9. You are in a public place which offers free wi-fi, like an airport or café. Is your information secure when you log into your school email or social media account?

A. Yes.
B. No.
C. The public wi-fi is secured, so why not?
D. If your friends do it, you can do the same.

Answer: B
When using a public wi-fi connection you should automatically assume that the connection is unsecured (unencrypted). On an unsecured network, people could see what sites you visit and this can put you at risk.

10. You just downloaded a wellness app or a personal health tracking app and want to link your information with your friends in order to grant them access to your sleep patterns, exercise times and locations, and other health information. Before allowing such access, you should:

A. Read app's Privacy Policy.
B. Review your privacy settings.
C. Ask your friends about their privacy settings.
D. Research the app developer before you download the app.
E. All of the above.

Answer: E
More than a quarter of the wellness app profiles are public and show the times, locations, start and finish points and other personal information about the user. User's gender, height, age, weight and fitness level, as well as the geo-location information, is just some of the information that could be identified and intercepted with quite basic software and hardware.

How well did you score?

If you answered 9 questions or higher correctly, you are a digital expert! Nice job! You've earned the right to call yourself an expert. Not only are you aware of how peoples lives may be affected by their online behavior, but you also have an excellent understanding of how to navigate through tough cyber experiences. We are impressed! Now it is time to share your expertise with your friends and family.

If you answered 5-8 questions correctly, you may be at risk of being a cyber victim. This means that even if you think that you have good insight into how your behavior online can affect yourself and others, you may be unaware of how to protect yourself and others online.

If you answered less than 5 questions correctly, watch out! Your choices would have exposed you, your friends and your family to unnecessary risks including spyware and identity theft. Just because the Web is "digital" doesn't mean that "real world" rules don't apply. If it feels wrong or risky, don't take the chance.

Learn more about cyber safety by visiting:
NJConsumerAffairs.gov/CyberSafe

Cyber Sense

Other Resources

www.nj.gov/lps/dcj/idtheft.htm
www.njsp.org/tech/identity.html
www.cyber.nj.gov/citizens
www.consumer.ftc.gov/
www.identitytheft.gov/

Contact

If you wish to report a suspected incident of cyber fraud, you can file a complaint with the Division of Consumer Affairs through the Division's main website or by calling **800-242-5846** (toll-free within New Jersey) or **973-504-6200**.

Cyber Sense -Quiz-

Take this Quiz to see if you are really protected when going online.

Check how Cyber-Savvy you really are.

New Jersey Division of Consumer Affairs
800-242-5846 ■ www.NJConsumerAffairs.gov

1. What is "Personal Information"?

A. Your name.
B. Your residential address.
C. Your parent or guardian's full name.
D. Student ID.
E. Your social security number.
F. None of the above.
G. All of the above.

Answer: G
Always guard your personal information.

2. You unlock your smartphone and notice that 7 of your apps have available updates. What do you do?

A. Ignore the prompts to update.
B. Update the apps.

Answer: B
Updating apps and operating systems help protect you from known vulnerabilities that put your information at risk.

3. What is the best way to use social networking sites?

A. Limit the amount of information you share about yourself.
B. Only talk to people you know.
C. Make your page private, except to the people you know.
D. All of the above.

Answer: D
Own your online presence. When available, set the privacy settings on your accounts to the strictest possible level for information sharing. It's okay to limit how and with whom you share information.

NJConsumerAffairs.gov/CyberSafe

NJConsumerAffairs.gov/CyberSafe

4. You are on social media and all of a sudden you receive a friend request from someone you don't know. You should…

A. Accept the friend request since it is rude to ignore the request.
B. Deny the friend request – who are they?
C. Send a message and ask how they know you.
D. You are not on social media.

Answer: B
Accepting strangers' requests for friendship increases the risk of giving them access to your personal information. Even seemingly innocuous information like friends' names, pet names, holiday plans and likes and dislikes can be used by a scammer to commit identity theft.

5. You posted a picture online, but decided later to take it down. You are worried that your friend might see it, but your friend doesn't have a computer, so they'll never see the photo, right?

A. True. B. False.

Answer: B
You never know who is going to see images that are posted online. Copies could be passed around and someone may have saved an image before you deleted it. Be a responsible online citizen. Think about what you post and whether you and/or your friends would be okay with it. Post only those things about others as you would have them post about you.

6. Anything you send in your private email, IM or chat cannot be seen by others, right?

A. True. B. False.

Answer: B
There are programs which can "see" into your private correspondence online and you never know whether someone will share it in the future. NEVER send personal information unless you are positive it is a secure site or connection.

7. Metadata is information embedded in photos. It tells people…

A. Where and when you took the photo.
B. Where you posted the photo.
C. How awesome your hair looks.
D. Your favorite color.
E. None of the above.

Answer: A
Before posting any photos, you may want to remove the metadata from the images so you do not release GPS coordinates for your photos.

8. After a disagreement at school, a group of schoolmates send you offensive messages on social media or your cell phone. You should…

A. Block them.
B. Keep the emails, messages and comments you receive.
C. Tell your parents/guardian.
D. All of the above.

Answer: D
If you believe that someone is bullying or harassing you online, you should tell your parents or a trusted adult. Block the person and save all messages. Many websites have ways to report the abuse and/or help you respond to messages that make you feel uncomfortable.

Cyber Sense