

Re: Item 7.1

**HALIFAX**

December 3, 2025



**Presentation to HRM Board of Police Commissioners  
Halifax Regional Police & RCMP Halifax Regional Detachment  
Cybercrime: An Overview**

# Definition of Cybercrime

- For national police-reported crime statistics, cybercrime is defined as *‘any criminal act as outlined in Canada’s Criminal Code where Information and Communication Technology (ICT) is the target of the offence, or whereby ICT is integral and vital in the commission of the offence.’*
- ICT includes, but is not limited to, the internet, computers, servers, digital technology, digital telecommunications devices, phones and networks.

# Definition of Cybercrime

- Cybercrime can be broadly defined as any criminal offence where technology plays a significant role.
- It can happen anywhere – criminals do not need to be local.
- Cybercrime is broken down into two categories.

HALIFAX

# Definition of Cybercrime

## TECHNOLOGY AS A TARGET



## TECHNOLOGY AS A TOOL



# Examples of Cybercrime



Criminal Harassment: texting or sending messages via social media.



Sextortion: threatening to share intimate images of a person if they do not comply with demands.



Ransomware: malware encrypts a victim's files or locks them out of their system, demanding a ransom payment in exchange for the decryption.

# Cybercrime Accessibility

Cybercrime was once considered only within the realm of those with specialized skillsets and technology. Not anymore...

- Cybercrime is cheap, fast and automated.
- Cybercrime groups operate like a business (cybercrime as a service).
- Frauds/scams are the top threat (phishing, investment fraud, romance scams).
- Everyday people are the primary victims, not just large companies.

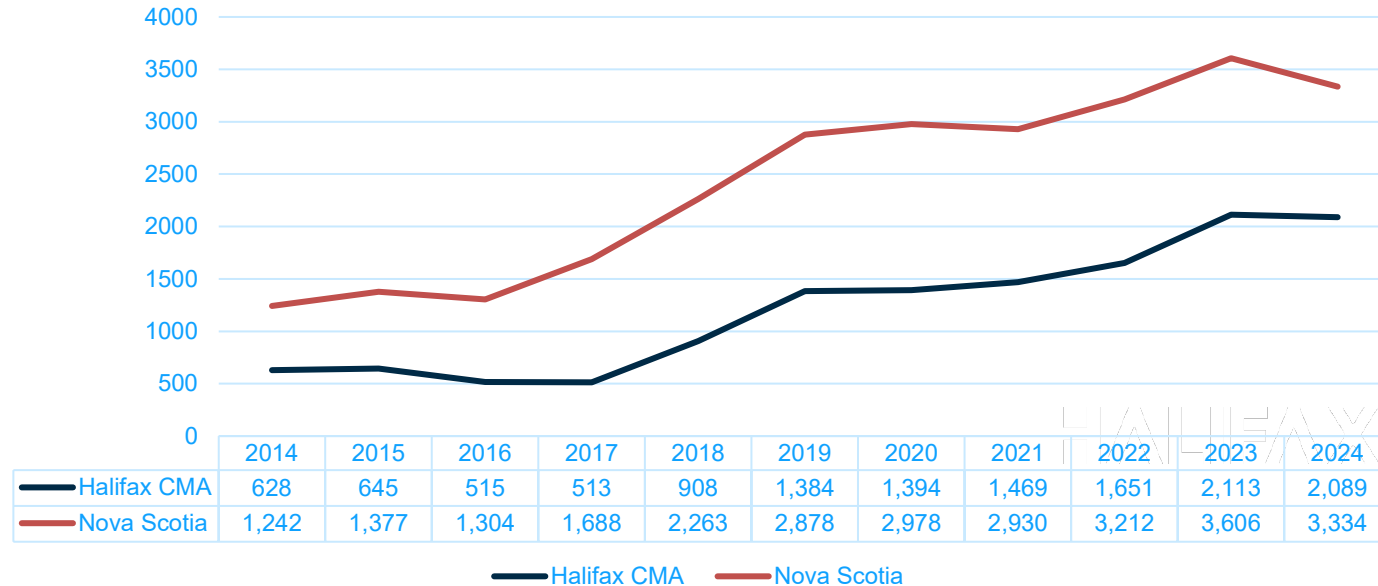
HALIFAX

# Police-reported Cybercrime

- National police-reported crime survey in place since 1962, with mandatory reporting and full coverage across Canada.
- Police follow standardized rules on how and where incidents are recorded, including cybercrime data. Reporting rules guide police agencies regarding location *e.g., if a person lives in Truro but opens a threatening email in Halifax, the file will be recorded and investigated by Halifax police.*
- Statistics Canada publishes data:
  - Annually: crime statistics at the Census Metropolitan Area level.
  - Quarterly: preliminary data at the national and regional level.
- Data are available via the Statistics Canada online portal.

