RCMP

ROYAL CANADIAN MOUNTED POLICE

Guide to
Filing a Cybercrime Complaint

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

The aim of this handbook is to explain the cybercrime complaint and investigative process. It highlights the benefits of filing a complaint with law enforcement. It will also facilitate the process of filing a complaint to ensure critical information is forwarded to law enforcement as quickly and efficiently as possible. The guidelines shared in this booklet are, in the RCMP's experience, critical to ensuring successful investigations and prosecutions.

CONTENTS

01 Introduction

02 RCMP Approach to Combatting Cybercrime

05 Filing a Complaint

10 The Investigative Process

12 Contacts

INTRODUCTION

THE ROYAL CANADIAN MOUNTED POLICE (RCMP) defines cybercrime as any crime where the internet and digital technologies, such as computers, tablets, and smartphones, have a substantial role in the commission of a criminal offence. It includes technically advanced crimes that exploit vulnerabilities found in digital technologies. It also includes more traditional crimes that take on new shapes in cyberspace.

The RCMP breaks cybercrime into two categories:

TECHNOLOGY-AS-TARGET

where a computer, network or the internet are targets of a criminal act, such as the unauthorized access of computers or data. Examples of technology-as-target crimes include using malware, hacking for passwords and banking information, and denial of service attacks.

TECHNOLOGY-AS-INSTRUMENT

where a computer, a network or the internet is the tool or modus operandi of a criminal offence. This generally involves traditional crimes, such as fraud, identity theft and extortion. Examples of technology-as-instrument crimes include online scams (i.e. phishing and identity theft), DarkNet markets, and money laundering.

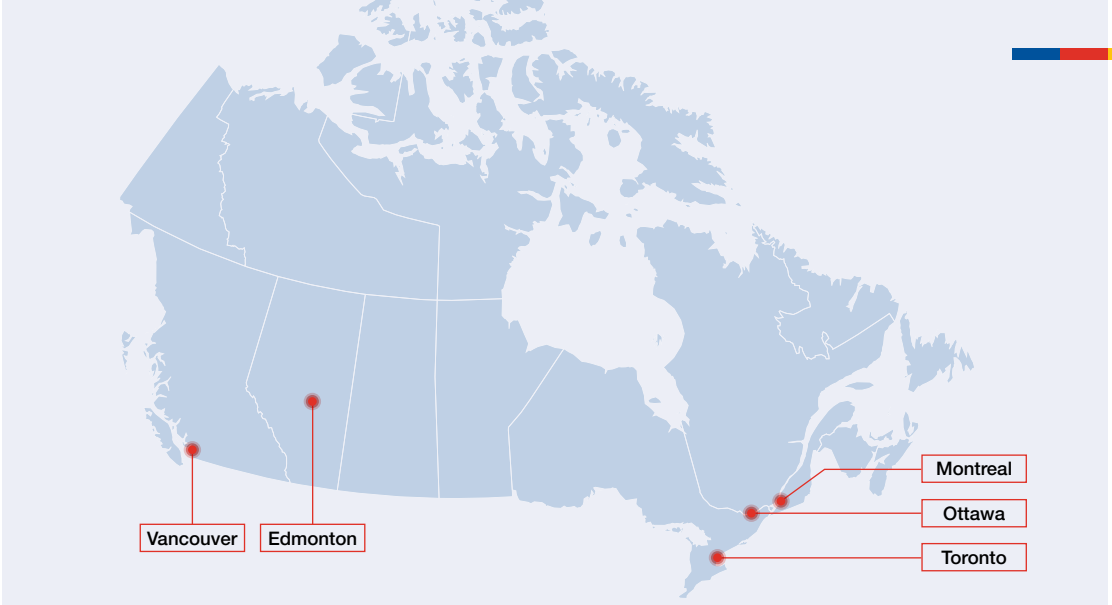
In order to successfully investigate and undertake cybercrime investigations and court proceedings the RCMP requires substantial assistance from our industry partners, who are in the best position to detect cybercrime.

