

Module 8: Protecting Your Identity



Welcome to **Module 8 – Protecting Your Identity**. Module 8 introduces participants to their “personally identifiable information” (PII), how that information can be used by thieves and ways that we can protect our information and identities.

Objectives:

- Understand what personally identifiable information (PII) is and why it is important to protect.
- Identify ways that people can steal your identity.
- Learn how to protect your identity.
- Learn what to do when you suspect your identity has been stolen.

Value of This Module:

Myth: My identity is protected because I receive a public benefit.

Reality: There are a variety of ways that an individual’s identity can be stolen and receiving a public benefit does not protect your identity.

MODULE 8: PROTECTING YOUR IDENTITY

FACILITATOR PREPARATION



Facilitator Preparation:

To prepare for the delivery of Module 8, the facilitator should read and review the following materials:

- Session Agenda
- Pre- and Post-Test Evaluation
- Facilitator Script
- Activity Instructions and Materials
- Referenced Resources
- PowerPoint Presentations
- Review the following websites:
 - consumer.ftc.gov/topics/privacy-identity-online-security
 - <https://www.consumerfinance.gov/about-us/blog/five-ways-you-can-guard-against-identity-theft/>
 - <https://www.idtheftcenter.org>
 - <https://reportfraud.ftc.gov/#/>

Gather:

- Laptop and LCD projector
- Sign-in sheet
- Easel pad and easel
- Markers
- PowerPoint presentation (*Make copies* to distribute to attendees.*)
- Agenda (*Make copies if you would like to distribute to attendees.*)
- Activities (*Make copies of activity handouts.*)
- Homework assignment (*Make copies.*)
- Evaluation (*Make copies.*)

**Don't forget large print copies, in size 20 font, if requested.*

MODULE 8: PROTECTING YOUR IDENTITY

PRE- AND POST-TEST EVALUATION



Location of session: _____

Date of session: _____










Trainers: _____, _____

Participant type (please check one):
 Person with a developmental disability
 Parent
 Other, please specify _____

Participant name (optional): _____

Please complete this section BEFORE the beginning of this training session.










1. How much do you know about the following topics?

	I don't know anything about this	I know a little about this	I know a lot about this
a. What Personally Identifiable Information (PII) is			
b. How my identity can be stolen			
c. How to protect my identity			












The remainder of the form will be completed at the end of this training.

2. How much do you know about the following topics?

	I don't know anything about this	I know a little about this	I know a lot about this
a. What Personally Identifiable Information (PII) is			
b. How my identity can be stolen			
c. How to protect my identity			

3. Please tell us how you felt about the following parts of the training.

	It was OK	It was really good	It was great
a. The information that I learned			
b. The way the training was organized			
c. The activities			

What is one thing you learned today?

Based on what you learned today, what is one thing that you are going to do to take more control of your money? _____

I would recommend this training to others. ___ yes ___ no ___ maybe

Thank you for your feedback!

MODULE 8: PROTECTING YOUR IDENTITY

AGENDA



Introduction	10 Minutes
Overview, Purpose and Expected Outcomes.....	5 Minutes
PowerPoint Presentation.....	30 Minutes
<ul style="list-style-type: none">• Understanding Personally Identifiable Information and why it is important• Why do people with disabilities need to protect their identity?• Ways people can steal your identity• Common mistakes• What to do to protect myself• Staying safe online• What to do when you suspect your identity has been stolen	
Activity	15 Minutes
<ul style="list-style-type: none">• Self-Assessment: Examine My Own Practices: In My Home, In the Community and Online	
BREAK	15 Minutes
Making Connections in Your Community	30 Minutes
Homework Assignment and Wrap-up	10 Minutes
Evaluation and Closing	5 Minutes

REMINDER: Please distribute part one of the Module 8 evaluation now during the introduction. Be sure to have the participants complete the second half of the evaluation at the end of the session.

MODULE 8: PROTECTING YOUR IDENTITY

SCRIPT FOR TRAINER



Introduction (10 Minutes)

Script for Trainer (corresponding PowerPoint Presentation Module 8: Protecting Your Identity)

My name is _____ Welcome to our ninth session of **Financial Wellness Training**. Today, we will learn about the importance of protecting our identity. We will introduce you to personally identifiable information (PII) and how that information can be used by thieves. We will also cover ways we can protect ourselves from becoming a victim of identity theft.

Overview, Purpose and Expected Outcomes (5 Minutes)

Script for Trainer (corresponding PowerPoint Presentation Module 8: Protecting Your Identity)

{Discussion} What do we mean when we say identity theft and why do you think people with disabilities need to protect their identities?

Today, we will learn how to keep your identity safe by understanding the variety of threats.

Identity theft is the number one consumer complaint received by the Federal Trade Commission (FTC).

First, we will watch a short video from the FTC that talks about why you should care about identity theft.

