STOP. THINK. CONNECT.
Online Safety Quiz

STOP | THINK | CONNECT™

Round 1: Safety and Security

Question 1:

Kristina is on Facebook and receives a friend request from a boy she doesn't know. What should she do?

A. Accept the friend request. It's rude to ignore him.
B. Deny the friend request.
C. Send him a message and ask him how he knows her.

Answer 1:

B. Deny the friend request.

A friend is someone you know and trust and have interacted with over time.

Question 2:

When you create passwords, you should make them easy to guess. (True or False)

Answer 2:

FALSE.

You should create passwords or use passphrases (a group of words) that are easy to remember, BUT hard to guess. Make your passwords long, strong and unique by using a combination of upper and lowercase letters, numbers and symbols. Don't use the same password for different accounts. Write your passwords down and keep them in a safe place away from your computer.

Question 3:

Hector unlocks his smartphone and notices he has 12 apps that need to be updated. What should he do?

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

Answer 3:

B. Update the apps.

It’s important to Keep a Clean Machine. Keeping a Clean Machine means having the latest operating system, software, web browser, anti-virus protection and apps on your computer and mobile devices. You should also only have apps on your phone that you actually use.

Question 4:

You don’t have to worry when you visit your favorite sites, like Facebook and gaming sites, because they are safe from spyware, malware and other online threats. (True or False)

Answer 4:

FALSE. Trusted sites can be safer. However, what you do on those sites – such as clicking on posts with links or using apps – can put you at risk. The best security step you can take is to Keep a Clean Machine. Keeping a Clean Machine means having the latest operating system, software, web browser, anti-virus protection and apps on your computer and mobile devices. Remember, when in doubt, throw it out! Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

Question 5:

When online, you should be careful whenever approached by a new person or asked to provide information about yourself. (True or False)

Answer 5:

TRUE. You always need to be on the lookout for online intruders! Be careful because they may be trying to get information from or about you. Remember to Be Web Wise and think before you act. Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.

Question 6:

You receive an email from a person that identifies themselves as your friend John. They want to meet you in the park after school. Do you:

A. Tell your parents about the email and ignore the request.

B. Ask the person a question only John would know to make sure it is John.

C. *Go to the park and meet your friend John.*

Answer 6:

A . Tell your parents about the email and ignore the request.

Some people will pretend to be other people and may be impersonating someone you know. It’s better to be safe than sorry! Unfamiliar email addresses and posts on social network sites should raise a red flag. Let your parents know and let them help you make the right decision about contacting John.

Question 7:

You should always know who you're talking to online. (True or False)

Answer 7:

TRUE. The Internet can be a place to meet people and join new communities. But just because you meet someone online, it doesn't mean you really know their identity. Use caution when interacting with new people. There is nothing wrong with being suspicious and extremely guarded about sharing any personal information.

Question 8:

You receive a chain email that tells you to pass it on to 10 of your closest friends. Do you:

A. Send the email to your friends – it’s so cool and you want them to see it too!

B. Delete the email. You're never sure what viruses these types of chain emails can have.

Answer 8:

B. Delete the email. You're never sure what viruses these types of chain emails can have.

When in doubt, throw it out! Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

Question 9:

Malware is a type of software designed to cause viruses. (True or False)

Answer 9:

TRUE. Malware, short for malicious software, is designed to cause damage or disruption to a computer system or to use a computer to send spam, distribute malware or launch an attack on other computers.

You can avoid malware by Keeping a Clean Machine and having the latest operating system, software, web browser, anti-virus protection and apps on your computer and mobile devices. Remember, all devices that connect to the Internet need protection.

Question 10:

When it comes to online shopping, you can safely shop from any site. (True or False)

Answer 10:

FALSE. When shopping online, you should always shop from trusted and well-known websites and always with a parent or other adult present.

When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with “https://,” which means the site takes extra measures to help secure your information. “Http://” is not secure.

Question 11:

You should be aware of pop-ups and downloads. (True or False)

Answer 11:

TRUE. Pop-ups and downloads can contain viruses that could infect your computer.

You can avoid viruses by Keeping a Clean Machine and having the latest operating system, software, web browser, anti-virus protection and apps on your computer and mobile devices.

Question 12:

You and a friend are on the computer, looking to download music and movies. You should:

A. Go to a site that your friend uses and download a few files onto the computer.

B. Only with your parent's permission, go to trusted websites or app stores to download music and movies.

Answer 12:

B. Only with your parent's permission, go to trusted websites or app stores to download music and movies.

Your friends may not know what websites are safe or unsafe for you to download. It's illegal to download music or movies from certain websites. Only purchase music and movies from established services for media distribution.

Round 2: Privacy and Being a Good Online Citizen

Question 13:

What is the best way to use Facebook, Tumblr, Instagram and other social networking sites?

A. Limit the amount of information I share about myself.

B. Only talk to people I know.

C. Make my page private, except to the people I have as my friends.

D. All of the above.

Answer 13:

D. All of the above.

Own Your Online Presence. When available, set the privacy and security settings on websites to your comfort level for information sharing. It’s ok to limit how and with whom you share information.

Question 14:

You posted a picture online, but soon decided to take it down. You are worried your friend may see it, but then soon remember that person DOES NOT have a computer. Your friend will never see the photo. (True or False)

Answer 14:

FALSE. You never know who is going to see things that are posted online.

