Identity Theft Protection Worksheet

Practice identifying risks and developing protection strategies

Part 1: Scenario Analysis

Read each scenario and answer the questions that follow.

> **Scenario A: The Data Breach**
>
> Maria receives an email from her favorite online retailer informing her that their database was breached. The hackers may have accessed customer names, email addresses, passwords, and partial credit card numbers (last 4 digits). Maria has shopped at this store for 5 years and uses the same password for multiple accounts.

1. What immediate actions should Maria take? (List at least 3)

1.
2.
3.

2. What long-term habits should Maria change to prevent future issues?

Describe changes Maria should make...

> **Scenario B: The Phone Call**
>
> James receives a phone call from someone claiming to be from the IRS. The caller says James owes back taxes and must pay immediately using gift cards or face arrest. The caller knows James's full name and home address.

3. What red flags indicate this is a scam?

Identify the warning signs...

4. What should James do in this situation?

Describe the appropriate response...

Scenario C: The Lost Wallet

Taylor's wallet was stolen at a concert. It contained their driver's license, debit card, two credit cards, health insurance card, and Social Security card.

5. In what order should Taylor address these losses? Why?

Prioritize the items and explain your reasoning...

6. What mistake did Taylor make by carrying all these items?

Identify the error and better practices...

Part 2: Personal Risk Assessment

Rate your current level of protection in each area.

I use unique passwords for each important account	Select...
I have two-factor authentication enabled on financial accounts	Select...
I review my bank/credit card statements for unauthorized charges	Select...
I check my credit reports regularly	Select...
I shred documents containing personal information	Select...
I am cautious about what I share on social media	Select...

Part 3: Knowledge Check - Matching Exercise

Match each term (1-6) with its correct definition (A-F)

1. Phishing

? A. Restriction on new credit accounts being opened

2. Credit Freeze

? B. Fraudulent attempt to obtain sensitive information via email

3. Skimming

? C. Alert placed on credit file warning of potential fraud

4. Fraud Alert

? D. Device that captures card data from ATMs or gas pumps

5. Social Engineering

? E. Using personal information to impersonate someone

6. Identity Theft

? F. Manipulating people to reveal confidential information

Part 4: Personal Protection Plan Development

Based on your risk assessment, create a plan to improve your identity protection.

Priority Action 1 - This Week

What will you do?

Specific action to take this week

Priority Action 2 - This Month

What will you do?

Specific action to complete within 30 days

Priority Action 3 - Ongoing Habit

What habit will you establish?

Regular practice to maintain long-term

Resources Needed

Tools or services to obtain

e.g., Password manager, shredder, credit monitoring...

Estimated cost

e.g., $0-50, free options available

Part 5: Reflection Questions

1. Why do you think identity theft continues to increase despite greater awareness?

Consider technology changes, human behavior, and criminal sophistication...

2. How might your digital footprint (social media, online shopping, etc.) make you vulnerable to identity theft?

Think about information you share online...

3. What is the difference between a credit freeze and a fraud alert? When would you use each?

Compare and contrast these protection tools...

4. If a family member's identity was stolen, what three pieces of advice would you give them?

1.
2.
3.