TRUST PASSING

Volume 3

We All Feel Secure Until We Are Not

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 3: We All Feel Secure Until We Are Not. [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 around 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.

THE FACT THAT THE PAST IS SET IN STONE

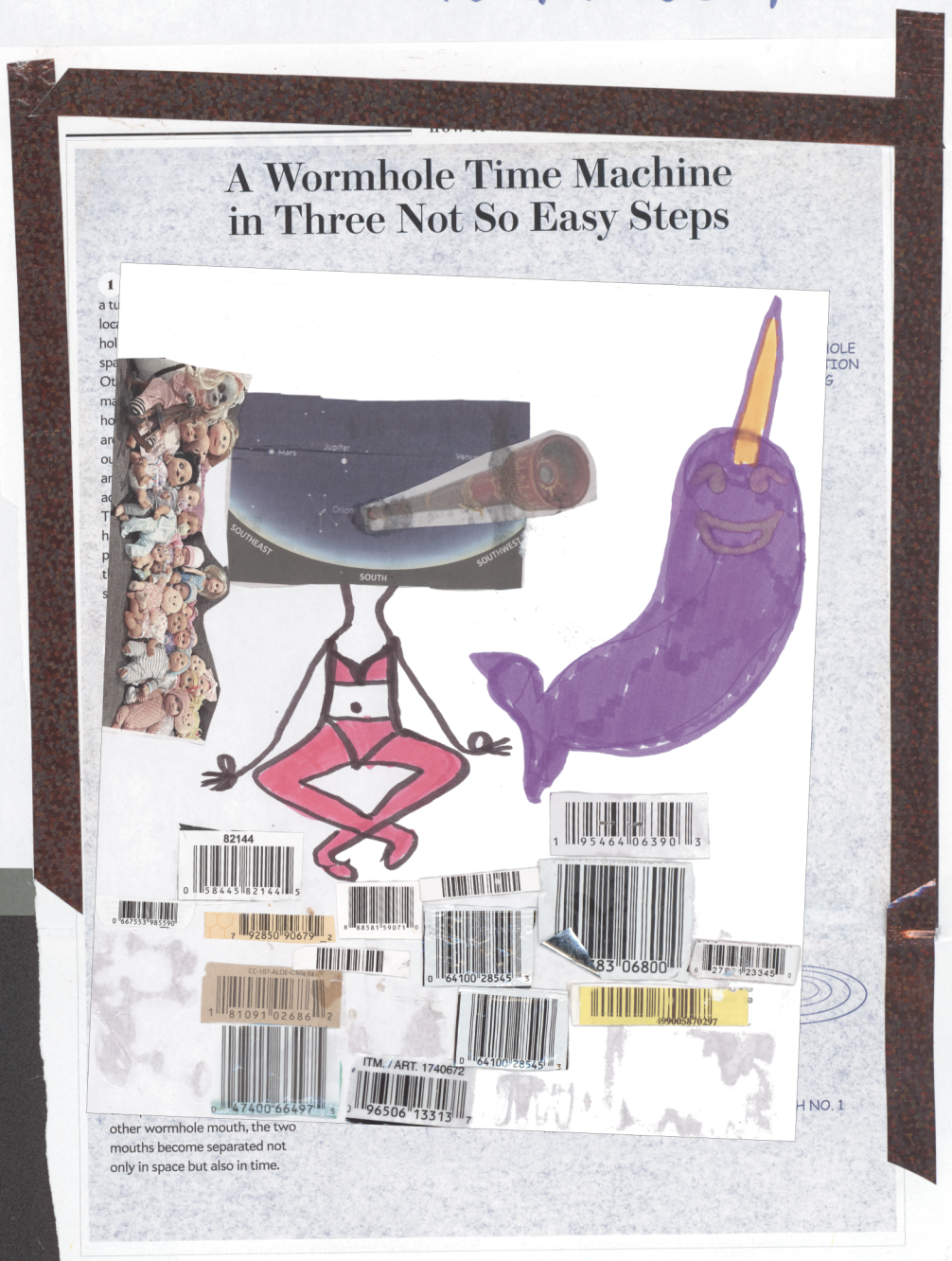
move safe places to go to stay safe

THE SAFETY IS SET ON SECURITY

- stay away from not safe places / protect others by spreading messages.

