NO PREP

Scams, Fraud, and Identity Theft

MORE LESSONS LESS PLANNING · MLLP · FREE TODAY · FREE TOMORROW · FREE FOREVER

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

Name: Period: Date:

Scams, Fraud, and Identity Theft

Nobody Thinks They Will Fall For It

The most dangerous belief a person can hold about fraud is that only careless or elderly people get caught by it. Federal Trade Commission fraud reports from past years have shown that adults in their twenties and thirties report losing money to fraud at a higher rate than adults over seventy, though older victims tend to lose larger amounts when they are hit. Younger people are online more, transact digitally more, and are

Name: Period: Date:

Scams, Fraud, and Identity Theft

Nobody Thinks They Will Fall For It

The most dangerous belief a person can hold about fraud is that only careless or elderly people get caught by it. Federal Trade Commission fraud reports from past years have shown that adults in their twenties and thirties report losing money to fraud at a higher rate than adults over seventy, though older victims tend to lose larger amounts when they are hit. Younger people are online more, transact digitally more, and are targeted with scams built specifically for the platforms they use. Confidence is not protection. It is the condition scammers count on. Fraud is deception carried out for financial gain, and modern fraud is not the work of a lone stranger improvising. It is an industry with scripts, call centers, quality control, and specialization, and the people running it test their approaches on thousands of targets and keep whatever converts best. That is why the messages feel professional now, with correct logos, real company phone numbers spoofed onto caller identification, and websites cloned pixel for pixel. The old advice to watch for bad spelling is largely obsolete, and where errors still appear they are frequently deliberate, filtering out skeptical readers so the operators only spend time on people likely to comply. The reliable defense is not spotting a typo. It is recognizing the structure of the request itself, because the underlying pattern has barely changed in fifty years even as the packaging has become flawless.

The Shape Every Scam Shares

Almost every scam, regardless of story, combines the same three ingredients, and learning that pattern is worth more than memorizing any list of specific frauds. First, an unexpected contact. The message arrives without you initiating anything, whether by text, email, phone call, direct message, or a pop-up. Second, manufactured urgency paired with a strong emotion, usually fear or excitement. Your account will be closed today, a warrant has been issued, your package cannot be delivered, you have won something that expires in an hour. The purpose of urgency is

uniform across all of them, which is to prevent you from stopping to verify, because verification kills every scam that exists. Third, an unusual method of payment or an unusual request for information. Legitimate organizations do not require gift cards, wire transfers, cryptocurrency, payment applications sent to strangers, or a code read aloud from your phone. Gift cards in particular are the single loudest alarm in consumer fraud. No government agency, utility, employer, bank, or court has ever accepted a gift card as payment, and any request for one is fraud without exception. When those three ingredients appear together, the story wrapped around them does not matter. The correct response is always the same and always simple: stop, do not use any contact information contained in the message, and independently verify through a number or website you locate yourself.

The Ones Aimed at Students

Several scams target high school and college-age people specifically, and they are worth naming because recognition is nearly instant once you have heard them. The fake check or overpayment scam is the most common. Someone hires you for a remote job, sends a check for more than the agreed amount, and asks you to deposit it and send back the difference or buy equipment from their vendor. Your bank makes the funds available in a day or two, which people mistake for the check clearing, and when it bounces a week later you owe the bank the full amount you sent. Banks make funds available before verification, and that gap is the entire scam. The job scam is close behind, advertising unusually high pay for vague work, requiring no interview, and eventually requesting a fee, personal financial information, or the use of your bank account to process payments, which is money laundering and is a crime even if you did not know. Rental scams post apartments below market with a landlord conveniently out of the country who needs a deposit before a showing. Concert and event ticket scams sell tickets that do not exist or are sold to several people at once. Romance and social engineering scams build trust over weeks before any money is mentioned. Scholarship scams charge for applications and guarantee awards, and legitimate scholarships never charge a fee. The thread running through every one of them is that the target is asked to send money or information first and receive the promised thing afterward, which is the exact reverse of how a legitimate transaction is structured.

Phishing and the Codes You Should Never Share

Phishing is the attempt to obtain credentials or personal information by impersonating a trusted organization, and it is the entry point for a large share of financial crime. It arrives by email, by text where it is sometimes called smishing, and by phone where it is called vishing. The message imitates a bank, a delivery service, a school, or a streaming account and directs you to a login page that looks correct and exists only to capture what you type. Two habits defeat nearly all of it. Never click a link in an unexpected message, and instead open the application or type the address yourself, because the destination of a link cannot be judged by the text displayed. Second, understand that a one-time verification code is a key to your account, not a confirmation of your identity to someone else. Every legitimate institution states that it will never ask for that code, and any caller requesting one is taking over an account in real time. Strong account hygiene closes most of the remaining gap. Use long unique passwords for each account so a breach at one company does not open up the others, use a password manager since remembering forty unique passwords is not realistic, and enable multi-factor authentication everywhere it is offered, preferring an authentication application over text messages where possible. Public wireless networks deserve caution for financial activity, and software updates matter because they patch the specific holes attackers use.

