TRUST PASSING

Volume 4

Digital Safety Doesn’t Mean You’re Safe

This work was supported by a Societal Impact Seed Grant from the Office of the Vice-President, Research, McMaster University.

Research Project Lead

Andrea Zeffiro, Department of Communication Studies and Media Arts, Faculty of Humanities, McMaster University

Community Partner Lead

Jelena Vermilion, Executive Director, SWAP Hamilton

McMaster University Research Team

Alexis-Carlota Cochrane (Workshop Facilitation)

Natasha Malik (Asset Digitization)

Kathryn Waring (Rapid Literature Review)

Project Supporters

YWCA Hamilton

The Sherman Centre for Digital Scholarship, McMaster University

The Office of Community Engagement, McMaster University

Centre for Community Engaged Narrative Arts, McMaster University

Cite This Zine

Trustpassing. Volume 4: Safety Doesn't Mean You're Safe. [Zine]. Data analysis, curation and design, Andrea Zeffiro. McMaster University. Hamilton, Ontario, 2025.

not matter what your level of education is or where you are in life! Everyone matters. Participants passed their trust when they allowed their personal experiences to be curated into a collective narrative to be shared publicly. *I want all of Hamilton to read this, and maybe they will really understand how much we need more people to support our community.*

As communicated through the zines, the stories and insights about digital vulnerabilities are inseparable from access to material forms of security and safety. The zines provide insights rooted in the local context of Hamilton, Ontario, regarding how digital (in)securities and vulnerabilities are interconnected with material ones, including but not limited to emergency housing, sex workers' rights, job security, food security, childcare, services for migrants, newcomers and immigrants, access to mental health care and services, substance abuse and addiction support, policing and law enforcement, and access to safe spaces.

Trustpassing provides a starting point for formulating crucial questions about how end-users who already face social stigmas are included in digital security and safety frameworks, while also acknowledging how these folks become targets of invasive and unwarranted surveillance, often under the guise of security. The zines advocate for a community-centred approach to understanding and documenting (digital) risks, threats and harms as contextual, local and inseparable from material (in)securities.

To this end, *Trustpassing* amplifies the voices that are often excluded from or overlooked in dominant discussions that shape the criteria for digital harms, as experts equipped with the knowledge to reshape mainstream digital safety and security frameworks. *We are all survivors, surviving together. We are the life force*.

We extend our deep gratitude to the project participants for generously sharing their time, perspectives and experiences with us. Your contributions were invaluable, and this project would not have been possible without you. Thank you for your collaboration, insights and trust.

- Andrea Zeffiro

Trustpassing, as a concept, conveys the intricate interplay between safety and security that unfolds when determining whether to place trust in a person or entity. Often, we pass our trust to others knowingly and with active, ongoing consent. At other times, passing trust becomes necessary for participating in or accessing services. In such situations, we may find ourselves taking a leap of faith, as is often the case with social services and big tech companies. *How can you keep yourself safe from something you cannot see?* When we pass trust to someone or something, ideally, we are met with a sense of confidence and reliability. That person or entity will uphold a certain standard, remain dependable and act as expected. Trust-passing, in this sense, enables us to feel safe and secure even when we are vulnerable.

At the same time, trustpassing is a play on 'trespassing'. It signifies committing an offence against trust, breaking someone's trust. *I don't understand how security and safety work because they have never worked for me.* When our trust is broken, it can be a profoundly emotional experience. We can feel betrayed, powerless, angry, disappointed, and doubtful. *I worry that if the readers of the zines know the participants are accessing the YWCA then maybe they will respect the content less.* A breach of trust can impact our willingness to trust again. How do we collectively regain and repair trust? *These kinds of projects are important because I believe that everyone has a right to be heard, accepted, understood, recognized and treated with respect.*

In the context of this project, trustpassing carries several meanings. In the workshops, being together in a shared space and feeling comfortable in the company of others requires a certain level of trust. *Community is important. We feel connected to one another in this space.* Trust was exchanged among the participants and the research team through the sharing of individual narratives and experiences of negotiating safety and security in digital spaces. *I think it's important for people to hear honest truths that not everyone is aware of.* How do researchers establish and sustain trust with research participants? How can researchers balance data collection with fostering spaces of mutual care and trust? *It does*

Trustpassing is the culmination of a year-long research partnership between researchers at McMaster University and the Sex Workers' Action Program (SWAP) Hamilton. The aim of the project was to develop a zine-based workshop model to document and share insights from equity-deserving communities frequently left out of dominant discussions about digital harms and vulnerabilities.

