Information Systems

… Organization and Security

Corporate Organization

Congratulations !

You are a success and your company has grown.

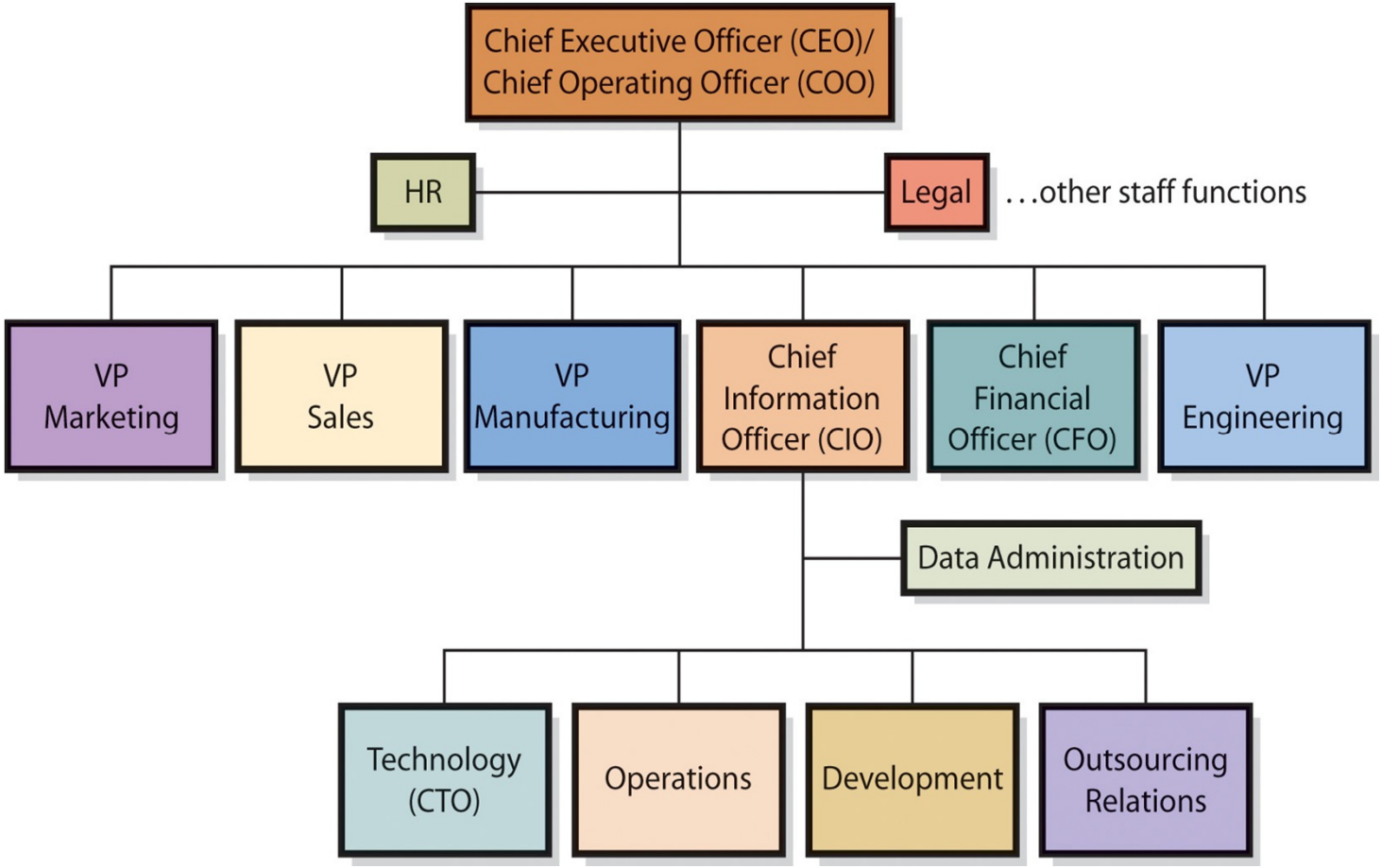
What is the structure of your company now ?

