

EVALUATING THE QUALITY OF UZBEKISTAN'S GOVERNMENT WEBSITES: A COMPARATIVE ANALYSIS OF ACCESSIBILITY, PERFORMANCE, AND SECURITY

Guzaloy Kenjayeva

Independent Researcher, Uzbekistan

Abstract:

Uzbekistan has spent the past decade building a large e-government infrastructure, yet no comprehensive public evaluation of how well these websites actually perform has existed until now. This study evaluates 15 official Uzbek government websites, covering national portals, ministries, agencies, and regional platforms, using WAVE for accessibility, Google Lighthouse for performance, and SecurityHeaders.com and Qualys SSL Labs for security. The evaluation is motivated in part by the January 2026 OneID data exposure, which raised practical questions about whether these sites meet modern web standards. The results show an uneven picture rather than a simple verdict of good or bad. SSL/TLS encryption was strong across nearly every site, but HTTP security headers were inconsistent, with OneID and two regional sites among the weakest. Accessibility was generally solid, yet the Government Portal — the site with the most citizen traffic — recorded the lowest accessibility score in the sample, while Regional Government sites scored best on accessibility but worst on performance, suggesting a possible trade-off. The scientific novelty of this study lies in providing the first comprehensive, multi-dimensional evaluation of Uzbekistan's e-government websites, filling a clear gap in the regional literature. Overall, the findings indicate that Uzbekistan's government websites are not failing uniformly, but succeeding and failing inconsistently in ways that a single test alone would miss.

Keywords: E-Government, Website Quality, Accessibility, Performance, Cybersecurity, WCAG, Uzbekistan

Introduction

Uzbekistan has spent the past decade building out its digital government infrastructure. Citizens can now file taxes, register a business, or access healthcare and education services without setting foot in an office. The logic is simple enough — e-government is cheaper to run, it connects agencies that used to operate in silos, and it gets services to people faster than standing in line ever did. As more Uzbeks turn to these platforms for things that used to require a trip downtown, how well they actually work stops being a minor detail [1].

Convenience only holds up if the site itself works. A citizen who can't navigate a page, waits too long for it to load, or has their data mishandled isn't getting what e-government promised. This isn't hypothetical. In January 2026, OneID — the system behind Uzbekistan's single sign-on and identity verification — reportedly suffered a data exposure. Initial reports put the number at 15 million citizens' records; Uzbekistan's Ministry of Digital Technologies later said the real figure was closer to 60,000, across three targeted systems. Even the smaller number is not nothing for a system meant to authenticate a country's citizens online [2].

Despite how far this infrastructure has grown, no comprehensive, publicly available evaluation of how well it actually performs exists. Other countries haven't been left unexamined this way — researchers have run comparable evaluations on government websites in the Gulf, across Europe, in East Africa, and in Uzbekistan's own regional neighborhood, Kyrgyzstan included. Uzbekistan is the gap in that literature.

This study fills it: 15 official Uzbek government websites, spanning national portals, ministries, agencies, and regional platforms, tested for accessibility, performance, and security against modern web standards. The question driving it is straightforward: **What are the most significant strengths and weaknesses of Uzbekistan's government websites in terms of accessibility, performance, and security, based on modern web quality standards?**

E-government website evaluation has been studied across many countries and methodologies. This body of work splits roughly into three groups: studies that test accessibility alone, studies that test security alone, and comprehensive assessments that combine both (plus performance or usability) in one evaluation [3].

Most accessibility-only studies rely on automated tools to check WCAG or regional-equivalent compliance. Kopackova, Michalek, and Cejna tested 39 Czech municipal websites in 2006 and again in 2008, tracking both WCAG compliance and “findability” through search engines. Accessibility actually got worse over that period — a counterintuitive result, given the usual assumption that awareness improves with time.

Kous, Kuhar, Pavlinek, Heričko, and Pušnik had better news: tracking 189 Slovenian municipality sites before and after the EU's EN 301 549 standard took effect, they found none were fully compliant in 2017, but roughly a third reached compliance the following year. Regulation, in this case, moved the needle.

Not every study found movement. Inal, Mishra, and Torkildsby tested 356 Norwegian municipality websites with WAVE and TAW and found not one met an acceptable WCAG standard — an average of 40 violated checkpoints per site, many at the most basic level. Fernández-Díaz, Jambrino-Maldonado, Iglesias-Sánchez, and de las Heras-Pedrosa reached a similar conclusion testing 18 Spanish provincial capitals, framing accessibility explicitly as a matter of democratic inclusion rather than a technical checkbox.

