Fraud protection module

Trainer's introduction

While the vast majority of financial transactions are legitimate and honest, the few fraudulent ones can be costly and damaging. By recognizing the warning signs for questionable transactions, people can avoid most of the risks for financial fraud and protect their assets. In this module, Mini-module 1 shows how to recognize the most common types of fraud and Mini-module 2 shows how to protect yourself from them. Mini-module 2 also reviews how to use credit and debit cards safely, create strong passwords and avoid risks on social networking sites.

Learning objectives

After covering the topics covered in the module and this workshop, learners will be able to:

- Describe how credit card fraud takes place and how it can affect them
- Recognize potentially fraudulent credit card transactions and take steps to avoid them
- Describe how identity theft takes place and how it can affect them
- Recognize potential risks for identity theft and take steps to avoid them
- Recognize potentially fraudulent e-mails, telephone calls and other messages and take steps to avoid them
- Recognize potentially fraudulent job offers and take steps to avoid them
- Recognize potentially fraudulent investment schemes and take steps to avoid them
- Describe appropriate and inappropriate types of personal information to include on social networking sites
- Recognize the need to set privacy options on social networking sites to reduce fraud risks
- Describe how to protect themselves from various frauds and scams
- Find up-to-date information about potential frauds and scams
- Assess their own risk for fraud or scams
- Take appropriate steps if they are victims of identity theft or fraud

Materials/equipment required

- Copies of selected mini-modules or activities for participants
- Chart paper and markers for the activity, Types of fraud (Mini-module 1)
- PowerPoint file: Fraud protection
- PowerPoint projector and screen
- Internet connection (if using)

Time required

	To do all the activities in this module would require approximately:	To complete the module in one hour, focus on:
Introduction	• 10 minutes	• Activity 1
1: How to recognize fraud	• 90 minutes	• Activity 3 (Types of fraud) • Activity 5 (How to spot fraud)
2: Protect yourself from fraud	• 30 minutes	• Slides 14 to 18 • Activity 10 (Avoiding investment scams)
Action plan	• 5 minutes to get started	• Activity 12 (Action plan)

Suggested activities and PowerPoints

Use the slides and the online modules. The text provides additional information, items that are not easily represented in a slide, worksheets and other references.

Select the slides you will need for your presentation. *You will not need all the slides if you don't plan to cover all the topics.*

Introduction

Customize the agenda as needed. Introduce the workshop topic and outline the contents.

Slide 1: Fraud protection title page

Fraud protection

Slide 2: Agenda

Agenda

Start time: _____
Break time: _____ (10 minutes)
End time: _____

Please set phones to silent ring and answer outside of the room

Activity Icebreaker: Fraud awareness

Have participants complete the Fraud awareness quiz in the How to recognize fraud mini-module. Use the slide, Fraud awareness quiz answers, to briefly review the correct answers.

Extend the discussion by asking questions such as the following:

- What do your results tell you about your own understanding of fraud?
- How extensive is the risk of fraud in Canada?
    - **Answer:** Although the majority of individuals and businesses are trustworthy, Canadians lose millions of dollars to fraud every year, and most people have probably seen many fraudulent emails and similar appeals. Canadians can avoid most financial frauds by being aware of the risks and taking simple steps to avoid them.
- If there's one thing you want to learn in this session, what would it be?
- What's the most important thing to know about financial fraud as you manage your personal finances?
- If there's one thing you could already tell your best friend about financial fraud, what would it be?

Conclude the activity by summarizing some things people already know. Explain that the session is going to build on what people know to help participants protect their finances more effectively.

Slide 3-4-5-6-7-8-9: Fraud awareness quiz answers

1. Fraud artists usually target people with little education.
   True or **false**?

2. Legitimate lotteries and sweepstakes charge fees to deliver your prize.
   True or **false**?

3. The top method used to solicit Canadian consumers for mass marketing fraud in 2009 was:
   a) telephone
   b) email
   c) Internet.

