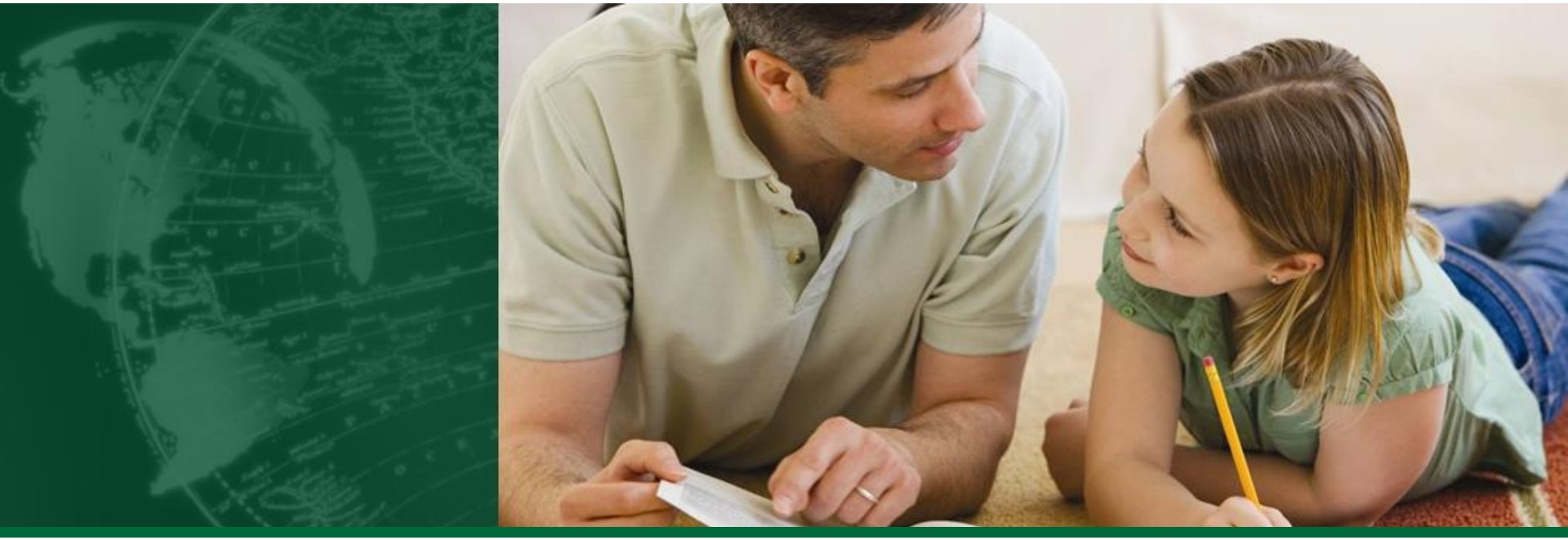
Manulife Financial

For your future™

Information Security (Canada, Other Asia and Support)
Self Learning Module



Manulife Business Processing Services

Source: https://manulife.csod.com, July 2011

Understanding Threats

- **Security threat or incident** – is any action that puts our information or resources at risk. Such incidents may result from malicious attempts to steal information or from simple inattention to a security policy or procedure.
- You have the power to stop most security threats. You are our organization's number one defense against security threats or incidents.

Understanding Threats: Types of Threats

Source: Compass

Understanding Threats: Types of Threats

- **Loss** – information is transported using many forms of media and, because it is transportable, it can easily be lost. Security breaches can occur as a result of losing:
  - USB drives
  - Laptops
  - Documents
  - CDs
  - Briefcases or purses
  - PDAs
  - Cell phones

Understanding Threats: Types of Threats

- **Theft** – can occur as a result of inattention to security procedures. For example, theft of confidential information can occur as a result of:
  - Leaving laptops left unlocked in the office, in cars, unattended in public places, or checked as luggage.
  - Leaving unsecured USBs in briefcases, purses, clothes pockets, or on a desk in the office.
  - Leaving documents containing sensitive information in plain view on an office desk.
  - Giving access to our building to people posing as an employee or repair person.
- **Theft** can also occur when you discuss sensitive information in public places or allow strangers to look over your shoulder at information on your computer.

