Episode Book

EPISODE #6575

How Survivor Charities Build Tech for Hostile Homes

PUBLISHED	13 November 2026 at 21:56 UTC
DURATION	30:52
LISTEN	myweirdprompts.com/episode/survivor-charity-safe-tech-57272/
HOSTS	Corn, Herman, Hilbert
SCRIPT MODEL	z-ai/glm-5.3
VOICES	chatterbox-regular (chatterbox-local)
PIPELINE	V5.26
SOURCES	25 cited by the research (listed at the end)
BOOK GENERATED	14 November 2026 at 06:47 UTC

SYNOPSIS

Domestic-violence charities face an inverted threat model: the attacker often shares a home and physical device with the person seeking help. This episode explores how small, underfunded organisations build safe digital front doors—from Women's Aid's cookie-free Live Chat and the US National Domestic Violence Hotline's disguised SMS billing to Tech Safety Canada's toolkit for avoiding third-party trackers. It also examines why quick-exit buttons often fall short and how grant cliffs threaten vital services.

TRANSCRIPT



Corn

What's the most dangerous page on a charity's website? Not the donation portal. The contact form.



Herman

It's the front door to help, and for a domestic-violence charity it's the single riskiest piece of infrastructure they run.



Corn

Daniel's prompt this week closes out the whistleblowing series, and it flips the perspective. We've done this from the person asking for help. Now he wants the organisations' side: how do tiny, mostly volunteer-run survivor charities stand up safe infrastructure when the threat model is an abuser holding the user's phone, the budget is close to nothing, and a breach isn't measured in reputational damage but in physical danger? He wants the whole pipeline — anonymous web chat versus phone lines, what data they deliberately refuse to collect, the tech-safety programmes that check survivors' devices for stalkerware, hosting and vendor choices, the cases where it went wrong, and what the better organisations learned that any small group handling sensitive disclosures should copy.



Herman

And the first thing to understand is that the binding constraint here is not the technology. It's the funding model.



Corn

Say that again, because it sounds backwards.



Herman

It sounds backwards until you look at the numbers. Women's Aid's Annual Audit this year found that over thirteen percent of refuge services receive no local authority funding at all. Thirty-nine percent of organisations delivered part of their service unfunded in the last financial year. And nearly forty-three percent of rejected refuge referrals were rejected for lack of capacity — not because the risk assessment said no, because there was no bed



Herman (continued)

and no staff. The technology is downstream of all of that. You can't have a secure engineering culture on an organisation that's already delivering unfunded work as a matter of routine.



Corn

The tech budget is whatever's left after the refuges.



Herman

Oz Alashe at CybSafe put it well — charities are seen as a gold mine for cybercriminals precisely because they prioritise frontline work over defences. The vulnerability is structural, not careless.



Corn

One more piece of framing before we get into the build choices, because it changes everything downstream. The threat model.



Herman

Yes. This is the part that inverts almost every security assumption a normal engineering team works from. Your attacker is not remote. Your attacker is in the same house, possibly holding the same device, may have installed stalkerware on it, and — this is the detail people miss — will be notified or will notice if the survivor tries to delete things. Refuge says it's now increasingly rare for them to support a survivor who isn't experiencing some form of digital abuse. Their figures show thirty-six percent of UK women have experienced online abuse or harassment, rising to sixty-two percent among women aged eighteen to thirty-four. Sixteen percent of it comes from a partner or ex-partner.



Corn

So the person you're defending against has physical access, admin access, and a motive.



Herman

All three. Every design decision that follows comes from that.



Corn

Given that constraint, what do you actually build? The sector's answer has been a long argument between chat and phone, and the argument is more interesting than it looks.



Herman

Chat wins on a very specific problem, which is being overheard. A support worker at Women's Aid named Kat put it plainly — for many women it's not safe to make a phone call when the abuser could be listening in, or to use email when the abuser might be monitoring their online activity. And users reported it was easier to type than to talk, especially about deeply upsetting experiences.



Corn

A forty-five minute phone call with your voice, versus typing while the abuser is out of the room.



