Experiencing MIS

Fifth Canadian Edition

Chapter 12

Managing Information Security and Privacy

Q12-1: What Is Identity Theft?

- **identity theft**: vital information is stolen to create a new identity
  - Can be done with just a person's name, address, date of birth, social insurance number, and mother's maiden name
- identity thief can take over a victim's financial accounts; open new bank accounts; transfer bank balances; apply for loans, credit cards, and other services

Q12-2: What Is PIPEDA?

- **PIPEDA**: Personal Information Protection and Electronic Documents Act
- Act intended to balance an individual's right to the privacy of his or her personal information, which organizations need to collect, use, or share for business purposes
- The Privacy Commissioner of Canada oversees this Act
- PIPEDA governs how data are collected and used

Q12-3: What Types of Security Threats Do Organizations Face?

- Three sources of security threats are:

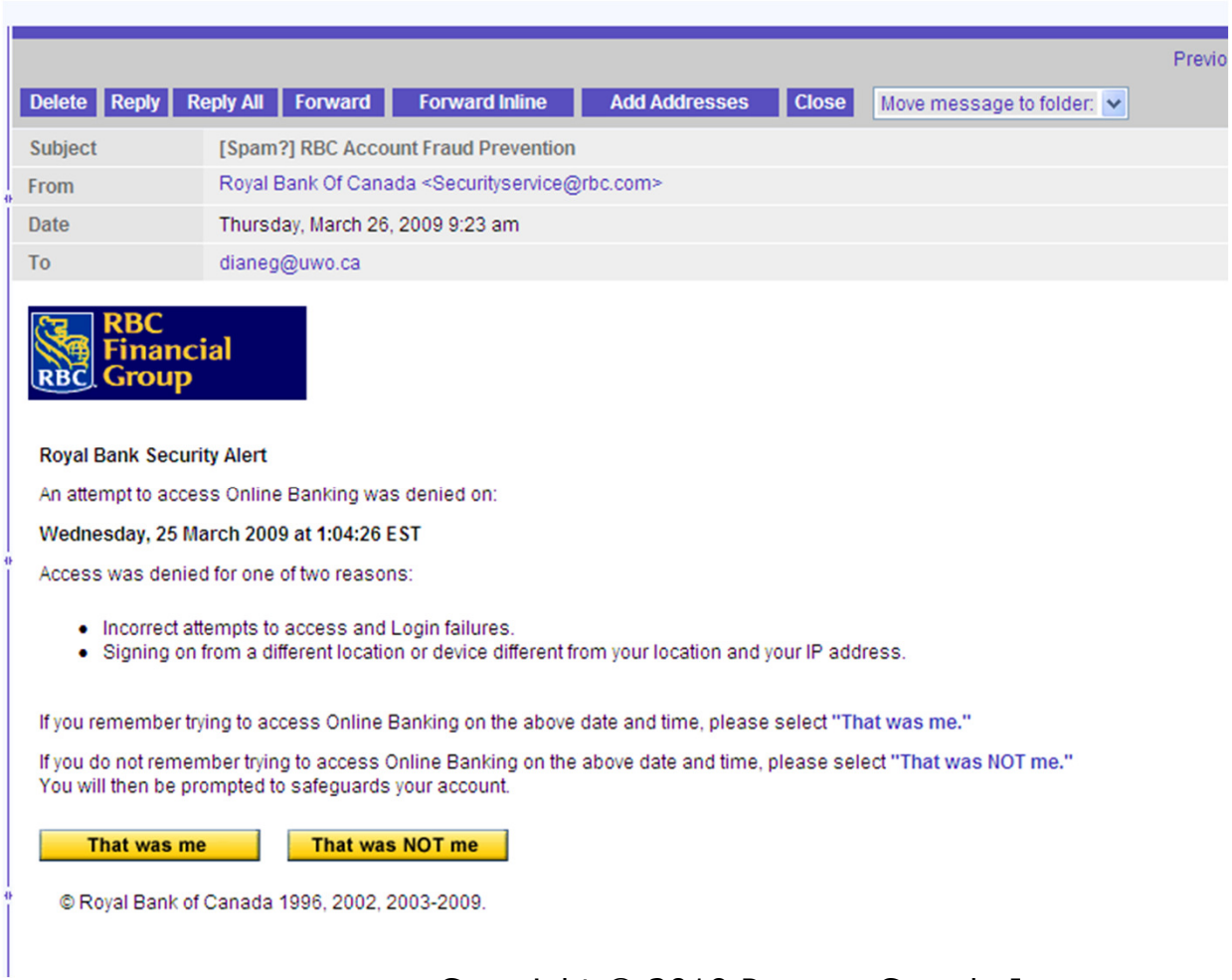
1. **Human errors and mistakes**
   - Accidental problems
     - Employee accidentally delete's a customer's records
     - Employee drives truck through wall of computer room
   - Poorly written programs
   - Poorly designed procedures
   - Physical accidents

