# Episode Book

EPISODE #6573

# When Changing Passwords Signals an Abuser

| | |
|---|---|
| PUBLISHED | 13 November 2026 at 21:53 UTC |
| DURATION | 20:39 |
| LISTEN | myweirdprompts.com/episode/domestic-tech-abuse-safety-32784/ |
| 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

Most technology-facilitated abuse does not rely on secret spyware, but on shared cloud accounts, Find My, car apps, and Bluetooth trackers set up while a relationship was fine. Because changing a password or removing a tracker triggers loss-of-access detection, standard cybersecurity advice can escalate danger. Drawing on guidance from Faraday, WomensLaw, TechSafety, and Tech Safety Canada, this episode explores how quiet surveillance works, why survivors sometimes leave trackers running while building a safety plan, and what charity quick-exit buttons actually do.

# TRANSCRIPT



### Corn

The whistleblower series has taken us to journalists, secure drop boxes, courtrooms. Daniel's latest takes it somewhere much smaller and much worse. The adversary isn't a government or an employer. It's the person on the other side of the bed, with the PIN to your phone and their name on the bill.



### Herman

And his framing is the interesting part, because he's not asking us to catalogue spyware. He's asking what safety even looks like when the person surveilling you shares your cloud account, your car, your front door lock, and your children's devices. Plus the part that hooked me: why the standard advice, the stuff we'd tell anyone else, can get someone hurt here.



### Corn

"Just change your passwords" is the headline of that. We'll get to why that's backwards. But the first thing to say is that this isn't a hacking problem. It's a safety problem wearing a tech costume.



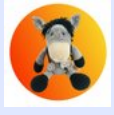
### Herman

That's almost a direct quote from Faraday, the New Zealand guide Daniel pointed us at. Their line is that technology-facilitated abuse "is not your fault, and it is not just a tech problem. Treat it as part of a safety problem, because how and when you make changes can affect how the other person reacts.Not whether you make changes. How and when.



### Corn

Which is a sentence no security professional says about anything else.



### Herman

Right. Against a government, the adversary wants to stay hidden. Against an employer, they want evidence. A partner in this situation wants control, and WomensLaw's framing is blunt about it. Surveillance is used to keep power and control, and, their words, "to try to discover or stop any plans you may be making to leave." The surveillance isn't incidental to the abuse. It's the point.



**Corn**

The mechanism that makes this different from every other threat model we've done is something I'd call loss-of-access detection. Faraday again: when someone loses access they're used to, they may notice straight away. Removing a tracker, changing a password, turning off location sharing. Each one is a signal that you know.



**Herman**

And for some people, that signal leads to escalation. Which means every fix has a side effect that no patch notes ever mention.



**Corn**

So the arc is: how they get in, which is quieter than everyone assumes. Then why the standard fixes backfire. Then the charity websites, which are doing something more honest than they look. And then the one legal lever that actually works without setting off the alarm.



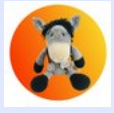
**Herman**

Let's start with how they get in, because the surprise is that it's usually not stalkerware.



**Corn**

I was going to say AirTags and be done with it.



**Herman**

That's the version in the news. The actual guidance from Faraday is that "most technology abuse uses access the other person already had, or that was set up while things were fine." The question "did they hack me?" is usually the wrong question. The answer is family sharing. Find My. A shared cloud backup. The car app. Acts of trust, repurposed.



**Corn**

A couple sets up Find My years ago to keep track of each other, it's sweet, it's practical, someone's always losing their phone. Then the relationship goes bad and it's a leash. Nothing changed technically. Only the relationship did.



**Herman**

And that's why the detection advice is so much stranger than "run a malware scan." Faraday lists stalkerware as less common than the quiet routes, and even its signs, battery drain, a warm phone, odd data use, they call unreliable. There's a paper from last year on Android's platform defenses against stalkerware that lands on almost the same conclusion from the other direction. It asks whether Android's privacy changes have actually thwarted these apps, and it argues that detection-and-removal may not necessarily be effective in this context. Not because the detection is bad. Because removal is the event.



**Corn**

The scan that finds it and the scan that announces it are the same scan.



**Herman**

Walk through the quiet routes, because this list is longer than most people imagine. Passwords and PINs they know or can guess, including your security questions. TechSafety makes a point I'd never thought about, an abusive partner "often knows intimate details about a survivor, and this can make their passwords less secure." Your mother's maiden name is not a secret from someone who's had Christmas dinner with your mother.