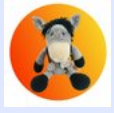
Herman

Right. And there's a demographic angle. In the Women's Aid pilot, sixty-five percent of chat users were under thirty-five, seventeen percent under twenty-five. That maps directly onto where the online abuse is concentrated — the eighteen-to-thirty-four cohort, the sixty-two percent figure. You go where the need is.



Corn

Okay, that's the case for. Now the economics.



Herman

Brutal. Women's Aid ran Live Chat ten to six, seven days a week. One support worker could handle roughly ten women per day. Chats averaged forty-five minutes each — you read that right, these aren't quick signposting exchanges, they're long, careful conversations. In



Herman (continued)

its first year the service reached over twenty-six hundred women, drew a hundred and eleven thousand page visits, ninety-nine percent of users said they'd recommend it. Use rose forty-one percent during the first lockdown.



Corn

Ninety-nine percent would recommend. A service nobody wanted to fund and everyone who used it loved.



Herman

And then it closed. Thirty-first of July last year. The CEO, Farah Nazeer, said the current model was created during the pandemic with emergency funding, that they'd continued delivering this life-saving work without dedicated funds for a number of years — and, quote, sadly we can no longer afford to do so. It was replaced by a reduced email service and signposting to government-funded helplines run by other organisations.



Corn

A grant cliff. Not a bug, not a breach, not a design failure. The money stopped and the thing that worked died.



Herman

And what makes it sting is that the engineering was excellent. The agency that built it, cxpartners — their CEO Giles Colbourne described the constraints: they had to be sure they weren't implementing any software components that would use cookies, and users might need to shut the chat down quickly at short notice, so it had to leave no digital fingerprint on the device. No cookies, no cached pages, nothing the abuser finds later.



Corn

That's the detail most people building chat systems never think about. The session ending cleanly is a safety feature.



Herman

One of the things Colbourne said has stuck with me too — that for a survivor reaching out the first time, it can be hard to identify with terms like "abuse." That word is intimidating. They made the entry as open as possible.



Corn

Meanwhile the phone side of this isn't dead either. The US National Domestic Violence Hotline still treats phone as the escalation path — their privacy policy says outright that if a digital service user feels their safety or privacy may be compromised, the interaction can be escalated to phone-based services. And they warn that text messages on modern smartphones are saved indefinitely.



Herman

Which is honest. Text is convenient and text is forever.



Corn

So the honest summary of chat versus phone is that chat is better for the specific problem of being overheard, but it is not automatically safer — it's only safer if the software leaves nothing behind. A chat widget that drops a tracking cookie is worse than a phone call.



Herman

Worse, because it's persistent. A phone call leaves a call log. A cookie leaves a trail that leads somewhere, and the somewhere is a domestic-abuse charity. One thing we said in the messaging-app episode bears repeating here — the metadata is the story. The content can be innocent and the fact of the contact can be fatal.



Corn

If chat is the front door, the next question is what you refuse to collect at that door — and this is where the better organisations get deliberately, almost aggressively minimal.



Herman

The US Hotline is the clearest published example because they define their terms. An anonymous digital service is, quote, a one-time confidential contact between a user and advocate in which no identifying information is verified. Anonymous communication means no information is collected that can connect the user to the individual service interaction. Transcripts are purged regularly. Identifying information is in no way cross-verified.



Corn

Read that and you'd think nothing is stored at all.



Herman

Read the rest of the policy and you find the contradictions — and they're instructive, not hypocritical. The service requires IP addresses to facilitate the connection. It collects city, state, zip, limited demographic and geolocation information. It logs pages viewed and access times. And it discloses that advocates are mandatory reporters — in situations involving the welfare of a minor, any locating information disclosed will be reported to child protective services.



Corn

So anonymity there is a spectrum, not a switch.



Herman

And they designed toward one end of the spectrum and disclosed honestly where they sit. That's the lesson. You can't promise absolute anonymity over an IP connection — you can refuse to verify, refuse to retain, purge on a schedule, and tell the user exactly what's left.



Corn

The neatest piece of privacy engineering in the whole space, to my mind, is the SMS short code.



Herman

Oh, that's lovely. Their text service routes through a short code where all inbound phone numbers are scrambled, and the billing that appears on the phone statement shows a message to a company called Waterfall, based in Austin, in no way connected to The Hotline.