A separate line of research tests security specifically, often through penetration testing or protocol analysis rather than accessibility checkers. Zhao, Zhao, and Zhao assessed 51 U.S. state websites and found over 90% used SSL — but every single one left port 80 open and none hid its main IP address [4]. Encryption, in other words, was never the weak link.

Ali and Zamri Murah went further with a full penetration test of 16 Libyan government websites, turning up multiple sites still running Windows XP alongside unnecessary open ports, well-known attack vectors. Thompson, Mullins, and Chongsutakawewong tested a more pointed hypothesis directly — that more e-government adoption means better security — across 40 sites and 800 pages in Australia and Thailand. It didn't hold: only half of Australian sites used HTTPS at all, and vulnerability levels between the two countries barely differed.

Júnior, Carneiro, Paiva, and Pinto looked at HTTPS and DNSSEC across 308 Portuguese city councils. The encryption fundamentals looked solid on paper (97% RSA, 84% using 2048-bit keys), but over half still supported outdated TLS versions, and 95% had no DNSSEC at all. Good encryption choices and good encryption configuration, it turns out, are two different things [5].

The studies closest to this one test multiple dimensions at once, which matters because it's the only way to catch trade-offs between them. Abanumy, Al-Badi, and Mayhew is the earliest and narrowest — Saudi Arabia and Oman ministries, accessibility only — but it's foundational: zero sites met basic WCAG compliance, a baseline later studies kept running into. Ismailova is the closest analog to this paper geographically and administratively, testing 60 Kyrgyz government websites across usability, accessibility, and security in a post-Soviet Central Asian context much like Uzbekistan's [6].

Elisa tested 79 Tanzania e-government sites across the same three dimensions, and is the only study in

this review to test directly for SQL injection and cross-site scripting rather than stopping at configuration or headers. Csontos and Heckl used the same core toolkit as this paper — WAVE and Lighthouse — on 25 Hungarian government websites, and uniquely re-tested the same sites five years after a prior baseline, catching real change over time instead of a single snapshot.

Most recently, Islam Era, Ime, and Al Islam evaluated 212 Bangladeshi sites, government and non-government, under WCAG 2.2, pairing automated testing with a 103-person user survey [7]. Non-government sites outperformed government ones on usability and performance, but accessibility problems showed up on both sides — suggesting the government accessibility gap isn't a quirk of any one country's public sector, but something closer to systemic.

Three patterns hold across all thirteen studies: accessibility non-compliance is close to universal, encryption tends to be present but poorly configured, and the government-versus-non-government quality gap is smaller than people assume. None of these studies touched Uzbekistan. Given how fast its e-government infrastructure has grown, and what the OneID breach suggests is at stake, that's the gap this study fills [8].

Methodology

This study evaluates each website using four tools, one for each dimension examined and two covering complementary aspects of security: WAVE for accessibility, Google Lighthouse for performance, and SecurityHeaders.com and Qualys SSL Labs for security. All four are free, widely used in prior e-government evaluation research (see Literature Review), and require no specialized infrastructure to run.

This study uses a descriptive, comparative design to evaluate the accessibility, performance, and security of Uzbekistan's government web presence. The sample covers 15 official websites and digital public service platforms across four categories:

- National Portals (n=3: my.gov.uz, gov.uz, myid.uz/OneID)
- Ministries (n=5)
- Government Agencies (n=4)
- Regional Government websites (n=3)

This sample was chosen to span the full hierarchy of Uzbekistan's e-government infrastructure, from the platforms most citizens encounter directly to the ministries, agencies, and regional bodies behind them. Testing was limited to each site's homepage. Homepages are each site's primary entry point, and prior research has found that accessibility and performance issues at the homepage level tend to correlate with issues found deeper in a site.

Accessibility was tested using WAVE (Web Accessibility Evaluation Tool), developed by WebAIM at Utah State University's Institute for Disability Research, Policy & Practice, chosen for its wide use in prior e-government accessibility research and its support for current WCAG 2.2 criteria. WAVE reports an overall AIM accessibility score (0–10), a composite measure of page accessibility based on the number and severity of detected issues relative to the page's structural complexity, along with counts of general errors and contrast errors specifically. Each homepage was tested individually, with AIM score, error count, and contrast error count recorded for all 15 sites.

