PFL Academy

Teacher Guide: Chapter 6.3 — Consumer Fraud Protection

OVERVIEW

TIME	MATERIALS	PREREQUISITES
45-50 Minutes	Student Activity Packet	Online Shopping (L-27)

LESSON FLOW

5 min — **THE CHALLENGE**

- Read Alex's phishing email scenario aloud.
- Ask: "What seems suspicious about this email?" List responses on board.

10 min — **CORE CONCEPTS**

- Define each fraud type with real examples.
- Emphasize: legitimate companies NEVER ask for passwords via email.
- Discuss why urgency and fear are manipulation tactics.

25-30 min — **APPLY IT**

- **Part A (15 min):** Scenario analysis. Discuss each as a class.
- **Part B (8 min):** Protection strategies and reporting resources.
- **Part C (7 min):** Prevention habit planning.

10 min — **CHECK YOUR UNDERSTANDING**

- Review Q3—emphasize direct contact through official channels.
- Discuss Q5—helping others recognize scams compassionately.

DIFFERENTIATION

Support

- Show actual examples of phishing emails (redacted).
- Create a visual "red flags" checklist poster.
- Role-play the scenarios as a class before analysis.

Extension

- Research a recent major data breach and its impact.
- Create educational materials for family members.
- Investigate how two-factor authentication works.

ANSWER KEY

Part A: Scam Identification

Scenario 1: PHISHING/SPOOFING. Red flags: Unofficial domain (secure-verify.net vs. bankofamerica.com), urgency ("24 hours"), requests SSN and password (banks never ask this), generic greeting likely.

Scenario 2: PHISHING/SPOOFING. Red flags: IRS never texts, unofficial domain (irs-refund-claim.com vs. irs.gov), requests SSN and bank info, unsolicited "refund" offer.

Scenario 3: BOTH (CATFISHING + PONZI). Red flags: Met online only, "guaranteed" returns (impossible), 50% return is unrealistic, wire transfer request (untraceable), relationship built before asking for money.

Part B: Protection Strategies

4. (1) Don't click any links, (2) Don't reply or provide information, (3) Contact company directly through official website/phone, (4) Report to FTC or forward to company's fraud department, (5) Delete the email.

5. FTC (ReportFraud.ftc.gov), FBI's IC3 (ic3.gov), your bank's fraud department, state Attorney General, local police for identity theft.

Part C: Prevention Planning

> *Good habits: Use strong unique passwords, enable two-factor authentication, verify sources before clicking, check credit reports regularly, be skeptical of unsolicited contacts, never share sensitive info via email/text, limit social media sharing.*

Check Your Understanding

1. C (Request to verify password and SSN)

2. The IRS initiates contact by mail, never by phone, text, or email. They never ask for sensitive information electronically and don't threaten arrest or demand immediate payment.

3. Go directly to bankofamerica.com (type it, don't click), log in normally, or call the number on his card. Check for any actual alerts through official channels.

4. All legitimate investments carry risk. "Guaranteed" high returns are mathematically impossible and legally prohibited for advisors to promise. This language is always a scam indicator.

5. *Responses should be supportive, not condescending. Explain that scams are sophisticated and victims aren't "stupid." Focus on specific tips: verify before clicking, when in doubt call the company directly, it's okay to hang up and call back.*

COMMON MISCONCEPTIONS

Misconception	Clarification
"Only gullible people fall for scams."	Scammers are sophisticated professionals. Anyone can be targeted, especially under stress or urgency. Awareness, not intelligence, is the key protection.
"If an email has a company logo, it's real."	Logos are easily copied. Always verify the sender's email domain and never trust visual appearance alone.
"I'll know a scam when I see one."	Modern scams are highly convincing. The best protection is systematic verification—always contact companies directly through official channels.