BEACON Consultant Services

FACTSHEET

Staying Data Safe Online

Overview

As we begin to settle into home schooling for yet another term, the number of children that are now online has never been greater. Cyber criminals and other 'threat actors' will take any opportunity to take advantage of this situation.

Most children spend a good proportion of their day using social media and surfing the internet, but do they know how to do it safely? There are hundreds of applications and privacy settings that you can use to protect your computers, keeping your family safe, but education and our internet behaviours are the most important security feature that can exist.

Read on for our 10 top tips for keeping your children, and your family's personal information safe.

1. Keep Updated

Keep the software that you are using up to date. Microsoft Teams, Zoom and Google Classrooms are constantly monitoring security vulnerabilities in their software, to reduce the risk of these platforms being used to deliver viruses and to gain access to your personal information.

2. Trusted Sites

Use trusted websites when researching information or browsing, this can be detected by seeing https:// or the padlock symbol in the address browser.

3. Social Media

Set social media accounts to Private to ensure your profile, and your children's isn't available to everyone. Cyber criminals will use information from your profile to build a profile of you which can be then used to crack your password, for example.

4. Email Security

Ensure your email account password is very strong, the recommendation is to create passwords using three random words. You just put them together, like 'coffeetrainfish'. If your email account is compromised cyber criminals can access many of your accounts using the password reset option as most use email to validate changes.

BEACON Consultant Services

FACTSHEET

Staying Data Safe Online

Key Points

5. Messaging

If you need to send personal information electronically, always use an encrypted service, such as Dropbox, Google drive or Whatsapp. Never use text messaging or email as these can be easily intercepted and there is always a trace left of your personal information.

6. Attachments

Never open email attachments if you're not sure who the sender is or not expecting an email with an attachment. This is the most common method of a cyber criminal delivering a virus which may allow access to your PC, tablet or mobile.

7. Passwords

Keep the meeting ID and password/PIN of meeting rooms secret. Divulging the ID & password into the wrong hands can result in 'Zoom Bombing' – the new term used for when your meeting gets hijacked by someone. Never post this information on social media sites as you never know who may join the meeting and be listening in on the conversations!

8. Location Setting

Switch off location settings or location tracking on your devices. This feature can detect where you are, on some mobile platforms, such as Snapchat location information can show the exact GPS location you are in.

9. Be Selective!

Never give too much personal information when requested, always ask why it is needed and if you're not comfortable providing it, say so! Consider personal information like money, if a stranger asked you to give them £10, I'm sure you'd want to know why!

10. Further Advice

Privacy and Internet Safety Parent Concern | Common Sense Media

a great resource of information for all the family.

https://ico.org.uk/for-organisations/childrens-code-hub

Information & code from the data protection regulators