Mainstream cybersecurity frameworks often perceive end-users in a generic way. We all encounter common threats, risks, and harms. By maintaining good 'cyber hygiene' we strengthen that first line of defence and ensure our safety. In this model, digital risks and threats are often framed as individual choices, placing the burden on end-users. You either failed to protect yourself adequately, made a mistake, were a willing participant, or even deserved the exploitation

This project takes a step back from viewing cybersecurity as a universal resource that benefits everyone equally, aiming to examine the cyber insecurities that are overlooked by mainstream models. How do cybersecurity frameworks identify and account for end-users who experience social stigmas? What are the varied impacts of digital safety and security across different social contexts? In what ways are digital (in)securities related to material security and access to basic necessities?

From January to May 2025, we hosted 11 workshops on Thursday evenings at the YWCA in downtown Hamilton, attracting a total of 220 participants. Most participants were accessing services at the YWCA for diverse personal needs. The first set of workshops concentrated on content generation through techniques such as collage and block-out poetry. In the second set, we worked with rough drafts of the zines, soliciting participants' feedback on content and other essential aspects, including intended audiences, outreach strategies, and dissemination plans.

This collaborative effort led to the creation of *Trustpassing,* a series of four zines that remix and curate personal reflections into collective narratives exploring the intersection of digital security, safety and broader social issues. The zines strive to make this shared knowledge more recognized, widely circulated, and integrated into mainstream discussions that shape our understanding of digital harms and vulnerabilities.

What is technology?

Is policing a form of technology? Is medicine a type of technology? Is science considered a technology? Sometimes, these work in your favour, but not always. It depends on your predicament and how you are perceived.

A range of people use technology in different ways across different age groups. Some people are being left out of the conversation. Not all realities are considered.

When I lived in ****, I would work near security cameras to track my whereabouts. There was a police constable who looked out for us, and it felt safe to do so. It isn't like that in every community. People understand security differently. I had a system with neighbours who would keep watch when I met a client at their car for a pre-interview and observe my place when I invited them in.

Security and safety are relative and depend on the context you're in. Digital safety doesn't mean you're safe! When you use tech on the streets, you can still disappear.

Tech doesn't keep you safe.

We need to protect our information.

We also need to protect our mental and physical well-being.

We need more resources to stay safe and secure in everything we do in life. It's difficult to keep working without resources.

We need accessible healthcare.

We need to change the language of sex work. Make it a professional designation with training and benefits. A professional companion or sensual artist. We aren't selling sex. We are selling time.

We need more secure spaces.

We need more user-friendly online platforms like Craigslist. Platforms can support safety and security because they reduce street-based work.

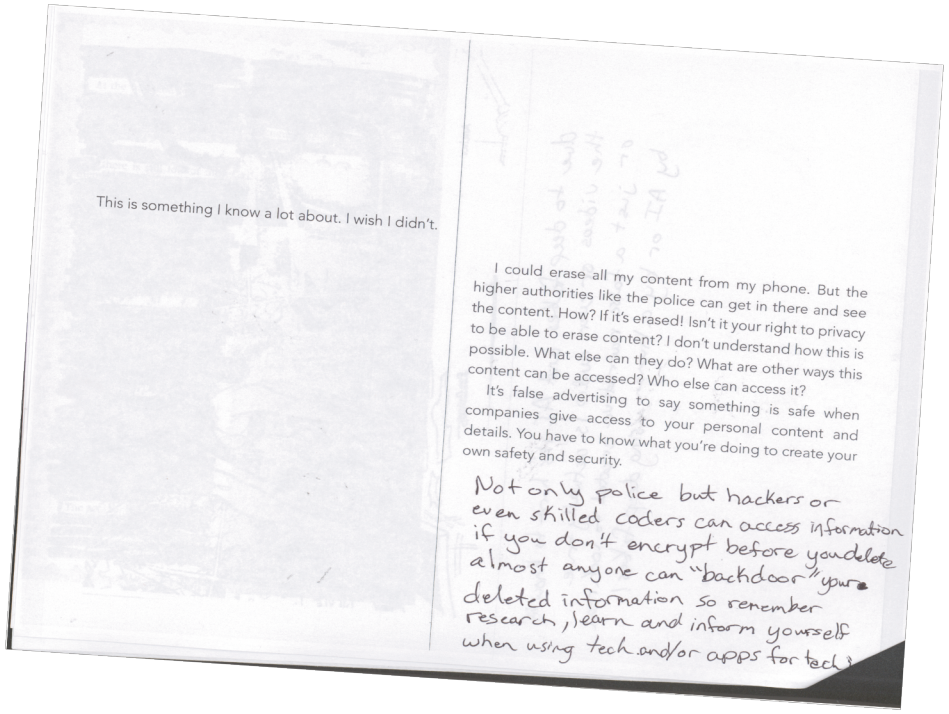
We need more pay phones.