Understanding Threats: Types of Threats

- **Cybercrime** – is any crime that involves a computer and a network. It can occur as a result of:
  - Connecting to an unsecured public hotspot to check e-mail messages.
  - Neglecting to keep security software up-to-date allowing malware to infect the computer.
  - Clicking a link in an e-mail to confirm personal information without verifying who the sender is.
  - Sending sensitive or confidential information in an unencrypted e-mail.
  - Opening e-mail attachments from unknown sources.
  - Posting sensitive or confidential information to social networking sites.

Practicing Safe Computing

- Our organization faces a rising number of computer-related threats that compromise the security of information and resources. We've developed safe computing practices to help combat electronic threats, protect against social engineering, create strong and secure passwords, safeguard your computer and network, and communicate securely. When you follow to our safe computing practices, you play an important role in preventing costly security breaches.

Practicing Safe Computing

- **Electronic Threats** – Most electronic threats involve malicious software, or malware. Any time you work online or download or share files, you expose our organization's computers and network to the risk of malware infection.
  - Be aware of warning signs of malware infection, including failed Web searches, a sluggish computer, firewall malfunction, and unexpected browser activities, such as excessive pop-ups. If you believe you are impacted by malware, follow our policies for reporting incidents.
- **Social Engineering** – is the clever manipulation of people in order to gain privileged information. Social engineers may attempt to gain access to buildings or try to elicit passwords or other sensitive information from you in person, on the telephone, or via online.
  - If you receive a suspicious request, always verify the identification of the person before acting and contact the appropriate person within our organization for assistance.

Practicing Safe Computing

- **Password Guidelines** – Password security is critical to keeping our organization's information secure. A strong password consists of a combination of normal characters (such as upper and lowercase letters and numbers) and possibly special characters (such as the pound sign or the dollar symbol).
- To make your password secure, change it frequently and protect it by not sharing it with others or leaving a written record of it on your desk.
  - Manulife's Password Requirements:
    - Minimum of 8 characters
    - Must meet complexity requirements (consists of a minimum of 3 of the following 4 attributes):
      - Uppercase letters,
      - Lowercase letters,
      - Numbers, and
      - Special characters (!, #, $, *, etc.)
    - Password life of 60 days
    - Maximum of 5 failed log-in attempts

Practicing Safe Computing

- **Electronic Safeguards** – The simple actions you take to protect your computer and other electronic devices are critical to our information security. Always remember to:
  - Follow our policies for keeping system security software running and up to date.
  - Never download unauthorized software or files.
  - Always turn on a password-protected screensaver when leaving your computer unattended.
  - Log off the network at the end of the day.
  - Secure laptops left at work in a locked drawer or with a locking cable.

Practicing Safe Computing

- **Electronic Communications Guidelines**
  - **Electronic communications** – including e-mail, instant messenger, testing, and social networking (such as Facebook, Twitter, and LinkedIn) –make it easy to communicate but also increase the risk of a security breach.
  - Follow these guidelines to secure information online:
    - Always encrypt e-mails that contain personal or sensitive information.
    - Be cautious when handling attachments or downloads, even if you know the sender.
    - Never assume that information you want to share is public knowledge. Do not send or post any sensitive, personal, or proprietary organization information on social networking sites or via e-mail.

Practicing Safe Computing

- **Instant Messaging** – treat instant messenger (IM) with the same caution as regular e-mail –be wary of attachments and do not send sensitive information via IM. Take extra care with hyperlinks embedded in instant messages. Because they take you directly to Internet sites, these links may be more dangerous than simple attachments. By clicking and IM link, you could initiate a dangerous download.