AND

TECHNOLOGY



Technology is advancing at a rapid pace. The movies we once watched as science fiction have now become reality. Everything seems amazing, but I wonder – what lies beneath it all?

In the past, during moments of boredom or free time, we used to imagine and create. Many inventions, like the wheel, were born in those moments of quiet reflection. But now, with all the screens, machines, and devices surrounding us, that empty time has vanished. We are so busy that we no longer have these pauses when creativity can naturally arise.

So, I ask myself: how will future inventions come to life if we no longer allow time for spontaneous thought?

Security is a big business.

Cyber security is supposed to protect personal information like banking details, passwords, and medical records from being compromised or stolen through online activities. It is supposed to ensure the security of my online accounts and safeguard my devices from malicious attacks, such as phishing emails or malware, which could disrupt access to essential services and information.

I try to avoid scam calls, but also get Canada Post and 407 scam texts. I'm not too familiar with safety strategies, but maybe understanding spam, protecting your email address, avoiding viruses, and using antivirus software would help.

Safety is being sold: VPNs, safety software.

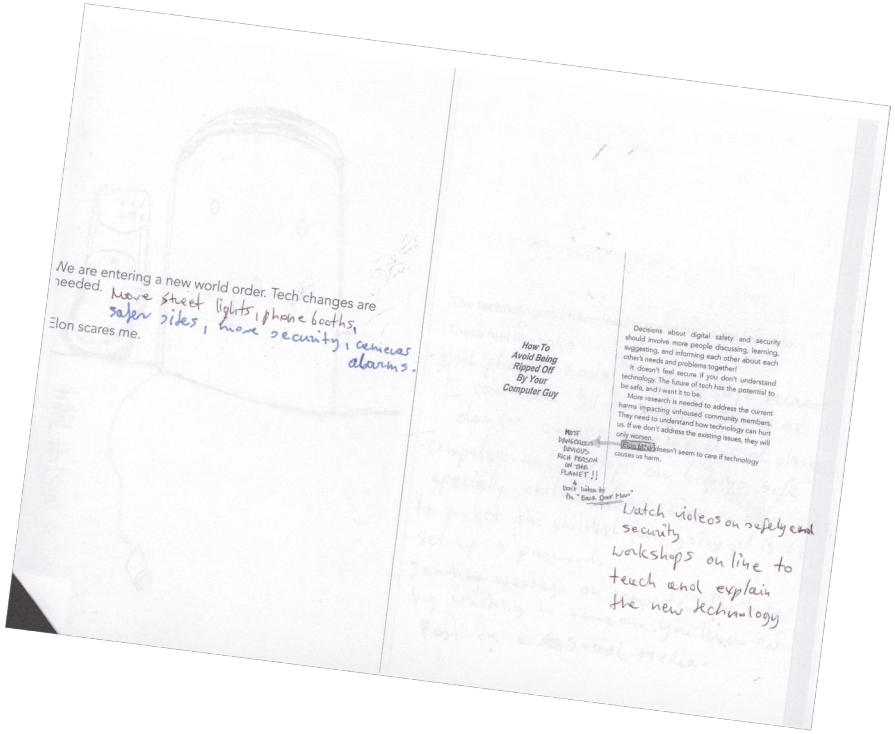
We all feel secure until we are not.

I never really considered it until the Hamilton data breach impacted programming, disrupting all communication.

Computer access at the library and services like Ontario Works were impacted, as everything now needs to happen online. Many people rely on those library services. No one could access the bus schedules online, and the digital signs didn't work, which caused a lot of confusion.