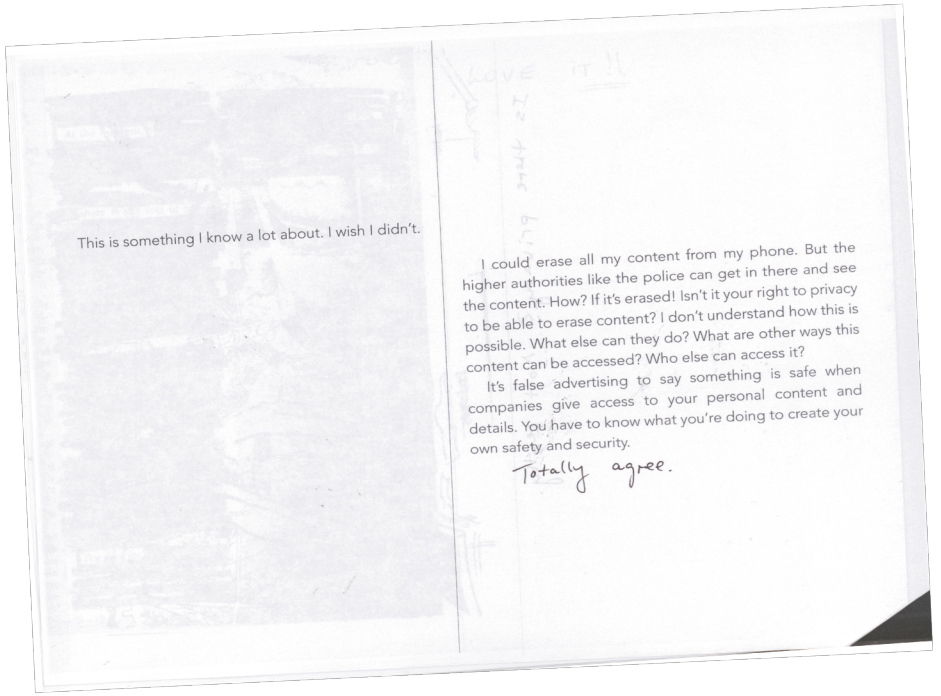
Tech is unsafe for me. I don't keep photos of my kid because pictures on my phone are risky. Not being seen keeps me safe when I am **** and ****. People can judge and think I am **** even when I am not.

No tech makes me feel safe. Being watched doesn't solve my problems. What is my phone going to do? Having a phone could make you a target.

Using cameras for work can be unsafe. What goes online stays online forever. There is a lot of uncertainty with long-distance work. How will the images or videos be used, and by whom? There is no delete button on the Internet.

Protect yourself.