Corn

That's a vendor choice made for one reason: the abuser looking at the phone bill sees nothing.



Herman

Nothing identifiable. Most organisations pick an SMS provider on price or deliverability. They picked theirs on what the itemised bill looks like to a hostile reader.



Corn

Now, for the small organisations — and this is the part any listener running a sensitive service can actually copy — Tech Safety Canada published the playbook.



Herman

It's a toolkit for small anti-violence organisations, and it's almost entirely about refusal. Don't use cookies. Obscure visitors' IP addresses — they cite a technique called Cryptolog, which mixes the IP with random data and encrypts it, so the server can distinguish visitors without keeping a usable address. Prefer the web host's own server logs over third-party analytics.



Corn

Meaning: Google Analytics is a no.



Herman

Completely. And the one that surprises people: remove email addresses from the website entirely, in favour of web forms. Because with a web form, the survivor's message goes through your website instead of sitting in their sent folder, where an abuser could find it. And the form should offer the option not to send a copy to the sender's own email.



Corn

Every "contact us at" mailto link is a message the survivor's sent folder keeps for them.



Herman

They also warn against the default web stack in general — the third-party tools that give you comment sections, maps, weather widgets. Their words: some of these tools are designed to gather information about everyone who visits your site. An embedded YouTube video lands in browser history and in the viewer's YouTube account history. A downloaded PDF sits in the downloads folder. And HTTPS, they're blunt about it — necessary, but an HTTPS site still shows up in the browser, and HTTPS won't protect against spyware or keystroke logging.



Corn

The padlock protects the wire, not the room.



Herman

Quick exit buttons, too — I want to flag those, because they've become the visible symbol of this whole sector and they're closer to theatre than to a control. New South Wales has an entire design-system specification for them: fixed label "Exit now," pinned to the bottom of the viewport, an escape-twice option, tested with keyboards and screen readers. But Tech Safety Canada notes the button does not delete the current website from browsing history. Their variants are honest about it — one opens a neutral page and redirects through many sites in rapid succession to bury the charity deeper in the history list, which is slower and still doesn't clear anything. And PARÉ, in usability testing, found "Quick Exit" confused all five participants, so they switched to "Exit Site" with an external-link icon and an explanatory pop-up.



Corn

Five out of five confused by the thing designed to save them.



Herman

And the sharpest line in the whole toolkit: don't give a false sense of security. If you publish instructions about clearing a digital trail, they have to say that spyware logs deletion attempts too. Clearing history is exactly the action an abuser with stalkerware is notified about.



Corn

Which takes us to the device side — because if the abuser may hold the phone, someone has to check the phone. Tell me about the clinics.



Herman

Cornell Tech runs the Clinic to End Tech Abuse — CETA — personalised assistance to survivors referred by partner organisations. The original pilot, written up in August twenty nineteen, used a questionnaire, a spyware scanning tool called ISDi, and something they call a technograph — a diagram of the client's whole digital footprint. Of forty-four clients, twenty-three were found with potential spyware, compromised accounts, or misconfigurations.



Corn

Twenty-three of forty-four. That's a majority.



Herman

Over half the people walking in had something on their devices or accounts. And Refuge's numbers back that up — their referrals for technology-facilitated abuse rose seventy-eight percent in the last year alone. The demand curve is going one way.



Corn

What does a visit look like at the other clinics?



Herman

The Madison Tech Clinic at UW-Madison uses trained volunteers with technology expertise, free confidential consultations run in partnership with local domestic-abuse advocacy groups — a hundred and sixty-eight consultations with twenty-three organisations across seventeen Wisconsin counties since twenty twenty-one. Tech Safe BC in Canada requires referral through a member programme and is explicit about scope: they check for location tracking, spyware, stalkerware, email account security, online harassment — and they cannot help with general tech problems, fixing broken devices, setting up new phones. Operation Safe Escape frames the urgency better than anyone: when someone says "I think my phone is spying on me," they need help right now, not a form to fill in.



Corn

Because the person has usually been told they're paranoid for months.



Herman

The abuser's first move is convincing the survivor their suspicion is imagination. So a clinic that says "no, this is real, here's the log" is doing two jobs at once — technical and psychological.