What Types of Security Threats Do Organizations Face? (1 of 2)

2. Malicious human activity

- Intentional destruction of data
  - Destroying system components
- Hackers
- Virus and worm writers
- People who send unwanted emails (spam)
- Criminals
- Terrorists

Phishing



Previo

Delete | Reply | Reply All | Forward | Forward Inline | Add Addresses | Close | Move message to folder:

Subject	[Spam?] RBC Account Fraud Prevention
From	Royal Bank Of Canada <Securityservice@rbc.com>
Date	Thursday, March 26, 2009 9:23 am
To	dianeg@uwo.ca

RBC Financial Group

Royal Bank Security Alert

An attempt to access Online Banking was denied on:

Wednesday, 25 March 2009 at 1:04:26 EST

Access was denied for one of two reasons:

- Incorrect attempts to access and Login failures.
- Signing on from a different location or device different from your location and your IP address.

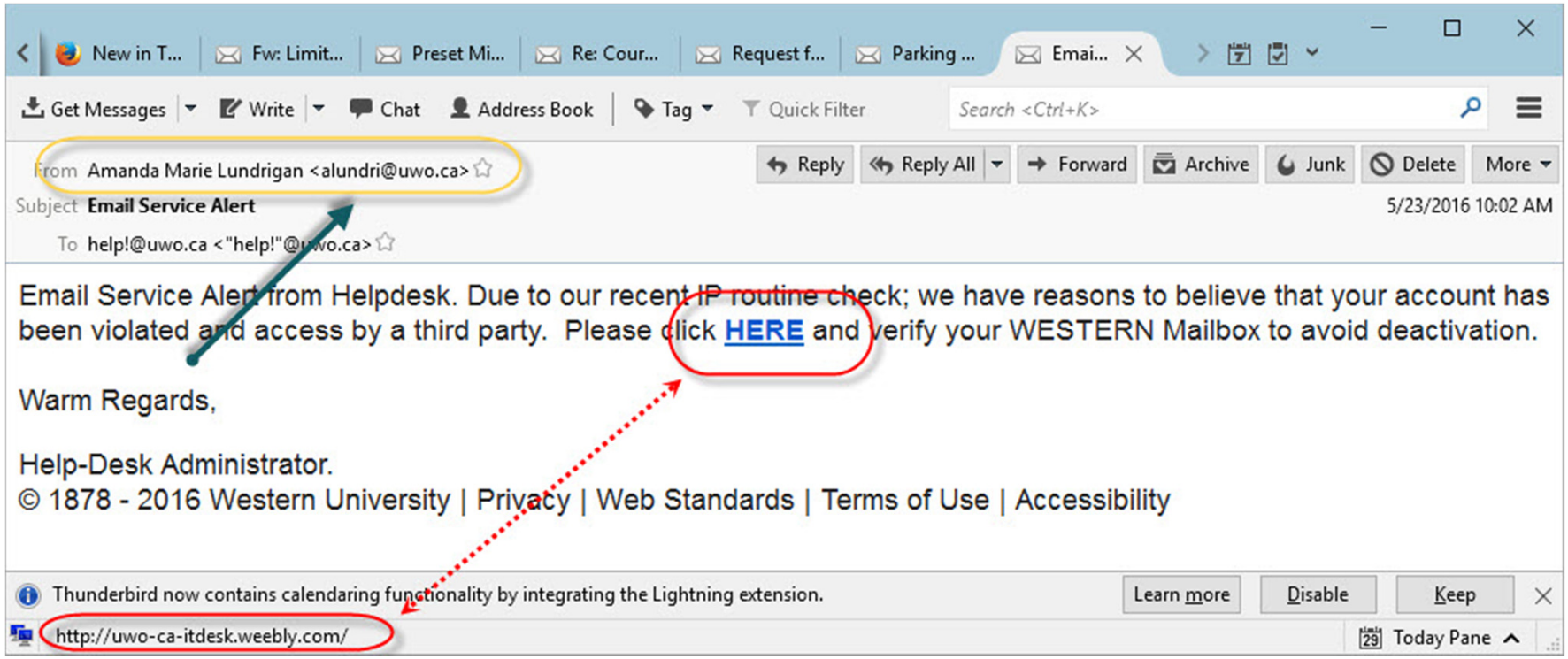
If you remember trying to access Online Banking on the above date and time, please select "That was me."