**Corn**

I keep a made-up answer to every security question in my password manager. Forty characters of gibberish where my first pet should be.



**Herman**

Good practice generally, and load-bearing here. Then shared accounts, Apple or Google. Account owners can often see devices, locations, purchases, backups. Location sharing through Find My, Google Maps, Life360, Family Link, Snap Map, WhatsApp, fitness apps, car apps, all "often set up once and forgotten." Cloud backups, where if someone can log



### Herman (continued)

into the account your phone backs up to, they see your photos, messages and notes without ever touching your phone.



### Corn

We did an episode on messaging app privacy once, and the piece that stuck with me was that the backups quietly undo the encryption. Same shape here.



### Herman

Then the physical layer. Bluetooth trackers in a bag, a car, a child's belongings. Connected cars, where the app shows location and trips. Smart homes, where cameras, doorbells, speakers and locks are controlled by whoever holds the account. And the kid's tablet set up by the other parent, which can share location or relay messages. That last one gets me. The child's device is the surveillance platform because it's the one thing both parents have a reason to touch.



### Corn

Tech Safety Canada has a piece of diagnostic reasoning I want to read out, because it's the best thing in all this material. If he only knows where she is when she's driven somewhere, the tracker is on the vehicle. If he knows when she has the child with her, look in the child's belongings. If he knows most of the time, that's spyware or a misused app like Find My Friends. It's triage. Symptoms to causes.



### Herman

A clinician's history-taking, basically. And the physical search instructions match: trunk, under the hood, inside the bumper, under or between the seats. In a bag, inside the lining, under shoe insoles, inside a child's toy. Some of these devices are as small as a quarter.



### Corn

So you're checking the seams of your own handbag like it's a rental car.



### Herman

The numbers say this isn't fringe. Freedom-of-information data from police in England and Wales, obtained by The Independent, shows stalking reports involving AirTags and GPS trackers going from fifty-seven in 2018 to five hundred and sixty-eight by the end of 2024. That's roughly a ninefold rise. Coercive-control cases involving trackers went from thirty-eight to four hundred and thirty-one. And only eighteen of forty-four forces responded, so the real figures are higher.



### Corn

And the other one, from Australia.



### Herman

The New South Wales Crime Commission went through the sales records. More than five and a half thousand tracking devices sold in 2023, more than three thousand customers. One in four buyers had a domestic violence history. One in four. These are marketed as "never lose your keys again" devices, and a quarter of the customer base is known to the system.



### Corn

That's the tracker equivalent of the parental-control problem.



### Herman

Which is worth a minute, because it's the dual-use story at its cleanest. There's a paper from the PETS community comparing twenty parental-control apps sideloaded from outside the Play Store with twenty from inside it. Of the sideloaded ones, eight out of twenty were flagged for stalkerware indicators of compromise. Three transmitted sensitive data unencrypted. Half had no privacy policy. And they conceal themselves on the device.



### Corn

So the same software is protection when a parent installs it and surveillance when a partner installs it, and the only difference is the installer.



**Herman**

The app can't tell. The phone can't tell. Honestly, the pattern-matching on "is this abuse" requires knowing the household.



**Corn**

The quiet routes being the common ones reframes the whole countermeasure question, because a shared cloud account isn't something you "remove."



**Herman**

And that's where the advice inverts. Take passwords. Women's Aid in the UK: "if you change your password, someone may realise this has happened when they attempt to log in and this could lead to them escalating their behaviours." TechSafety in Australia went further in their March 2025 password guide. Updating passwords "can even be dangerous." Their instruction is to create a safety plan before changing anything.



**Corn**

Their guidance is also that the alternative is cleaner. New accounts, not linked to the old ones. A fresh email, nothing recovered through the old one.



**Herman**

The Hotline in the US describes the mechanism precisely. Password changes "sometimes send a flag message to the email accounts listed in their system." A reset notification lands in an inbox the abuser controls. The system thinks it's helping you secure the account. It's informing on you.



**Corn**

Every recovery email is a little witness.



### Herman

And the same logic governs the tracker you just found. Faraday: "before you change anything, record what you've found. Take photos or screenshots of trackers, unfamiliar apps, account changes and messages." Because evidence disappears, and a survivor who changes their mind about going to the police can't get it back. Tech Safety Canada adds the detail that haunts me: plan for safety around the police station visit itself, because if the tracker is still on the car, the abuser learns exactly when the report was filed.



### Corn

The counterintuitive version of that, and it took me a beat to accept it: sometimes you leave the tracker running. On purpose. Until the safety plan is in place.