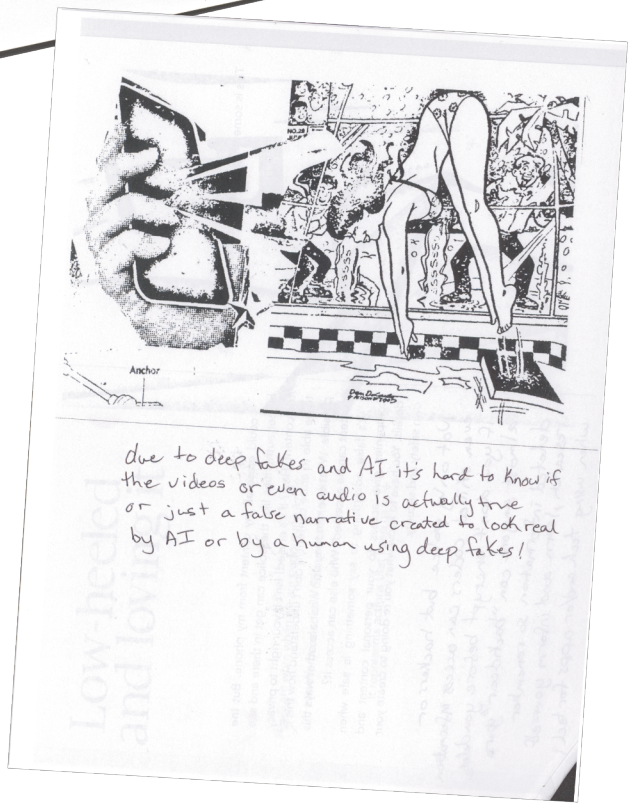
You have to know what you are doing and create your own safety and security. This is something I know a lot about. I wish I didn't.

I could erase all my content from my phone. But the higher authorities, like the police can get in there and see the content.

How? If it's erased! Isn't it your right to privacy to be able to erase content? I don't understand how this is possible. What else can they do? What are other ways this content can be accessed? Who else can access it?

It's false advertising to say something is safe when companies can access your personal content and details. You gotta make sure no one gets your shit!

Know your rights. Including your digital rights.



Cybersecurity is important because I don't usually feel safe, so I want to feel safe online. I used to like being online, but now I'm too scared to try.

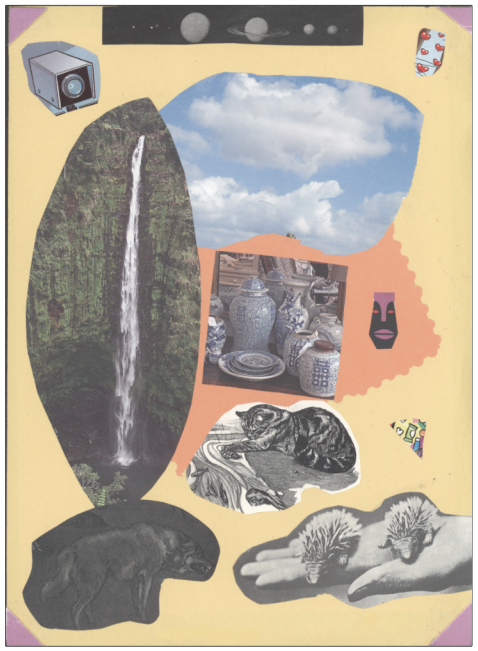
It's been three years since I had a cell phone for more than a month at a time because I don't want to worry about being stalked or hacked. I don't trust cell phones, which seem leaky.

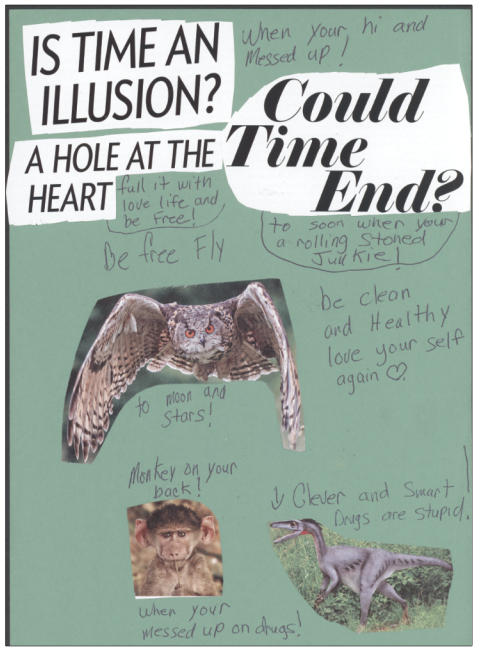
As safety and security measures, I shut down my accounts and avoided social media altogether. I stopped using the Internet because I didn't want to be caught. I don't trust anything because it makes it easier for them to find me.