RCMP APPROACH TO COMBATTING CYBERCRIME

RCMP Federal Policing Cybercrime Mandate

The RCMP Federal Policing (FP) cybercrime investigative mandate targets the most significant threats to Canada's political, economic, social, and reputational integrity. The FP cybercrime mandate focuses on criminal activity that:

1. Targets the federal government
2. Threatens Canada's critical infrastructure
3. Uses computer systems to attack or compromise Canadian institutions by groups or organizations acting on behalf of foreign states and
4. Threatens key business assets with high economic impact



Locations of the RCMP Cybercrime Investigative Teams (CITs)

Federal Policing Cybercrime Investigative Teams (FP CITs):

The RCMP presently has five dedicated FP CITs to investigate cybercrimes. They are located in Quebec (Montreal), Ontario (Ottawa and Toronto), Alberta (Edmonton), and British Columbia (Vancouver). The FP CITs are not geographically bound and therefore may undertake an investigation anywhere in the country.

Some RCMP cybercrime investigations require collaboration with internal or external stakeholders. Specifically the RCMP collaborates with:

- **Internal RCMP units**
- **RCMP cybercrime specialists deployed abroad within cybercrime and other investigative responsibilities**
- **Domestic and international law enforcement agencies**
- **Government of Canada stakeholders**
- **Where appropriate, industry partners**

Under the FP mandate, cybercrime investigations seek to identify and target both cybercrime as a service, as well as illicit activities conducted by criminal networks in the cyber realm, which can include hostile foreign actors (state and non-state).

Cyber criminals typically operate as malware developers and distributors, cybercrime infrastructure developers and operators (i.e. botnets, forums), financial network operators facilitating the laundering and monetization of proceeds of cybercrime, and state sponsored actors.

While arrests and prosecutions have typically been at the forefront of cybercrime threat reduction efforts, when technologies like encryption and anonymization are at play, the RCMP can use disruption to prevent any further harm.

For law enforcement, disruption means lawfully dismantling cybercrime infrastructure and assets, seizing command and control servers, shutting down DarkNet marketplaces, and taking down malicious websites and email addresses used to harm and exploit victims. Where arrests are simply not possible, disruption is an important way to prevent cybercriminals from continuing their criminal activities.

Cybercrime Partner Responsibilities

The RCMP works with the following key partners to prevent, detect, disrupt, and investigate cybercrimes:

National Cybercrime Coordination Unit (NC3): The NC3 is a national police service that coordinates and de-conflicts cybercrime investigations in Canada that do not fall under the FP mandate of the RCMP, and provides investigative advice and guidance to all Canadian police.

Canadian Anti-Fraud Centre (CAFC): The CAFC is Canada's central repository for information about fraud and identity theft. Information and awareness are provided to individuals and businesses on how to recognize, report and protect themselves against fraud. The CAFC assists individuals and can share information with law enforcement as needed, to support investigations and contribute to the security of Canada's economy.

Canadian Centre for Cyber Security (Cyber Centre): The Cyber Centre is Canada's authority on cyber security and leads the government's response to cyber security events. It aims to protect and defend valuable cyber assets and works alongside both private and public sectors to solve complex issues. The Cyber Centre alerts Canadians of new and ongoing cyber incidents and notable threats. They also provide advice and guidance to various sectors including: small and medium-size organizations, government departments and agencies, critical infrastructure, and industry partners, by providing best practices, strategies, and tools to enhance the protection and security of their digital technologies and business assets

FILING A COMPLAINT

BEING A VICTIM OF CYBERCRIME is a stressful experience and the damage to your business can be significant. Knowing why and how to file a complaint with law enforcement and understanding the investigative process is important for mitigating the harm caused by cybercrime.

Why File a Cybercrime Complaint

Cybercrime incidents are criminal offences in Canada with real victims and real impacts. By reporting to law enforcement, your organization will help police pursue cybercriminals, making Canada more resilient to cybercrime.