Even if your friend doesn't have a computer, there are many other ways he could see the photos after they have been shared with friends. Copies could be passed around and someone may have saved an image before you deleted it. Be a good online citizen. Think about images you post and whether your friends would be okay with them. Post only about others as you would have them post about you. Whenever possible, get permission before posting pictures or videos of others. Likewise, let others know they need your permission before posting pictures or videos of you.

Question 15:

The great thing about the cyber world is that you can say things you might not always say directly to someone's face. (True or False)

Answer 15:

FALSE. Statements you make online about people can be just as hurtful as saying them face-to-face.

Being nice in the cyber world is equally as important as when you talk face to face. If you don't want it done to you, don't do it to someone else! Be a good online citizen. Post only about others as you have them post about you.

Question 16:

It is okay to download FREE music from music sharing sites, as long as no one finds out. (True or False)

Answer 16:

FALSE. This is the same as stealing from a store and you are stealing from your favorite artists as well!

Only purchase music from established services for music distribution. Some file sharing sites are also well known sources of malware distribution. Remember, safer for me more secure for all. What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

Question 17:

The pictures you decide to post online today can affect your future reputation. (True or False)

Answer 17:

TRUE. The photos you post online may never go away!

In the digital age, you need to pay attention to your reputation from the moment you start going online. Your online reputation can be both positive and negative, depending on the choices you make and can affect the future when you apply for colleges or jobs. You can manage your online reputation by remembering to Own Your Online Presence and setting privacy and security settings to your comfort level for information sharing.

Question 18:

You and your parents have established rules when you use the Internet. You are over a friend's house and decide to use the internet. Do you:

A. Do everything your friend does online, because you're at their house.

B. Respect your parents' rules, even if you're at a friend's house.

C. It doesn't matter. You can't get in trouble because your parents will never find out!

Answer 18:

B. Respect your parents' rules, even if you're at a friend's house.

Your parents are trying to help you establish good online habits with all the devices you use to access the Internet, even if they are not your own.

Question 19:

You are playing a game on a smartphone and the app asks for your current location. It's okay to enable location services because all of your friends play the game and if they do it, it must be okay. (True or False)

Answer 19:

False. Think before you app.

Many apps do not need geo-location services enabled in order to provide the service. Make sure you decline or opt-out of the location service feature on your phone. If you don't know how to do this, ask your parents. Protect your personal information by reading the privacy policy of an app before you download it to understand what information the app accesses and how it uses your information.

Question 20:

Stealing other people's work online – from sites like Wikipedia and Google – is a crime. (True or False)

Answer 20:

TRUE. Stealing other people's work is considered theft. If you cut and paste content into your homework without citing the source, it is cheating and plagiarism.

Question 21:

You are deciding on what personal information to post about yourself in an online profile. You decide to:

A. Review the information carefully before you post it because you do not want to post too much information about yourself.
B. In order to prevent misuse of your information, don't post too much information about yourself on Facebook, personal websites, your blog, or in chat rooms.
C. Go ahead and post information about yourself online, because you can always choose to edit it later if you don’t want people viewing certain information.
D. BOTH A & B.

Answer 21:

D. Both A&B

Own your online presence. When available, take the time to understand and set privacy and security settings on websites to your comfort level for information sharing. You should know who will see the content before you post it.

Question 22:

Post only about others as you would have them post about you. (True or False)

Answer 22:

TRUE. You should always practice digital respect.

Treat others as nicely as you would like to be treated. Remember, safer for me more secure for all. What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

Question 23:

Jessica's friend Sophie asks for Jessica's password to her Facebook account. What should Jessica do?

A. Give Sophie her password. Sophie is her friend and Jessica can trust her.

B. Tell Sophie her password and change it as soon as she gets home.

C. Don't give her password to Sophie.

Answer 23:

C. Don’t give her password to Sophie.

Protect your personal information. Passwords are never to be shared with anyone other than a parent or guardian. It is a good idea for parents and guardians to keep passwords to make sure you remain safe and secure. Just because you spend time with friends, doesn’t mean you have to follow everything they do. If they are doing something that doesn’t seem right, you should feel completely comfortable standing up for what you think is right.

Question 24:

After a disagreement at school, a group of kids send Jaedon threatening messages on Facebook. What should he do?

A. Block them from his page.

B. Keep the emails and comments he receives.

C. Tell his parents.

D. All of the above.

Answer 24:

D. All of the above.

If someone is bullying or harassing you online, you should tell your parents or a trusted adult. Ignore and block the person and save all messages. Many websites, including Facebook, have ways to report the abuse and/or help you respond to messages that make you uncomfortable.

Question 25:

Creating a fake Facebook page for someone you know in your class, or for someone you don't even know, is illegal. (True or False)

Answer 25:

TRUE. Impersonating someone else online is one form of identity theft! Penalties can be as high as $100,000 fine plus a minimum of ten years in prison.

Question 26:

When you are connected to the Internet, you are responsible for your actions. (True or False)

Answer 26:

True. Remember to STOP. THINK. CONNECT. Make sure you have taken security precautions, understand the consequences of your actions and behaviors and enjoy the Internet. Remember, the Internet is a shared resource. When you are safer online, you make the Internet more secure for everyone!

The End

For more online safety tips, visit stopthinkconnect.org

STOP | THINK | CONNECT™