You couldn't use anything. Even public WiFi was spotty. I had no data at all. What was I supposed to do? It prevented me from applying to other government agencies. In my case, it interrupted my application for housing and identification.

We all felt the implications of the malware attack. It's rarely discussed how real people are impacted. I wish people understood how not having these basic services impacts us. It's dangerous, and safety is life or death.



Since new technology like AI is not yet regulated by laws, it is easier for others to invade personal space or security. From personal experience, I would say that in the right hands, technology could enhance one's daily life; however, in the wrong hands, the outcome could be disastrous, depending on the creator's motives. The security of AI is fleeting.

What kind of future will we have?

So much funding goes to tech development.

The government needs to smarten up and invest in the right things. Invest in the future. Our kids are our future! What will their futures be like?

More research is needed to address the current harms impacting unhoused community members. They need to understand how technology can hurt us. If we don't address the existing issues, they will only worsen. Elon M*sk doesn't seem to care if technology causes us harm.

We need more resources to learn how to stay safe and secure in everything we do in life.

* Homelife and family life.

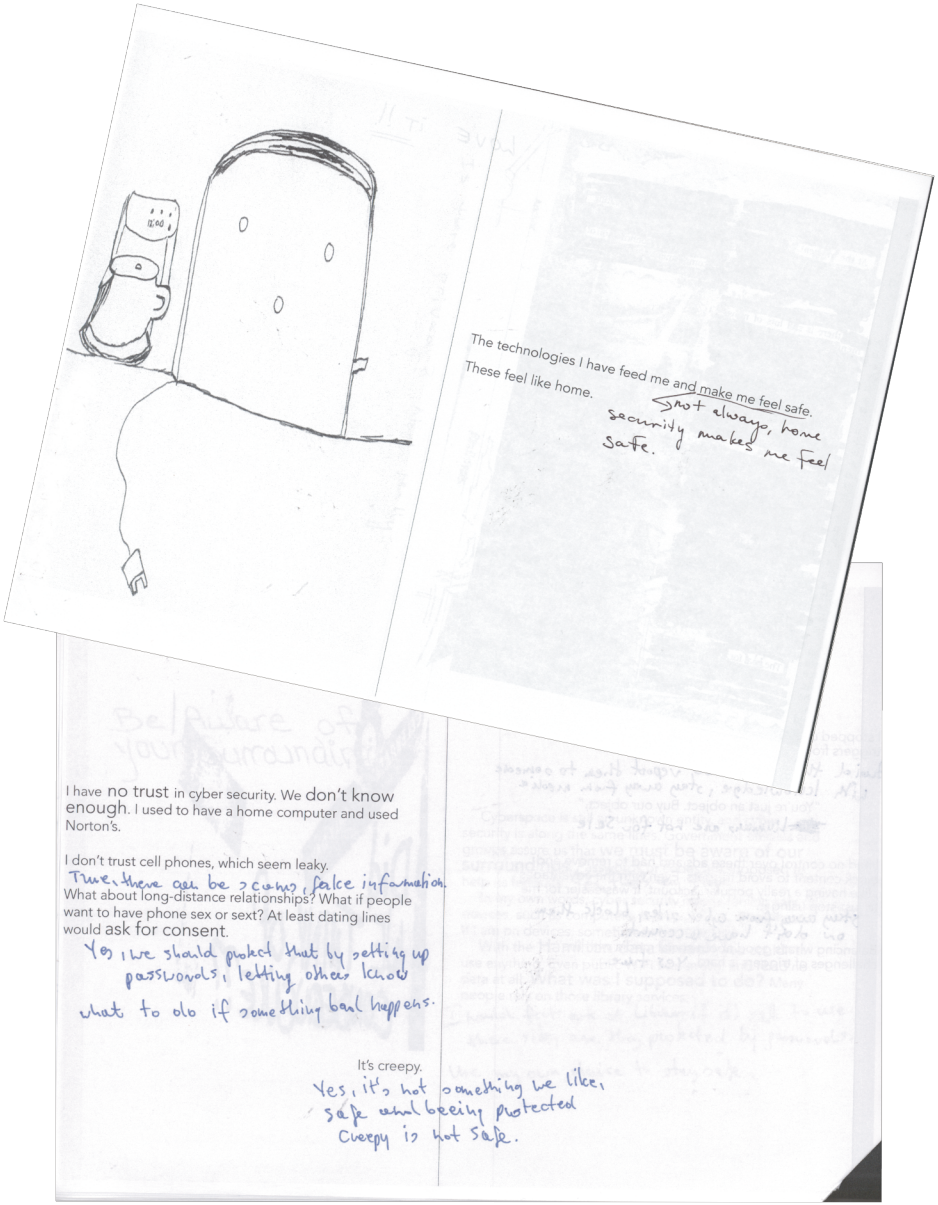
* Drugs, alcohol and partying.

