



IDENTITY THEFT IQ. QUES



1. The person who steals someone's identity is most often:
 - A. Someone they know
 - B. An employee at a financial institution
 - C. An online criminal

2. While surfing the internet, a pop-up ad takes you to a site offering a free game for your computer. What is your best course of action?
 - A. Do a little research to decide whether it's safe to download the game.
 - B. Download it now, and decide later whether to use it or give it to a friend.
 - C. Go ahead and download it to play right away – you can always uninstall it later if there's a problem.

3. If someone has stolen information about your financial accounts, it's best to wait for several weeks to see what they do with it before taking any action.

TRUE **FALSE**

4. Identity theft refers only to the theft of drivers' licenses or name badges.

TRUE **FALSE**

5. You can get a free credit report from a lot of different websites – all you have to do is search "free credit report" in your internet browser.

TRUE **FALSE**

6. Some file-sharing programs install spyware that can monitor your browsing habits and send that data to third parties.

TRUE **FALSE**

7. One of the benefits of file-sharing (like mp3s) is that each file has already been scanned by other users' computers for viruses, so they are safe to download immediately.

TRUE **FALSE**

8. You receive an email from your bank informing you that it suspects an unauthorized transaction on your account. To protect your account, the email advises you to click on a link to verify your identity. Should you do so?
 - A. No way! The whole thing sounds 'phishy'! If you're concerned about your account, contact your bank directly using a phone number or Web address you know is genuine.
 - B. Yes. If someone is using your bank account, you don't have a second to lose. Immediately click on the link to verify your identity.
 - C. Yes – but first you should make sure the message looks like it's legitimate.

9. You should review your credit card and bank account statements as soon as you receive them.

TRUE

FALSE

10. One of the best ways to protect your identity is by using online passwords only you would know – like your mother’s maiden name or the last four digits of your Social Security Number.

TRUE

FALSE

11. Someone who’s a friend of a friend posts a message on your social networking webpage that says “Hi – I just saw the coolest cell fone online. I’ll get it 4 u – what’s your #?” Do you give them your phone number?

A. Yes, right away. If they know my friend, they’re totally cool.

B. Yes, but only after I check with my friend to see if they really know them.

C. No way. That’s my information and I won’t give it out to anyone online.

12. If you accidentally put personal information on your Social Networking webpage and you delete it, no one will be able to view that information anymore.

TRUE

FALSE

13. The public “hot spots” offered by many cafes, hotels, airports, and other establishments offer the safety of secure network communication.

TRUE

FALSE

14. What might it mean if your computer slows down, displays repeated error messages, serves up a lot of pop-up ads, and appears to send email messages you didn’t write?

A. You need to turn off your computer and let it take a week long vacation.

B. You’ve got spyware.

C. Your warranty is up.

15. Name at least one thing that you should find out before entering your personal information online. _____