# Police-reported Cybercrime

Number of cybercrime incidents in Halifax CMA  
and Nova Scotia 2014-2024

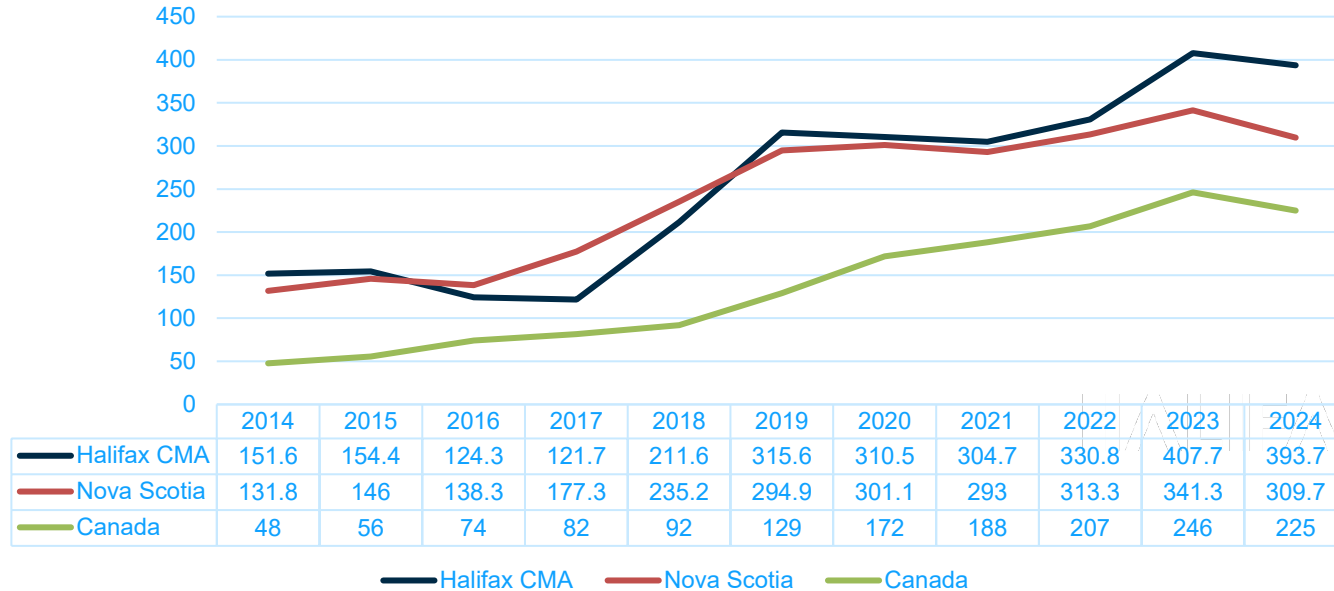


Source: Statistics Canada. [Table 35-10-0002-01 Police-reported cybercrime, number of incidents and rate per 100,000 population, Canada, provinces, territories, Census Metropolitan Areas and Canadian Forces Military Police](#)



# Police-reported Cybercrime

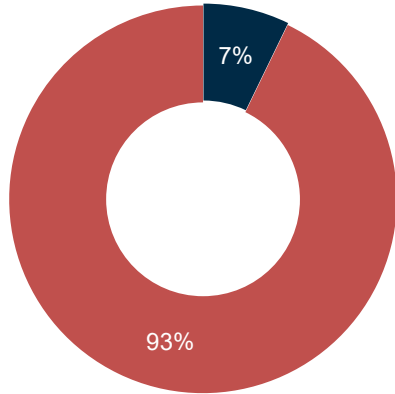
Rate of cybercrime incidents in Halifax CMA and Nova Scotia  
per 100,000 population, 2014-2024



Source: Statistics Canada. [Table 35-10-0002-01 Police-reported cybercrime, number of incidents and rate per 100,000 population, Canada, provinces, territories, Census Metropolitan Areas and Canadian Forces Military Police](#)