If you do not remember trying to access Online Banking on the above date and time, please select "That was NOT me."
You will then be prompted to safeguards your account.

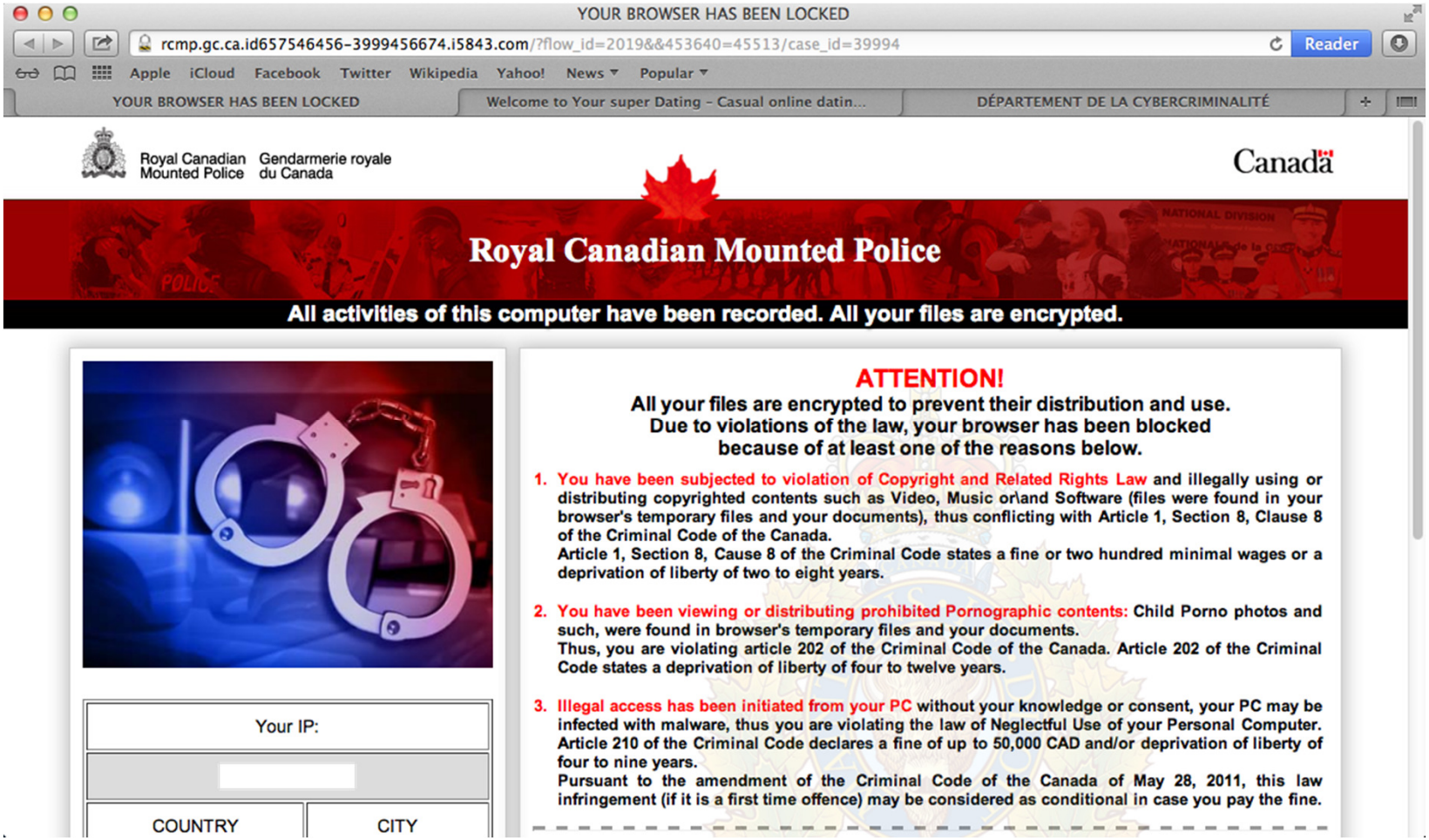
That was me | That was NOT me

© Royal Bank of Canada 1996, 2002, 2003-2009.

Phishing



Ransomware



What Types of Security Threats Do Organizations Face? (2 of 2)

- **Natural events and disasters**
  - Fires, floods, hurricanes, earthquakes, tsunamis, avalanches, tornados, and other acts of nature
  - Initial losses of capability and service
  - Plus losses from recovery actions

Sources and Types of Security Threats,

- Five types of security problems :
  1. Unauthorized data disclosure
  2. Incorrect data modification
  3. Faulty service
  4. Denial of service
  5. Loss of infrastructure

Unauthorized Data Disclosure

- Human error
  - Posting private information in public place
  - Placing restricted information on searchable Web sites
  - Inadvertent disclosure
- Malicious release
  - Pretexting
  - Phishing
  - Spoofing
  - Sniffing (intercepting)

Incorrect Data Modification

- **Human errors**
  - incorrect entries and information
  - procedural problems
  - systems errors
  - **Hacking**

Faulty Service

- **Faulty Service**
  - Incorrect system operation
  - Usurpation

Denial of Service, Loss of Infrastructure

- **Denial of service (DOS)**
  - Human error
  - Denial-of-service attacks
- **Loss of infrastructure**
  - Accidental
  - Theft