* Healthy relationships with the people we let into our lives.

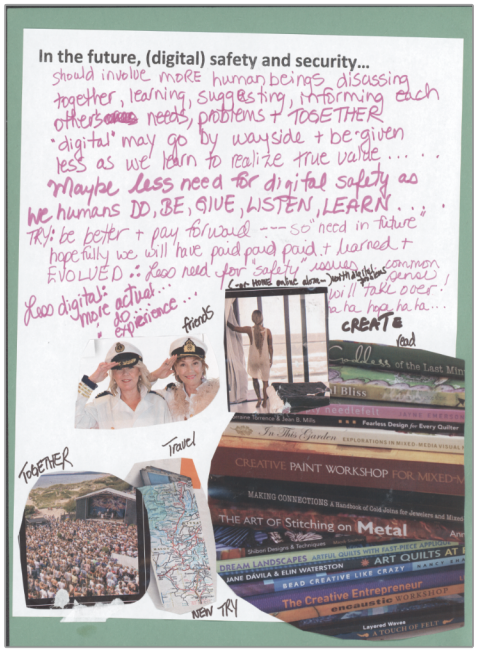
* Food and clothing supplies (e.g. food banks, churches, charities).

* The effects of anxiety and depression.

* Ultimately, taking care of your overall mental health (e.g. yoga exercise, meditation, sleep, reading, music, art).

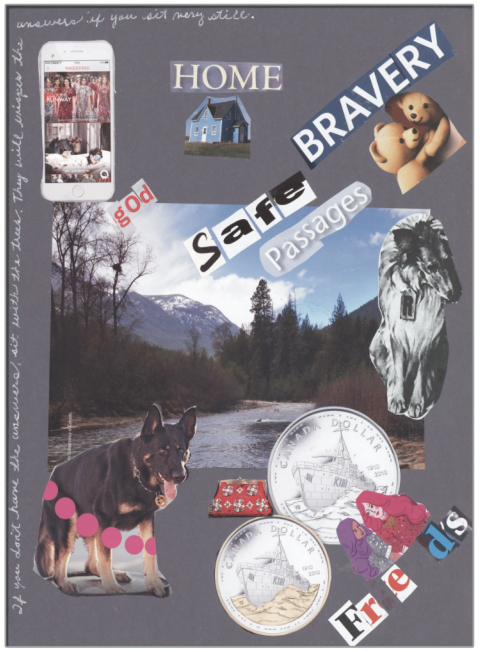



In the future, (digital) safety and security... Make a plan
digital
Online
Health & Fitness
Start small
Social
Find support
FREQUENCIES
People Threads
Be realistic
YOU CAN DO IT!
YOU CAN STILL CANCEL THAT FLIGHT


In the future, (digital) safety and security...
should involve MORE human beings discussing together, learning, suggesting, informing each others needs, problems + TOGETHER
"digital" may go by wayside + be given less as we learn to realize true value . . . .
Maybe less need for digital safety as we humans DO, BE, GIVE, LISTEN, LEARN . . .
TRY: be better + pay forward --- so need in future
hopefully we will have paid paid paid + learned + EVOLVED ∴ less need for "safety" issues
less digital: more actual . . . go experience . . .
CREATE
Travel
TOGETHER
NEW TRY


MULTIPLE EYES
Future
NEW ORDER
CAUTION
ESCAPE -
UNKNOWN!