### Herman

Their guidance is literally to decide when to keep the tracker active and when to turn it off. It's not a paradox, it's sequencing. The tracker is a known quantity. What you're actually doing is buying time to get the new phone, the new accounts, the people who know what's happening. Removing it first is the loud door slam.



### Corn

Which leads us to the quick-exit button, which I've always found a bit of theatre. The red bar at the top of every domestic violence charity page. "Leave this site quickly."



### Herman

It's theatre with one honest use case, and NNEDV in the US says it plainly: the button "is helpful only if someone is watching over your shoulder or enters a room and you need to quickly switch to another website. It will not prevent the other person from going through your browser history or from knowing you were on that website if they are monitoring your device or internet activity remotely." It defeats the over-the-shoulder glance. That's the whole job.



### Corn

Faraday's version is charmingly concrete. Their button takes you to the MetService, the weather site, and stops the Back button returning. It doesn't remove the visit from your history.



### Herman

Tech Safety Canada has two actual coding tricks to stretch that. One, the button opens a fresh tab and then redirects through a whole chain of sites in rapid succession, burying the charity's page deeper in the history so Back doesn't land on it. Costs you loading time. Two, code the destination page so there is no Back button at all.



### Corn

A redirect chain as a smokescreen. That's a technique you'd otherwise find in malvertising.



### Herman

Same machinery, opposite intent. And their design guidance for charities is the honest part. "Don't give a false sense of security. Spyware, also called stalkerware, monitors all activity, including attempts to delete browsing history." If your safety page promises cover your tracks and the reader's phone is owned, the page is a trap. So the good sites say both things. Here's the button, and here's what the button cannot do.



### Corn

The browser history advice has the same inversion. "Clear your history" is standard hygiene.



### Herman

Faraday: "Suddenly clearing all browsing history can draw attention. Removing just the specific pages can be less noticeable." Which is counterintuitive and also obviously correct the moment you say it out loud. An empty history is a louder signal than a boring one. NNEDV hedges the same way, "if it is safe to do so," and then the real instruction, which is the one under all of it: use a device the abuser has never had access to. A trusted friend's phone, a work computer you control, a library machine.



### Corn

The answer to almost every question in this episode is "another device."



### Herman

It really is. Faraday's leaving checklist runs: a phone and accounts they've never touched. If you suspect monitoring software, set the new phone up as new, not from a backup they could reach. Change the recovery details on every important account. Move the number into your own name or get a new one. Review the banking, who can see the transactions. And ask police and a lawyer whether the technology behaviour belongs in a protection order. They also prefer crisis lines over email and social, which Tech Safety Canada calls "generally not secure or confidential ways to communicate." A hotline leaves no inbox.



### Corn

There's one lever that works quietly, though, and I want to give it room. The Safe Connections Act.



### Herman

Twenty twenty-two US federal law. Mobile providers have to separate a survivor's line from an account shared with an abuser. The FCC's rules took effect in early 2024, with carrier compliance by mid-July of that year. The separation has to happen within two business days of a completed request. No fees. And this is the operative part: without the primary account holder's approval.



### Corn

Two business days, and the abuser is never asked.



### Herman

That's the genius of it. Every other fix, the survivor performs, and the performance is the alarm bell. Here the carrier performs it, and the mechanism is a request, not a confrontation. From late 2024 there's also emergency Lifeline support, up to six months of discounted service for survivors in financial hardship, because "get a new phone plan" presumes money.



### Corn

It's also the only item on the leaving checklist that's a right rather than a favour.



**Herman**

Compare that with the tracker-alert situation, where the protection you get depends on your hardware. Apple and Google shipped the joint unwanted-tracker alerts in 2024, iOS and Android, one spec. The testing since then, there's a USENIX piece from last year, found alerts reliable on iPhones but received by only fourteen of twenty-five Android participants. So a bit over half.



**Corn**

You find out you're being tracked only if you also had the nicer phone.



**Herman**

And if the phone is on someone else's plan, which in this threat model it often is, there's a whole second problem, because who controls the plan controls the line. Cheaper phones, borrowed phones, weaker protection. The alert gap is an equity problem dressed as an engineering problem.



**Corn**

Even Faraday's caveat is the quiet one. Alerts don't catch every tracker type.



**Herman**

So the coverage you're sold on the box is not the coverage you have in the situation it's for.



**Hilbert**

Corn, you said check the seams of your handbag like it's a rental car. I did that this week.



**Herman**

You checked your handbag?