  - Use of IM services other that the company issued Lotus Notes Sametime Instant Messaging program at Manulife is not allowed.

Protecting Data: Introduction

- Mishandling sensitive data can cause our organization serious problems. Take a moment to read an example of what can go wrong when sensitive data is disclosed inappropriately.

Protecting Data

EMPLOYEE DISCLOSES MERGER IN ONLINE CHAT ROOM

- Today we're talking about the impact that inappropriate disclosure of sensitive data, or data leaks, can have on an organization. This type of information leak is in the news all the time. How does it happen?
  - *Guest: Data leaks most often occur when people simply forget to safeguard, or protect, sensitive information. In one recent case, an employee of a well-known local company was excited about a potential joint venture with one of his company's clients. Before the partnership was announced, the employee inappropriately disclosed some details about the impending deal in an online industry chat room.*
  - That sounds like trouble. What happened?
  - *Guest: Well, the employee responsible for the leak didn't mean any harm; he had simply made a few off-hand comments. But it caused serious problems for both organizations. There was a lot of press speculation and the partnership nearly fell through.*
  - I'm sure the employee didn't realize the possible impact of his casual chat.
  - *Guest: No, and that's the problem. We all need to stop and think before discussing business information about our company or our clients. This is true whether we're in a restaurant eating lunch with a fellow employee, exchanging e-mails with friends, or posting information on personal websites or public message boards. Company business needs to stay within the company—period.*

Protecting Data: Data Classifications

Source: Compass

Protecting Data: Data Classifications

- **Regulated** – Information for which unauthorized disclosure, access, modification or destruction has negative legal, statutory or regulatory impact. Regulated information is protected by law and any unauthorized external or internal access to this information would be detrimental to MFC and its stakeholders.
  - **EXAMPLES:**
    - Protected Health Information (PHI)
    - Personally Identifiable Information (PII), such as Social Security/Insurance Number, Identification Card number, etc.
    - Credit card numbers
    - Stock or mutual fund transaction information and other regulated financial data

Protecting Data: Data Classifications

- **Restricted** – Information for which unauthorized disclosure, access modification, or destruction, would have a negative impact to MFC and its stakeholders. Unauthorized access to restricted information could influence MFC's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence.
  - EXAMPLES:
    - Information restricted to specific individuals on a need-to-know basis (e.g., merger and acquisition deals)
    - Legal cases
    - Human Resource issues
    - Any information that you would not want everyone in the Company to be able to see
  - DEFAULT CATEGORIZATION: When attempting to classify your data, and you are unsure how to rate it, always use "restricted" as the default classification.

Protecting Data: Data Classifications

- **Internal** – External access to this information is to be prevented or can only be provided upon approval from the Information Owner. Internal information is widely-disseminated within the Company and access to the information is not restricted internally.
  - **EXAMPLES**
    - Company news and articles
    - Organization charts/Employee telephone lists
    - Policy, standards, and process documentation
- **Public** – Information intended for public consumption.
  - **EXAMPLES:**
    - Press releases
    - Annual reports
    - Product and services brochures and other marketing materials
    - Marketing materials that are approved for release to the public

Protecting Data: Data Transmission Guidelines

- If the nature of your work requires you to transmit sensitive data, whether electronically or non-electronically, be sure to follow our organization's approved procedures. Review the guidelines for data transmission.

