Internet Safety Quiz

1. What's a good strategy for keeping your passwords safe?

A) Use a long string of random letters and numbers for each password. Write them on a post-it note and stick it near your computer so you don't forget.

B) Come up with a secure password you can remember and use it for every online account

C) Choose a unique memorable phrase/sentence for each account

2. You take a video of your best friends dancing. You want to post the video on Instagram. Which <u>two</u> things should you do before uploading it?

A) Compress the video file

B) Check with your parent/carer

C) Make sure it's less than 3 minutes long

D) Ask your friends if they are happy for it to be uploaded

3. A new film comes out and you really want to watch it, but you don't have enough money to pay for the cinema. You see a link to download it for free. What should you do?

A) Go into 'Incognito' mode, then download it and delete it if it doesn't work properly

B) Download it at your friend's house

C) Wait until it's released for DVD/online video rental



4. Someone you don't know messages you on social media. What would be the most sensible response?



A) Ask them to send a picture of themselves doing a certain pose so you can make sure they're really who they say they are

B) Tell a trusted adult or parent/carer

 \overrightarrow{C} Have a casual conversation but don't tell them your address



The Warwickshire School Health & Wellbeing Service is here to support you with a range of health/wellbeing topics, including online safety. If you're aged 11 - 19, you can text a school nurse for free, confidential advice on 07507331525.



5. A social media site is requesting you share personal information to go on your public profile. What information do you think is ok to add? (Choose as many as you think are appropriate)

A) Your address, but don't include the house number

- B) What school you go to
- C) Your mobile phone number
- D) None of the above

6. Someone you really like has asked you to send them a revealing photo of yourself. Why could doing so put you at risk? (Choose all that apply)

A) If the relationship turns bitter, they could share it onlineB) They might show their friends, which could be embarrassing for youC) The app/device/website used to share the photo could be hackedD) All of the above

7. Your friend is crying because her ex-boyfriend has shared a revealing photo she sent online. Which of the below could you advise her to do?

(Choose as many as you think are appropriate)

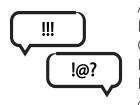
A) Share a revealing photo of him online and tell him she will only take it down if he removes hers

B) Tell a trusted adult or parent/carer

- C) Don't tell any adults, as she might get into trouble for breaking the law
- D) Message him and ask him to remove the picture
- E) Report the picture to the website/social network it is posted on
- F) Delete all her social media accounts

8. Some people from your school start sending you nasty messages via social media. Which of the below should you do? (Choose all that apply)

C) Select 'ghost mode' in your Snapchat settings, or manage which apps can access your location in



A) Uninstall Google MapsB) Turn off your Bluetooth

your phone's settings

A) Send aggressive messages back and get your friends to back you up

B) Tell a trusted adult

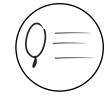
C) Confront them at school the next day

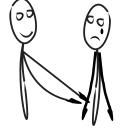
D) Take screenshots of the messages

E) Block them and do something nice to take your mind off it, like chat to a friend or hug your pet

9. Snapchat has 'location sharing' options that can show your Snapchat 'friends' where you are. How can you stop this from happening?







D) Don't use Snapchat whilst connected to 4G

Internet Safety Quiz - answers, talking points & resources

- C don't write your passwords down or use the same for each account, as this increases the chance of being hacked. Instead, choose a unique memorable phrase, and if possible add a special character or number and mixture of cases - for example 'Reddocmartens100".
- 2. B and D talk to a parent/carer before uploading videos of you or your friends to check the content won't put you at risk. Check with the people in the video as well as you would like to be asked if someone was uploading a video of you.

3. C — downloading videos illegally can often put malware on your computer. You're also breaking the law, and your IP address can be tracked even if you are in 'Incognito' mode, meaning your location, operating system and browser are still visible!

- 4. B even if you know what someone looks like, they may not be who they say they are, which could put you at risk. A trusted adult will be able to give you advice to help you stay safe.
 - 5. D stay as anonymous as possible online, particularly when using public-facing accounts. You should always set your profile to 'private' if possible so only your friends can see your posts.
- 6. D if a revealing photo of you is shared online, it can be almost impossible to delete, and could lead to you being blackmailed or bullied.

7. B, D and E — if something like this happens to you or a friend, don't panic — you're not alone and there are steps that can be taken to minimise the effects. Tell a trusted adult or parent/carer — it might be a difficult conversation but their main concern will be keeping you safe. You should also report the photo to any social network it is posted. Although sending an explicit picture of someone under 16 is illegal, the law is meant to protect people who are victims of having their photo shared online, not get them in trouble. More information can be found here: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/

8. B, D and E — speak to a trusted adult, who will be able to support you in taking steps such as speaking with your school or reporting the abuse to the social media site. You will most likely feel better if you walk away from the situation rather than retaliate. Remember it's not your fault and anyone can be a victim of cyberbullying.

9. C — if you're ever unsure about whether your phone is sharing your location, ask a trusted adult for help.

Resources:

Internet safety advice for teens

https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/ https://teens.webmd.com/features/teen-internet-safety-tips

> Internet safety resources for parents and children/young people: <u>https://www.internetmatters.org/</u> <u>https://www.net-aware.org.uk/</u>

Snapchat safety advice - <u>https://www.snap.com/en-GB/safety/safety-education</u> Instagram safety advice - <u>https://help.instagram.com/667810236572057</u> Facebook safety advice - <u>https://en-gb.facebook.com/help/122006714548814?helpref=popular_topics</u> Twitter safety advice - <u>https://about.twitter.com/en_us/safety.html</u> Tiktok safety advice - https://www.net-aware.org.uk/networks/tiktok/