NO PREP

Forensic Science

Online Romance Scams

Includes: Student reading, case study, differentiated questions, teacher key

Name: Period: Date:

Forensic Science: Online Romance Scams

The Valentine Scam Spike: How "Love" Becomes a Crime Scene

Online romance scams increase around Valentine's Day because scammers take advantage of emotions and expectations. They know the holiday makes people more likely to want connection, feel lonely, or feel pressure to give gifts. The scam is not just "someone lies." It's a planned method of social engineering—manipulating trust and urgency to get money, gift cards, or account access. From a forensic science perspective, the "crime scene" is digital: messages, account histories, payment receipts, device logs, and metadata. A key idea is that scam cases often look messy because victims feel embarrassed. That embarrassment can delay reporting, and delays give scammers time to delete accounts, move money, and create new identities. In forensic investigation, speed matters—but so does careful evidence handling. Investigators and victims must preserve data correctly so it can be used to identify patterns and support legal action. Another important point for students: scammers rarely start with a big request. They build

Name: **Period:** **Date:**

Forensic Science: Online Romance Scams

The Valentine Scam Spike: How "Love" Becomes a Crime Scene

Online romance scams increase around Valentine's Day because scammers take advantage of emotions and expectations. They know the holiday makes people more likely to want connection, feel lonely, or feel pressure to give gifts. The scam is not just "someone lies." It's a planned method of social engineering: manipulating trust and urgency to get money, gift cards, or account access. From a forensic science perspective, the "crime scene" is digital: messages, account histories, payment receipts, device logs, and metadata. A key idea is that scam cases often look messy because victims feel embarrassed. That embarrassment can delay reporting, and delays give scammers time to delete accounts, move money, and create new identities. In forensic investigation, speed matters, but so does careful evidence handling. Investigators and victims must preserve data correctly so it can be used to identify patterns and support legal action. Another important point for students: scammers rarely start with a big request. They build trust first, then test compliance with a small request ("Can you help me just once?"), then escalate. That step-by-step pattern is evidence. Investigators look for repeating structures: fast intimacy, refusal to verify identity, isolation tactics ("don't tell anyone"), and financial pressure. This topic fits Valentine's Day because it teaches a real-life safety skill: love never requires secrecy, payment deadlines, or sharing codes. If a person turns affection into a transaction, that's not romance. It's a red flag.

Digital Fingerprints: Metadata, Message Patterns, and Identity Clues

Digital forensics focuses on what can be proven from data. Investigators start with account-level evidence: usernames, profile creation dates, linked emails, phone numbers, device information (when available), and IP-related logs (usually accessed through legal requests). Students should understand that investigators don't

"magically hack" people. They use lawful processes and preserved records to connect actions to accounts and, sometimes, to individuals. Even without advanced tools, message patterns can reveal a lot. Scammers often reuse scripts: dramatic backstories, fast declarations of love, and repeated crises. They may avoid specific details, dodge video calls, or claim their camera is broken. They often push victims to move platforms ("let's talk on a private app"), which reduces oversight and makes reporting harder. That behavior pattern becomes part of the evidence file. Metadata matters too. A screenshot shows what you saw, but a full message log can show timestamps, edits, deletions, and context. Email scams can be traced through email headers, which may reveal the route a message took (not always the scammer's true location, but a clue). Images can contain hidden information like metadata (sometimes stripped by apps), and reverse-image searching can reveal stolen photos (a common scam strategy). For students, the big lesson is practical: keep evidence. Don't just block and delete immediately. Save messages, usernames, payment details, and dates first. Then block and report. Evidence preservation turns "I feel like I was scammed" into "Here is proof."

Money Trails: Gift Cards, Wires, and Why Scammers Love Speed

Once money moves, scammers try to make it untraceable or difficult to recover. That's why they prefer gift cards, wire transfers, and money apps. Gift cards are especially attractive because once someone sends a code, the value can be spent immediately. That doesn't mean investigation is impossible: investigators can sometimes track where the card was redeemed, but it is harder than reversing a normal purchase. Another common method is money "mules," where scammers convince or pay someone else to receive funds and forward them. This creates distance between the scammer and the money. In forensic terms, that's a laundering step. Investigators look at account histories, transaction timestamps, and patterns across multiple victims. When many people send money to the same account, that account becomes a major lead. Crypto is sometimes used, but students should avoid the myth that "crypto is invisible." Transactions can be traced on public ledgers, though identifying the person behind an address may require additional evidence and legal steps. The main scammer advantage is speed and victim confusion, not magic invisibility. A strong prevention habit is simple and powerful: never send money, gift cards, or verification codes to someone you haven't verified. If someone reacts with

anger, guilt, or urgency, that reaction is evidence of manipulation. Healthy people respect boundaries. Scammers punish them.

