



UnScam Yourself

Teacher's Guide

INSTRUCTIONS: Divide students evenly into two teams. Explain that there will be a quiz to see who can unscam themselves the most. The team has to work together to answer the questions correctly. Each member of the winning team will get a prize. Give each team a buzzer (otherwise ask them to raise their hands). If they're just guessing, only award points if they can explain why they gave that answer. If they can't answer, let the other team try to explain what the right answer is, and why.

OPTIONAL: Wastebasketball. Each time a team gets the right answer, that team gets to shoot a wadded up piece of paper at the wastebasket. If they make the basket, the team gets an extra 2 points.

1 How can you protect yourself from identity theft?

- Never tell anyone who you are. Ever.
- Use fake names.
- Only give out your Social Security number if you HAVE to.**
- Only give out fake Social Security numbers.

Comment: Sometimes you have to give your SS# - to apply for a job or a credit card, for example. But in the doctor's office or some other office, you might not have to. You can always ask. Suggestion: Make sure students understand what a Social Security number is.

2 How might you know that your identity was stolen?

- You get a bill for something you didn't buy.
- You meet someone who looks just you.
- You stop getting your credit card bill.
- A and C**

Comment: An identity thief might change the address on your credit card, so you stop getting the bill. But you might look at your bill and see a charge for something you didn't buy. Either could be a sign of identity theft.

3 What should you do if your wallet is stolen?

- Shut off any credit cards or debit cards that were in your wallet
- Put a fraud alert on your credit report
- Review your free copy of your credit report
- All of the above**

Comment: Call all the cards first to turn them off, so the thief can't use them. Then call one of the three major credit reporting companies to put a fraud alert on your credit report. That keeps a thief from getting new accounts in your name. That will also give you a free credit report, which you can review.

4 If you find charges or accounts aren't yours, what should you do?

- Don't worry. It will all get sorted out.
- Pay the charges. The company will pay you back when you prove they're not your bills.
- Call and explain, follow up with a letter, and keep a file of your letters.**
- Keep your fingers crossed.

Comment: Don't ignore the problem or hope it goes away. Call the companies involved and explain. Write who you talked to and the time you called. Then write a letter to confirm what you discussed. Keep copies of everything.

5 What would be a secure password to use online?

- The word "password"
- 12345678
- Your birthdate
- 1Ha\$p&Ud**

Comment: You want something easy to remember but hard for someone else to guess. Think about swapping symbols or numbers for letters and using the initials for a phrase you'd remember. The right answer stands for: I have a secure password and you don't.

6 If you're using your credit card online, the safest place to do that is:

- The library. Nothing bad ever happens there.
- Your own computer.**
- A coffee shop. Nothing bad happens there, either.
- Nowhere. Just don't do it.

Comment: You can safely use a credit card online if the computer has good security software and firewall. So I hope the answer is your own computer. Libraries and coffee shops often have open wireless that lets anybody see the information you transmit, so never do personal business in public spots.

7 It's safe to use a wifi hotspot to buy something on your smartphone, right?

- How lucky are you feeling?
- If the hotspot and the site use encryption...but most public hotspots don't.**
- If you're willing to share your credit card number with others who can see it.
- Sure, I do it all the time.

Comment: Most wifi hotspots are not secure and don't encrypt the information you send over the Internet. If you log on using an unencrypted system, or to an unencrypted site, other users can see anything you send over the Internet, and maybe even what's stored in your phone.

8 You find an online listing for the perfect house to rent. You should:

- Drive by the house to see what it looks like.
- Wire the deposit money right away, so you can get your keys.
- Never wire money to someone you don't know.**
- Rent a moving van.

Comment: This is a common scam. Scammers pretend to rent a house that's not even theirs. Sometimes the ads are copies of real or old real estate listings, but you won't get the house. Never, ever wire money to someone you don't know, even if the story sound good.

9 You get an email from your bank: your account has been hacked and they need your account number and PIN. You should:

- Delete the email. The bank already has your account number and PIN.**
- Call the bank to see if your account was really hacked.**
- Quickly click the link or call the number to give them the information.
- A and B**

Comment: Definitely A, but you could do B, too, if you want. (A, B and D are all acceptable right answers.) This is another common scam called phishing. Scammers are trying to get you to give them information, like your account number or PIN. Never click on a link or open an attachment in an email like this – and call your bank using a number you find yourself, not one in the email.

10 You get a pop-up or an email that says your security software is out of date. You should:

- Click on the link to update your security software, right away!
- Close the pop-up or delete the email.**
- Click the link to see if it looks legit, then update your security software.
- A and C

Comment: These messages are designed to look alarming so you'll click on them. If you do, you might load spyware onto your computer.

11 You find the best car for sale online – and it's cheap. You:

- Ask what color it is and decide to hold out for red.
- Wire the down payment right away so you don't lose the deal.
- Ask for more information and then wire the money.
- None of the above.**

Comment: Is this different from the home in question #8? No. We've seen a lot of these ads lately – often saying someone has just been sent overseas in the military. So what do you do if someone you don't know asks you to wire them money?

- 12 On your Facebook page, it's a good idea to:**
- Post lots of pictures of your friends without asking them.
 - Tell people where you are and what you're doing, all the time.
 - Know your privacy settings and check them when the site's policies change.**
 - Be outrageous, since nobody but your friends will see what you post.

Comment: Privacy settings change enough that you can never be sure who's seeing what things you post. We know that college admissions offices, teachers, employers—all look at Facebook to learn about you. Consider that before you post.

- 13 You won the lottery! Yay, you! Now, just wire \$400 for the taxes. You:**
- Won! You won! You wire the money so you can get rich.
 - Do not wire money to people you don't know. It's your rule. You stick to it.**
 - Ask all your friends what to do...and then you send the money.
 - A or C but not B

Comment: How many ways can people ask you to wire money? Well, this is another one. Some people don't even remember entering a lottery, but they still believe they won and send money to collect their prize. But what do we know now? Never wire money to people you don't know.

- 14 You find out you can make big money working from home. You:**
- Call the phone number on the poster and give them your credit card number.
 - Click the link in the ad, fill out the form, and give them your credit card number.
 - Realize that it's a bogus offer. Ignore it.**
 - Ask your friends what to do, then sign up with your credit card number.

Comment: These offers are online and even on posters on street corners. There are legit work-from-home jobs, but they don't usually advertise on a telephone pole. Most of these offers want you to pay for supplies or a list to get you started – but you'll never actually make big (or any) money.

- 15 You get a message from a friend who's in trouble in another country. She needs you to wire her money to help. What do you do?**
- You reply to that message to see how you can help.
 - You get in touch with your friend a different way to see what's up.**
 - You tell your friend her account might have been hacked.**
 - Either B or C**

Comment: So why can't we wire money to people we DO know? You can, of course, but there are lots of these scams going around. People's email or Facebook accounts get hacked, and scammers pretend to be your friend, asking for money. Get in touch with your friend through another account, or by phone. Find out what's up. And you might want to tell her she's been hacked, too.

- 16 The best prepaid debit cards are the ones recommended by someone famous.**
- They wouldn't say it was good if it was a bad deal. Would they?
 - I look for the lowest fees. I don't care who advertises it.**
 - Who would know better than the financial people with their own TV shows?
 - I don't care if it's the best deal ever, I'm not carrying a THAT guy's card.

Comment: Almost all prepaid cards charge some kind of fee – maybe a monthly charge to use the card, or a fee to take cash out of an ATM. But you can shop around to find the best deal for you. Celebrities get paid to advertise things like these cards. It doesn't make it a good deal.