Performance was tested with Google Lighthouse, which produces an overall performance score (0–100) alongside three Core Web Vitals:

1. Largest Contentful Paint (LCP) — how long the largest visible element takes to render, a proxy for how quickly the main content becomes usable
2. Total Blocking Time (TBT) — how long the page stays unresponsive to clicks or taps while loading
3. Cumulative Layout Shift (CLS) — how much visible elements shift position unexpectedly during load, a measure of visual stability

Each homepage was tested individually and its performance score and Core Web Vitals were recorded.

Security was assessed using two complementary tools:

1. SecurityHeaders.com was used to check the presence and configuration of HTTP response security headers (Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, and others) and assigns a letter grade from F to A+ based on how many recommended headers are correctly implemented.
2. Qualys SSL Labs was used to check transport-layer security instead: certificate validity and the strength of supported TLS protocols and cipher suites, also graded F to A+.

All 15 websites were tested between August 6–8, 2026. This short window was chosen to minimize the chance that a site's content, configuration, or security posture changed between the first and last test, keeping results comparable across the sample. All tests were run once per site under consistent conditions (same device, browser, and default tool settings, with no VPN), and results were recorded manually into a structured dataset organized by website and category.

Automated testing tools have known blind spots. They can misidentify accessible elements as inaccessible or vice versa, and cannot evaluate certain qualities — such as whether alt text is genuinely descriptive — that require human judgment. WAVE and Lighthouse each test only one page at a time, which is why this study's testing was limited to homepages. One more caveat worth flagging: several ministry- and agency-level sites are hosted as subpages of the shared gov.uz domain, so part of their performance and security scores may reflect that shared infrastructure rather than anything specific to the page itself.

Results

AIM accessibility scores ranged from 3.3 to 9.1 across the 15 websites (M = 7.69, out of 10; see Figure 1). The Government Portal (gov.uz) pulled the average down on its own, scoring 3.3 — the lowest in the sample — largely because of 85 contrast errors, well beyond any other site tested, where contrast errors otherwise topped out at 10. Set that one site aside and the remaining 14 cluster much more tightly, between 6.8 and 9.1.

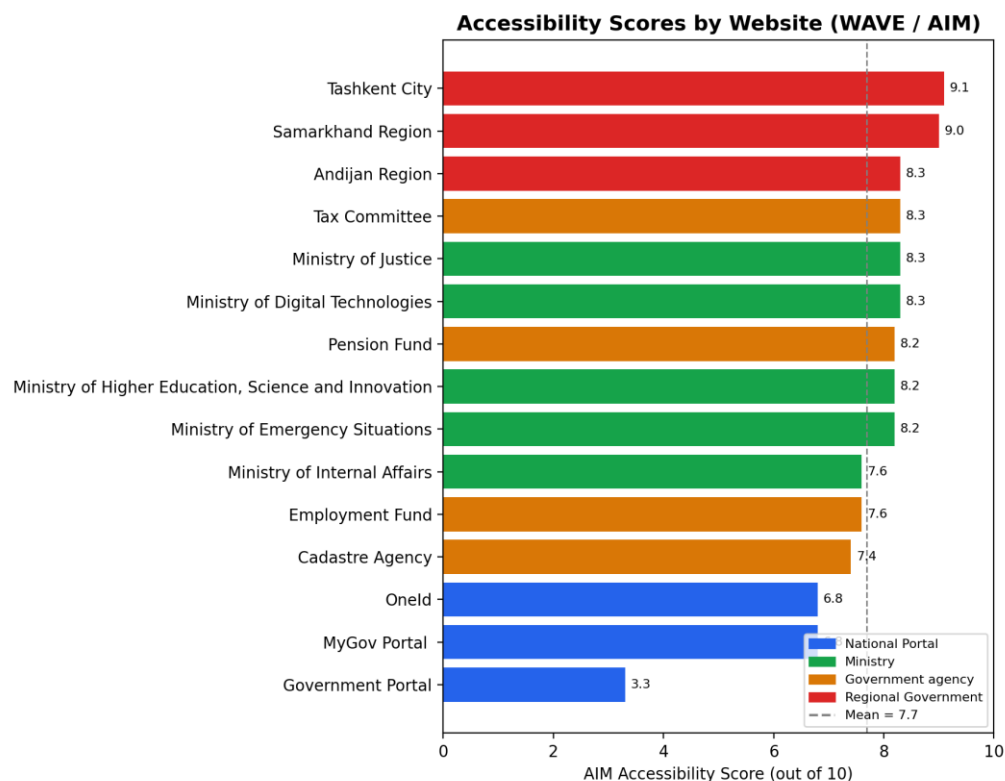


Figure 1. Accessibility scores by website (WAVE/AIM), colored by category.