4. If a telemarketer offers you a low-interest credit card, you must send money before your card is activated.
   True or **false**?

5. If you receive an email from an organization asking that you verify your account information within 24 hours or your account will be frozen, the best thing to do is:
   a) reply to the email asking them why they want this information
   b) reply to the email with the information asked for
   c) report the email to the actual organization and then delete the email.

6. In 2009, the total reported dollar loss by victims of identity theft in Canada was about:
   a) $7 million
   b) $9 million
   c) $11 million

7. Most fraud is committed by strangers who get your personal financial information through illegal means.
   True or **false**?

Slide 10: Fraud protection

This module covers:

- What the most common frauds and scams are, and how they work
- How to spot the warning signs that an offer or a communication may be fraudulent
- How to protect your money and your financial identity
- What to do if you, or someone you know, becomes a victim of fraud

Mini-module 1: How to recognize fraud

Slide 11: Title slide: How to recognize fraud

How to recognize fraud

Overview

Slide 12: How to recognize fraud

This section covers:

- What the most common frauds and scams are, and how they work
- How to spot the warning signs that an offer or a communication may be fraudulent

Activity Fraud awareness quiz

If you skipped the Icebreaker activity on the Fraud awareness quiz, do the activity now.

Types of fraud

Activity Types of fraud

Divide participants into five groups, and have each group read one section of the Types of Fraud section of the How to recognize fraud mini-module, as follows:

- Group 1: Mass marketing fraud
- Group 2: First half of Investment fraud
- Group 3: Second half of Investment Fraud
- Group 4: Payment scams and Credit card and debit card fraud
- Group 5: Other Frauds, including Affinity Fraud

Have each small group make a chart summarizing their section, present it to the whole group and answer questions for clarification. Extend discussion with questions such as the following:

- How can you keep track of all these types of fraud?
    - **Answer:** You don't have to know all the details to be aware of the risk of fraud and how to avoid it. Be alert for anything that looks like one of the common

types of fraud, that presents information or tips that you cannot check out, or that seems too good to be true.

- How much should you rely on advice by your friends and colleagues?
  - **Answer:** If you can check out their research and confirm it yourself, it may be worthwhile. But remember that family, friends and colleagues can be mistaken or victims of fraud, and scammers sometimes pretend to be a friend just to defraud you.
- How can you keep aware of common scams?
  - **Answer:** Organizations like the police, the Canadian Anti-Fraud Centre and the Better Business Bureau publish information about current scams on their websites, in newspapers and in other media.

Slide 13: Why do people fall for financial frauds?

- Many of us want something for nothing
- We believe what people tell us
- Fraud artists are very convincing
- Fraud artists use pressure tactics
- Fraud artists play on our desire to support a good cause
- We're embarrassed if we fall for a scam

Activity VIDEO: Debit and credit card fraud

Introduce the video and give participants a copy of the video response sheet. Have them answer the questions on the sheet as they view the video and when it ends.

Following the video, ask some participants to share their comments with a neighbour or with the group.

Extend the discussion by asking questions such as the following:

- Can anyone describe a time when they or someone they know had a debit or credit card compromised and what happened?
- What other electronic devices could be compromised like a debit card?
  - **Answer:** Devices like a cell phone could be compromised if you use it for financial transactions, and new technologies such as electronic transit passes or passports could become compromised if you do not keep them and any passwords secure.

Video response sheet Name: _____ Date: _____ Name of video: _____	
What points in the video do you agree with?	What points in the video do you disagree with?
What points in the video do you need more information about?	
If you had to summarize the video for a friend, what would you say were the most important points?	

How to spot fraud

Activity How to spot fraud

Divide participants into groups of three or four and assign each group to one of the following examples of fraud from the How to spot fraud – The Warning Signs section of the How to recognize fraud mini-module: Phishing, Brilliant Equity Marketing Associates and Item for Sale. Have the groups read the Warning Signs, and then find any signs in the examples of scams in the mini-module.