Evidence Handling: Chain of Custody for Screenshots, Chats, and Receipts

Digital evidence needs structure, just like physical evidence. Investigators care about authenticity (is it real?), integrity (was it altered?), and continuity (who had it and when?). That's chain of custody in the digital world. A screenshot alone can be questioned because it's easy to edit. That's why it helps to collect multiple forms of proof: screen recordings showing the account in-app, exported chat logs when possible, email headers, transaction receipts, and a written timeline of events (dates, amounts, platforms). Students should learn a practical routine: Save usernames, profile links, and the platform used. Capture conversations with timestamps visible. Save payment confirmations (receipts, emails, app transaction IDs). Write down a simple timeline: first contact → major requests → payments. Report to the platform and tell a trusted adult. Why does this matter? Because investigators often need to connect pieces across victims. One person's screenshot might be weak, but ten victims with the same script, same account pattern, and matching payment destinations creates a strong case. Valentine's Day is when students are most likely to get pressured with "gift" requests. The forensic response is calm and boring: stop payment, preserve evidence, report, and get support. Boring is safe.

Key Information: Digital Scam Evidence Table

Evidence Item	What It Proves	Best Student Action
Chat logs + timestamps	pattern, escalation, urgency	screenshot + screen-record account page
Payment receipts	money movement	save transaction IDs and confirmations
Profile links/usernames	identity anchor	copy link and note platform
Email headers (if used)	routing clues	forward to trusted adult/investigator

Evidence Item	What It Proves	Best Student Action
Reverse-image results	stolen identity proof	document match with screenshots

Case Study: "I Need Help Tonight"

Evan met "Sofia" on a social app in early February. Sofia messaged constantly, used pet names within days, and said she had "never felt understood like this." When Evan asked for a video call, Sofia claimed her camera was broken and suggested moving to a private messaging app. On February 13, Sofia described a crisis: her bank account was "frozen," and she needed money for a hotel because she was "unsafe." She asked for a $30 gift card code immediately and said, "If you care about me, please don't hesitate." Evan felt guilty and sent the code. Within hours, Sofia asked for $150, saying the problem got worse. Evan finally told his older cousin, who helped him preserve evidence: screenshots with timestamps, the profile link, the gift card receipt, and the exact wording of the requests. They reported the account. The platform responded that the profile was linked to multiple reports and was removed. Evan's cousin explained that the evidence mattered because it showed a pattern—fast intimacy, refusal to verify identity, urgency, guilt pressure, and escalating money requests.

1. Identify three scam red flags from the excerpt and explain how each one supports the conclusion that this was social engineering.

2. What evidence did Evan preserve that would be most helpful for an investigation, and why?

Multiple Choice

1. The strongest sign a "romance" account is likely a scam is:

    a) they use emojis very often in every message

    b) they refuse verification but request money or codes

    c) they message you late at night when you are tired

    d) they like the same music and hobbies you do

2. In digital forensics, chain of custody is most important because it helps prove:

    a) the scammer always lives in the same nearby area

    b) the victim should feel embarrassed about being scammed

    c) screenshots alone are automatically accepted as perfect proof

    d) the evidence was handled reliably and not altered

3. Gift cards are commonly used in scams because they:

    a) can be redeemed quickly and are hard to recover

    b) require no internet connection to spend the codes

    c) prove someone's true love and emotional commitment

    d) can be easily reversed and refunded by the original buyer

Matching

Write the letter of the correct definition on the line next to each term.

Term	Definition
1. ___ Social engineering	A) Confirming identity (ex: video call, consistent evidence)
2. ___ Metadata	B) A person used to receive/transfer stolen funds
3. ___ Email header	C) Manipulation to gain trust and compliance
4. ___ Money mule	D) Data showing how an email traveled and where it came from
5. ___ Verification	E) Hidden info like timestamps or file data that adds context

Fill-in-the-Blank

1. A scam tactic that pressures someone to act quickly is called _____.

2. A saved record that shows payment details is a transaction _____.

3. Moving a conversation to a private app can reduce oversight and make _____ harder.

Short Answer

Answer each question in 2-4 complete sentences.

1. Explain why "fast intimacy" is a useful red flag in romance scam cases.

_____

_____

_____

2. Describe two steps a student should take before blocking a suspected scam account.

3. Write a firm boundary response to a message asking for a gift card "to prove you care."