**Hilbert**

A coat, actually. It went through the wash on a cycle it should not have gone through, and something started rattling in the lining. A Bluetooth tracker, sewn in near the left pocket. I opened the lining to get at it and made a proper job of it, the wrong kind of proper, and the coat's no good now. I'm fairly sure I put it there myself, years back, for a luggage test, and forgot. That's the part I don't like.



**Corn**

The part you don't like is that you did it.



**Hilbert**

The part I don't like is what came after. I didn't take the battery out for three weeks, because I wanted to see if anyone noticed it was gone. Herman spent a whole segment explaining that nobody notices the tracker, only the absence of the tracker. Nobody noticed the absence either.



**Herman**

So your finding is the mirror of ours, from the outside.



**Hilbert**

It's in the desk drawer now, with a label on it. I take it out every few months and check it's still there. Which I can hear is not sensible, so don't bother saying so, Herman.



**Corn**

Nobody sensible labels a tracker they found in their own coat.



**Hilbert**

The label says what it is and the month I found it. The claws are wrong for the little screws on the casing, so I never did open it, and that's fine by me.



**Herman**

Three weeks is a long time to leave a live tracker in a coat you're wearing, though. If it had been someone else's, the battery on that thing was your location the whole time.



**Hilbert**

It was in the coat I don't wear. That was rather the point of the three weeks.



**Corn**

That's the one scenario where the advice holds. Leave it running, but only because it's going nowhere.



**Hilbert**

It went to the drawer in the end. Same as yours would.



**Corn**

The drawer being where all the tech we don't understand goes.



**Herman**

There's a bigger question underneath all this, and it's the one I'd leave people with. If the standard security playbook inverts the moment the adversary is intimate, what does that say about who the security industry thinks it's building for? Every default assumes an attacker outside the house. Rotating passwords, revoking sessions, alerts when something changes. All of it presumes you want to know, and want them not to.



**Corn**

The industry's threat model has a stranger in it. The dangerous threat model has the person who set up your phone.



**Herman**

And the quiet routes in are acts of trust. Family sharing. The cloud backup. The plan in someone else's name. None of them are vulnerabilities until the trust is, and by then the fix isn't technical. It's the legal lever like the Safe Connections Act, a device nobody has touched, a safety plan made before anything changes.



**Corn**

Faraday's line is the one to end on. It is not your fault, and it is not just a tech problem. Safety first, the technology second. That's not a checklist, it's an ordering, and it's the only ordering that works.



**Herman**

Thanks as always to our producer, Hilbert Flumingtop, at the desk. If this was your kind of episode, go back for episode eighteen sixty-one, Emergency Prep You Can Sing To; and episode ten, How ASR Went From Frustration To … Whisper Magic. This has been My Weird Prompts. If today's subject touched something close to home, the domestic violence hotlines and tech-safety programmes we drew on today are where real help lives. Find us at my weird prompts dot com, and leave us a review if the show earns it. We'll be back soon.

## SOURCES

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

1. **TechSafety (Australia), Passwords, and Password Safety V2.3 PDF, https://techsafety.org.au/wp-content/uploads/2025/03/HDT_TSA_Password_Safety_V2.3_2025.pdf [primary]**

   document dated March 2025, retrieved 2026-11-13.
   https://techsafety.org.au/resources/resources-women/passwords/

2. **FCC, FCC Adopts Rules Implementing the Safe Connections Act for Survivors of Domestic Abuse [primary]**

   2023-09-15, retrieved 2026-11-13.
   https://www.fcc.gov/consumer-governmental-affairs/fcc-adopts-rules-implementing-safe-connections-act-survivors-domestic-abuse

3. **Federal Register, Supporting Survivors of Domestic and Sexual Violence; Lifeline and Link Up Reform Modernization [primary]**

   published 2023-12-05, effective 2024-01-14, retrieved 2026-11-13.
   https://www.federalregister.gov/documents/2023/12/05/2023-25835/supporting-survivors-of-domestic-and-sexual-violence-lifeline-and-link-up-reform-modernization

4. **FCC, WCB Announces Compliance Date of July 15, 2024 For Safe Connections Act Rules [primary]**

   retrieved 2026-11-13.
   https://www.fcc.gov/document/wcb-announces-compliance-date-july-15-2024-safe-connections-act-rules

5. **47 U.S.C. § 345 [primary]**
retrieved 2026-11-13.
https://uscode.house.gov/us/usc/119-138/t47/s345/