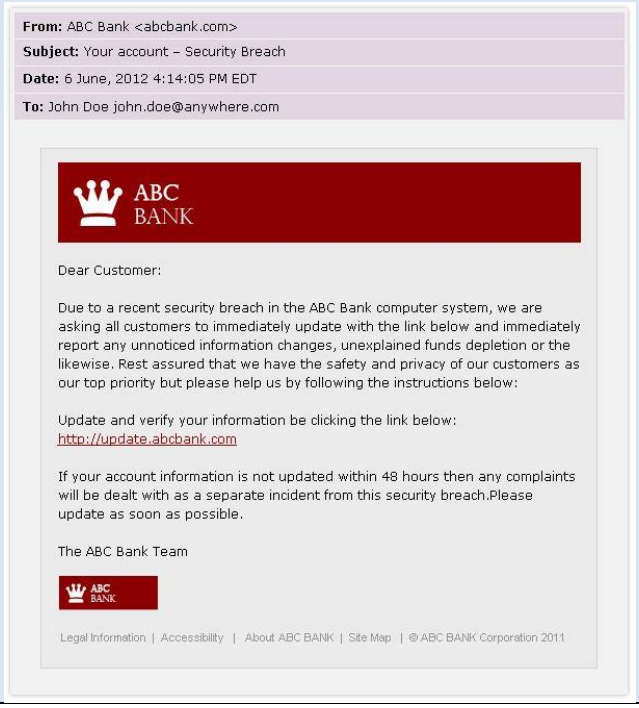
Using the slides following, review the examples with the class, and have the groups point out the signs of a scam that they found in the sample they reviewed.

Extend discussion with questions such as the following:

- Can anyone describe a time when they or someone they know saw a scam similar to the ones in the examples?
    - **Answer:** The examples are based on common financial and consumer scams, so participants may have seen various scams like them.
- How can you avoid common scams like these?

- **Answer:** Be aware of the warning signs and be sceptical of anything that looks too good to be true. Don't be rushed and find out what a legitimate offer looks like.

Slide 14: Phishing



From: ABC Bank <abcbank.com>
Subject: Your account – Security Breach
Date: 6 June, 2012 4:14:05 PM EDT
To: John Doe john.doe@anywhere.com

ABC BANK

Dear Customer:

Due to a recent security breach in the ABC Bank computer system, we are asking all customers to immediately update with the link below and immediately report any unnoticed information changes, unexplained funds depletion or the likewise. Rest assured that we have the safety and privacy of our customers as our top priority but please help us by following the instructions below:

Update and verify your information be clicking the link below:
http://update.abcbank.com

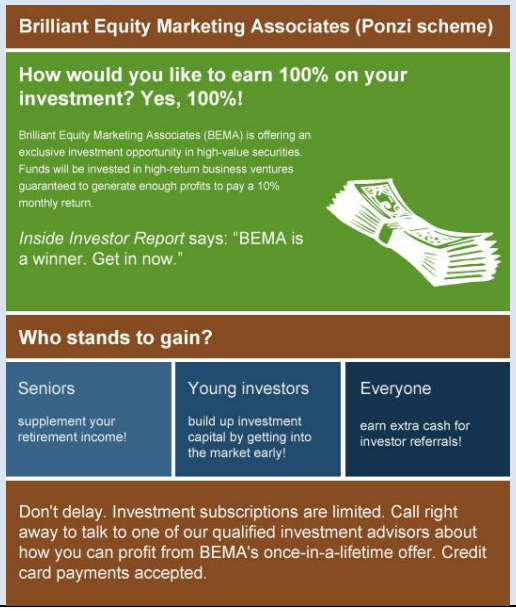
If your account information is not updated within 48 hours then any complaints will be dealt with as a separate incident from this security breach.Please update as soon as possible.

