Technology

The Cyberattack That Stole 280,000 Identities – and Showed How Easily We Can Be Duped

Hackers are now using AI to mimic voices, deepfake executives, and drain accounts in minutes

BY KUNAL CHAUDHARY

Updated 8:33, Oct. 16, 2025 | Published 6:30, Oct. 16, 2025

Brain light / Alamy

EARLIER THIS YEAR, staff at Nova Scotia Power submitted a proposal to upgrade their cybersecurity. The privately owned company, which supplies most of the province's electricity, had gone three years since an internal threat assessment flagged key vulnerabilities, specifically the power plants and substations that fed the grid. If approved, the work would have wrapped by year's end.

They never got the chance. Just three weeks after the proposal was submitted, hackers struck. But not to sabotage infrastructure. Instead, they made off with the personal data of at least 280,000 customers: emails, phone numbers, home addresses, bank details—enough for determined malcontents to impersonate individuals and wreak havoc. Then came the shakedown. The company insists it didn't pay, and some of the plundered information was posted online. A few weeks after the attack was made public, a Nova Scotia couple, and clients of the utility, logged into their bank account and found $30,000 gone.

Nova Scotia Power is hardly an outlier. Ransomware gangs have turned public institutions into easy prey, breaking in, locking files, and holding them hostage for money. Refuse, and the information goes public. High-profile breaches include Alberta Dental Service Corporation and the Toronto District School Board.

The situation in the private sector is, if anything, more dire. Eighty-three percent of Canadian businesses surveyed by Telus in 2021 reported experiencing a ransomware attack. Nearly half admitted they paid up. In a recent report, the Canadian Centre for Cyber Security warns that ransomware is now "the top cybercrime threat facing Canada's critical infrastructure," with the average payout in 2023 exceeding $1 million. The wider toll is staggering: in 2024, Canadians lost more than $600 million to fraud and cybercrime—most of it tied to identity fraud, made possible by the kind of personal data stolen in the Nova Scotia Power attack.

While Canada has been slow to adapt to the threat, ransomware has raced ahead in the past five years, turbocharged by pandemic-related security challenges and advances in artificial intelligence. Today's malware is smarter, faster, and harder to detect. For organizations, these attacks can mean reputational damage, a loss of trust with employees and customers, and recovery costs that run into the millions. Globally, companies doled out a total of more than $1 billion in hacker payoffs in 2023.

But for victims, the attacks can translate into years of uncertainty and vulnerability as their most confidential records are bought and sold across the darkest corners of the web.

RANSOMWARE IS BASICALLY AS OLD as the World Wide Web. The first known attack came in 1989, when 20,000 copies of a floppy disk with what looked like AIDS-related research were mailed to researchers who had attended a World Health Organization AIDS conference. Instead, anyone who inserted it eventually found their computer locked and a note demanding up to $378, payable to a post office box in Panama. The culprit, a Harvard-educated evolutionary biologist and AIDS researcher named Joseph Popp, was arrested and charged with multiple counts of blackmail. He is widely considered the inventor of the form.

Ransomware evolved with the technology that enabled it. The rise of cryptocurrencies, like Bitcoin in the 2010s, gave cybercriminals an irreversible way to move huge sums of money. The spread of 5G and the "internet of things"—smart fridges, lights, locks, alarms—opened new doors for hackers, who could tunnel into broader systems through everyday devices. And while telecoms, tech giants, and public agencies rushed to fortify their defences, attackers kept circling back to one of the weakest links: people. Phishing emails and "malvertising"—infected ads—remained some of their most effective weapons.

By the end of the 2010s, ransomware had become a full-on business, with hackers selling their software to affiliates who ran attacks and split the profits. Kits went for as little as $40 a month, dramatically widening the field of criminals involved. While the affiliate model broadened the pool of targets and made it harder for law enforcement to trace viruses back to their creators, it also created headaches of its own: LockBit, once the world's most pervasive ransomware strain, issued a rare public apology after one of its affiliates hacked Toronto's Hospital for Sick Children, prompting the group to announce it severed ties with the affiliate.