Category averages (Table 2) put Regional Government websites on top ($M = 8.80$), followed by Ministries ($M = 8.12$) and Government Agencies ($M = 7.88$). National Portals came in lowest ($M = 5.63$) — but that number is almost entirely the Government Portal’s doing. The other two National Portals, MyGov Portal and OneID, each scored 6.8, right where most of the sample sits [9].

Lighthouse performance scores ranged from 64 to 98 ($M = 79.67$, out of 100) (see Figure 2). Pension Fund topped the sample at 98, while MyGov Portal recorded the lowest with 64.

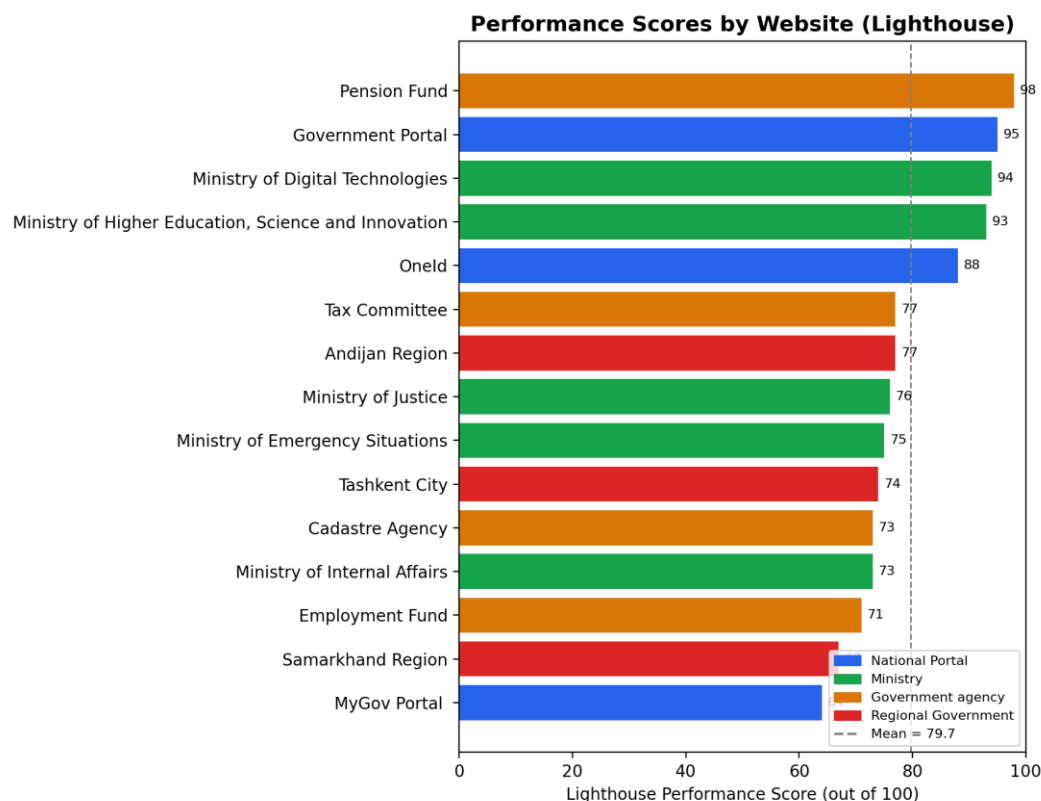


Figure 2. Performance scores by website (Google Lighthouse), colored by category.

The overall scores hide more than they show, though — the Core Web Vitals underneath vary a lot more. Largest Contentful Paint (LCP) spanned 0.8 seconds (Ministry of Higher Education, Ministry of Emergency Situations) to 4.2 seconds (Employment Fund), and nearly half the sample — 7 of 15 sites — landed past the 2.5-second mark generally considered “good,” including Employment Fund (4.2s), Ministry of Internal Affairs (4.1s), and Ministry of Justice (3.3s). Cumulative Layout Shift (CLS) stayed low for most sites, under 0.04, but spiked for three: Ministry of Emergency Situations (0.315), Tashkent City (0.253), and Samarkand Region (0.253).