The ABC Bank Team

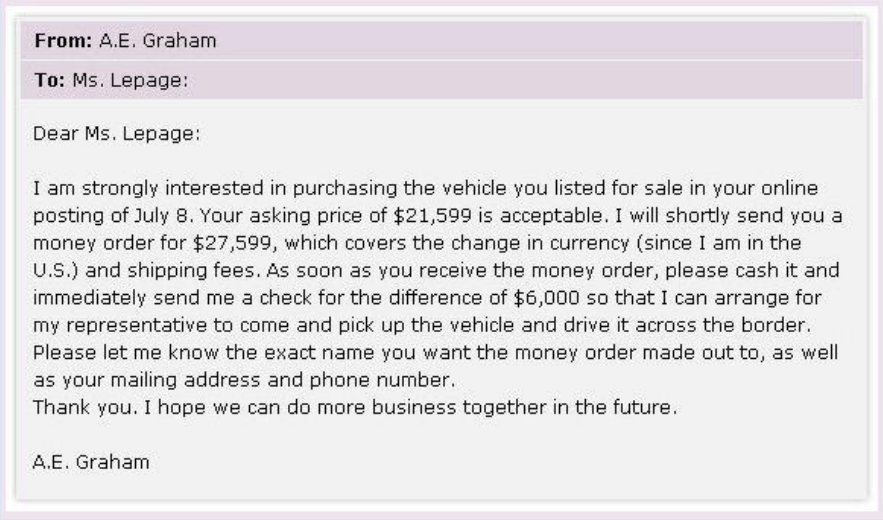
ABC BANK

Legal Information | Accessibility | About ABC BANK | Site Map | © ABC BANK Corporation 2011

Slide 15: Brilliant Equity Marketing Associates



Slide 16: Item for sale



From: A.E. Graham

To: Ms. Lepage:

Dear Ms. Lepage:

I am strongly interested in purchasing the vehicle you listed for sale in your online posting of July 8. Your asking price of $21,599 is acceptable. I will shortly send you a money order for $27,599, which covers the change in currency (since I am in the U.S.) and shipping fees. As soon as you receive the money order, please cash it and immediately send me a check for the difference of $6,000 so that I can arrange for my representative to come and pick up the vehicle and drive it across the border. Please let me know the exact name you want the money order made out to, as well as your mailing address and phone number.
Thank you. I hope we can do more business together in the future.

A.E. Graham

Activity AUDIO: Phone solicitation

Refer participants to the How to spot fraud – The Warning signs section in the How to recognize fraud mini-module, and have them refer to the tips as they listen to the audio dramatization of a fraudulent phone call.

Play the audio link and have participants take notes as they listen about what the person on the phone does right or does wrong as they listen. (Replay the audio if necessary for participants to understand the situation.)

Following the audio, ask some participants to share their responses with the group.

Extend the discussion by asking questions such as the following:

- What other types of phone scams have you heard of?
    - **Answer:** Automated calls may ask you to enter an account number or PIN on the phone's key pad, or switch you to another line that charges high fees.
- What should you do if you suspect a scammer is on the phone?
    - **Answer:** Don't give any information and hang up. Banks and other institutions do not ask for your personal information on the phone, unless you phone them at an official phone number.

Activity Summary of key messages

Have participants in pairs or small groups discuss and write down the three or four most important things they learned during the session.

Ask a few to compare their lists with the Summary of key messages (in the text or PowerPoint slide).

Clarify any misunderstandings and point out how the messages build on the topics participants identified in the first activity.

Slide 17: Summary of key messages

- Fraud can target anyone
- Watch for many different types of fraud
- Be aware of the tricks that fraud artists use
- Never send money unless you know an offer is legitimate
- Never give personal information unless you know the person asking is legitimate

Mini-module 2: Protect yourself from fraud

Slide 18: Title slide: Protect yourself from fraud

Protect yourself from fraud

Overview

Slide 19: Protect yourself from fraud

This section covers:

- Steps to take to protect yourself and your family
- How to safeguard your passwords and PINs
- How to use social networking sites safely
- What to do if you are approached or become a victim of fraud

Activity Your risk for fraud

Have participants complete the Your risk for fraud quiz in the Protect yourself from fraud mini-module and score themselves.