As your company has grown, so has your security needs and concerns

Where do you go from here ?

MIS - Organization and Security

Corporate Organization



MIS - Organization and Security

Corporate Organization

Information Technology (IT) Departmental Organization

- Chief Information Officer (CIO)
- Technology office
- Operations
- Development
- Outsourcing Relations
- Data Administration

MIS - Organization and Security

Corporate Organization - IT Department

- most organizations rely on information technology services

- all these services
  - email systems,
  - accounting applications,
  - desktop computers,
  - mobile devices
- used in an organization require some form of technical support

The department of people who support this is often referred to as "IT Services" or "Information Systems Services"

Corporate Organization - IT Department

What Jobs exists in IT Services?

- IT industries have a wide range of interesting and well-paying jobs

- Some think that the industry consists only of programmers and computer technicians who have great technical skills

- **The reality is that most jobs that are in the highest demand in the IT industry require a mix of interpersonal and technical skills**

- The industry needs people who can bridge the knowledge gap between computer technicians and business system users

Corporate Organization - IT Department

What Jobs exists in IT Services?

- For most technical positions, knowledge of business specialty increases marketability
- High-paying jobs require communication, leadership, and business skills
- For students, a dual major can be an excellent choice to open up opportunities

MIS - Organization and Security

Corporate Organization - IT Department

What Jobs exists in IT Services?

Title	Responsibilities	Knowledge, Skills, and Characteristics Requirements	2006 Cdn. Salary Range ($CDN)
Computer technician	Install software, repair computer equipment and networks	Associate degree, diagnostic skills	$30 000–$60 000
Quality Assurance (QA) test engineer	Develop test plans, design and write automated test scripts, perform testing	Logical thinking, basic programming, superb organizational skills, detail oriented	$40 000–$75 000
User support representative	Help users solve problems, provide training	Communications and people skills, product knowledge, patience	$35 000–$60 000
Technical writer	Write program documentation, help-text, procedures, job descriptions, training materials	Quick learner, clear writing skills, high verbal and communications skills	$35 000–$60 000
Programmer/ Developer	Design and write computer programs	Logical thinking and development, skills, programming	$45 000–$110 000
Website Designer	Work with clients to develop designs for websites, work with developers to finalize designs	Excellent interpersonal skills, design skills, detail oriented, good technical skills, flexible business/marketing skills	$45 000–$110 000
Network administrator	Monitor, maintain, fix, and tune computer networks	Diagnostic skills, in-depth knowledge of communications, technologies, and products	$65 000–$120 000+
Database administrator	Manage and protect database (see Chapter 12)	Diplomatic skills, database technology knowledge	$65 000–$120 000
Systems analyst, Business analyst	Work with users to determine system requirements, design procedure	Strong interpersonal and communications skills, business and technology knowledge	$50 000–$110 000
Consultant	Wide range of activities: programming, testing, database design, communications and networks, project management, strategic planning	Quick learner, entrepreneurial attitude, communications and people skills, respond well to pressure, particular knowledge depends on work	From $35 per hour for a contract tester to more than $400 per hour for strategic consulting to executive group
Salesperson	Sell software, network, communications, and consulting services	Quick learner, knowledge of product, superb professional sales skills	$65 000–$200 000+
Project manager (PM)	Initiate, plan, manage, monitor, and close down projects	Management and people skills, technology knowledge, highly organized	$75 000–$150 000
Enterprise Architect (EA)	Manage and document the technological infrastructure of the firm	Diplomatic skills, database technology knowledge, strategic planning	$100 000–$200 000
Chief technology officer (CTO)	Advise CIO, executive group, and project managers on emerging technologies	Quick learner, good communications skills, deep knowledge of IT	$100 000–$250 000+
Chief information officer (CIO)	Manage IT department, communicate with executive staff on IT- and IS-related matters, member of the executive group	Superb management skills, deep knowledge of business, and good business judgment; good communicator, balanced and unflappable	$150 000–$300 000, plus executive benefits and privileges