Source: Compass

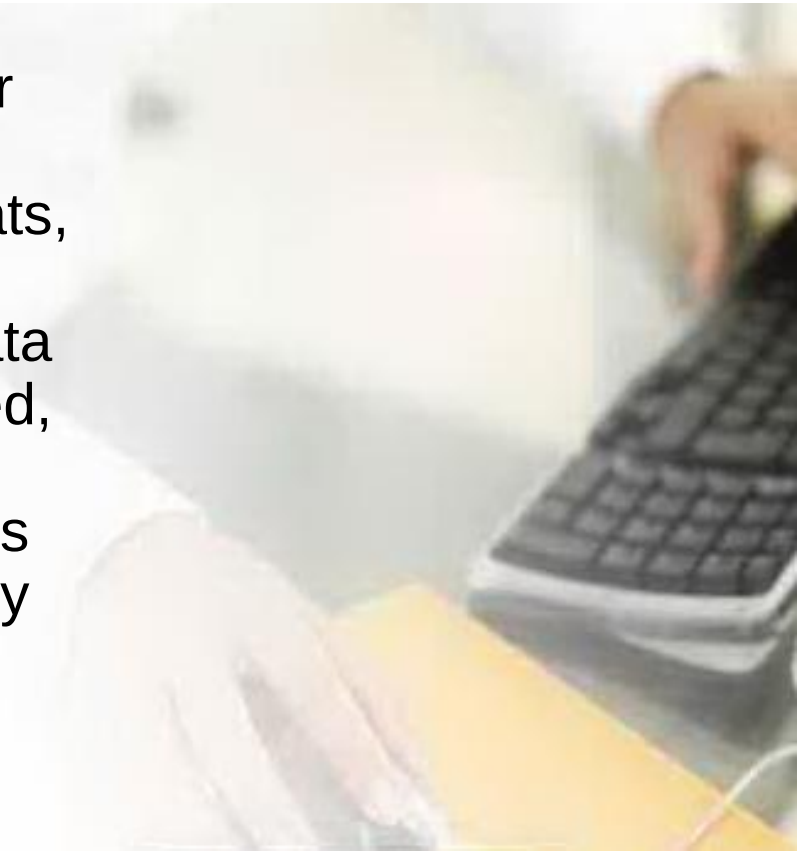
Protecting Data: Data Transmission Guidelines

- **File Transfers Via FTP** – FTP stands for 'File Transfer Protocol.' This is the language used to transfer files on the World Wide Web. An 'anonymous' FTP site is a file transfer server that does not require users to log in with a username and password. An anonymous FTP site is not secure because it can be accessed by many other users.
  - If you transfer files via an FTP server, be sure you follow our company's policies to secure the transaction.

Source: Compass

Protecting Data: Data Transmission Guidelines

- **System Backup** – Losing sensitive data can cause serious problems for any organization. Data loss can be caused by malicious computer threats, but it can also be caused by carelessness or natural disaster. Data loss can be reduced, if not eliminated, by one simple solution—backing up essential files. While backup routines take time, the payoff in data recovery is worth it. Be sure to follow our organization's backup procedures. Below are some tips to help prevent data loss.



Source: Compass

Remote and Mobile Computing: Introduction

- You need to be extra careful if you use a laptop or other portable devices. Take a moment to read several stories about mobile computing risks and some tips on how to protect yourself.

Source: Compass

Remote and Mobile Computing: Privacy

- **WATCH OUT WHEN YOU WORK WHILE TRAVELING**

  You really need to use extra caution to keep your conversations private in public places. And make sure your computer screen is secure from onlookers who can be watching from the seat next to or behind you.

  There was one recent case in which a sales representative from our company was completing a proposal for a client meeting while traveling by plane. The proposal included some very sensitive pricing adjustments. Although the sales rep had turned her screen away from her neighbor, she didn't think about the fellow behind her. The man had a clear view of the sales rep's laptop screen and also happened to be a friend of the rep's main competitor. Using the technique known as 'shoulder surfing,' he read the proposal and made a mental note of the pricing structure. You can imagine how shocked the sales rep was when she later met with her prospective client and discovered that her competitor had come in right below her price.

  Make sure you don't fall victim to this sort of information theft. Don't work in public spaces if you can't ensure the privacy of your work.

Remote and Mobile Computing: Security

- **MAKE SURE THAT PUBLIC WIRELESS CONNECTIONS ARE SECURE**

  You've probably heard stories about information being hijacked over wireless connections. Well, here's my story.

