

Why cybercrime victims

don’t report to the police

Conclusions from Alpha 1 research for the “report a cybercrime” service

These conclusions are from four rounds of concept validation tests and interviews with victims and potential victims of cybercrime. In total, we spoke with 62 individuals who might identify as seniors, small business owners and employees, newcomers to Canada, and people with low digital literacy.

Why learn about people who don’t report?

During Discovery, the Canadian Digital Service, in partnership with the Royal Canadian Mounted Police, uncovered motivations (and subsequent needs) that victims and potential victims of cybercrime have for reporting a cybercrime. These included reporting for **altruistic** reasons, for **justice-seeking** reasons, and **to problem solve**. In Alpha 1, these findings were reaffirmed when speaking with people about their past experiences reporting cybercrime, and in gauging their expectations for a future public-reporting service.

In Alpha 1, we also discovered the reasons for why people may **not** report a cybercrime to law enforcement. Those reasons are:

* Victims are unsure if what they experienced was actually a crime;
* Victims don’t know what their options are for reporting;
* Victims had been disappointed or intimidated by law enforcement in the past.

*How does this knowledge help us build a service for the public?*

**When people are let down, confused, or overwhelmed by a reporting service, they become less likely to trust or engage with it in the future**. We investigated the barriers that cause people to give up, not return, or never reach a reporting service. This knowledge will help CDS & RCMP design a service for those who *should* report a cybercrime but cannot due to service-related barriers, or are unsure of the benefits of doing so.

The following pages seek to illuminate the journey that victims of cybercrime follow while reporting a cybercrime to the police (and the points along this journey where they may stop due to barriers or lack of knowledge). These learnings come from listening to victims’ past experiences in reporting crimes, and their expectations for a future public-reporting service.

# *(This header indicates points at which people stop reporting.)*

# 1) Before becoming victims, people take small steps to prevent cybercrime.

# If people have been exposed to the subject of cybercrime before, they tend to be wary of sharing their information online.

## People who have heard of scams, online fraud, or cybercrime, and those who have fallen victim to these crimes in the past, are wary and in some cases even fearful of interacting with forms online, (especially forms that ask for personal information). While testing a prototype at a senior centre, one woman told us that she would not put her information into a form field since it was just the kind of thing her son had warned her about. *“Is this a scam… I would treat this with some doubt,”* she told us.

**If the origin or the purpose or a site is not clear, individuals become worried that it may be a scam.** Repeat cybercrime victims are especially protective of their data, telling facilitators that *“they wouldn’t use this at home,”* when viewing early prototypes.

# Victims cope with cybercrime by taking small steps to deal with issues as they arise. They rely on people they trust for IT support and knowledge.

Victims take minor preventative measures, or adjust to the new norm:

**Many potential victims were unsure as to where to begin in terms of cybercrime prevention and maintenance.** One participant described *“things as fine the way they are”* despite being aware of the potential dangers of being hacked or scammed. Another stated that she tells her employees to *“delete [scam messages] as we go, because it’s so commonplace.”*

One newcomer to Canada stated that she had become very mistrustful of new contacts and messages. She told us that *“many people try [to scam me], but I trust no one.*” Another newcomer, a woman from Beijing, told us that *“there are many strange numbers on my phone, but I never open them.”*

**Victims of cybercrime develop coping mechanisms to do their best to control what they can. They find ways to navigate problems as they arise.** For many, their primary defense against cybercrime is to avoid engaging with the suspicious email, phone call, etc., ***if*** they have the knowledge to do so. This knowledge comes from having previously experienced a cybercrime, or from warnings from family, friends, and other trusted sources.

Victims will rely on IT experts, service providers, family, and friends that they really trust to bridge gaps in knowledge and best practices online.

Many newcomers to Canada and small business owners reported trusting banks and credit card companies as authorities to track down scammers or prevent issues. More information on the relationship between victims of cybercrime and banks and service providers can be found in the Discovery research.

# 2) When people become victims they may be unable to explain what just happened to them.

# Many cybercrime victims were very unsure if what they experienced was actually considered a crime.

This is often the case with low-impact crimes like recurring phone scams. Victims are also less likely to consider cybercrime a crime worth reporting if nothing was lost or damaged. **Nearly everyone we interviewed was unsure or curious about if what they had experienced was a crime.** While some asked us *“what is a cybercrime?”* others used their own experiences to better understand the definition: One person asked us *“what about\_\_\_\_\_\_\_\_\_\_, is that a scam?”*

This was discussed in Discovery Research as well.