Prompt discussion by asking questions such as the following:

- What do your results tell you about your own risk for fraud?
- Is it better to be too trusting or too suspicious?
    - **Answer:** You should be sceptical about anything involving your money, even if you think that a financial opportunity is a good one. Healthy scepticism will protect your money and let you safeguard it for the things that really matter to you.

Password do's and don'ts

Slide 20: Password do's and don'ts 1

Don't:

- Store PINs and passwords where anyone can find them
- Use the same PIN and password for different uses
- Use personal information that is easy to figure out
- Use a password that is the same as your account name
- Use PINs and passwords that are easy to spot while typing

Slide 21: Password do's and don'ts 2

Do:

- Use at least eight characters
- Use at least:
    - One capital letter
    - One lowercase letter
    - One number or special character
    - No spaces
- Use many different characters
- Change PINs and passwords often

Activity Create a password

Use the slide, Create a password, to review how to create a password and demonstrate how to use the online password tool.

Have participants use the tips on the slide or the password tool to create a secure password and check it using the checklist in the PIN and Password do's and don'ts section of the Protect yourself from fraud mini-module.

Prompt the discussion by asking questions such as the following:

- What makes these passwords more secure than other ones?
  - **Answer:** They are hard to guess because there are many characters and the variations are not logical, but they are still easy to remember so you don't have to write them down.
- How can you keep these passwords secure?
  - **Answer:** Change them regularly by using variations based on a regular pattern you know.

Slide 22: Create a password

- Use the initials from a phrase you'll remember
- Misspell the words
- Switch numbers or symbols for letters
- Use an online password tool
  - E.g.: FCAC password tool

Fraud protection in other areas

Slide 23: Tips for social networking

- Never post anything that scammers could use (date, birthplace, etc.)
- Set security and privacy options for maximum security
- Limit your "friends" to people you know
- Be alert for scam messages
- Don't allow services to scan your addresses
- Watch out for apps that could read your data

Tip

Point out that there are fraud protection tips for a variety of situations in the Protect yourself from fraud mini-module, which participants can review any time.

Activity VIDEO: Avoiding Investment Scams

Introduce the video and give participants a copy of the video response sheet. Have them answer the questions on the sheet as they view the video and when it ends.

Following the video, ask some participants to share their comments with a neighbour or with the group.

Extend the discussion by asking questions such as the following:

- How can investors avoid potential investment frauds?
  - **Answer:** Be aware of the red flags, always get advice from a licensed investment professional, always ask for proper documentation, don't invest if you have any concerns.
- How should you respond if a friend offers a good investment tip?
  - **Answer:** Research thoroughly if you think the investment matches your investing goals and get independent advice. Even friends can be mistaken or victims of fraud.

Video response sheet

Name: _____ Date: _____

Name of video: _____

What points in the video do you agree with?	What points in the video do you disagree with?
What points in the video do you need more information about?	

If you had to summarize the video for a friend, what would you say were the most important points?

Slide 24: If you become a victim

Report frauds to stop the fraudsters

Type of fraud or scam	Whom to contact

Identity theft or Internet fraud	• Local police or Royal Canadian Mounted Police (RCMP)
	• In Quebec: Sûreté du Québec
	• Your financial institution
	• Canada's two main credit bureaus:
	  ◦ Equifax Canada
	  ◦ TransUnion Canada

Investment fraud	• Your provincial or territorial securities regulator (A list of all regulators is on the Canadian Securities Administrators website).
Tax fraud or a questionable charitable organization	• Canada Revenue Agency
Consumer fraud or fraudulent business activity	• Better Business Bureau • Local police
Credit card and debit card fraud	• Your financial institution • Financial Consumer Agency of Canada
General frauds	• Local police or RCMP • Financial Consumer Agency of Canada • Canadian Anti-Fraud Centre

Activity Summary of key messages

Have participants in pairs or small groups discuss and write down the three or four most important things they learned during the session.