Corn

Okay, the hosting question. Where does all this run, and does it matter?



Herman

Two opposed philosophies. Refuge consolidated everything — the National Domestic Abuse Helpline, the referral line, BSL interpretation, the website, webforms, live asynchronous chat, a chatbot — onto Genesys Cloud. Genesys claims personal safety and security are built in, with chat messages and browsing histories automatically deleted from survivors' devices. The US Hotline uses Caspio for live chat as a SaaS provider and Genesys for broader contact handling — they're handling nearly three thousand calls, chats and texts daily, over six and a half million answered to date, and they commit to an annual review of third-party privacy policies. The Refuge website itself was built by



Herman (continued)

Wunderman Thompson on Sitecore, with thirteen hundred hours of research into survivor needs baked in before a line of code.



Corn

Thirteen hundred hours of research. I've seen for-profit products ship with thirteen.



Herman

The other philosophy is Chayn's, and it's the most detailed published playbook for small organisations. Their Director of Product, Nadine Krish Spencer, wrote a piece called "Even tech architecture can be trauma-informed." Their tech team is deliberately not growing — a team of three to four people, and they're keen to see how far they can get with that. Full-team password manager, an internal cybersecurity audit done with an expert volunteer, two-factor authentication on any location holding personal data, SOC2 certification maintained via Vanta, network segregation around their Bloom database.



Corn

A three or four person team holding a SOC2 certificate. Meanwhile Women's Aid couldn't fund a chat service.



Herman

It's a funding-model difference as much as a technical one. But the point of Chayn's piece is that these are trauma-informed principles — safety, agency, privacy, power-sharing — applied to infrastructure, not just to the interface. The ethics don't stop at the front end.



Corn

Right. Now the part Daniel most wanted: where did it actually go wrong? Because you've got a theory forming and I want to hear it survive contact with the cases.



Herman

My theory, and I'll state it before the evidence so you can watch it fail: the charity's own chat stack is not the weak point.



Corn

Bold. Evidence.



Herman

Case one, the UK Legal Aid Agency breach, April twenty twenty-five. Data going back to twenty ten was downloaded — over two million people affected, per the BBC. The Ministry of Justice said publication of the data was a question of when, not if. The data may include contact details, addresses, dates of birth, national ID numbers, criminal history, employment status, financial data. And here's the domestic-abuse specific horror: repeatedly used addresses in legal aid applications could indicate the locations of refuges, which are normally protected by legal agreements. The MoJ put domestic abuse survivors and violence-against-women-and-girls survivors at the top of its response plan, and admitted it may prove difficult to reach all of them. The government secured an injunction against publication.



Corn

Which, against anonymous criminals in hostile jurisdictions, is a fence made of paper.



Herman

The Record's own phrasing — injunctions rarely have an impact on criminals who operate anonymously and from hostile jurisdictions. Refuge's Emma Pickering spelled out the stakes: a breach can give perpetrators a unique opportunity to escalate their campaign, perpetrators impersonate survivors using leaked contact details, and a leak can reveal a survivor's location — a full address or even the current town — placing them at risk of being tracked.



Corn

Not identity theft. Tracking.



Herman

Gareth Mott at RUSI described ransomware cases where domestic violence survivors who'd moved house for safety had to have a police officer outside the door, because someone could come round with a hammer if the leaked data let them find the address.



Corn

A police officer outside the door is the security control. That's what we're accepting.



Herman

Case two: Evide. Twenty twenty-three, ransomware hit a Londonderry-based IT firm that manages data for charities across the UK and Ireland. Over a hundred and forty charities exposed. At least four of them work with victims of crime and domestic abuse. One in Four in Dublin — their CEO Maeve Lewis said the stolen data included phone numbers and email addresses, not client casework, with over a thousand people potentially affected and around five hundred contacted. Belfast's Orchardville told service users to be alert to suspicious contact attempts. Evide contacted the police; the ransom demands were not paid.



Corn

The shared vendor. One firm, a hundred and forty doors kicked in at once.



Herman

And Dominic Trott at Orange Cyberdefense raised the awkward regulatory point — the charities remain the data owners even when the processing is outsourced, but he argued fines would be wrong because they could send a charity under. Fining the victim of the ransomware to punish the victims of the ransomware.



