

Pourquoi les victimes de cybercriminalité ne font-elles pas de signalement à la police?

Conclusions de l’étude de la phase alpha 1 pour le service « Signaler un cybercrime »

Ces conclusions sont tirées de quatre séries de tests de validation de concept et d’entrevues avec des victimes et des victimes potentielles de la cybercriminalité. Au total, nous avons parlé à 62 personnes qui s’identifient comme étant des aînés, des propriétaires et des employés de petites entreprises, des nouveaux arrivants au Canada et des personnes ayant un faible niveau de littératie sur le plan technique.

# Pourquoi apprendre à connaître les personnes qui ne signalent pas les incidents?

Durant la phase Découverte, le Service numérique canadien, en partenariat avec la Gendarmerie royale du Canada, a découvert les motivations (et les besoins subséquents) qu’ont les victimes et les victimes potentielles de la cybercriminalité pour signaler un cybercrime. Les signalements avaient lieu notamment pour des raisons **altruistes**, de **recherche de justice** et de **résolution de problèmes**. Au cours de la phase alpha 1, ces constatations ont été réaffirmées lorsqu’on a parlé aux personnes de leurs expériences passées de signalement de cybercrime et lorsqu’on a évalué leurs attentes à l’égard d’un futur service de signalement destiné au public.

Au cours de la phase alpha 1, nous avons également découvert les raisons pour lesquelles les gens ne signalent **pas** un cybercrime aux organismes d’application de la loi. Ces raisons se présentent comme suit :

* les victimes ne savent pas trop si ce qu’elles ont vécu était vraiment un crime;
* les victimes ne savent pas quelles sont leurs options de signalement;
* les victimes avaient été déçues des services d’application de la loi dans le passé ou elles ont été intimidées par ces derniers.

*En quoi ces connaissances nous aident-elles à bâtir un service pour le public?*

**Lorsque les gens sont laissés pour compte, perplexes ou dépassés par un service de signalement, ils deviennent moins susceptibles de lui faire confiance ou d’y participer ultérieurement.** Nous avons examiné les obstacles qui poussent les gens à abandonner le signalement, à ne pas réutiliser un service de signalement ou à ne jamais s’y rendre. Ces connaissances aideront le Service numérique canadien (SNC) et la Gendarmerie royale du Canada (GRC) à concevoir un service pour ceux qui *devraient* signaler un cybercrime, mais qui ne peuvent pas le faire en raison d’obstacles liés au service, ou qui ne sont pas convaincus des avantages de le faire.

Les pages suivantes visent à mettre en lumière le parcours des victimes de cybercriminalité lorsqu’elles signalent un cybercrime à la police (et les étapes de ce parcours où elles peuvent interrompre le signalement en raison d’obstacles ou d’un manque de connaissances). Ces apprentissages découlent de l’écoute des expériences passées de signalement des victimes et de leurs attentes à l’égard d’un futur service de signalement destiné au public.

# *(Cet en-tête indique les points où les gens cessent de signaler un incident.)*

# 1) Avant de devenir des victimes, les gens font de petits gestes pour prévenir la cybercriminalité

# Si les gens ont déjà été exposés au sujet de la cybercriminalité, ils ont tendance à se méfier du partage de leurs renseignements en ligne.

## Les gens qui ont entendu parler d’escroqueries, de fraude en ligne ou de cybercriminalité, et ceux qui ont été victimes de ces crimes par le passé sont sur leurs gardes et, dans certains cas, craignent même de remplir des formulaires en ligne (surtout les formulaires qui demandent des renseignements personnels). Lors de la mise à l’essai d’un prototype dans un centre pour aînés, une femme nous a dit qu’elle n’inscrirait pas ses renseignements dans un champ de formulaire puisque c’était le genre de choses dont son fils l’avait prévenue. *« Est-ce une arnaque? Je traiterais ça avec une certaine méfiance »,* nous a-t-elle dit.

**S’il y a un manque de clarté sur la provenance ou le but d’un site Web, les gens craignent qu’il s’agisse d’une escroquerie.** Les victimes de cybercrimes répétés protègent particulièrement leurs données et lorsqu’elles consultent les prototypes, elles disent aux facilitateurs qu’elles *« n’utiliseraient pas ça à la maison »*.