  Last week, I was stuck in an airport terminal for six hours due to bad weather. Since I had so much time on my hands, I decided to check my e-mail. My laptop has wireless access, so I managed to tap into a 'free' wireless service from a local vendor instead of paying the $15 fee to access the airport-endorsed site. Choosing a cheap alternative didn't pay off.

  A wireless hacker accessed my work e-mail account and sent obscene messages to all of the people in my address book, including my boss and a number of our major clients. I was humiliated! It took countless phone calls and many, many apologies to get the whole mess straightened out.

  I never imagined how much that 'free wireless service' would end up costing me!

Remote and Mobile Computing: Sensitive Information

- **KEEP CONFIDENTIAL CUSTOMER INFORMATION SECURE**

  Last week, I was involved in a client presentation with one of my coworkers. We made a presentation using files stored on his thumb drive.

  When the presentation was complete, we neglected to retrieve the thumb drive from the client's USB port before dashing off to our next appointment. The client called to let my colleague know that she had the thumb drive—and also to express her concern about the lack of security of confidential information. The thumb drive stored other files that contained confidential information about a number of our clients.

  Although this client did not use the information (she said she hadn't even looked at it), she was very upset about our handling of such sensitive files. The client's confidence was definitely eroded, and my colleague and I will really have to work to rebuild that trust.

Remote and Mobile Computing

Working in Public Places

- Be wary when you work in public places—remember that you are not alone! Sensitive information may be at risk when you work on public computers, use your laptop or other portable devices in a public place, or conduct business on your cell phone. In today's fast-paced world, it's sometimes necessary to work with sensitive information while commuting or in other public areas. But there are risks you need to be aware of. Let's look at some of these risks and ways you can protect yourself.

Remote and Mobile Computing

Working in Public Places

- **Using public computers** – public computers in libraries, Internet cafes, airports, and copy shops are convenient, but they are not necessarily safe. They are prohibited for work use, even the checking of e-mail. If you plan to use one personally, the following tips will help you protect your sensitive information.
  - Always log out of Web sites by pressing “logout” on the site.
  - Avoid entering sensitive information into a public computer.
  - If you have access sensitive information, don’t leave the computer unattended with the information on the screen.
  - Erase your tracks. If you access sensitive information. Clear the browser list of all of the sites you’ve accessed.

Remote and Mobile Computing

Working in Public Places

- **Eavesdropping** – occurs when someone secretly listens in on a private conversation. Here are some ways to protect yourself from eavesdropping:
  - Watch your volume when conducting business in restaurants or over cell phones.
  - Make sure you're aware of people within listening range of your conversations.
  - To be completely safe, hold sensitive conversations in private locations.

Remote and Mobile Computing

Working in Public Places

- **Shoulder Surfing** – refers to looking over a person's shoulder to obtain information. In some cases, shoulder surfing is done for no other reason than simple curiosity. However, shoulder surfing may be a deliberate attempt to steal private information such as your password, credit card number, or pin number.
  - Keep your laptop and other portable devices protected and away from the sight lines of other people.
  - If you're dealing with sensitive information and can't be sure that you won't be observed, postpone working until you are in a private location.

Remote and Mobile Computing

Protecting Mobile Computing and Communications Devices

- Physical protection of your laptop and other mobile computing and communication devices is an important responsibility. Theft of your mobile equipment could result in the loss of sensitive data, resulting in financial loss, legal problems, and damaged relationships.
- Mobile computing devices, such as PDAs, cell phones, laptops, and portable drives are susceptible to security attacks. Take a look at some mobile computing tips that will help you protect the devices that you carry in your pocket, purse, or briefcase.

Source: Compass

Remote and Mobile Computing

Protecting Mobile Computing and Communications Devices

- **Mobile Computing Tips**
  - Keep your mobile computing devices in your possession at all times to protect them from theft.
  - Lock your mobile devices and protect them with secure passwords when not in use.
  - Download programs and content, such as photos, ring tones, mobile device themes, and games, only from reputable sources.
  - Record serial and model numbers. Reference numbers can help police and security personnel to recover stolen devices.
  - Encryption software has been installed on your company issued device(s) to protect the data contained on them.