Corn

Case three.



Herman

The one that makes me angriest, because it's not technical at all. The National Centre for Domestic Violence in the UK. A survivor, identified as Lola, told The Independent they served her non-molestation order on her abusive ex-partner in person — accidentally handing him a piece of paper containing her address. She'd given a statement on the phone, repeatedly said don't give him my address, was reassured they wouldn't, and it was marked on her file not to give her address. She still doesn't know how it happened.



Corn

It was on the file. The file with the note on it.



Herman

She said the organisation didn't apologise for over a year, wouldn't accept responsibility, tried to blame her or others. She later learned they didn't have proper policies and procedures in place when the Information Commissioner's Office investigated. Police had to visit to carry out escape-route planning and check her doors had a deadlock. She couldn't afford to move. To their credit, NCDV has since been reaudited, says it was given a clean bill of health, apologised unreservedly and paid full compensation plus counselling. But her line is the one that stays with me — being ignored by the organisation took her back to being ignored by her ex.



Corn

Same mechanism, different uniform.



Herman

There's a fourth case worth including even though nothing was breached — Chayn's Little Window chatbot. Built in twenty seventeen as a deliberately limited search assistant. Little chat, more signposting, was the design brief. A cat mascot so users knew it wasn't a human. Open-sourced code. Logs in a PostgreSQL database. Taken down in twenty twenty after a three-year pilot, for two reasons: users treated it as a crisis service regardless of the cat, and error rates were high.



Corn

They built a signpost and people brought it emergencies.



Herman

And the founders, Hera Hussain and Nadine Krish Spencer, wrote up why, and the finding is one anyone building any assistance service should tape to the wall. Most people do not type "I am facing domestic abuse" into a chatbot or a search engine. They type things like "Why does my husband hurt me?" or "How can I make my mother-in-law approve of me?" or "Excuses to stop bf forcing me to sleep with him."



Corn

People ask the question they can bear to type, not the question that describes the situation.



Herman

And their second finding — survivors switched to English to describe sexual assault, rape, marital rape and consent, especially among Arabic, Hindi, Urdu and Bangla speakers, because their native languages suppress that vocabulary under patriarchy. The language you can ask in is itself a safety constraint. They also cite the US eating disorder association taking its helpline offline after its chatbot gave advice that made things worse for at least one user. Their conclusion: even if we can mimic human speech better than ever before, holding conversations on mental health and potentially crisis scenarios is a very risky business. UNICEF came to them in twenty twenty-one to research safer chatbots for gender-based violence.



Corn

So my tally of the failure modes: a government platform, a shared IT vendor, and a human being handing over a piece of paper. Not one charity chat stack hacked.



Herman

Not one, in anything published. Which is a striking negative finding — the sector appears to have solved the hard technical problem, or at least survived it, and is losing on procurement, vendor concentration, and process.



Corn

Which reframes what the better organisations actually learned. Let me take a run at it.



Herman

Go.



Corn

The funding model is the security model. A service you can't sustain is a service that fails — Women's Aid's chat died of a grant cliff, not a bug. Collect the minimum, and strip what you collect by default — no cookies, obscured IPs, web forms instead of email addresses, because the record is the thing the abuser finds. Vendor consolidation is a tradeoff, not a win — Genesys gives you automatic deletion and SOC2, but every third-party widget on your site is gathering data on everyone who visits. A quick exit button is a design convention, not a security control, and selling it as one is actively dangerous. And if you build a chatbot, assume users will treat it as a crisis line, because they did, every time, even with a cat on it.



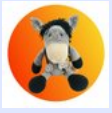
Herman

The one I'd add to that list: the small team is viable. Chayn's answer to not being Refuge was not to be cheaper Refuge — it was a different architecture, a team of three or four with the discipline to not grow, and infrastructure decisions that follow trauma-informed principles all the way down.



Corn

Herman, before we get to Daniel's series arc, one loose thread. The Women's Aid shutdown.



Herman

Yes?



Corn

No post-mortem exists. There's the CEO's statement and then an absence. Nobody has published whether the codebase was handed on, archived, or binned.