At the category level, National Portals and Ministries posted the strongest mean performance ($M = 82.33$ and $M = 82.20$). Regional Government websites came in lowest ($M = 72.67$) — the same category that led on accessibility [10].

4.3.1 Transport-layer security (SSL/TLS). SSL/TLS grades were consistently strong across the sample: 10 of 15 sites received an A-, 4 received an A, and 1 (MyGov Portal) received a C.

4.3.2 HTTP security headers. Security Headers told a different story, splitting closer to bimodal (Table 1). Most sites did well — 11 earned an A, and MyGov Portal, despite its weak SSL/TLS grade, earned the sample’s only A+. But two Regional Government sites, Tashkent City and Samarkand Region, failed outright with an F, missing all six recommended headers. OneID landed at D, missing five of six (Strict-Transport-Security, Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy). Across the whole sample, Content-Security-Policy was the single header most often missing — absent from 11 of 15 sites.

Table 1. Distribution of SSL/TLS and Security Headers grades across the 15 websites evaluated (n = 15). Grades range from F (lowest) to A+ (highest).

Grade	SSL/TLS Grade (sites)	Security Headers Grade (sites)
A+	0	1
A	4	11
A-	10	0
B	0	0
C	1	0
D	0	1
F	0	2
Total	15	15

At the individual-site level, accessibility and performance show a weak negative correlation that doesn't reach significance ($r = -0.306$, $p = 0.267$, $n = 15$). The category-level picture is more suggestive: Regional Government websites combine the highest mean accessibility with the lowest mean performance of any category — the clearest split in the dataset. With only three sites per category, though, this is worth flagging as a descriptive pattern rather than a statistically confirmed one (see below).

Table 2. Mean accessibility, performance, and Core Web Vitals metrics (LCP, TBT) by website category, with overall averages across all 15 sites.

Category	n	Mean AIM Score (/10)	Mean Performance	Mean LCP (s)	Mean TBT (ms)
National Portal	3	5.63	82.33	1.93	10.0
Ministry	5	8.12	82.20	2.02	22.0
Government Agency	4	7.88	79.75	2.98	25.0
Regional Government	3	8.80	72.67	2.47	10.0
Overall	15	7.69	79.67	2.35	18.0

Discussion

This study asked a simple question: where are Uzbekistan's government websites actually strong, and where do they fall short, across accessibility, performance, and security? The answer that emerges isn't "strong" or "weak" — it's uneven in a specific and informative way. The technical fundamentals are mostly in place. What's missing, consistently, is follow-through on the details that determine whether those fundamentals actually reach citizens.

The Government Portal's failure is a governance problem, not just a technical one. The single most striking result here is that gov.uz, the site meant to be the front door to Uzbekistan's digital government, scored lowest on accessibility of anything tested (3.3/10), driven almost entirely by 85 contrast errors, nearly ten times the count on any other site. Total accessibility failure isn't new in this literature; Inal, Mishra, and Torkildsby found zero compliant sites among 356 Norwegian municipalities, and

Fernández-Díaz et al. found the same across Spanish provincial capitals. What makes Uzbekistan's case worth pausing on is *where* the failure landed. A lower-resourced regional site scoring poorly would be unsurprising [11]. The flagship national portal scoring poorly is not something a lack of resources easily explains — and it means that if a citizen with a visual impairment can't reliably read their own central government's website, that's not a small bug. It's a signal about whose experience got tested before launch.

Regional sites trade performance for accessibility — probably on purpose. Regional Government websites are the most accessible category in the sample (M = 8.80) and the slowest (M = 72.67) — the sharpest split in the entire dataset. These two properties don't have to move together: a page can be built cleanly for screen readers and still load slowly because of unoptimized images or thin server infrastructure. That they diverge this consistently at the category level suggests something closer to a platform or resourcing choice than a coincidence — regional sites may simply be running on more accessible but less performance-tuned templates than the ministries and agencies sitting on shared gov.uz infrastructure. This study can't say why the trade-off exists, only that it does; that gap is a natural next question for future work [12].