MIS - Organization and Security

Security

Criminal Code of Canada

Unauthorized use of computer

342.1

(1) Every one who, fraudulently and without colour of right,

(*a*) obtains, directly or indirectly, any computer service,

(*b*) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system, or

(*d*) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

MIS - Organization and Security

Security

Understanding threats to your own privacy

Identity theft

- Fastest growing crime
- Stealing, misrepresenting or hijacking the identity of another person
- Information on identity theft , (www.publicsafety.gc.ca)
- Vital information (name, address, date of birth, sin) is acquired to complete impersonation

With this information, the identity thief

- Take over a victim's financial accounts
- Open new bank accounts, transfer bank balances
- Apply for loans, credit cards, and other services

Security - Computer Threats

Malware

short for **malicious software**
- software used to:
  disrupt computer operation,
  gather sensitive information, or
  gain access to private computer systems

Malware includes:
computer viruses (**computer crime against a computer**),
ransomware,
worms,
trojan horses,
keyloggers,
spyware,
adware

Security - Computer Threats

Spyware

is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge

"Spyware" is mostly classified into four types:

- system monitors,
- trojans,
- adware,
- tracking cookies

Security - Computer Threats

Adware

advertising-supported software,

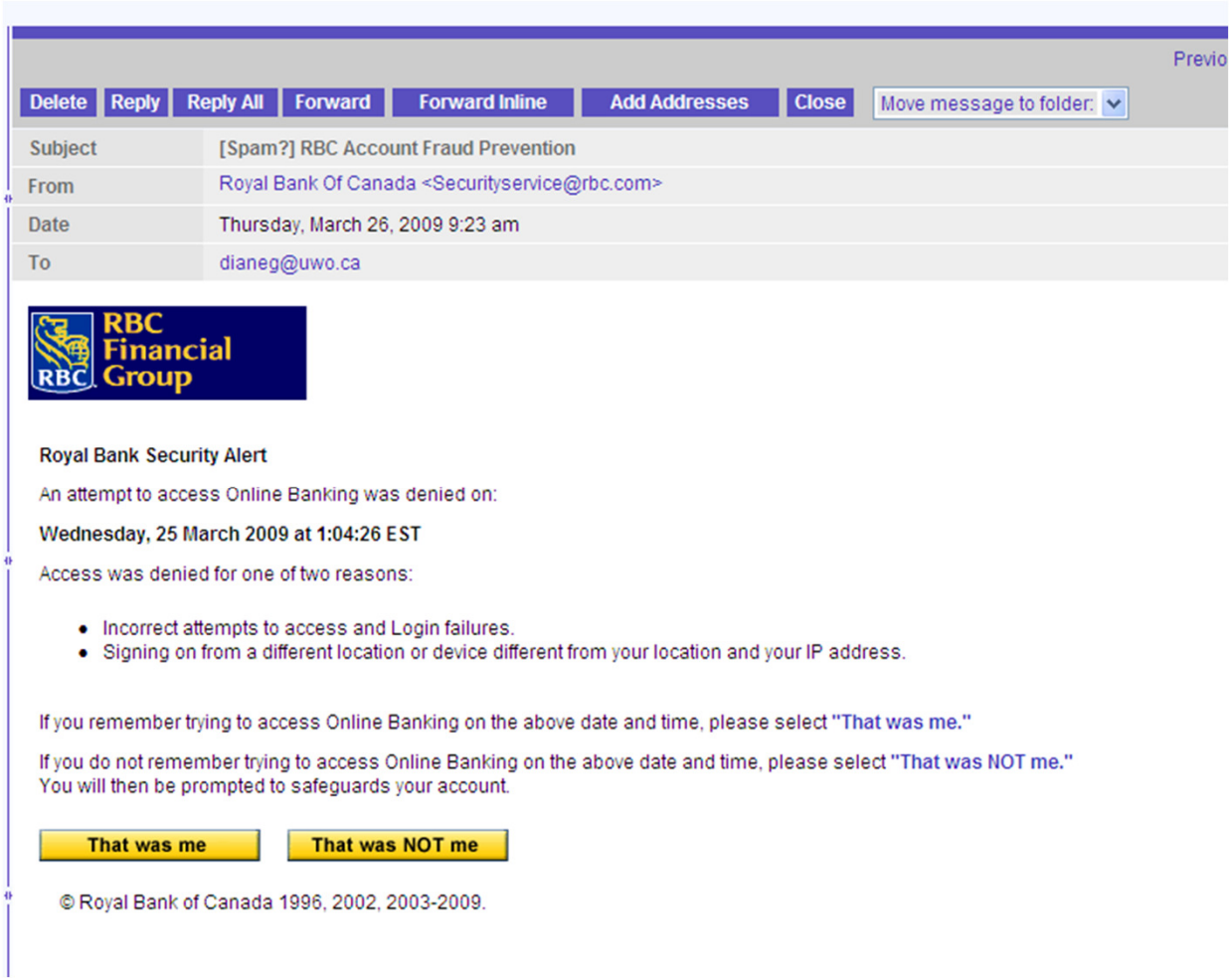
any software package which automatically renders advertisements in order to generate revenue for its author.