# Les victimes affrontent la cybercriminalité par de petits gestes qui règlent les problèmes à mesure qu’ils surviennent. Elles comptent sur des personnes en qui elles ont confiance pour obtenir du soutien et des connaissances en matière de TI.

Les victimes prennent des mesures de prévention mineures ou s’adaptent à la nouvelle norme :

**De nombreuses victimes potentielles ne savaient pas trop par où commencer en ce qui a trait à la prévention et au soutien en matière de cybercriminalité.** Un participant a décrit que *« les choses étaient bien comme elles sont* », même s’il était conscient des dangers potentiels du piratage ou de la fraude. Une autre participante a mentionné avoir dit à ses employés de « *supprimer [les messages d’escroquerie] au fur et à mesure, parce que c’est tellement courant*».

Une nouvelle arrivante au Canada a déclaré beaucoup se méfier des nouveaux contacts et des nouveaux messages. Elle nous a dit : *« Beaucoup de gens essaient [de m’escroquer], mais je ne fais confiance à personne. »* Une autre femme, nouvelle arrivante de Beijing, nous a dit : *« Il y a souvent des numéros inconnus dans mon téléphone, mais je ne les ouvre jamais. »*

**Les victimes de la cybercriminalité élaborent des mécanismes d’adaptation pour contrôler du mieux qu’elles peuvent ce qu’elles peuvent contrôler. Elles trouvent des façons de faire face aux problèmes à mesure qu’ils surviennent.** Pour bon nombre d’entre elles, leur principal moyen de défense contre la cybercriminalité consiste à éviter d’interagir avec le courriel, l’appel téléphonique suspect ou autre ***si*** ellesont les connaissances nécessaires pour le faire. Cette connaissance vient d’une expérience passée de la cybercriminalité ou d’avertissements provenant de la famille, d’amis et d’autres sources de confiance.

Les victimes comptent sur des experts en TI, des fournisseurs de services, des membres de leur famille et des amis en qui elles ont vraiment confiance pour combler leurs lacunes en matière de connaissances et de pratiques exemplaires en ligne.

Beaucoup de nouveaux arrivants au Canada et de propriétaires de petites entreprises ont dit faire confiance aux banques et aux compagnies émettrices de cartes de crédit pour repérer les fraudeurs ou prévenir les problèmes. Vous trouverez de plus amples renseignements sur la relation entre les victimes de la cybercriminalité et les banques et les fournisseurs de services dans l’étude de la phase Découverte.

# 2) Lorsque les gens deviennent des victimes, ils peuvent être incapables d’expliquer ce qui vient de leur arriver

# De nombreuses victimes de la cybercriminalité ne savaient pas trop si ce qu’elles avaient vécu était vraiment considéré comme un crime.

C’est souvent le cas pour les crimes à faible incidence, comme les arnaques téléphoniques récurrentes. Les victimes sont également moins susceptibles de considérer la cybercriminalité comme un crime valant la peine d’être signalé si rien n’a été perdu ou endommagé. **Presque toutes les personnes que nous avons interviewées étaient incertaines ou curieuses de savoir si ce qu’elles avaient vécu était un crime.** Certaines nous ont demandé ce qu’était un cybercrime. D’autres ont utilisé leurs propres expériences pour mieux comprendre la définition. Une personne nous a demandé : « *Qu’en est-il de \_\_\_\_\_\_\_\_\_\_? Est-ce de l’escroquerie?*»

Cette question a également été abordée lors de l'étude de la phase Découverte.

Les victimes étaient également moins susceptibles de considérer la cybercriminalité comme un crime réel parce qu’elles **se blâmaient de ne pas être suffisamment « prudentes » ou « technophiles » pour prévenir l’incident.** Certaines victimes avaient honte d’avoir perdu de l’argent en ligne et étaient déçues d’elles-mêmes.

Certaines personnes définissent le fait d’être une victime comme le fait d’avoir perdu quelque chose :

Un petit groupe de personnes a fait la distinction entre être *témoin* d’une tentative d’escroquerie et être *victime* d’une escroquerie *« réussie*». Certaines personnes ont décrit les cybercrimes comme des *« échecs »* s’ils n’avaient pas perdu d’argent. D’autres ont uniquement décrit les *« victimes »* comme celles qui avaient perdu quelque chose de tangible ou qui avaient été blessées. **Il y avait une croyance récurrente selon laquelle le fait d’être exploité n’est pas un crime, et qu’il ne vaut donc pas la peine de signaler un tel incident à la police.**

**Comme les victimes ne savent pas ce qu’est un cybercrime (en termes juridiques), elles ne savent pas vers qui se tourner pour obtenir de l’aide.**

# *Les gens cessent de faire des signalements lorsqu’ils ne savent pas que leur expérience justifie la recherche d’aide, ou encore, lorsqu’ils sont incapables de trouver cette aide au départ.*

Les prototypes que nous avons montrés aux victimes mentionnaient à la fois la Gendarmerie royale du Canada et le gouvernement du Canada sous la forme d’une bannière en haut de la page Web.