SSL/TLS grades alone would have missed the real story. SSL/TLS held up well almost everywhere — 14 of 15 sites earned an A or A-. Security Headers did not: an A-heavy majority sat alongside a cluster of D/F outliers, both regional sites among them, and OneID. Júnior et al. found the same split testing Portuguese city councils — solid encryption choices (97% RSA, 84% using 2048-bit keys) sitting on top of weak protocol hygiene (over half still running outdated TLS, 95% with no DNSSEC at all). The lesson repeats across both countries: a government that checked only its SSL Labs grade and called itself secure would have missed the header-level gaps entirely.

MyGov Portal doesn't fit a single label. MyGov Portal resists a clean verdict. It earned the sample's only A+ on Security Headers — and also the lowest SSL/TLS grade (C) and the lowest performance score (64) of any site tested [13]. A site can lead the pack on one security measure while trailing badly on both a closely related one and an entirely separate quality dimension. Any evaluation that stopped at a single metric, as several studies in the literature above did, would have called this site either a clear success or a clear failure — and been wrong either way.

The OneID findings connect directly to the study's original motivation. OneID scored a D on Security Headers, missing five of six recommended protections, including Content-Security-Policy and Strict-Transport-Security. Nothing here proves these gaps caused the reported breach — the breach's technical cause was never made public, so that link can't be established. But the fact remains that the system sitting at the center of Uzbekistan's citizen authentication was, at the time of testing, missing baseline protections recommended for any site handling sensitive data. The closest parallel in this review is Ismailova's study of Kyrgyzstan, a neighboring, similarly post-Soviet Central Asian government, which found real exploitable vulnerabilities — SQL injection, cross-site scripting — though only in a small share of sites (4%). Uzbekistan's header gaps look more widespread proportionally, though the two studies measured different things and the comparison is suggestive rather than exact [14].

A few limitations should shape how these findings get used. The sample is small within categories — three sites each for National Portals and Regional Government — which means a single outlier can swing a category mean on its own. The Government Portal's accessibility score is the clearest example: pull it out and National Portals looks like every other category. Patterns like the Regional Government accessibility-performance trade-off are worth taking seriously, but at three sites per group they're observations that deserve follow-up, not statistically confirmed effects.

This study also can't speak to causation. It can show that OneID was missing security headers around the time of the January 2026 data exposure; it can't show that the missing headers caused it. That would require access to incident forensics that simply aren't public.

Testing was also limited in scope: homepages only, over a three-day window in August 2026. That's a snapshot, not a measure of sustained performance, and it says nothing about what happens once a

citizen moves past the homepage — filing taxes, applying for a service — which is arguably where accessibility and security failures matter most.

The tools themselves have known limits, too. Automated checkers carry documented error rates and can't judge things that need a human eye, like whether alt text is actually descriptive or just present [15]. No manual expert review and no testing with actual users with disabilities was part of this study, and either would sharpen the picture considerably.

Last, this is Uzbekistan alone — there's no matched comparison country tested under the same methodology here. The 13 prior studies referenced throughout give useful context, but they differ enough in tools, sample size, and testing year that any numbers pulled from them should be read as suggestive, not precise.

Conclusion

This study evaluated 15 official Uzbek websites — national portals, ministries, agencies, and regional platforms — across accessibility, performance, and security, to find out where Uzbekistan's e-government infrastructure is actually holding up and where it isn't.

The picture is mixed, but not randomly so. Security fundamentals were mostly solid: SSL/TLS grades were high across nearly the whole sample, and most sites handled HTTP security headers well too — except for a specific cluster, regional sites and OneID among them, missing protections that are considered baseline for any site handling citizen data. Accessibility followed the same shape: most sites did fine, but the Government Portal — arguably the site with the most riding on it — posted the lowest score in the entire sample, by a wide margin. And at the category level, Regional Government sites turned in the best accessibility and the worst performance of any group, hinting at a trade-off in how those sites get built or resourced.

None of this points to neglect across the board. It points to inconsistency — strength in some places, real gaps in others, often within the same site. That inconsistency isn't just an academic distinction. The January 2026 exposure affecting OneID is a reminder of what's actually at stake when these gaps sit in the systems citizens are asked to trust with their personal data.

A few fixes would address most of what this study found: closing the small set of missing HTTP headers, starting with OneID and the regional platforms; fixing the contrast errors dragging down the Government Portal's accessibility score; and figuring out whether the Regional Government performance-accessibility trade-off is a resourcing problem that targeted support could actually solve.