The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process.

The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there.

MIS - Organization and Security

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."

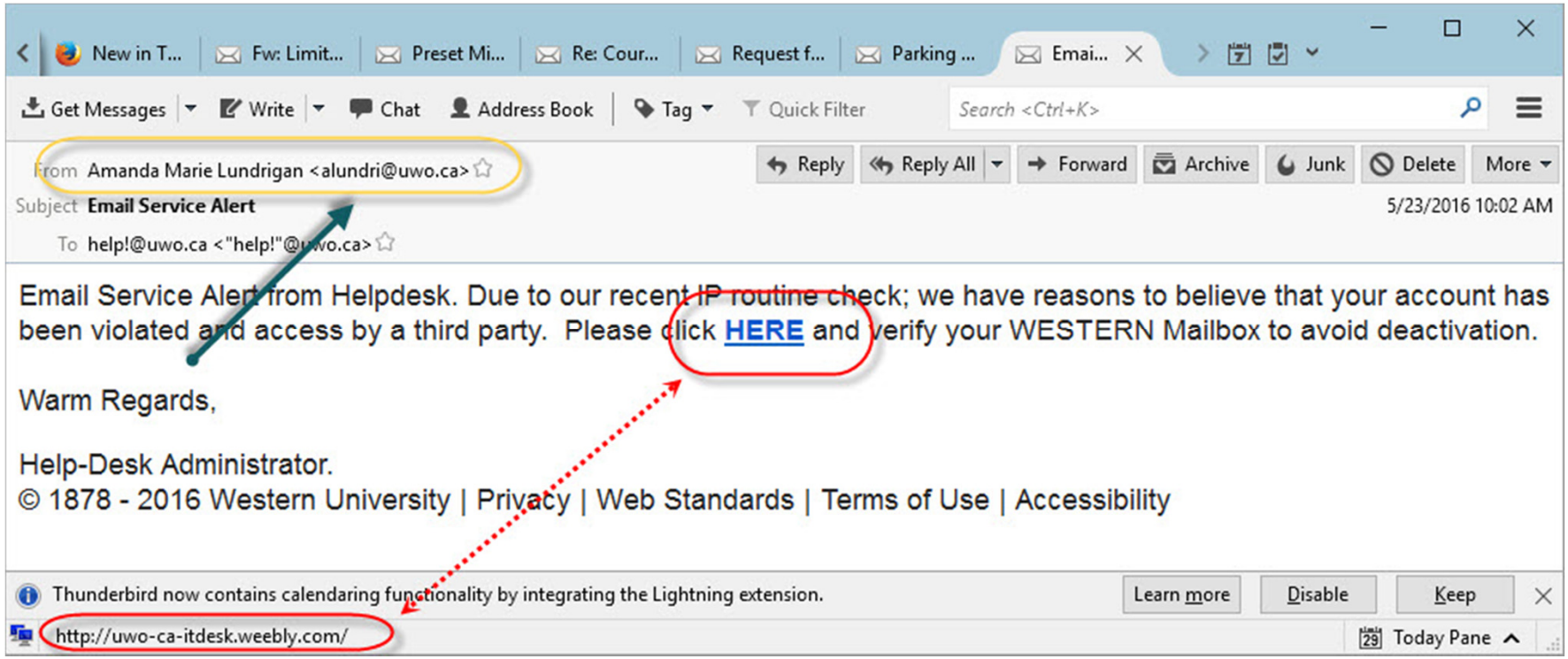
If you do not remember trying to access Online Banking on the above date and time, please select "That was NOT me."
You will then be prompted to safeguards your account.