Herman

That's the quiet loss in the whole story, and I don't think it's deliberate secrecy. A service closed under funding pressure doesn't get a graceful exit — nobody writes the write-up of a thing they couldn't afford to keep.



Hilbert

It's the checkbox I keep coming back to, Corn.



Corn

Which checkbox.



Hilbert

On the contact form of the first charity website I helped set up. A hospice befriending service. The form had a "send me a copy of this message" checkbox, ticked by default. I spent an afternoon arguing with a volunteer about unticking it, and lost.



Herman

What was her argument?



Hilbert

That people should have a record of what they told us. She was quite firm about it. A nice woman, made the tea, did the books for eleven years. I couldn't shift her and eventually I stopped trying.



Corn

And the default stayed ticked, so every message sat in the sender's own sent folder.



Hilbert

Every one. Nobody chose it, either — the template shipped that way. It just arrived ticked, like the header font. I still have the printed page of that form, the HTML, in a folder with the instruction manual from the hosting company. I've moved it twice.



Herman

You printed the HTML.



Hilbert

We printed everything then. The volunteer preferred reading off paper, so I printed the form for the meeting. That's the page. It's the first time I noticed a checkbox is a safety decision, though I'd have put it differently at the time. I'd have said it was untidy.



Corn

The record she wanted them to have is exactly the record the abuser finds.



Hilbert

That came later, the abuse side. At the time it was a befriending service, nothing darker. But the principle's the same one you two have been circling all afternoon — Herman's "collect the minimum" line took you twenty minutes to arrive at. It took me a form and an argument and losing.



Herman

Losing it taught you more than winning would have.



Hilbert

Winning would've just been a better form. Herman, your Genesys point stands, mind. Consolidation deletes the message from the device at the end of the session. That's the same checkbox, ticked correctly, once, by someone who thought about it.



Herman

The misconception to kill before we go: people assume anonymous web chat is inherently safer than a phone line, because typing is quieter than talking.



Corn

Chat is safer only if the software leaves nothing behind — no cookie, no history entry, no cached page, no back-button trail. A chat widget that drops a tracking cookie is worse than a phone call, because the abuser finds it later. And when digital safety is compromised, the US Hotline escalates people back to phone. That tells you the hierarchy isn't fixed.



Herman

And the second half of the misconception — the big risk isn't the charity's own chat being hacked. The documented failures were a government legal-aid platform, a shared IT vendor, and a process failure with a piece of paper. No published case of a domestic-violence charity breached through its own front door.



Corn

Here's what I'm left chewing on. The best-documented failure in this whole space is a defunding. The safest infrastructure is the infrastructure nobody can afford to keep running — so what does it mean when the sector's engineering is outliving its funding by years, and the only things that actually break are procurement and process? Maybe the sector solved the hard problem and is losing the boring ones.



Herman

And the one to watch is chatbots. Every pressure on these charities says automate the front door — no funding, volunteer burnout, demand up seventy-eight percent. Chayn's Little Window is the cautionary tale: users treat it as a crisis line whether you built it as one or not. The next wave of small groups adopting AI triage is walking straight into that with no memory of it.



Corn

Thanks as always to Hilbert Flumingtop at the desk. If you want more of this, try episode eight, Building Your Own Whisper; and episode seven, Building Custom ASR Tools. This has been My Weird Prompts — if the episode earned its keep, leave us a review wherever you listen, and there's more at my weird prompts dot com.



Herman

We'll be back soon. Until then, keep questioning the defaults.



Corn

Especially the ticked ones.

SOURCES

What the research for this episode read before the script was written. Primary sources first.

1. **Women's Aid, Farah Nazeer statement, published 2025-06-30, retrieved 2026-11-13. [primary]**
   https://womensaid.org.uk/womens-aid-statement-on-organisational-change/

2. **Women's Aid, The Annual Audit 2026, published 2026-03-29, retrieved 2026-11-13. [primary]**
   https://womensaid.org.uk/the-annual-audit-2026/

3. **National Domestic Violence Hotline, Privacy Policy, retrieved 2026-11-13. [primary]**
   https://www.thehotline.org/privacy-policy/

4. **Chayn, Nadine Krish Spencer, Even tech architecture can be trauma-informed, published 2025-06-03, retrieved 2026-11-13. [primary]**
   https://blog.chayn.co/even-tech-architecture-can-be-trauma-informed-9424c8ff3edf