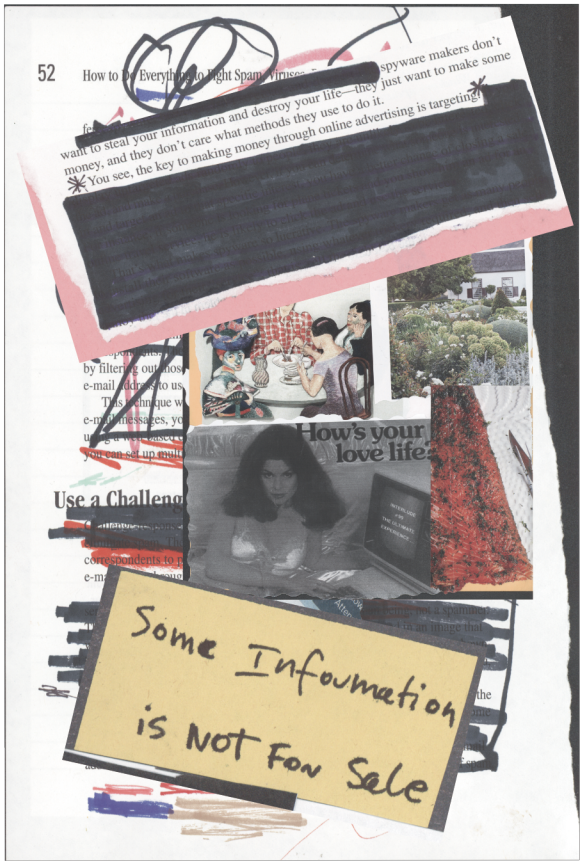
Much of our lives takes place with or within technology in some form or another, and our safety and well-being should always take priority. There are literally thousands of different ways we can be targeted. I want automatic safety when using technology.

Cybersecurity is something that should nowadays be in the same category as blinking or breathing. We need built in anonymity. We should be running our own show.


NOT HAPPY
NOT
SAFE




IS TIME AN ILLUSION?
A HOLE AT THE HEART
Could Time End?
when your hi and messed up!
Fill it with love life and be Free!
Be free Fly
to soon when your a rolling Stoned Junkie!
be clean and Healthy love your self again
to moon and stars!
Monkey on your back!
Clever and Smart Drugs are stupid.
when your messed up on drugs!


52
spyware makers don't want to steal your information and destroy your life—they just want to make some money, and they don't care what methods they use to do it.
You see, the key to making money through online advertising is targeting!
How's your love life?
Some Information is Not For Sale


Want to hear it again?
Safety!
CELEBRATE THE EARLY DAYS
Did WE THINK of CONSEQUENCE??
Veronica
Opinion
SEX WORK IS WORK!
SPLASH INTO THE HISTORIC HIJINKS!
DIGITAL
WAS IT RAPE?

Security is how you protect yourself.

* Have a dedicated number for work that is separate from your personal line.

* Protect your personal information, such as your name, home address, and personal cell number.

* Keep records of clients, including identifiers such as phone numbers and vehicle descriptions.

* Keep the data at home so the content is less likely to be confiscated in a raid.

* Protect your personal information with strong passwords.

* Make sure your devices are secure.

* Pay attention to software updates.

* Be cautious with WIFI.

* Use a VPN.

* Be cautious with how you share your information online. A lot can be done with a small amount of information.

* Keep your personal information private.

* Privacy is safety.

* You need a working phone. Make sure it is charged.

* Try not to work under the influence, if possible.

* Don’t go alone. Have a buddy system regardless of whether the work is digital or street-based.

* Always let someone know your plans: where you’re going, how to reach you, and who you’re with.

* Keep plenty of your supplies with you, like condoms and lube.

* Use locations that provide some safety, such as well-lit areas.

* Things might look safe. If you’re not sure about something, ask for help.

* Be careful and aware when interacting with people you don’t know and even those you do!

* Don’t go with people you don’t trust or aren’t comfortable with.

* Call 911 if something happens.

* Don’t trust anyone. You never know!

* Always trust your instincts.