THE CHALLENGE

Alex received an urgent email from "BankofAmerica1@secure-verify.net" claiming suspicious activity on his account. The email asked him to click a link and verify his information immediately or his account would be frozen. The email looked professional with the bank's logo and colors.

How can Alex tell if this email is legitimate, and what should he do?

Learning Objectives

- Identify common types of consumer fraud including phishing, spoofing, and identity theft.
- Recognize warning signs and red flags that indicate potential scams.
- Apply prevention strategies to protect personal and financial information.

CORE CONCEPTS

Term	Definition
Phishing	Fraudulent emails/messages designed to trick you into revealing sensitive information.
Spoofing	Impersonating legitimate companies through fake emails, websites, or caller IDs.
Identity Theft	Using stolen personal information to open accounts or make purchases fraudulently.
Ponzi Scheme	Investment scam paying earlier investors with money from newer investors.
Social Engineering	Manipulating people into revealing confidential information through psychological tactics.

Background: Scammers are increasingly sophisticated, creating professional-looking emails, websites, and calls that seem legitimate. They exploit urgency ("act now!"), fear ("your account will be closed"), and greed ("you've won!"). The best defense is **verification**: never click links in unsolicited messages, contact companies directly through official channels, and remember that legitimate organizations never ask for passwords or Social Security numbers via email or text.

APPLY IT

PART A: SCAM IDENTIFICATION

For each scenario, identify the type of fraud and list the warning signs.

Scenario 1: Email from "Your Bank"

Alex received an email from "BankofAmerica1@secure-verify.net" with the subject "URGENT: Verify Your Account." It includes the bank's logo and asks him to click a link to confirm his SSN and password within 24 hours.

Type of fraud: _____ (phishing / spoofing / identity theft)

Red flags: _____

_____

Scenario 2: Text Message "Refund"

Jessica received a text: "IRS Notice: You are eligible for a $1,247 tax refund. Claim now at www.irs-refund-claim.com. Enter your SSN and bank routing number to receive your money."

Type of fraud: _____ (phishing / spoofing / Ponzi scheme)

Red flags: _____

_____

Scenario 3: Investment "Opportunity"

Miguel met someone online who claimed to be a financial advisor. After weeks of chatting, they offered him a "guaranteed 50% return" investment. The advisor asked Miguel to wire $5,000 to get started.

Type of fraud: _____ (catfishing / Ponzi scheme / both)

Red flags: _____

_____

> **Hint:** *Look for: unofficial email domains, urgent language, requests for sensitive info, "guaranteed" returns, wire transfer requests, and too-good-to-be-true offers.*

PART B: PROTECTION STRATEGIES

4. List FOUR actions you should take if you suspect you've received a phishing email.

_____

_____

_____

_____

5. Where can you report suspected fraud? List TWO resources.

PART C: PREVENTION PLANNING

6. Create a list of THREE habits that can help protect you from consumer fraud.

CHECK YOUR UNDERSTANDING

1. Which of the following is a major red flag indicating a potential phishing attempt?

- [ ] A. An email from your actual bank's domain (@bankofamerica.com)
- [ ] B. A message with no sense of urgency
- [ ] C. A request to verify your password and Social Security number
- [ ] D. Information about your recent legitimate transactions

2. Explain why the IRS would NEVER contact you by text message asking for your Social Security number.

3. What should Alex (from The Challenge) do instead of clicking the link in the email?

4. Why are "guaranteed returns" on investments always a warning sign of potential fraud?

5. Reflection: Think about an older relative or friend who might be vulnerable to scams. How would you explain phishing to them in a supportive way? What specific advice would you give?