Ask a few to compare their lists with the Summary of key messages (in the text or PowerPoint slide).

Clarify any misunderstandings and point out how the messages build on the topics participants identified in the first activity.

Slide 25: Summary of key messages

- Learn the steps to protect yourself from fraud
- Use strong PINs and passwords
- Limit personal data on social networking sites
- If you are a victim of fraud, contact the authorities right away

Fraud protection Action plan

Activity	Fraud protection Action plan

Have participants review the Fraud protection Action plan.

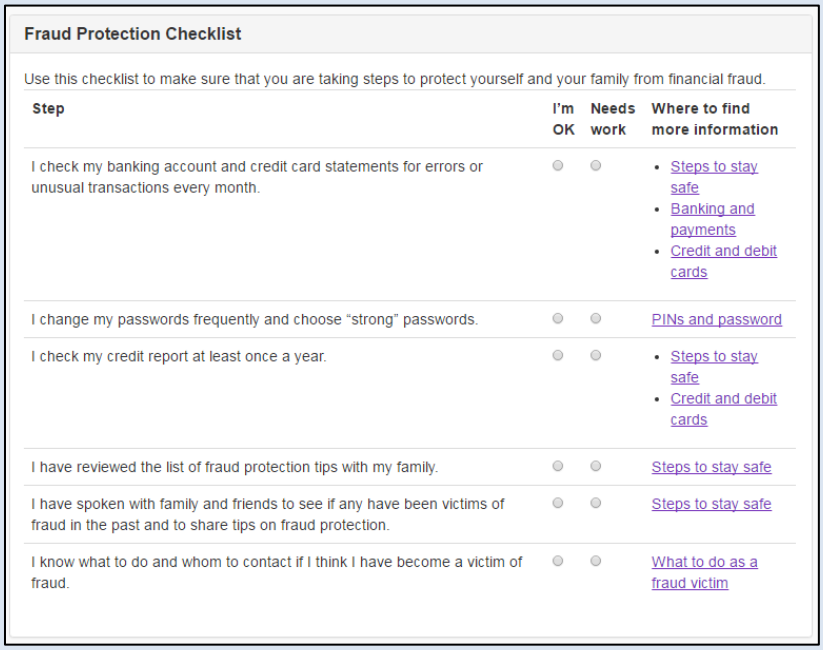
Have participants check off any action that they may need to take. Ask participants to decide when and how they will take the action they need.

Ask if any participants are willing to share their plans for action.

Extend discussion with questions such as the following:

- What's the first step you need to do to better protect yourself from fraud?
- What items on the checklist need the most work?
- What makes some items on the checklist harder to do than others?
- What other types of fraud protection do you need more information about?

Slide 26: Fraud protection Action plan



Fraud Protection Checklist

Use this checklist to make sure that you are taking steps to protect yourself and your family from financial fraud.

Step	I'm OK	Needs work	Where to find more information
I check my banking account and credit card statements for errors or unusual transactions every month.	○	○	• Steps to stay safe • Banking and payments • Credit and debit cards
I change my passwords frequently and choose "strong" passwords.	○	○	PINs and password
I check my credit report at least once a year.	○	○	• Steps to stay safe • Credit and debit cards
I have reviewed the list of fraud protection tips with my family.	○	○	Steps to stay safe
I have spoken with family and friends to see if any have been victims of fraud in the past and to share tips on fraud protection.	○	○	Steps to stay safe
I know what to do and whom to contact if I think I have become a victim of fraud.	○	○	What to do as a fraud victim