Video: consumer.ftc.gov/media/video-0057-why-care-about-identity-theft

PowerPoint Presentation (30 Minutes)

Script for Trainer (corresponding PowerPoint Presentation Module 8: Protecting Your Identity)

Our personally identifiable information (PII) is what we are attempting to protect.

PII is:

Any information that can be used on its own or with other information to identify, contact or locate a particular person.

Like other information, it can exist physically on paper or electronically in computers and smartphones.

Examples of PII include:

- Name
- Social Security number
- Date and place of birth
- Mother's maiden name
- Medical information
- Information related to benefits
- Employment history
- Education information
- Home address
- Vehicle information
- Criminal records
- Gender or race
- Driver's license number
- Bank account number
- Passport number
- Email address

Some PII may be more important or sensitive than other PII. For example, someone else may have the same name as you but they will not have the same social security number or driver's license as you.

To make sure we all understand what we're talking about, here is a definition of identity theft: Identity theft occurs when someone uses your PII to commit fraud or other crimes AND this happens without your knowledge or permission.

There are many ways thieves can steal your identity; we are going to talk about the most common ways and why it is so important to protect your PII, especially information unique and relevant to you.

One important thing to remember is that the ways of stealing identity change, so it is important to learn about new protections as information becomes available.

- **Dumpster Diving** – when someone rummages through trash looking for bills or other paper with your personal information on it.
- **Skimming** – when someone steals credit/debit card numbers by using a special storage device when your card is processed.
- **Password** - when someone captures your online identity. Can happen when you use public wi-fi to connect your phone or computer, like at a store or hotel.

- **Phishing** – when someone pretends to be financial institutions, federal agencies or other companies calling or sending spam (fake messages) or pop-up messages to get you to reveal personal information.
- **Door to Door** - when someone comes to your house and asks you questions about your habits—maybe to return later or to trick you into revealing PII.
- **Changing Your Address** – when someone diverts your billing statements to another location by completing a change of address form at the local U.S. Post Office.
- **Data Breaches** – when hackers penetrate databases (business or personal) where your PII is on file; Target and Home Depot are examples of businesses who were hacked. When Experian was hacked, the PII of 143 million people was revealed.
- **Old-Fashioned Stealing** – when someone steals wallets and purses, mail (including bank and credit card statements), pre-approved credit offers and new checks or tax information. Identity thieves can steal personnel records or bribe employees who have access.
- **Pretexting** – when someone lies about who they are to obtain your personal information from financial institutions, telephone companies and other sources.
- **Electronics—old and new:** computers and smartphones.
- **Social Media** – when someone uses your information to create a social media profile in your name. They may use a photo or other information stolen from the web about you to create an account that could trick others that know you into thinking they are you.

So, what are ways thieves steal and use your personal identifying information?

Identity theft can fall into the following categories:

Financial Gains – Identity thieves could be interested in stealing money, using your identity, opening new accounts and changing the address on your existing accounts to increase their own finances.

Governmental - A scam that has increased in frequency in the past few years is the theft of income tax refunds. Thieves steal identities, file fraudulent tax returns that request refunds and, when the victim files the real return, they receive a message from the Internal Revenue Service that the return has been filed. Also, thieves may try to steal a public benefits payment.

Criminal - There is a market for PII and there are many ways that thieves can sell your PII for gain.

Medical – Identity thieves sometimes go to see doctors and check into hospitals under false names in order to receive services. Hospitals and medical providers have been the targets of corporate hacks where millions of records were stolen.

Next, we will watch the FTC video: Five Ways to Help Protect Your Identity:

[youtube.com/watch?v=lp_8cvNm_vE](https://www.youtube.com/watch?v=lp_8cvNm_vE).

So, how do we protect ourselves?

Be proactive!

- Monitor checking and credit accounts monthly and your credit report annually.
- Protect your Social Security card and number.
- Protect your trash by shredding all documents with personal information that you no longer need.
- Keep important documents such as marriage, birth certificate, social security cards, and photo identification cards forever but keep them in a safe place where no one else can access them.
- Protect your mail—incoming and outgoing.
- Do not give out private information such as your name, address, date of birth, social security number, credit card, etc. to callers or individuals you do not know or trust.
- Limit what you carry in your wallet/purse. Do not carry your social security card, letters from the Social Security Administration and such with you on a regular basis.
- Consider a credit freeze with the credit reporting agencies.
- Be careful on the internet with information you provide.
 - Protect your passwords and do not share them with others.
 - Only keep your passwords in a secure password manager or in a locked file where no one else can get them.
 - Use passwords that are difficult to guess and update them at least once a year.
 - Do not use the same password over and over, mix them up and make sure they are unique.
- Keep your smartphone, tablet or computer safe and use a strong password with numbers, letters and symbols so no one can get into your devices if they do get lost or stolen.
- Delete all PII from and safely dispose of all old electronics.
- Beware of scams and frauds.