Although it is challenging to apprehend cybercriminals due to the scope and magnitude of cyber threats, the international dimension of cybercrime, and the difficulty of attributing responsibility for cybercrime, the benefits to filing a complaint are:

- Reporting to police can help provide information towards intelligence sharing efforts which may assist in preventing attacks or minimizing their impact, thus reducing further victimization.
- Police can work with foreign counterparts to stop organized cybercrime activity, which can help reduce the number of attacks on a particular company or business sector.
- Assist law enforcement and the government in developing a more accurate understanding of the nature and extent of cybercrimes in Canada affecting individuals and businesses.
- Victims will directly inform law enforcement priorities and help in aligning investigative resources to address the most critical and high impact threats.

When considering whether to make a complaint or not, remember, law enforcement will not:

- Take over any internal or third-party investigation (i.e., incident response, technical mitigation and remediation measures) or disrupt the ability for business to resume. Law enforcement interest is in finding the perpetrator and will work with your company to gather evidence while allowing internal investigation/remediation to proceed with minimal business disruption. It is best to file a complaint early so there is collaboration in ensuring evidence is preserved without slowing down remediation measures.

- Disclose information to the media without consulting you. Your organization's information will remain secure and private according to law enforcement policies and Government of Canada standards. Active investigations are never discussed in detail with the media, as doing so could compromise ongoing investigative activities. However, in the event of the investigation going to court, it is likely that details will be publicly disclosed during the proceedings. It is also important to remember that others may alert the media, such as the alleged perpetrator, indirect victims, or employees. Therefore, having an incident response plan in place can be helpful in managing communications around a cyber incident.

When to File a Complaint

If you suspect that you have been a victim of a cybercrime, file a complaint as soon as possible. This will enable law enforcement to discuss the complaint with you in order to ensure all investigative avenues are fully explored. Early contact allows the RCMP and law enforcement to coordinate our investigation with your organization's legal support team and/or mitigation actions.

Attempted breaches are also criminal offences so you should also file complaints about cyber breaches. Although not every complaint will result in an active investigation, the data informs prevention effort, and contributes to law enforcement's efforts to disrupt criminal activities and infrastructure, through measures such as domain takedowns, and disruption or seizure of command and control servers.[1]

1 A command and control server is a computer controlled by a cybercriminal to coordinate attacks on other infected machines/network.

How to File a Complaint

The following is a suggested list of information to have ready to share with police:

Complainant Contact Information

- Name
- Mailing address
- Business Address
- Telephone Number
- Cellular Number
- Email Address

Description of cybercrime activity

- Generally describe the cybercrime incident or activity and how it affected your business. Assign a real dollar value lost as a result of the cybercrime. Identify the number of affected employees and/or customers.
- How and when did the cybercrime activity come to your attention?

Suspect Information

- Have you identified a suspect individual/organization?
- Attach known information regarding the suspect including:
  - Name(s)
  - Address(es)
  - Vehicles
  - Corporate or company documents
  - Email address and web sites
- Has this suspect been the subject of previous civil or criminal enforcement action?
- Include information on any previous civil action including:
  - Dates
  - Court
  - File number(s)
  - Lawyer Name(s)
  - Status of case and attach copies of any previous cease and desist letters
- Do you have an investigator's report of this activity? If so, attach a copy of the report to your complaint including the investigator's contact information.
- Have you or a third party conducted any internal investigation? If so, please attach the report.

Investigative Considerations

In cases where your organization conducts its own investigations, law enforcement realizes that you will gather significant information including evidence from witnesses, acquisition of potential exhibits or evidence, surveillance reports, offender information and other types of intelligence.

In these cases, we ask that you please ensure the following:

- **Notify Law Enforcement**
  Where feasible, notify police of your intent to conduct your own investigation. This will assist us to deconflict against possible ongoing investigations against the same individuals or entities. The information may also help enhance our criminal investigations, in which case we will attempt to corroborate information supplied before proceeding with a search warrant or the laying of criminal charges.

- **Document all investigative actions**
  Please ensure your investigative actions are well documented and sourced when possible. This will enhance your initial complaint submission to the police and reduce duplication of efforts.