That was me **That was NOT me**

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

MIS - Organization and Security

Phishing



Phishing

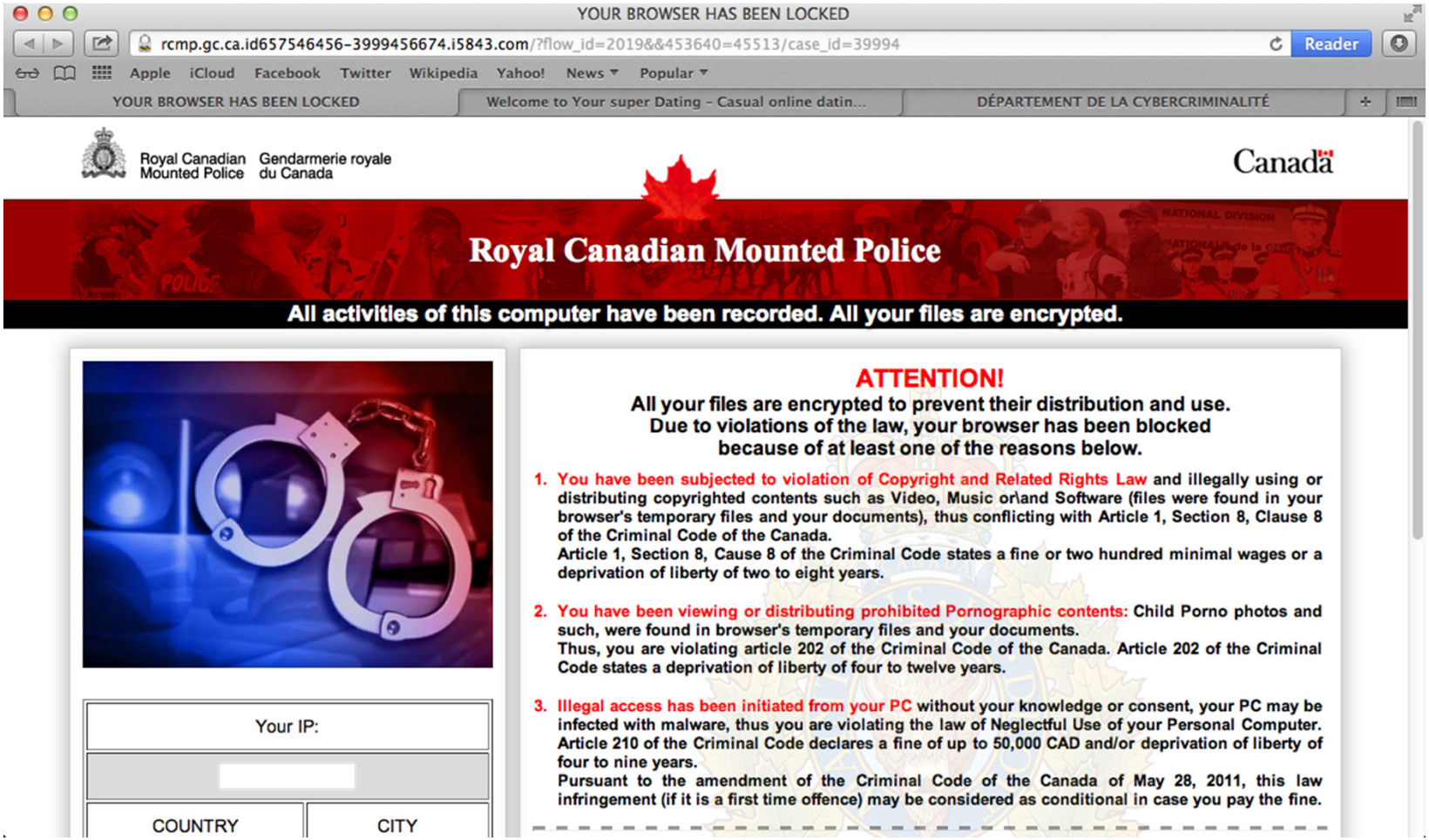
- Create a replica of an existing Web page to fool a user into submitting personal, financial, or password data
- Email is sent to direct you to the website that appears to be from a legitimate company.
- You are advised that information or a security check is needed on your account, and advised to click on a link to the company's website to provide the information.
- Link connects to a website that is an imitation of the spoofed company's actual website.
- These counterfeit websites and emails appear very authentic. **About ninety percent of all computer viruses are spread via eMail**

