Next

Before any commercial or sensitive engagement, an independent party should validate the named legal entity and its Minsk contact details through an authoritative corporate registry or an offline business channel. Any authorization required for wholesale distribution of medical devices or registered products should be confirmed directly with the relevant Belarusian authority. Sensitive browser interaction should remain disabled until those checks are complete, and any subsequent payment process should use independently verified invoicing and payment-protection controls.

EVIDENCE

- The company identity and business description are presented on the homepage and company-information pages.
- The site describes a product catalogue containing medical, orthopedic, rehabilitation, and registered products.
- The contact page provides the business address and telephone channels that can be independently cross-checked.
- The site has no online checkout or sensitive form identified in the supplied page analysis.

Summary Verdict

The overall posture is **critical trust risk**. The site presents a plausible wholesale-distributor profile, but that apparent legitimacy is outweighed by confirmed blacklist and malicious-detection signals, together with unresolved identity verification. The available evidence does not support login, credential submission, or financial activity through the site.

Infrastructure Integrity

The site resolves directly to a single IP address, with no CDN or WAF detected and one likely origin address exposed. This configuration provides no identifiable edge-layer mitigation; infrastructure characteristics alone, however, do not establish whether the operator is legitimate.

Closing Assessment

Interaction should be limited to non-sensitive, read-only research unless independent corporate, authorization, and transaction checks materially resolve the outstanding concerns.

Written analysis generated 2026-08-21 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by analysis engine, behaviour in a sandbox, external reputation.

01 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- The page contained a form a visitor cannot see.
Behaviour in a sandbox rule:BEHAV_HIDDEN_FORMS
- The page rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.
Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	50%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of anmedplus.by.

- The request stayed on anmedplus.by. It was not redirected to another domain. CLEAR
- Registration is published under Active Technologies LLC. CLEAR
- DNS for this domain is served by activeby.net, across 3 name servers. NOTED
- The registration is paid up to 2027-07-15. NOTED
- The earliest public archive of this site is from 2010-07-04. CLEAR
- It is hosted on BELPAK-AS, from a server in BY. NOTED

Domain intelligence

Registrar	Active Technologies LLC
Hosting	BELPAK-AS - Republican Unitary Telecommunication Enterprise Beltelecom, BY
Country	BY
Server IP	178.159.242.204
Name servers	ns1.activeby.net, ns2.activeby.net, ns3.activeby.net
SSL issuer	YR2
SSL expiry	2026-10-17
Domain age	17.15 years (continuous registration)
Domain expiry	2027-07-15
Archive first seen	2010-07-04
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 4 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about anmedplus.by at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a

legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/anmedplus.by> · assessed 2026-08-21