Grâce à ces prototypes, nous avons appris que certaines victimes ignorent s’il y a des organismes autres que la GRC ou le service de police local qui peuvent les aider à régler leurs problèmes de cybercriminalité. **Il y avait une confusion quant à savoir quel organisme allait réussir à les aider une fois qu’elles sont victimes.**

Le gouvernement du Canada en tant qu’entité chargée de soutenir les victimes :

Le gouvernement du Canada (GC) inspire confiance en la crédibilité d’un service pour de nombreuses victimes de cybercriminalité. Les victimes connaissent un peu ce que le GC leur offre (citoyenneté, passeports, etc.). Toutefois, ils ont une idée limitée de ce à quoi ils peuvent s’attendre des services en ligne du GC.

Les organismes d’application de la loi en tant qu’entité chargée de soutenir les victimes :

De nombreuses victimes ne peuvent pas faire la distinction entre le pouvoir et la compétence des services de police locaux et ceux de la GRC à l’échelle nationale. Elles considèrent généralement ces organisations comme des « organismes d’application de la loi » ou la « police » et **les croient donc souvent suffisamment puissantes pour mettre fin à la plupart des fraudes en ligne**.

**Certaines victimes veulent parler aux gens en personne ou par téléphone pour se rassurer et raconter leur histoire.**

Les victimes trouvent presque toujours du réconfort à savoir qu’elles ne sont pas seules. Raconter son histoire ou « *la partager*», comme une personne l’a décrit, aide à alléger le fardeau d’être une victime et le sentiment d’isolement qui découle de la peur, de l’embarras ou de la honte. Toutefois, il peut être difficile pour certaines personnes d’en parler. Certaines victimes veulent être rassurées et encouragées à parler de leurs expériences ouvertement et en détail. **Lorsqu’elles se sentaient en sécurité et qu’elles estimaient que ce n’était pas leur faute, elles communiquaient davantage et fournissaient plus de détails à l’équipe du SNC et de la GRC.**

**Remarque**: Dans la prochaine section, nous discuterons de l’expérience des personnes qui font un signalement à la police. Toutefois, des recherches antérieures nous ont montré que de nombreuses victimes ne se tournent pas vers la police pour résoudre des problèmes liés à la cybercriminalité ou pour obtenir de l’aide à cet égard. Les gens décrivent aussi des cas où ils ont ignoré le problème, fait un signalement aux banques et aux fournisseurs de services, ou demandé l’aide d’experts en TI, de membres de la famille et d’amis.

#

# 3) Les victimes s’adressent aux organismes d’application de la loi pour obtenir une aide immédiate

# Pour de nombreuses victimes et victimes potentielles, parler directement au service de police local est le seul moyen de communiquer avec les organismes d’application de la loi qu’elles ont déjà utilisé ou qu’elles connaissent.

# Elles risquent de composer le 911 ou de visiter le service de police en personne pour les raisons suivantes :

Elles croient que c’est la seule façon de communiquer avec la police...

Nombreux sont ceux qui considèrent **le 911 comme le seul point d’entrée connu pour parler à la police** (mis à part certaines personnes qui ont mentionné qu’elles s’étaient déjà rendues, ou préféreraient se rendre, aux postes de police locaux en personne). Cela est particulièrement vrai pour les nouveaux arrivants au Canada et ceux qui ont une expérience limitée de la police canadienne.

… ou elles croient que ce qu’elles viennent de vivre est une urgence.

**Les victimes mesurent l’urgence d’un cybercrime en fonction du potentiel de perte ou de dommage.** Une personne nous a dit : *« C’est une urgence parce qu’ils* (les fraudeurs) *ont les renseignements de ma carte de crédit. »* Une autre personne nous a dit quelque chose de semblable : « *Si j’avais fourni des renseignements de carte de crédit à un escroc, je composerais le 911.*»

De nombreuses personnes ont dit qu’elles demanderaient de l’aide à la police si l’escroquerie était *« grave »*. Presque toutes celles qui ont dit vouloir obtenir l’aide de la police s’attendaient à recevoir une rétroaction immédiate ou presque immédiate.