It wasn't just freelancers cashing in. The affiliate model opened the door for foreign states—among them Russia, Iran, and China. North Korea, in particular, turned it into a revenue stream, reportedly pulling in an estimated $3 billion from cyberattacks between 2017 and 2023, money thought to be funding its nuclear ambitions.

And when COVID-19 hit, hackers were handed a windfall. Personal logins from remote work multiplied and, with them, millions of potential breach points. As criminals crept in through unsecured laptops and phones, the damage added up fast. From 2021 to 2023, total recovery costs for Canadian companies doubled from $600 million to $1.2 billion.

Then came generative AI. Ali Ghorbani, director of the Canadian Institute of Cybersecurity at the University of New Brunswick, says the technology has given hackers a new edge. They are now able to churn out countless variations of the same attack. It's also making phishing scams more convincing, with personalized emails, lifelike voice clips, and deepfake videos. In one case, an employee at a British engineering firm was duped into wiring $25 million (US) after a video call with AI-generated "executives."

All of this has rewritten the rules of ransomware. In 2019, mounting an attack took about sixty days. Today, it takes just four. "The attacks have gotten bigger," says Ghorbani. "And the ransoms have gotten bigger too."

RELATED LINKS:

- Big Tech Is Hiding the Environmental Cost of Chatbots
- ArriveCAN Was a Fiasco—and Just the Tip of Ottawa's Failing Tech Strategy

- The Indigo Cyberattack Is a Warning of Things to Come

CANADIAN INSTITUTIONS HAVE LAGGED. Between 2021 and 2023, the cost of recovery for businesses doubled, yet investment in preventative cybersecurity actually declined. Instead, companies are leaning on insurance: nearly one in four now count on policies to absorb hacker payouts. Paying after the fact can seem cheaper than preventing attacks in the first place.

A chronic shortage of talent isn't helping. As of 2021, Canada was missing 25,000 cybersecurity professionals, with one in six jobs unfilled. The pipeline is slow: it can take years of specialized education and training before recruits are ready for permanent roles, leaving critical positions vacant as the threats mount. Meanwhile, Ottawa's big legislative fix fizzled. Bill C-26, the government's first serious attempt to harden critical infrastructure, required key institutions in telecommunications, banking, and transportation, among others, to build defences. The bill died when Parliament was prorogued this past January. Its twin, Bill C-8, was tabled in June but must start the process all over again before it becomes law.

For the millions whose data has already been exposed—and the millions more still at risk—Canada's sluggish reforms are cold comfort. As Ghorbani puts it, once a breach happens, it can't be undone. "No matter what we say, mitigation is not possible." Customers have no way of knowing if their personal information is circulating on the dark web—and little power to stop it from being weaponized. "Any data has value, no matter how small," Ghorbani says. And once it's out there, criminals will find a way to use it.

A cancelled credit card number, for example, may lose much of its worth, but paired with a name and address, it can still fuel identity theft and fraud. In some cases, credit card payments can even slip through after cancellation if they are processed with certain vendors.

The response from institutions that lose their customers' data is often underwhelming. Nova Scotia Power, for instance, offered what has become the standard post-breach gesture: a few years of free credit monitoring, a service that flags changes in a credit file—like when a new card or line of credit is opened in your name. Customers also received a checklist of steps to reduce the chances of further compromise. There are few reports of actual compensation or reimbursement.

Ultimately, Ghorbani argues, the emphasis needs to shift to prevention, such as through public education and early investment by Canadian companies in their own defences. For individuals, that means simple but consistent habits: changing passwords, two-factor authentication, and keeping software up to date. For institutions, it means relying on in-house cybersecurity staff rather than outside consultants, training employees on best practices, and being careful about what customer data they keep. Yet even with stronger safeguards, Ghorbani warns, ransomware isn't going anywhere.

"We put locks on our houses and cars," he says. "Cybersecurity solutions work the same way." But unlike a lock you install once, this is a process without an end. "It's something that will be with us forever."

About Kunal Chaudhary (View All Articles)

Kunal Chaudhary is a journalist whose work has appeared in outlets such as *The Local*, the *West End Phoenix*, *The Breach*, *Spacing*, the *Globe and Mail*, and TVO. He is based in Toronto.