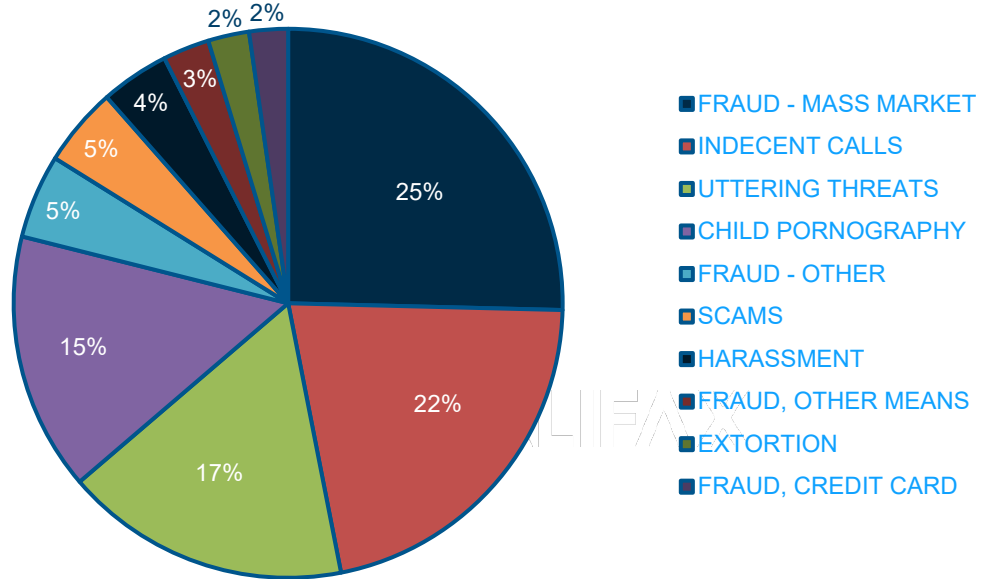
# Police-reported HRP & HRD data

Cybercrime Type  
2020-2025 YTD



■ Target ■ Instrument

Most common types of police-reported cybercrime  
HRP & HRD, 2020-2025 YTD



- FRAUD - MASS MARKET
- INDECENT CALLS
- UTTERING THREATS
- CHILD PORNOGRAPHY
- FRAUD - OTHER
- SCAMS
- HARASSMENT
- FRAUD, OTHER MEANS
- EXTORTION
- FRAUD, CREDIT CARD

# HRP Cyber Operations Unit

- Established in 2016 with two HRP positions: one civilian, one sworn.
- Located within the Integrated CID.
- Supports police investigations by CID and Patrol officers in HRP and HRD which involve an online element.
- Enhances investigative outcomes by providing expert assistance on cases with cyber components.

# RCMP Responsibilities

- The mandate for the provincial RCMP Cybercrime unit is to assist frontline members and other units outside of HRM with their investigations.
- The unit regularly assists RCMP members in other NS divisions needing cyber support.
- If an investigation falls under National Interest the NC3 will take the lead, as they see fit.
- This includes critical infrastructure, Department of National Defence and other entities.

HALIFAX

# RCMP National Cybercrime Coordination Centre (NC3)

- Established in response to the continuous rise of cybercrime in Canada and around the world.
- Consists of police officers and civilians from various backgrounds and areas of expertise.
- Works with Canadian law enforcement as well as national and international partners to help reduce the threat, impact, and victimization of cybercrime in Canada.

HALIFAX

[National Cybercrime Coordination Centre | Royal Canadian Mounted Police](#)

# RCMP National Cybercrime Coordination Centre (NC3)

NC3 is responsible for:

- Coordinating cybercrime investigations with domestic and international partners.
- Supporting Canadian law enforcement agencies to combat cybercrime by:
  - providing advice, guidance, technical expertise and capabilities in investigations.
  - providing actionable cybercrime intelligence.
  - providing notifications to Canadian victims of cybercrime through local police.

[National Cybercrime Coordination Centre | Royal Canadian Mounted Police](#)

# RCMP National Cybercrime Coordination Centre (NC3)

- Providing Canadian law enforcement agencies with a centralized source of information and guidance for addressing cybercrime in their communities.
- Collaborating with partners from private, public and non-governmental sectors.
- Leading national cyber offender prevention initiatives in close cooperation with partners.

HALIFAX

[National Cybercrime Coordination Centre | Royal Canadian Mounted Police](#)

# Challenges with Cybercrime Investigations

- There is no mandate to report an incident.
- Many persons of interest are not located in Canada or a co-operative nation; this hinders investigations.
- Most organizations do not involve the police to limit liability after seeking legal advice.
- For victim organizations, it is expensive to create, maintain, and test an effective Security Operations Centre (SOC) and backup system, then train personnel in its use. This limits available data after an incident.



# Questions?

HALIFAX