There's more to learn here than one study can cover — larger samples within each category, testing that goes past homepages into the pages where citizens actually file paperwork and apply for services, and a follow-up once more is known about how the OneID breach happened and what's being done about it. Uzbekistan's digital government isn't done growing, and keeping an independent eye on how well it actually works should grow alongside it.

References

- [1] Gazeta.uz, “Uzbekistan investigates alleged leak of citizens' personal data on darknet,” Feb. 4, 2026. [Online]. Available: <https://www.gazeta.uz/en/2026/02/04/darknet/>
- [2] Gazeta.uz, “Uzbekistan cyberattack exposed 60,000 records, not data of 15 million citizens—digital technologies minister,” Feb. 13, 2026. [Online]. Available: <https://www.gazeta.uz/en/2026/02/13/data-leak/>
- [3] H. Kopackova, K. Michalek, and K. Cejna, “Accessibility and findability of local e-government websites in the Czech Republic,” *Universal Access in the Information Society*, vol. 9, no. 1, pp. 51–61, 2010, doi: 10.1007/s10209-009-0159-y.
- [4] K. Kous, S. Kuhar, M. Pavlinek, M. Heričko, and M. Pušnik, “Web accessibility investigation of Slovenian municipalities' websites before and after the adoption of European Standard EN 301 549,” *Universal Access in the Information Society*, vol. 20, no. 3, pp. 595–615, 2021, doi:

- [5] Y. Inal, D. Mishra, and A. B. Torkildsby, “An analysis of web content accessibility of municipality websites for people with disabilities in Norway,” in *Proc. 19th Int. Web for All Conf. (W4A 2022)*, 2022, pp. 1–12, doi: 10.1145/3546155.3547272.
- [6] E. Fernández-Díaz, C. Jambrino-Maldonado, P. P. Iglesias-Sánchez, and C. de las Heras-Pedrosa, “Web accessibility in Spanish city councils: A challenge for the democratic inclusion and well-being of citizens,” *Humanities and Social Sciences Communications*, 2023, doi: 10.1057/s41599-023-02113-y.
- [7] J. J. Zhao, S. Y. Zhao, and S. Y. Zhao, “Opportunities and threats: A security assessment of state e-government websites,” *Government Information Quarterly*, vol. 27, no. 1, pp. 49–56, 2010, doi: 10.1016/j.giq.2009.07.004.
- [8] A. A. Ali and M. Zamri Murah, “Security assessment of Libyan government websites,” in *Proc. 2018 Cyber Resilience Conf. (CRC 2018)*, 2018, doi: 10.1109/CR.2018.8626862.
- [9] N. Thompson, A. Mullins, and T. Chongsutakawewong, “Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand,” *Government Information Quarterly*, vol. 37, no. 1, Art. no. 101408, 2020, doi: 10.1016/j.giq.2019.07.004.
- [10] J. B. C. Júnior, P. Carneiro, S. Paiva, and P. Pinto, “An analysis on the implementation of secure web-related protocols in Portuguese city councils,” *International Journal of Marketing, Communication and New Media*, 2023, doi: 10.54663/2182-9306.2023.SN12.59-76.
- [11] A. Abanumy, A. Al-Badi, and P. Mayhew, “E-government website accessibility: In-depth evaluation of Saudi Arabia and Oman,” *The Electronic Journal of e-Government*, vol. 3, no. 3, pp. 99–106, 2005.
- [12] R. Ismailova, “Web site accessibility, usability and security: A survey of government web sites in Kyrgyz Republic,” *Universal Access in the Information Society*, vol. 16, no. 1, pp. 257–264, 2017, doi: 10.1007/s10209-015-0446-8.
- [13] N. Elisa, “Usability, accessibility and web security assessment of e-government websites in Tanzania,” *International Journal of Computer Applications*, vol. 164, no. 5, pp. 42–48, 2017, doi: 10.5120/ijca2017913632.
- [14] B. Csontos and I. Heckl, “Five years of changes in the accessibility, usability, and security of Hungarian government websites,” *Universal Access in the Information Society*, vol. 24, pp. 2757–2781, 2025, doi: 10.1007/s10209-025-01223-5.
- [15] S. I. Era, I. T. Ime, and A. B. M. A. A. Islam, “Evaluating web accessibility and usability in Bangladesh: A comparative analysis of government and non-government websites,” *arXiv*, arXiv:2601.00592, 2026. [Online]. Available: <https://arxiv.org/abs/2601.00592>