The Giving AI.

SAMPLE / EXAMPLE

What Your Free Comprehensive Audit Looks Like, and How to Read It

This is a representative example of the report every nonprofit receives when they request the free audit. The organization below is illustrative, your report contains your real, live results, scanned the day we run it.

Why we do this, our philosophy

Mission-driven organizations run on one thing above all: **trust**. Trust between staff, volunteers, donors, and the people you serve. Two quiet forces erode that trust, and most leaders never see either one coming:

1. **You are invisible to the people who need you.** Donors, families, and reporters increasingly find help by asking an AI assistant (ChatGPT, Google's AI answers, Perplexity, Gemini) or by searching. If those systems cannot read and cite your site, you are not in the conversation, no matter how good your work is.
2. **You can be impersonated.** If your domain is not locked down, anyone can send email that looks exactly like it came from you. Bad actors exploit the trust between your people, and AI now makes that faster and cheaper. Most breaches start with an honest person trying to help.

So we check both. We believe the audit should be a **gift, not a sales pitch**, and that we earn a relationship by being useful first. That is also why every audit comes with a **free quarterly re-audit** for as long as you want it: threats change and AI platforms change, so we keep checking and you stay current at no charge.

How to read your report

Your report has **two pillars** and a **plan**:

- **Pillar 1, Authority & AI-search positioning.** Can donors, families, and AI assistants find and cite you? Scored 0-100.
- **Pillar 2, Security & deliverability.** Can someone impersonate you, and does your real mail reach the inbox? Scored by severity.
- **A prioritized action plan** written in plain language, with the exact technical records your web person needs (copy-and-paste ready) and an honest estimate of effort.

You do not need to be technical to use it. Read the executive summary and the plan; hand the technical pages to whoever manages your website and domain.

Pillar 1 — Authority & AI-search positioning (donor reach, awareness, mission)

This is what determines whether the people who would support your mission can actually find it. Here is the full set of checks we run:

CHECK	WHAT IT ANSWERS
AI-crawler accessibility	Can the AI assistants (GPTBot, ClaudeBot, PerplexityBot, Google-Extended and others) reach your pages at all?
Content extractability	Do crawlers and AI see your actual content, or a blank JavaScript shell?
Structured data (schema)	Is your site marked up as an Organization / NGO with your services and a `sameAs` trust web (GuideStar, Facebook, etc.)?
Title & description	Does each page have a clear, machine-readable headline and summary?
Heading (H1) hierarchy	Is the strongest on-page topic signal present and meaningful?
Sitemap / robots / llms.txt	Are crawlers given a clean map and an AI-discovery file?
Brand-mention floor	Do independent sources (news, directories, partners) cite you, so AI can verify who you are?
Entity disambiguation	Is your name unambiguous, or confused with similar organizations?
AI-search citation testing	We actually ask the major AI engines your mission questions and record whether you are cited.
Freshness & local readiness	Is content current, and can local searches ("near me") match you?

Example finding (illustrative): Composite authority score **18 / 100**. The site is a JavaScript app, so search engines and AI assistants receive a near-empty page. No Organization schema, no H1, no sitemap. Result: when a donor asks an AI assistant "youth nonprofits near me," this organization cannot be surfaced or cited, not because of competition, but because there is nothing machine-readable to cite. **The fix is a few days of work and moves them from invisible to citable.**

Pillar 2 — Security & deliverability (protecting the trust you run on)

This is where impersonation lives. Here is the specific danger, the kind of message that is possible the moment a domain is unprotected:

⚠ EXAMPLE — WHAT A SPOOFED EMAIL FROM YOUR OWN DOMAIN LOOKS LIKE

From: Executive Director <director@**yournonprofit.org**>
To: Bookkeeper
Subj: Quick wire before the board call

Hi, I'm in the board meeting and can't talk. Please wire $18,500 to the vendor below today so we don't lose the grant match. I'll explain after. Thanks for jumping on this.

The address is real. Nothing flags it, because the domain was never locked down. The money is gone before anyone confirms. The same weakness also pushes your legitimate appeals and receipts into donors' spam, so it costs you twice.

The full set of security checks we run:

CHECK	WHAT IT ANSWERS
SPF	Is there a record listing who is authorized to send as you?
DKIM	Is your outbound mail cryptographically signed, and is the key current and strong (2048-bit)?
DMARC	Are receivers told to reject mail that fails authentication (the anti-spoofing lock)?
MX / mail routing	Where does your mail flow, and is the path consistent and safe?
Spoofability assessment	Can a stranger impersonate your domain today? (The example above.)
Deliverability signals	Are your real emails likely to land in the inbox or in spam?
HTTPS / SSL & DNS hygiene	Is the site secure, and is the DNS free of stale, exploitable entries?

Example finding (illustrative): SPF missing · DKIM missing · DMARC missing. The most exposed possible state, anyone can send as this domain. Remediation is three DNS records per domain, about 30 minutes, copy-and-paste ready in the report. We always include a safety check so the lockdown never blocks your real mail.

Your prioritized action plan (sample)

Every report ends with a plain-language, ordered plan. A typical one looks like:

1. **Week 1 (web person, ~half a day):** make the homepage server-readable; add the three email-protection records; redirect any dead secondary domain.
2. **Week 2-3:** add Organization/NGO schema and your trust links; write real staff bios; publish a sitemap and meta descriptions.
3. **Ongoing:** one short impact update per month; quarterly re-audit from us at no charge.

You are not alone in this, here is the field

Of the **74 Front Range nonprofits and mission-driven organizations we have audited in 2026**, **51% were fully exposed** with no email-spoofing protection at all, and **85% were not fully locked down**. Only **15% were fully protected**. Your report tells you exactly where you fall on that spectrum, and the plan tells you how to reach the protected minority. The point of sharing the benchmark is not to alarm you; it is to show that these gaps are normal, common, and entirely fixable.

The relationship, not the transaction

Every nonprofit that requests the audit gets a **free quarterly re-audit, for as long as you want it**. Threats change and AI platforms change, so we keep checking and you stay current. That is how we earn a relationship. The audit is the gift.

The Giving AI. Enterprise security, AI-authority positioning, and technology for mission-driven organizations. **www.thegiving.ai**
Methodology: real audits draw only on public sources, live DNS lookups, your published website and its delivered HTML, AI-crawler request testing, public email-authentication records, and direct AI-search testing. No private systems, no credentials, no surveillance. Everything is independently verifiable. The figures in this sample are illustrative; your report contains your live results.