SMART
Safety
A STRONGER LOVING WORLD
inspiration
Thanks For The Memories.
Community
THE TIMES THEY ARE A'CHANGING
LEARN
No place like home
INSIDE STORY
SPEAKING OUT


answers if you sit very still.
If you don't have the answers, ask within the book. They will inspire this
HOME
BRAVERY
god
Safe
Passages
friends


For the Love of Animals + Flowers
8 CUTEST CRITTERS

There is security in feeling tech safe...

What about job security?

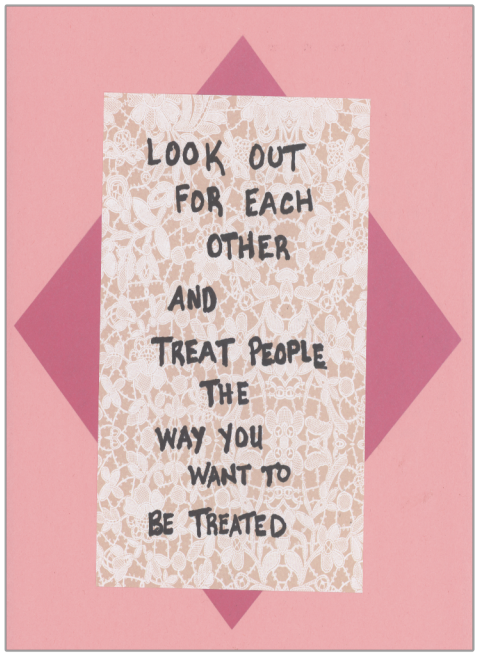
We need affordable housing for families. We need daycares.

A decrease in the cost of living is security! Times are so tough! There is too much homelessness going on, and it's getting worse, not better.

What about food security?! Access to healthy foods is security! Growing food is hard without housing. Eating healthy, being happy, and being in good health are forms of security and safety.

Digital safety and security can be achievements in health care, such as new ways of treating depression.

... but there is more than one security.



Decisions about digital safety and security should involve more people discussing, learning, suggesting, and informing one another about each other's needs and problems together!

Cover Myself in Shadow
of Light
My Mind has gone numb
Over a Series of time
Safe is not near
as others I fear
Will Know who I am

How is leading the charge against rising cyber threats

From protecting online users to educating the public, comprehensive cybersecurity efforts are helping secure Canada's digital future

Cybercriminals are increasingly adopting cutting-edge technologies, reshaping the landscape of digital threats. But the defenders aren't just reacting — they're taking the fight to the next level. Companies like have been using AI for over a decade to stay ahead of the curve, outthinking, outpacing, and outsmarting bad actors.

Over the past five years, the Canadian Centre for Cyber Security discovered that two-thirds of Canadians aged 15 or older experienced state-sponsored or financially motivated cyber incidents. For — who began his career at working on anti-malware products — it's all part of the job. He and his team work hard to protect Canadians by building bigger and better solutions.

Now, as director of software development and site lead in oversees a team dedicated to securing Canada's online ecosystem. They work around the clock to protect their products and users from ever-evolving threats. His team works on in for example, which safeguards billions of users from malicious sites and attacks. They also collaborate with businesses of all sizes, deploying advanced security measures to protect critical infrastructure. Beyond product security, they support local initiatives, fund research, and promote cybersecurity education across Canada to strengthen the entire digital landscape.

"We're being confronted more and more by the reality of the risks out there and the reality of hacks." "They're

As cyber threats continue to grow, efforts to enhance online security are helping keep Canadians safe with products such as