Victims were also less likely to consider cybercrime an actual crime because they **blamed themselves for not being “careful”, or “tech-savvy” enough to prevent the event.** Some victims were ashamed of having lost money online and disappointed in themselves.

Some people define being a victim as having lost something:

A small group differentiated between *witnessing* an attempted scam, versus *falling victim* to a *“successful”* scam. Some described cybercrime events as *“failing”* if they had not lost money. Others described *“victims”* only as those who had lost something tangible, or were hurt. **There was a recurring belief that being taken advantage of is not a crime, and thus not worth reporting to the police.**

**Because victims don’t know what a cybercrime is (in legal terms), they don’t know who to turn to for help.**

# *People stop reporting when they are not aware that what they experienced warrants finding help. Or, when they are unable to find that help to begin with.*

The prototypes we shared with victims mentioned both the Royal Canadian Mounted Police, and the Government of Canada in the form of a banner across the top of the web-page.

From these prototypes we learned that some victims don’t know if there are agencies beyond the RCMP or the local police who are able to help them with their cybercrime-related issues. **There was confusion as to who would successfully help them after they became victims.**

The Government of Canada as an entity for supporting victims:

The Government of Canada inspires confidence in a service’s credibility for many victims of cybercrime. Victims have some degree of familiarity with what the GoC offers to them, (citizenship, passports, etc.). However, they have a limited idea of what to expect from online GoC services.

Law Enforcement as an entity for supporting victims:

Many victims cannot differentiate between the power and jurisdiction that local police have, and the RCMP at a national level. They generally view these organizations as “law enforcement” or “the police” and **thus often see them as powerful enough to stop most online scams.**

**Some victims want to speak with people face-to-face or via the phone for emotional reassurance and to tell their story.**

Victims almost always find comfort in knowing that they are not alone. Telling their story, or *“sharing it”* as one person described, helps alleviate the burden of being a victim and the sense of isolation that comes from being afraid, embarrassed, or ashamed. Talking, however, can be difficult for some people. Some victims want reassurance and encouragement to talk about their experiences openly and in greater detail. **When they felt safe, and felt that it wasn’t their fault, they opened up more and provided more details to the CDS + RCMP team.**

**Note:** In the next section we will be discussing the experience of people who report to the police. However, past research has shown us that many victims do not turn to the police to solve or seek help for cybercrime related issues. People also describe instances of ignoring the issue, reporting to banks and service providers, or seeking help from IT experts, family, and friends instead.

# 3) Victims reach out to law enforcement in seek of immediate help

# For many victims and potential victims, speaking with local police directly is the only way of contacting law enforcement that they have used before, or know of.

# They might call 911 or visit the police in-person because they either:

See it as the only way of contacting the police…

Many consider **calling 911 the only known point of entry to speaking with police** (aside for some, who mentioned that they had or would prefer to go to local police stations in-person). This is especially true for newcomers to Canada and those with limited experience with Canadian police.

…or believe that what they have just experienced is an emergency

**Victims measure the urgency of a cybercrime based on the potential for loss or damage.** One person told us that *“it’s an emergency because they* (the scammers) *have my credit card information,”* while another similarly stated that *“If I had provided credit card information to a scammer, I would call 911.”*

Many mentioned that they would seek help from the police if the scam was *“serious”*. Nearly all who mentioned wanting to see help from the police expected immediate, or near-immediate feedback.

A few victims that we spoke with told us that they could *not* foresee how a cybercrime could be a situation in which they might need urgent help. In general, this group had fallen victim to low-impact scams where little to nothing was lost.

**Several, when given the choice, chose to call or contact the police for help.**

# *For those who have had negative interactions with the police before, or minimal interactions, reporting a cybercrime to the police feels like a dead-end (especially for “problem solvers”).*

In early interviews, when speaking to several individuals about their past experiences reporting to the police, one person asked us quite directly *“can you go to the police? How will they stop it? There is a lot of grey area.”*

**4)** **Victims find reporting to the police a challenging process to navigate**

# Victims of cybercrime currently do a lot of guesswork when it comes to managing expectations and collecting evidence of a cybercrime. They navigate a lot of grey area.