- **Preserve evidence**
  In cases where you acquire evidence or receive exhibits for analysis, ensure that these items are secured and all handling or movement is well documented. Police need to ensure that the chain of custody of these items can be traced from initial contact up until the time they are required for court proceedings. Examples of digital evidence that may requested:

  Threat and Threat Actor Identifiers:

  - Ransom Note
  - Suspicious (Phish) email
  - Email addresses provided to communicate with the attackers
  - Copies of emails used to communicate with the attackers (with IP header info intact)
  - Cryptocurrency address (e.g. Bitcoin) provided for ransom payment
  - Decryption keys provided

System Indicators:

- Suspicious file(s) (e.g. Malware or Executables) (date created & file path found)
- Suspicious Internet communications or IP connections
- Live memory (RAM) capture from affected system
- Suspicious running processes or scripts (e.g. PowerShell, RDP connections, Exploit Kits)
- Any unknown user accounts created in Active Directory or endpoints
- Log files (Application, Security, System, Task Scheduler History, Firewall, RDP, IDS, etc.)

Please provide any other information and attach any additional reports, photographs or documentation which you believe will assist law enforcement.

Industry Commitment Considerations

- Are you able to supply an internal analysis of the cybercrime incident?
- Are you able to supply witnesses for all court proceedings at your expense?
- Are you able to supply a victim impact statement?
- Are you able to share third-party mitigation reports or server images?
- Are you able to share details of the financial impact of the breach (i.e. cost of mitigation, value of data compromised)?

THE INVESTIGATIVE PROCESS

THE RCMP WILL RESPOND to all complaints involving cybercrime and will deal with each matter on a case by case basis. Our enforcement resources will focus on large scale cybercrime involving cross border, multi-jurisdictional investigations, attacks on critical infrastructure, links to organized crime and attacks on industry partners that impact the Canadian public. We may investigate smaller cases in order to generate intelligence, to ascertain if there are connections to ongoing investigations, or to target larger cybercrime operations.

Complaint Intake and Assessment

Complaints will be reviewed and assessed according to the following:

1. **Does it fall within the Federal RCMP mandate and established cybercrime policy parameters for investigation?**
2. **Where does it fall in regards to current operational priorities?**
3. **Have we received a commitment from the victim organization to assist with the investigation and prosecution?**
4. **What resources are currently available to effectively respond to the complaint?**
5. **Will either the Department of Justice or the Provincial Crown Attorney's Office undertake to prosecute the matter?**
6. **Is there a reasonable expectation of a successful prosecution?**

Information Sharing

Cooperation between law enforcement and your organization is critical during the investigation process and investigators will make every effort to keep you informed as the investigation progresses. However, it is important to understand that certain aspects of the investigation, such as tactical decisions or investigative techniques, will remain solely under law enforcement's purview due to their sensitive nature. The investigators will advise you of any limitations to information sharing with respect to the investigation process.

Where Charges Cannot Be Laid

In cases where charges cannot be laid, the RCMP will attempt to disrupt the criminal activity and continue to work with industry partners, government agencies and law enforcement in whatever capacity we can to mitigate further harm.

WHERE TO FILE A COMPLAINT

To file a report, please contact the local police of jurisdiction **and** the Canadian Centre for Cyber Security (cyber.gc.ca). If the cybercrime activity was a fraud, **also** report to the Canadian Anti-Fraud Centre through the online reporting system (antifraudcentre-centreantifraude.ca) or by phone at 1-888-495-8501 (regardless of whether any money or data was stolen).

CONTACTS

Federal Policing Strategic Engagement and Awareness

For more information about the contents of this booklet, please contact Federal Policing Strategic Engagement and Awareness (FP-SEA): FP-SEA_ESS-PF@rcmp-grc.gc.ca

Additional Resources

National Cybercrime Coordination Unit (NC3)
rcmp-grc.gc.ca/en/nc3

Of note: The National Cybercrime Coordination Unit (NC3) will also soon have a new cybercrime and fraud reporting system, to make it easier for Canadians and businesses to report cybercrime and fraud, developed in partnership with the Canadian Anti-Fraud Centre.

New cybercrime and fraud reporting system | Royal Canadian Mounted Police (rcmp-grc.gc.ca)

Canadian Centre for Cyber Security
cyber.gc.ca/en

Canadian Anti-Fraud Centre
antifraudcentre-centreantifraude.ca