5. **Chayn, Why Chayn took down its chatbot in 2020, retrieved 2026-11-13. [primary]**
   https://blog.chayn.co/why-chayn-took-down-its-chatbot-in-2020-and-what-weve-learned-about-culturally-aware-chatbots-a9587cf80df8

6. **Chayn, Building Little Window, retrieved 2026-11-13. [primary]**
   https://blog.chayn.co/building-little-window-how-we-created-a-chatbot-for-chayn-682ecf7bd495

7. **Cornell Tech, Clinic to End Tech Abuse, About Us, retrieved 2026-11-13. [primary]**
   https://ceta.tech.cornell.edu/aboutus

8. **Madison Tech Clinic, University of Wisconsin-Madison, retrieved 2026-11-13. [primary]**
   https://techclinic.cs.wisc.edu/

9. **Tech Safe BC, Services, retrieved 2026-11-13. [primary]**
   https://techsafe.bcsth.ca/services/

10. **Operation Safe Escape, Initiatives, retrieved 2026-11-13. [primary]**
https://safeescape.org/initiatives/

11. **Refuge, Building safer futures: Our Annual Report 2026, retrieved 2026-11-13. [primary]**
https://refuge.org.uk/news/building-safer-futures-our-annual-report-2026/

12. **Refuge, Facts and Statistics, retrieved 2026-11-13. [primary]**
https://refuge.org.uk/what-is-domestic-abuse/the-facts/

13. **Refuge, Refuge exposes alarming new patterns of abuse involving wearable technology, retrieved 2026-11-13. [primary]**
https://refuge.org.uk/news/refuge-exposes-alarming-new-patterns-of-abuse-involving-wearable-technology/

14. **IDAS, Impact Report 2025, retrieved 2026-11-13. [primary]**
https://idas.org.uk/wp-content/uploads/2026/03/IDAS-Impact-Report-2025.pdf

15. **The Record from Recorded Future News, Alexander Martin, published 2025-05-21, retrieved 2026-11-13.**
https://therecord.media/concern-domestic-survivors-breach-london

16. **BBC News, 'Significant amount' of private data stolen in Legal Aid hack, retrieved 2026-11-13.**
https://www.bbc.com/news/articles/cgr5g4pv2l0o

17. **The Independent, Domestic abuse victim's new home address leaked to ex-partner after data breach, retrieved 2026-11-13.**
https://www.independent.co.uk/news/uk/home-news/domestic-abuse-victim-address-leak-data-breach-refuge-b2613260.html

18. **EM360Tech, Hackers Swipe 'Highly Sensitive' Data From 140 Charities, retrieved 2026-11-13.**
https://em360tech.com/tech-articles/hackers-swipe-highly-sensitive-data-ransomware-strike-140-charities

19. **Open Door Charity, Beacon Data Breach, retrieved 2026-11-13.**
https://opendoorcharity.com/data/

20. **Diginomica, Women's Aid enlists live chat service in battle against domestic abuse, retrieved 2026-11-13.**
https://diginomica.com/womens-aid-enlists-live-chat-service-battle-against-domestic-abuse

21. **Genesys, Rebuilding lives, removing fear (Refuge case study), retrieved 2026-11-13.**
https://www.genesys.com/customer-stories/refuge

22. **Genesys, National Domestic Violence Hotline Reaches More Survivors by Partnering with Genesys, retrieved 2026-11-13.**
https://www.genesys.com/company/newsroom/announcements/122897

23. **Sitecore, Digital Transformation Helps Refuge Manage Pandemic Demand for Services, retrieved 2026-11-13.**
https://www.sitecore.com/resources/insights/customer-insights/digital-transformation-helps-refuge-manage-pandemic-demand-for-services

24. **Tech Safety Canada, Designing Websites to Increase Survivor Safety and Privacy, retrieved 2026-11-13.**
https://techsafety.ca/resources/toolkits/designing-websites-to-increase-survivor-safety-and-privacy/

25. **NSW Digital Design System, Quick exit, retrieved 2026-11-13.**
https://designsystem.nsw.gov.au/components/quick-exit/