Quelques victimes à qui nous avons parlé nous ont dit qu’elles ne pouvaient *pas* imaginer comment un cybercrime pourrait être une situation nécessitant une aide urgente. En général, ce groupe a été victime d’escroqueries à faible incidence n’ayant engendré que peu ou pas de perte.

**Plusieurs victimes, lorsqu’on leur a donné le choix, ont choisi de communiquer avec la police pour obtenir de l’aide.**

# *En ce qui concerne les victimes qui ont eu des interactions négatives ou des interactions minimales avec la police auparavant, signaler un cybercrime à la police semble être une voie sans issue (surtout pour les « solutionneurs »).*

Au cours des premières entrevues, lorsqu’on a parlé à plusieurs personnes de leurs expériences passées de signalement à la police, une personne nous a demandé de façon assez directe : « *Pouvez-vous vous adresser à la police? Comment va-t-elle empêcher qu’un crime soit commis? Il y a beaucoup de zones grises. »*

**4) Les victimes trouvent difficile de s’y retrouver dans le processus de signalement à la police**

# À l’heure actuelle, les victimes de cybercriminalité font beaucoup de conjectures lorsqu’il s’agit de gérer les attentes et de recueillir des preuves de cybercriminalité. Elles traversent plusieurs zones grises.

Il est difficile pour les victimes de déterminer et de recueillir des éléments de preuve aux fins d’un signalement.

**Les victimes trouvent difficile de recueillir des preuves, même si elles estiment qu’elles pourraient savoir quelles preuves sont utiles.** Elles ont de la difficulté à identifier les cybercriminels et à en sauvegarder l’information. Un homme a mentionné qu’il pourrait peut-être *« chercher l’information du fraudeur dans Google, ou appeler la banque ».*

**Les victimes ont du mal à savoir si les éléments recueillis *constituent vraiment* une preuve.** Une femme qui avait été appelée à plusieurs reprises par des escrocs a demandé à un facilitateur : *« Comment puis-je savoir s’il s’agit du numéro du suspect? »*

**Comme la définition de la cybercriminalité est vague pour le public, la définition de la preuve est tout aussi vague.** Une victime potentielle a presque été victime de fraude pour plusieurs milliers de dollars dans une fausse annonce de Kijiji. Selon elle, si elle avait été en mesure de recueillir l’adresse IP du fraudeur, elle aurait peut-être eu suffisamment de preuves. Elle ne savait pas si les conversations en ligne et téléphoniques qu’elle avait eues avec le fraudeur pouvaient ou devaient être communiquées à la police.

De plus, les victimes ont de la difficulté à communiquer des preuves et des renseignements pour les raisons suivantes :

1. **Elles sont dans un état de confusion ou de stress élevé** et, par conséquent, elles deviennent très alertes au danger ou au danger potentiel. Les personnes à qui nous avons parlé dans une bibliothèque locale ont trouvé que l’auto-évaluation de la « gravité » de leur incident faisait peur ou prêtait à confusion.
2. **Elles naviguent dans un processus nouveau ou ambigu** et ne savent donc pas à quoi s’attendre ou comment évaluer leur situation d’un point de vue technique. Un propriétaire de petite entreprise nous a dit : *« Les lois sont difficiles à comprendre et à lire. Je ne vais pas pouvoir passer tout ça en revue. »*

**Les définitions juridiques et politiques de la cybercriminalité, des escroqueries en ligne et de la fraude sont vagues, imprécises ou tout simplement inconnues des personnes qui subissent ces crimes quotidiennement.** Lorsque les victimes ne savent pas à quoi s’attendre, que ce soit d’une page à l’autre dans un outil en ligne ou tout au long d’un service, elles trouvent le processus accablant ou décevant.

Il est également difficile pour de nombreuses victimes de cybercriminalité de séparer des éléments de preuve distincts (comme des messages, des numéros de téléphone, des relevés bancaires, etc.) de l’histoire qu’elles veulent communiquer. Les preuves sont considérées comme un appui à l’histoire de l’expérience.