Remote and Mobile Computing

Public Wireless Connections

- If your work requires you to use public wireless connections, these tips will help you keep your work secure:
  - **Use a software firewall.** A firewall is a protective boundary that monitors and restricts information that travels between your computer and a network or the Internet.
  - **Use secure, encrypted networks.** If a network is not encrypted, you should not use it to access sensitive data.
  - **Don't type in passwords and other sensitive information.** Firewalls and hidden files will provide some protection against casual hackers and identity thieves who prey on wireless networks. But if the intruders are determined, they will eventually find a way to get around any security system. If you want to be safe, avoid typing any sensitive information into your computer while using a public wireless network.

Remote and Mobile Computing

Wireless Connections at Home

- If you work at home using a wireless network, take these precautions:
  - Use Wi-fi Protected Access (WPA), a standard method for encrypting traffic over a wireless network that can deter casual hackers.
  - Change the default service set identifier (SSID) set by the wireless router's manufacturer and disable its broadcast. This helps to prevent hackers who know the common device default 'pass phrases' from using your wireless connection.
  - Disable or modify simple network management protocol (SNMP) settings. If you don't take this step, hackers can use SNMP to gain important information about your network.
  - Use access lists. If possible, implement an access list to further secure your wireless network. Doing so will allow you to specify exactly what machines are allowed to connect to your access point.

Remote and Mobile Computing

Wireless Connections at Home

OUR POLICY

- **Prohibited Activities:**
  - 1. Modifying the MFC laptop configuration in any unauthorized way is prohibited, including changing wireless configuration.
  - 2. Wireless access point MUST NOT be connected to MFC's internal network unless explicitly authorized by MFC's Information Security Office and Network Support Organization.
  - 3. Connections from MFC-owned computing devices must not be made to non-public Wireless Access Points for which the owner has not provided explicit connection permission.

Remote and Mobile Computing

Remote Access to Company Network

- If you connect to our company's network remotely, you must follow specific procedures for accessing our network and restrict your activities to those authorized for remote access. Otherwise, you may jeopardize network security.
- OUR POLICY: Remote access to the company network is only allowed through a company issued and authorized VPN solution. Access to the company network from a kiosk or "public" PC (library, airport, etc.) is prohibited.

Source: Compass

Remote and Mobile Computing

Traveling Securely

- Take extra safety precautions if you travel for business. For example, carry your laptop onto airplanes instead of checking it with your luggage. Put a marker, such as a sticker or label, on the laptop so that you can easily recognize it when you pass though airport security; many laptops look alike. During airport screening, always maintain control of your laptop. Keep an eye on it as it goes through the security scanner; do not pass through the security entrance until your laptop moves into the scanning area. Retrieve it on the other side before putting on your shoes or collecting your other belongings.

Source: Compass

Remote and Mobile Computing

Traveling Securely

- Here are more safety precautions to keep in mind when traveling:
  - Update your contact information and alternate numbers in company records before you leave.
  - Pack lightly, carry a minimum amount of valuables, and use discreet luggage.
  - Allow plenty of time to make travel departures; criminals prey on travelers who are in a hurry.
  - When in transit, keep your carry-on luggage and mobile devices with you at all times.
  - Avoid displaying company logos or references to geographic locations.
  - Secure your laptop and other hand-held devices when you are away from your hotel room; for example, lock them in a room safe.
  - If possible, do not leave your laptop and other hand-held devices in your hotel room or with the front desk.
  - On public transportation, hold your laptop securely at all times.
  - Consider buying and using a laptop security alarm and lock.

Thank you. This is the end of the module. Please proceed to answering the Information Security (Canada, Other Asia and Support) Quiz.

Thank you

Manulife Financial

For your future™