Case Study: #7 The Phishing Trap - Protecting Your Digital Identity

Introduction

Meet Maya, a high school junior who loves connecting with friends online and exploring new apps. She's recently received an email that appears to be from her bank, urging her to update her account information due to a security breach. Excited about a potential scholarship opportunity, she also clicked on a link in a social media post promising easy money for college. Little does Maya know, she's about to fall prey to sophisticated phishing scams that could jeopardize her financial future.

The Problem

Maya's situation highlights the growing threat of identity theft and online scams:

- **Sophisticated Scams:** Scammers are becoming increasingly clever, using tactics like phishing emails, fake websites, and social media scams to trick people into revealing personal information.
- **Vulnerable Targets:** Young people, like Maya, may be particularly vulnerable due to their frequent online activity and lack of experience with scams.
- **Devastating Consequences:** Identity theft can have severe financial and emotional consequences, including damaged credit scores, drained bank accounts, and difficulty obtaining loans or housing.

Questions for Students:

1. **Spot the Red Flags:** What are the warning signs that the email Maya received might be a phishing scam? What clues in the social media post should have raised suspicion?
2. **Consequences of Falling Victim:** What are the potential consequences if Maya falls for these scams and provides her personal information?
3. **Protective Measures:** What steps can Maya take to protect herself from identity theft and online scams?
4. **Technology's Role:** How can technology be both a tool for scammers and a means of protection against identity theft?
5. **Recovery and Reporting:** If Maya becomes a victim of identity theft, what steps should she take to recover and report the crime?