Alberta Government

Cyber Crime: Are You Protected?

18 October 2018

Kelly Coffin

Alberta Security & Strategic Intelligence Support Team (ASSIST)

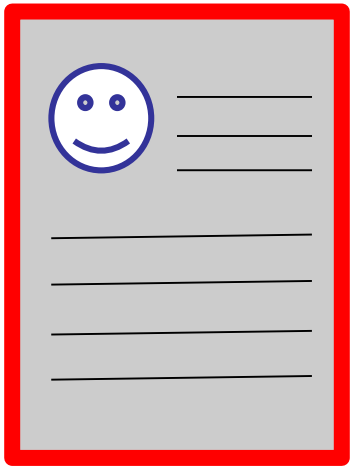
Sheriffs Branch

Public Security Division

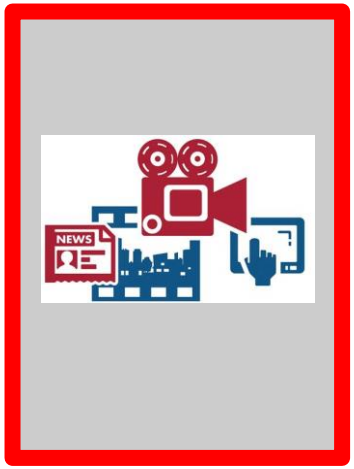
Justice & Solicitor General

Information Security: What are the risks?

Monetary Loss Theft/Fraud



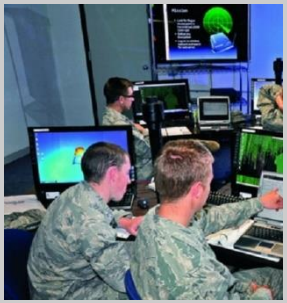
Theft of Private Information



Reputational Loss

Information Security: Who are the intruders?

Financially Motivated



Professionals & Nation-States

Hacktivists & Vandals

Information Security: Financially Motivated Intrusions

Ransomware

Cryptocurrency Mining

Business Email Compromise

Financially Motivated Intrusions: Ransomware

- Objective: Ransom payment
- Intruder installs software which locks the computer and prevents use or access to files, demands payment to unlock
- Countermeasure:
  - Perform regular backups on separate hard drive
  - Perform regular updates of software
- Response:
  - CCIRC recommends not paying ransom
  - Contact professionals who can attempt recovery

Financially Motivated Intrusions: Ransomware

- Case Study: Town of Wasaga Beach, April 2018
- Ransomware compromised system
- Cost:
  - $34,950 to recover data (3BTC + fees)
  - $37,181 for consultants
- No personal data believed to be compromised

Financially Motivated Intrusions: Cryptocurrency Mining

- Objective: Passive income
- Intruder installs software which “mines” currency. Can cause hardware/software issues.
- Countermeasure:
  - Use antivirus service
  - Perform regular updates of software

Financially Motivated Intrusions: Business Email Compromise

- Objective: Defraud Organization of Funds
- Intruder contacts organization, typically spearphishing and attempts to:
  - Fraudulently request payment by posing as a trusted vendor
  - Acquire financial credentials to intercept or steal funds
- Countermeasure:
  - Don’t click on links/open attachments from emails unless you’re expecting them
  - Confirm financial requests using two separate systems (phone/text/messenger & email)
- Response:
  - Contact police of jurisdiction immediately!

Information Security: Personal Information Theft Intrusions

John Smith

May 15, 1970

123 Smith St
Aetna, AB

Personally Identifying Information

Username

Password

Account Credentials

Reputation Hijacking

Protect Yourself: Cyber Security Best Practises

- Be security aware
  - Don’t click on links in emails unless you’ve asked for them
  - Don’t open attachments in emails if you don’t know what’s in them
- Use complex passwords
  - Use letters, numbers and symbols
  - Never use default passwords!
- Update computer programs regularly
  - Follow manufacturer’s recommended updates (important for security!)
- Backup your data
  - Use removable hard drive, backup on a schedule (set reminder or use program!)
- Use antivirus protection

Contact

assist@gov.ab.ca

After Hours or Emergency 24/7:

780-644-2680