6. **FCC, FCC Announces Domestic Abuse Survivors May Get Discounted Phone Services [primary]**
2024-09-10, retrieved 2026-11-13.
https://www.fcc.gov/consumer-governmental-affairs/fcc-announces-domestic-abuse-survivors-may-get-discounted-phone-services

7. **Apple Newsroom, Apple and Google deliver support for unwanted tracking alerts in iOS and Android [primary]**
2024-05-13, retrieved 2026-11-13.
https://www.apple.com/newsroom/2024/05/apple-and-google-deliver-support-for-unwanted-tracking-alerts-in-ios-and-android/

8. **Faraday (NZ), A safety guide to technology-facilitated abuse**
retrieved 2026-11-13.
https://faraday.co.nz/guides/people/tech-abuse/

9. **Tech Safety Canada, Conversation Guide: Location Tracking**
retrieved 2026-11-13.
https://techsafety.ca/resources/toolkits/conversation-guide-location-tracking/

10. **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/

11. **NNEDV Safety Net Project, Exit From This Website Quickly**
retrieved 2026-11-13.
https://www.techsafety.org/exit-from-this-website-quickly

12. **NNEDV Safety Net Project, NNEDV Resource Highlight: Technology Safety and Your Website**
published 2018-02-05, retrieved 2026-11-13.
https://www.techsafety.org/blog/2018/2/5/nnedv-resource-highlight-technology-safety-and-your-website

13. **Women's Aid (UK), Cover your tracks online**
retrieved 2026-11-13.
https://womensaid.org.uk/information-support/what-is-domestic-abuse/cover-your-tracks-online/

14. **The Hotline, My Abusive Partner Stole My Identity**
retrieved 2026-11-13.
https://www.thehotline.org/resources/identity-theft-in-abusive-relationships/

15. **WomensLaw.org, Abuse Using Technology: Electronic Surveillance**
retrieved 2026-11-13.
https://www.womenslaw.org/about-abuse/abuse-using-technology/ways-survivors-use-and-abusers-misuse-technology/electronic

16. **WESNET, Survivor's Guide to Location Tracking V1.0**
dated 2023-07-31, retrieved 2026-11-13.
https://techsafety.org.au/wp-content/uploads/2023/08/WESNET_Survivors-Guide-to-Location-Tracking-V1.0-31-July-2023.pdf

17. **The Independent, Revealed: How stalkers are weaponising AirTags and GPS trackers to harass their victims**
retrieved 2026-11-13.
https://www.the-independent.com/news/uk/crime/stalking-gps-trackers-apple-airtags-b2876552.html

18. **The Guardian, Tracking devices increasingly used by DV offenders to 'stalk, harass, intimidate and monitor victims**

2024-06-24, retrieved 2026-11-13.
https://www.theguardian.com/world/article/2024/jun/25/tracking-device-domestic-violence-offenders-stalking-apple-find-my-friends

19. **USENIX ;login:, Gerhardt & Fassl, The Hidden Cost of Location Tracking**

2025-07-15, retrieved 2026-11-13.
https://www.usenix.org/publications/loginonline/hidden-cost-location-tracking

20. **Suffolk Journal of High Technology Law, Tag, You're It: The Legal Fallout of AirTag Misuse**

2025-10-10, retrieved 2026-11-13.
https://sites.suffolk.edu/jhtl/2025/10/10/tag-youre-it-the-legal-fallout-of-airtag-misuse/

21. **Jadhav, Bao, Bindschaedler, Thwart Me If You Can: An Empirical Analysis of Android Platform Armoring Against Stalkerware, arXiv:2508.02454v1**

2025-08-04, retrieved 2026-11-13.
https://arxiv.org/abs/2508.02454v1

22. **Maier, Tanczer, Klausner, Surveillance Disguised as Protection: A Comparative Analysis of Sideloaded and In-Store Parental Control Apps, arXiv:2504.16087v1**

2025-03-08, retrieved 2026-11-13.
https://arxiv.org/abs/2504.16087v1

23. **Rogers, Fisher, Ali et al., Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review, *Trauma, Violence & Abuse***

2022, retrieved 2026-11-13.
https://doi.org/10.1177/15248380221090218

24. **Tseng, Sabet, Bellini et al., Care Infrastructures for Digital Security in Intimate Partner Violence, CHI 2022**

retrieved 2026-11-13.
https://doi.org/10.1145/3491102.3502038

25. **Mangeard, Tejaswi, Mannan et al., WARNE: A stalkerware evidence collection tool, *FSI: Digital Investigation***

2024, retrieved 2026-11-13.
https://doi.org/10.1016/j.fsidi.2023.301677