  - Terrorism
  - Natural disasters

Elements of a Security Program

- Senior management involvement
  - Must establish a security policy
  - Manage risk
    - balancing costs and benefits
- Safeguards
  - Protections against security threats
- Incident response
  - Must plan for prior to incidents

How Can Technical Safeguards Protect Against Security Threats?

- Technical safeguards involve the hardware and software components of an information system.
  - Identification and authentication
  - Encryption
  - Firewalls
  - Malware protection
  - Design for secure applications

Identification and Authentication

- User names and passwords
  - Identification
  - Authentication
- Smart cards
  - Personal identification number (PIN)
- Biometric authentication
  - Fingerprints, facial features, retinal scans
- Single sign-on for multiple systems

Technical Safeguards (1 of 2)

- Encryption and Firewalls
- Malware Protection
  - Viruses
  - Worms
  - Spyware & Adware
    - Symptoms: slow performance, pop-up advertisements, suspicious browsers homepage changes, and more)

Technical Safeguards (2 of 2)

- Malware safeguards
  - Install antivirus and anti-spyware programs
  - Scan your computer frequently
  - Update **malware definitions**
    - Patterns the exist in malware
  - Open e-mail attachments only from known sources
  - Install software updates promptly
  - Browse only reputable Web sites

Q12-5: How Can Data Safeguards Protect Against Security Threats?