# *Les gens cessent de signaler les incidents lorsqu’ils ne comprennent pas clairement ce dont la police a besoin pour ouvrir un dossier.*

# *Les gens cessent de faire des signalements lorsqu’ils sont dépassés par un processus ambigu.*

# 5) Les victimes se sentent « délaissées » lorsque la police n’est pas à la hauteur de leurs attentes et ne peut conserver leur confiance

# *Lorsque les victimes font un signalement, elles s’attendent à un suivi et au respect de la police. Lorsque ce n’est pas le cas, la confiance se transforme en méfiance et il est peu probable qu’elles effectuent un signalement à l’avenir.*

De nombreuses victimes ont dit qu’elles souhaitaient signaler un cybercrime aux organismes d’application de la loi. Pour ces victimes, le suivi est un signe qu’un incident est pris au sérieux.

Un homme dont le courriel avait été « piraté » à de nombreuses occasions a demandé un suivi quelconque (un appel téléphonique, un message, etc.). Il nous a dit que le **suivi signifiait non seulement qu’il avait été pris au sérieux, mais aussi qu’il avait *« été entendu »*.**

Une personne s’attendait à ce que la police assure un suivi en informant le grand public de l’escroquerie. Selon elle, cela montrerait que l’incident avait été « *pris au sérieux… comme si les policiers disaient : “Nous vous comprenons et nous nous chargeons de l’affaire” ».*

Bien que certaines personnes aient aimé le fait d’avoir une option de suivi, elles ne savaient pas trop comment cela pourrait être possible. L’une d’elles a mentionné : *« La gravité de mon problème est ce qui justifierait une entrevue. »*

**Les personnes qui n’ont jamais été victimes de cybercriminalité** ou qui sont confrontées à une cybercriminalité particulièrement grave **s’attendent très fortement à ce que les organismes d’application de la loi expriment leurs préoccupations par des moyens comme le suivi** et la lutte contre le crime, dans la mesure du possible.

Si les services de police ne répondent pas aux victimes, celles-ci évitent d’y retourner pour obtenir de l’aide lorsqu’un autre incident survient.

|  |
| --- |
| Voici pourquoi Keeran ne signale plus les incidents à la police :Nous avons aussi parlé à Keeran, un jeune homme qui, malgré un grave problème de harcèlement et de traque en ligne (sur plusieurs années), a choisi de ne pas signaler le problème à la police. Il nous a dit : « *Je n’ai pas signalé l’incident parce que je ne voyais pas la possibilité d’une conclusion positive »*. Il nous a décrit la dernière fois où il a choisi de signaler un crime à la police. Au cours d’un événement traumatisant de son passé, il s’était fié à cette dernière pour obtenir du soutien et des conseils. Il estimait qu’il avait été plutôt difficile de communiquer avec la police locale et qu’on avait ignoré ses craintes. Pour Keeran, cela signifiait qu’un événement déjà traumatisant devenait plus difficile, douloureux et déroutant. Ce n’était pas une expérience qu’il voulait répéter, malgré les nouvelles circonstances et malgré son besoin d’aide. Comme il estimait que la police n’avait pas donné priorité à ses besoins de communication ouverte et de suivi au cours d’un incident précédent, il ne la considérait plus comme une source de sécurité.  |

**Les victimes cessent de dénoncer les crimes lorsque la police ne répond pas à leurs attentes ou trahit leur confiance.** Comme Keeran, qui *« n’a pas fait de signalement parce qu’il ne voyait pas la possibilité d’une conclusion positive »,* de nombreuses victimes deviennent épuisées sur le plan émotionnel, nous disant qu’elles ont cessé de signaler des expériences passées parce qu’elles *« ne voyaient pas comment les choses pourraient s’améliorer ».*

Les victimes élaborent leurs propres mécanismes d’adaptation lorsque la police *« les ignore »*, ne réagit pas ou *« les laisse tomber »*.

Certains nouveaux arrivants se retrouvent dans des situations semblables à celles de citoyens canadiens qui ne font plus de signalement. Une personne, qui a presque été victime d’un escroc se faisant passer pour son fils, nous a dit qu’elle ne l’avait pas signalé parce que *« la police ne croit pas que c’est assez important »*. Ces groupes ressentent un **manque de lien avec la police canadienne à cause des barrières linguistiques, d’une présence minimale dans leurs collectivités et du sentiment d’être ignorés.**