It is challenging for victims to identify and collect evidence for the purpose of a report

**Victims find it challenging to collect evidence**, even if they feel they might know what evidence is useful. They have a hard time identifying and then saving information from cybercriminals. One man mentioned that maybe he could *“google the scammer’s info, or call the bank”* for it.

**Victims find it hard to know if what they have collected actually *is* evidence**. One woman who had been called several times by scammers asked a facilitator *“how do I know if this is the number of the suspect?”*

**Just as the definition of cybercrime is vague for the public, the definition of evidence is equally vague.** A potential victim had been nearly scammed through a fake kijiji ad for several thousand dollars. She felt that if she *had* been able to collect the scammer’s IP address she might have had enough evidence. She was unsure if the online and phone conversations she’d had with the scammer could or should be shared with police.

Victims also find it difficult to share evidence and information because they are either:

1. **In a state of confusion and/or elevated stress** and as a result become on high-alert of danger or potential danger. Those we spoke with at a local library found self-assessing the *“severity”* of their incident to be scary, or confusing.
2. **Are navigating a new or ambiguous process** and thus do not know what to expect or how to assess their situation from a technical point of view. One small-business owner told us that *“laws are hard to understand and read. I’m not going to be able to go through all this.”*

**Legal, policy-driven definitions of cybercrime, online scams, and fraud are vague, unclear, or simply unknown to the people who experience these crimes on a daily basis.** When victims are not prepared for what to expect next, whether if it is from page to page on an online tool or throughout an entire service, they find the process overwhelming or disappointing.

It is also challenging for many victims of cybercrime to separate discrete pieces of evidence (like messages, phone numbers, bank statements, etc.) from the story they want to share. Evidence is viewed as a support to the story of the experience.

# *People stop reporting when they do not have a clear understanding of what police need to open a case.*

# *People stop reporting when they are overwhelmed by an ambiguous process.*

# 5) Victims become “let-down” when the police don’t live up to their expectations and keep their trust

# *When victims complete a report, they expect follow-up and respect from the police. If this doesn’t happen, their faith becomes mistrust and they are not likely to report in the future.*

Many voiced that they were interested in reporting a cybercrime to law enforcement. For these victims, follow-up is a sign that an incident is being taken seriously.

When asking for follow-up of some sort (a phone-call, a message, etc.) one man who had had his email “hacked” on numerous occasions told us that **follow-up meant he had not only been taken seriously, but *“had been heard”* as wel**l.

One individual expected police to follow up by alerting the general public to the scam. They said it would show that the incident had been *“taken seriously… like the police are saying ‘we get you, and we’re on this.’”*

While some appreciated having a follow up option, they were unsure as to how it might be possible. One noted that *“the severity of my issue is what would warrant an interview”*.

**Those who have not been victims of cybercrimes before,** or are facing a particularly severe cybercrime, **have a very high expectation that law enforcement will express concern in ways that include following-up**, and stopping the crime where possible.

If police are not responsive to victims, victims avoid going to them for help when another incident occurs down the road.

|  |
| --- |
| Why Keeran does not report to the police anymore:  We also spoke with Keeran, a young man who, despite finding himself in the midst of a severe online harassment and stalking issue (that had been ongoing for several years), chose to not report the issue to the police.  He told us, *“I didn’t report because I didn’t see the possibility of a positive conclusion,”* and described to us the last time he chose to report a crime to the police: During a traumatic event in his past he had relied on the police for support and guidance. Instead, he felt that local law enforcement had been difficult to communicate with and dismissive of his fears. For Keeran, this meant experiencing an already traumatic event became all the more difficult, painful, and confusing. This wasn’t an experience he wanted repeated, despite his new circumstances, and despite needing help. Because he felt that the police had not prioritized his need for open communication and case updates during a previous incident, he no longer trusted them as a source of safety. |

**Victims stop reporting when the police do not meet their expectations or break their trust.** Like Keeran, who *“didn’t report because [he] didn’t see the possibility of a positive conclusion,”* many *v*ictims become emotionally exhausted, telling us that they stopped reporting past experiences because they *“didn’t see how things could get better”.*

Victims develop their own coping mechanisms when police *“ignore them,”* are unresponsive, or *“let them down”.*

Some newcomers find themselves in similar situations to Canadian citizens who no longer report as well. One individual, who nearly fell victim to a scammer posing as their son, told us thatshe hasn’t reported because *“the police don’t think it is important enough”.* These groups feel a **lack of connection to Canadian police due to language barriers, minimal presence in their communities, and a sense of being ignored.**