- **Data safeguards** protect databases and other organizational data
- **Data administration,** an organization-wide function
  - develops data policies
  - enforce data standards
- Database administration, particular database function
  - procedures for multi-user processing
  - change control to structure
  - protection of database

Data Safeguards (1 of 2)

- Encryption keys
  - Key escrow
- Backup copies
  - Store off-premise
  - Check validity

Data Safeguards (2 of 2)

- Physical security
  - Lock and control access to facility
  - Maintain entry log
- Third party contracts
  - Safeguards are written into contracts
  - Right to inspect premises and interview personnel

Q12-6: How Can Human Safeguards Protect Against Security Threats?

- Involve **people** and **procedure** components of information system
- User access restriction requires authentication and account management
- Design appropriate security procedures
- Security considerations for:
  - Employees
  - Non-employee personnel

Human Safeguards for Employees (1 of 2)

- User accounts considerations
  - Define job tasks and responsibility
  - Separate duties and authorities
  - Grant least possible privileges
  - Document security sensitivity
- Hiring and screening employees
- Dissemination
  - Employees need to be made aware of policies and procedures
  - Employee security training

Human Safeguards for Employees (2 of 2)

- Enforcement of policies
  - Define responsibilities
  - Hold employees accountable
  - Encourage compliance
  - Management attitude is crucial
- Create policies and procedures for employee termination
  - Protect against malicious actions in unfriendly terminations
  - Remove user accounts and passwords

Human Safeguards for Non-Employees (1 of 2)

- Temporary personnel and vendors
  - Screen personnel
  - Training and compliance
  - Contract should include specific security provisions
  - Provide accounts and passwords with the least privileges

Human Safeguards for Non-Employees (2 of 2)

- Public users
  - Harden Web site and facility
  - Hardening: Take extraordinary measures to reduce system's vulnerability
- Partners and public that receive benefits from the information system
  - Protect these users from internal company security problems

Account Administration (1 of 3)

- Account management procedures
  - Creation of new user accounts
  - Modification of existing account permissions
  - Removal of unneeded accounts
- Password management
  - Acknowledgment forms
  - Change passwords frequently

Account Administration (2 of 3)

- Help-desk policies
  - Authentication of users who have lost their password
  - Password should not be e-mailed (just a notification of password change)
- System procedures:
  - Normal operation
  - Backup
  - Recovery

Account Administration (3 of 3)

- Procedures of each type should exist for each information system
- Definition and use of standardized procedures reduces the likelihood of computer crime
- Each procedure type should be defined for both, system users and operations personnel
  - Different duties and responsibilities
  - Varying needs and goals

Security Monitoring (1 of 2)

- Activity log analyses
  - Firewall logs
  - DBMS log-in records
  - Web server logs
- Security testing
  - In-house and external security professionals

Security Monitoring (2 of 2)

- Investigation of incidents
  - How did the problem occur?
- Lessons learned
  - Indication of potential vulnerability and corrective actions

MIS in Use

- Privacy and the Federal Government
  - Social networking sites, such as Facebook, LinkedIn, Pinterest, and Twitter, are cultural phenomena that have attracted billions of people
  - Users easily communicate with other users
  - Some serious concerns raised about their impact on productivity and personal privacy
  - The Office of the Privacy Commissioner of Canada acted on a complaint from the Canadian Internet Policy and Public Interest Clinic (CIPPIC)

Q12-7: What Is Disaster Preparedness? (1 of 2)

- A substantial loss of computing infrastructure caused by acts of nature, crime, or terrorist activity can be disastrous for an organization
- Best safeguard is appropriate location
- Backup processing centers in geographically removed site

Q12-7: What Is Disaster Preparedness? (2 of 2)

- Identify mission-critical systems and resources needed to run those systems
- Prepare remote backup facilities
  - Hot and cold sites
- Train and rehearse cutover of operations

Q12-8: How Should Organizations Respond to Security Incidents?

- Organization must have plan
  - Detail reporting and response
- Centralized reporting of incidents
  - Allows for application of specialized expertise
- Speed is of the essence
- Preparation pays off
  - Identify critical employees and contact numbers
  - Training is vital
- Practise incidence response!