Phishing for Personal Data

- **Usually initiated by e-mail request**
  - Designed to cause you to click
  - Asks for personal data
  - May install spyware, malware, adware
- **Defenses**
  - Know your purchases and deal directly with vendors
  - Implausibility of e-mail
  - Don’t be misled by legitimate-looking graphics, addresses

MIS - Organization and Security

Ransomware



Sources of Security Threats

- **Human errors and mistakes**
  - Accidental problems
  - Poorly written programs
  - Poorly designed procedures
  - Physical accidents

Unauthorized Data Disclosers

- **PIPEDA**: **Personal Information Protection and Electronic Documents Act**
- Personal information is defined under this Act
  - information about an identifiable individual
  - not including name, title, business address, or telephone number of an employee of an organization
- **Act gives individuals the right to know why an organization collects, uses, or discloses their personal information**
- Act requires organizations to identify anyone who is responsible for keeping personal information private and secure

Unauthorized Data Disclosers

- **PIPEDA**: Types of problems
  - Human error
    - Posting private information in public place
    - Placing restricted information on searchable Web sites
    - Inadvertent disclosure
  - Malicious release
    - Pretexting
    - Phishing
    - Spoofing
    - Sniffing

Unauthorized Data Disclosers

- Malicious release
  - **Sniffing**
    - **Interception of computer communications**
    - Wired network
      - Requires physical connection
    - Wireless network
      - Access gained through unprotected network
      - "Drive-By"
    - Packet sniffers
      - Programs capturing data from information packets as they travel over the Internet or company networks.
      - Confidential information taken from the captured data

Unauthorized Data Disclosers

- Malicious release
  - Breaking into networks
    - Stealing data
      - Customer lists
      - Product information
      - Employee information
      - Other confidential data

Malicious Intent

- Hacking
  - Unauthorized access to and use of computer systems—usually by means of a personal computer and a telecommunications network.
  - Most hackers break into systems using known flaws in operating systems, applications programs, or access controls.
  - Some are simply motivated by curiosity and a desire to overcome a challenge, while some have malicious intent and do significant damage.

Malicious Intent

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

Technical Safeguards to protect against Threats

Involves hardware and software components

User names and passwords **(primary means of authentication)**

- Identification
- Authentication

Smart cards

- Personal identification number (PIN)

Biometric authentication

- Fingerprints, facial scans, retina scans

Single sign-on for multiple systems

Technical Safeguards to protect against Threats

Encryption and firewalls

Malware Protection against:

- Viruses
- Worms
- Spyware
- Adware

Technical Safeguards to protect against Threats

Data Safeguards

Malware safeguards

- Install antivirus and anti-spyware programs
- Scan hard drive and e-mail frequently
- Update malware definitions
- Open e-mail attachments only from known sources
- Install software updates promptly
- Browse only reputable Web sites

Technical Safeguards to protect against Threats

Account Administration

System procedures:

- Normal operation
- Backup
- Recovery

Definition and use of standardized procedures reduces the likelihood of computer crime

Security Complication

BYOD

Bring Your Own Device

- Laptop, Tablet and Smartphone

- how to secure devices brought into the workplace ?

- how to secure internal data from these devices ?