When It Is Your Identity They Take

Identity theft is the use of another person's identifying information, such as a Social Security number, date of birth, or account numbers, to commit fraud, and it is a longer and more damaging problem than a single stolen purchase. Thieves open credit cards, take out loans, file fraudulent tax returns, obtain medical care, and give false names during arrests. Warning signs include unfamiliar charges, bills for accounts you never opened, calls from collection agencies about unknown debts, a tax return rejected as already filed, and unexpected credit denials. Because young adults have clean, unused credit files, they are attractive targets, and a child's identity may be exploited for years before anyone checks. Prevention is mostly routine. Review account statements regularly rather than glancing at the balance, check your credit reports free through AnnualCreditReport.com, the federally authorized site, shred documents containing account numbers, keep your Social

Security number private and never carry the card, and place a credit freeze, which is free by law and prevents new accounts from being opened in your name until you lift it. If it happens, act in order. Report to the Federal Trade Commission at the government identity theft site, which generates a recovery plan and an official affidavit. File a police report. Contact each affected institution's fraud department in writing. Place a freeze and dispute every fraudulent account. Federal law limits your liability for unauthorized credit card charges to fifty dollars, and reporting quickly protects debit card losses as well.

Key Information: Recognizing and Reporting Fraud

Detail	Information
The Three-Part Pattern	Unexpected contact, manufactured urgency, unusual payment request
Gift Card Rule	No agency, utility, court, or bank ever accepts gift cards
Fake Check Scam	Funds are available before the check clears; you repay the bank
Phishing	Impersonating a trusted organization to capture logins or data
One-Time Codes	A key to your account; no legitimate caller will ever request one
Identity Theft	Using another person's identifying data to commit fraud
Credit Freeze	Free by law; blocks new accounts until the owner lifts it
If It Happens	Report to the FTC identity theft site, file a police report, freeze credit

Case Study: Tyler's Remote Job Offer

Tyler is a high school senior who posted on a job board that he is looking for weekend work. Four days later he receives a message offering a remote position as a personal assistant paying six hundred dollars a week, with no interview required. The employer explains that Tyler will need a specific laptop and printer, and mails him a check for two thousand one hundred dollars. The instructions are to deposit it, keep four hundred as his first payment, and send the remaining one thousand seven hundred to the company's approved equipment vendor by wire transfer that same day, because the vendor is holding the order. Tyler deposits the check on Tuesday. On Wednesday his banking app shows the full balance available. He is reaching for his phone to send the wire when his older sister, who took a consumer science course two years ago, asks him one question: who did he interview with?

1. Identify each of the three scam ingredients from the reading in Tyler's situation and explain how each one appears.

2. Tyler's app showed the money as available. Explain why that is not proof the check is good and what would happen if he sent the wire.

Multiple Choice

1. Which combination does the reading identify as the shape shared by nearly every scam?

a) A stranger, a written contract, and a delayed shipment date

b) Unexpected contact, urgency, and an unusual payment method

c) A pop-up ad, a free trial, and a monthly subscription

d) Poor spelling, a foreign phone number, and a small fee

2. Why is a request for payment by gift card described as an alarm without exception?

a) Gift card balances expire before any refund can reach the victim

b) Gift cards charge higher fees than other payment methods

c) No legitimate agency or business ever accepts them as payment

d) Retailers are required to report all gift card purchases

3. What does the reading say a one-time verification code actually is?

a) A receipt confirming a completed transaction

b) Proof that a caller actually works for your bank

c) A key that gives someone access to your account

d) A temporary password that expires after use

Matching

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

Term	Definition
1. ___ phishing	A) Requiring a second proof of identity beyond a password to log in
2. ___ identity theft	B) Overpayment by check with instructions to return the difference
3. ___ fake check scam	C) Impersonating a trusted organization to capture logins or personal data
4. ___ credit freeze	D) Using another person's identifying information to commit fraud
5. ___ multi-factor authentication	E) A free block preventing new accounts from being opened in your name

Fill-in-the-Blank

1. Impersonating a trusted company to steal logins is _____.

2. A free block on new accounts in your name is a credit _____.

3. Urgency exists in a scam to stop you from taking time to _____.

Short Answer

Answer each question in 2-4 complete sentences.

1. Explain why the reading says watching for spelling errors is no longer a reliable defense.

_____

_____

_____

2. Why does the reading say confidence about fraud can make a person more vulnerable, not less?

3. Describe the correct order of actions after discovering identity theft, and why order matters.