We are going to quickly mention online shopping since more and more of us depend on the internet for purchases. There is a lot of information on how to be a wise consumer, but briefly:

- The FBI estimates that every computer that connects to the internet is scanned for weaknesses by criminals within 45 seconds of connecting.
- The Identity Theft Resource Center, at idtheftcenter.org, has a complete guide for shopping, including specifics on websites, payment, confirmation, electronic signatures and more.

So, what do you do if you think your identity has been compromised?

- Close accounts that have been tampered with or opened fraudulently.
- Review and place a Fraud Alert on your credit reports.
- File a complaint with the Federal Trade Commission (FTC)
- Contact your smartphone plan if your smartphone is stolen.

This can be accomplished by:

1. Calling the FTC's Identity Theft Hotline at **1-877-ID-THEFT**.
2. Visiting identitytheft.org and reportfraud.ftc.gov to complete an online complaint form.

Most importantly, file a report with local police in the community where you believe the theft took place.

Activity: Self-Assessment (15 minutes)

Make a plan to keep your PII secure. We will start on this worksheet today and then you can complete it at home.

{Distribute Worksheet: Keeping Your Personally Identifiable Information Secure}

Making Connections in Your Community: Guest Speaker(30 minutes)

Trainer will introduce a local law enforcement representative or a financial services partner to talk about identity theft in the community.

Homework Assignment and Wrap-Up (10 Minutes)

Develop a plan for the safe storage of personally identifiable information, account numbers and passwords.

Evaluation and Closing (5 minutes)

Trainer should thank the participants for participating in today's training and congratulate them on first steps toward improving their financial wellness.

REMINDER: Be sure to have the participants complete the second half of the evaluation and collect.

MODULE 8: PROTECTING YOUR IDENTITY

ACTIVITY: SELF-ASSESSMENT



Behaviors

	Yes	No
Do you cover the ATM keypad when you enter your PIN?		
Do you only carry the identification, checks, credit cards or debit cards that you really need?		
Do you use direct deposit for paychecks, tax refunds and benefit payments?		
Do you use complex passwords with a mix of numbers, symbols and letters instead of easily guessed words?		
Do you use secure mailboxes for incoming and outgoing mail?		
Do you avoid sharing PII except on a “need to know” basis?		
Do you quickly fix mistakes that are on bills and monthly statements?		
Do you review your credit report annually and fix mistakes?		
Do you review medical service statements (Medicare Summary Notices and Explanations of Benefits) for suspicious charges?		
Do you maintain appropriate insurance coverages (property, liability, health, auto, home, etc.) and review coverages and costs as needs change?		
Do you communicate with the people you have named in a durable power of attorney and health care power of attorney?		

Documents and Secure Storage

Yes

No

Do you cover the ATM keypad when you enter your PIN?

Do you only carry the identification, checks, credit cards or debit cards that you really need?

Do you use direct deposit for paychecks, tax refunds and benefit payments?

Do you use complex passwords with a mix of numbers, symbols and letters instead of easily guessed words?

Do you use secure mailboxes for incoming and outgoing mail?

Do you avoid sharing PII except on a “need to know” basis?

Do you quickly fix mistakes that are identified on bills and monthly statements?

Do you review your credit report annually and identify/correct errors?

Do you review medical service statements (Medicare Summary Notices and Explanations of Benefits) for suspicious charges?

Do you maintain appropriate insurance coverages (property, liability, health, auto, home, etc.) and review coverages and costs as needs change?

Do you communicate with the people you have named in a durable power of attorney and health care power of attorney?

Do you shred documents with personal/financial information before disposing of them or recycling?

Do you open all mail and review bills, communications and monthly statements for errors?

Do your family members or close friends know where your emergency documents are?

Do you copy or keep electronic copies of important communications and documents as backups?

Do you maintain a durable power of attorney in a secure location? This document enables you to name one or more people to handle finances and remains in effect if you become incapacitated.

Do you maintain a health care power of attorney in a secure location? This document enables you to name one or more people to handle health care and life-prolonging procedure decisions if you become incapacitated.

Do you keep documents that can't be replaced in a safe deposit box or other secure location away from your home? (birth certificates, passports, important contracts, power of attorney, etc.)

Planning for the Unexpected

Yes

No

Do you maintain:

- Adequate insurance
- Durable power of attorney
- Health Care power of attorney
- Will

Do you keep your emergency documents in a safe location?

- Forms of identification (driver's license, state identification for non-drivers, insurance cards, Social Security cards, passport, birth certificate)
- Checkbook and enough blank checks to last one month
- ATM/debit cards and credit cards
- Cash
- Telephone numbers for financial service providers, insurance companies, loans and your ABLE account
- Important account numbers (bank accounts, credit cards, loans, insurance policies)
- Key to your safe deposit box

Source: Money Smart for Older Adults: Prevent Financial Exploitation, CFPB and FDIC, June, 2013