Identity Theft Case Studies Worksheet

Analyzing Real-World Identity Theft Scenarios

This worksheet presents four real-world identity theft scenarios. For each case, analyze what happened, identify the vulnerabilities that were exploited, and determine what could have been done to prevent the theft. Use these analyses to strengthen your own identity protection strategies.

Case Study 1: Social Media Impersonation

Victim: Taylor, 19-year-old college student

Scenario: Taylor received a message from a friend on Instagram asking about pictures from a recent event. The friend sent a link to view the photos, which required Taylor to log in with their Instagram credentials. Taylor clicked the link and entered their username and password. Within hours, their account was taken over, their profile picture and name were changed, and the impersonator began sending similar phishing messages to Taylor's contacts. The impersonator also gained access to Taylor's email because they used the same password for both accounts. Through the email account, the thief accessed Taylor's online banking information and attempted to transfer funds.

Impact: Taylor lost control of their social media and email accounts for several days, had to spend hours on identity recovery steps, and had to explain to friends and family that they had been hacked. Taylor's bank froze the account due to suspicious activity before any money was transferred, but Taylor had to close the compromised account and open a new one.

What vulnerabilities were exploited in this case?

What specific prevention measures could have prevented this identity theft?

What steps should Taylor take to recover from this identity theft?

How could you apply lessons from this case to your own digital security?

Case Study 2: Mail Theft and Account Takeover

Victim: The Rodriguez family

Scenario: While the Rodriguez family was on vacation for two weeks, they did not put a hold on their mail. During this time, someone stole mail from their unlocked mailbox, including bank statements, credit card offers, and utility bills. Using the personal information gathered from these documents, the thief opened several credit cards in Mr. Rodriguez's name. The thief also called the family's credit card company, used the personal information to pass security questions, and had a new card sent to a different address. The family didn't discover the fraud until they returned home and Mr. Rodriguez received a call from a credit card company verifying a large purchase he hadn't made.

Impact: Over $12,000 in fraudulent charges across three credit cards, severely damaged credit score, and more than six months spent resolving the fraud and repairing credit. The family also had to place credit freezes, file police reports, and deal with collection agencies for accounts they never opened.

What vulnerabilities were exploited in this case?

What specific prevention measures could have prevented this identity theft?

What steps should the Rodriguez family take to recover from this identity theft?

How could you apply lessons from this case to your own physical document security?

Case Study 3: Data Breach and Synthetic Identity Theft

Victim: Marcus, 25-year-old young professional

Scenario: Marcus received a notice that his information had been compromised in a data breach at a major retailer where he frequently shopped. The breached data included his name, address, phone number, email, and the last four digits of his credit card. He was concerned but didn't take immediate action since the full card number wasn't exposed. Six months later, Marcus applied for a mortgage and discovered that there were several loans and credit cards on his credit report that he had never opened. The identity thief had used Marcus's personal information combined with a fabricated Social Security number (a technique called synthetic identity theft) to create a hybrid identity. The thief had been building credit with this synthetic identity for months before maxing out all the accounts.

Impact: Marcus's mortgage application was denied, his credit score dropped by over 150 points, and he had to delay buying a home for more than a year while he worked to clear his credit report. The process involved numerous disputes with credit bureaus, filing reports with the FTC and police, and many hours documenting and following up on the fraud.

What vulnerabilities were exploited in this case?

What specific prevention measures could have prevented this identity theft?

What steps should Marcus take to recover from this identity theft?

How could you protect yourself after learning your information was part of a data breach?

Case Study 4: Medical Identity Theft

Victim: Eleanor, 67-year-old retiree

Scenario: Eleanor received an explanation of benefits (EOB) from her health insurance company for a surgical procedure she never had at a hospital in another state. When she called her insurance company to report the error, she learned that someone had used her insurance information to receive over $35,000 in medical care over the past three months. The thief had somehow obtained her insurance ID number, name, and date of birth. Eleanor later discovered that a phishing email disguised as coming from her insurance provider had tricked her into providing her insurance details six months earlier. She had thought she was updating her information for the new insurance year.

Impact: Eleanor's insurance benefits were nearly exhausted for the year, and she had to pay out-of-pocket for her own medical needs until the fraud could be resolved. More concerning, her medical records were contaminated with someone else's medical information, including different blood type and allergies, creating a potentially dangerous situation for her future medical care. It took nearly a year of working with her healthcare providers and insurance company to correct her records and restore her benefits.

What vulnerabilities were exploited in this case?

What specific prevention measures could have prevented this identity theft?

What steps should Eleanor take to recover from this identity theft?

How might you protect your medical information from identity theft?

Create Your Own Case Study

Research a real identity theft case from a news article, podcast, or other source. Document the case below and analyze it using the same framework.

Case Title:

Scenario Description:

What vulnerabilities were exploited in this case?

What specific prevention measures could have prevented this identity theft?

How could you apply lessons from this case to your own identity protection?

Case Study Analysis Tips

When analyzing identity theft cases, consider these questions:

- What specific pieces of personal information were compromised?
- What was the initial point of vulnerability that the thief exploited?
- What warning signs appeared before the theft was fully discovered?
- What made recovery particularly difficult or time-consuming?
- What specific prevention measures would have been most effective?
- How could the victim have detected the theft earlier?