Cyber Crime in Canada

Presented by
C/M Dave Black
Manager, RCMP Cyber Crime Fusion Centre
Technological Crime Program

dave.black@rcmp-grc.gc.ca
Cyber Security Awareness Month

Never given your online risk much thought before? This month’s the perfect time.

Learn more
Cyber Security Strategy…to…Cyber Crime Strategy (Domestic Partnerships)
The Cyber Security Strategy is government’s plan for making cyberspace more secure. The Strategy is built on 3 pillars:

1. Securing Government systems
2. Partnering to secure vital cyber systems outside the Federal Govt
3. Helping Canadians to be secure online

1.7 million Canadians were victims of identity theft in 2008. The annual cost of identity theft in Canada has been estimated at nearly $1.9 billion (McMaster University)
The “Cyber Crime Fusion Centre”

The CCFC is TCB’s plan for building a comprehensive approach to cybercrime.

1. Exclusively administrative in nature.

2. Secretarial support to the RCMP’s internal *Cyber Crime Council*


4. Source of RCMP “situational awareness”
Public Safety’s DG Cyber (Committee)

- Coordination of federal Cyber Activities
- DG Cyber – workgroups
  - Information Sharing – PS & DoJ
  - Situational Awareness – PS
  - Cyber Incident Handling – CSEC and PS
  - Industrial Control Systems - PS
Criminal Intel Brief 2012: Hacktivism

- Activist hackers or “hacktivists” have over the last year, increasingly engaged in cyber threat activities such as Distributed Denial of Service (DDoS) attacks, to advance their political/ideological agendas.

- Hacktivist groups are becoming more aggressive and their tactics could be used for extortion, intimidation, and harassment.

- Given the anonymity and the global reach of the Internet, the risk of reprisal for hacktivists is low, but the potential impact of their activities can be significant.

- The use of social media by hacktivist groups could, in future, lead to larger, more coordinated cyber attacks coupled with physical demonstrations, with potential for major disruption of vital systems.

- Our limited knowledge about hacker groups has created an intelligence gap that constrains law enforcement’s ability to develop a proper criminal profile and threat assessment regarding intent versus capability.
International Implications

- Council of Europe’s Convention on Cybercrime
- INTERPOL’s Global Centre for Innovation – Singapore - 2014
- UN – Cybercrime Survey – Organized Crime and Drugs
- ICANN – Internet Governance Forum
- Other:
  - G8-G20
  - OAS
  - NCFTA.ca
- ?? How to “expedite” cyber investigations ??
Canadian Anti-Fraud Centre

Français  |  Home  |  Contact Us  |  Help  |  Search  |  canada.gc.ca

**RECOGNIZE IT**
- Scam Types
- Identity Theft
- Have I Been Scammed?
- Samples

**REPORT IT**
- How do I report Fraud?

**STOP IT**
- Fraud Prevention
- Forum
- FAQ's
- Resource Material
- Identity Theft
- Testimonials

**National CAFC**
- About CAFC
- Newsroom
- SeniorBusters
- Intelligence Unit
- Privacy Policy
- Proactive Disclosure

---

**Are you a target?**

**U.S. Federal Trade Commission:**
FTC to provide refunds to victims of bogus scareware scam...
[read more]

---

**Scams of the week**

**Anti-Virus Scam**

**Computer scam goes viral in Canada**

The virus scam has grown to epidemic proportions in Canada, now accounting for between 70 and 80 per cent of frauds reported daily to the Canadian Anti Fraud Centre (CAFC).
[read more]

**WARNING:** Your computer may be infected by a virus. Take preventative action now!

[Alert message]
Questions?

C/M Dave Black
613-993-6579
dave.black @ rcmp-grc.gc.ca