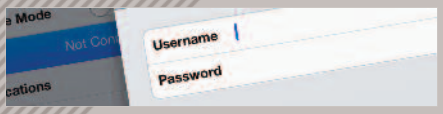
Safer Internet Day

TOP 10 TIPS

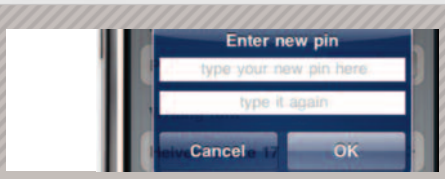
1 DON'T GIVE OUT YOUR PERSONAL INFORMATION – Don't put personal details such as your home address, telephone numbers or parent's work address online as cybercriminals can use this information to create a fake profile with your details.

2 WHAT GOES ONLINE, STAYS ONLINE – Everything you put online including photos, videos and status updates are there for the world to see! Only post information that you don't mind people knowing. Often university admissions teams and potential employers will look at your social networking profile to find out more about you so be sensible.

3 CHECK YOUR SECURITY AND PRIVACY SETTINGS – Make sure your social network privacy settings are secured so only your friends can see your personal information and use your privacy settings to restrict who can see your posts, videos and photos.



4 PASSWORD SAFETY – Choose a password with a mixture of letters, numbers, and upper and lower case characters and a word which people won't be able to guess instantly to ensure your information is safe. Also, avoid sharing your password with your friends, even if they promise they won't tell anyone!



5 ALWAYS PROTECT YOUR MOBILE DEVICE – Make sure your mobile phone is pin-protected so all your personal information stored on it is safe. Download a security app which allows you to wipe any personal data, should your mobile be lost or stolen.

6 DON'T TALK TO STRANGERS ONLINE OR OFFLINE – Let your parents know if someone has tried to contact you online that you don't know and don't meet up with strangers. If you are concerned about someone who has contacted you, tell an adult and report it immediately.

7 LISTEN TO THE ADULTS WHO KNOW – Adults will always be worried about your safety on the internet as we increasingly hear about more and more cybercriminals targeting unsuspecting teenagers. Share any concerns about phone calls, text messages and photos with a trusted adult if you feel worried.

8 BE WARY OF UNSECURED OR UNKNOWN WEBSITES – When shopping online, always use reputable outlets and known retailers. Make sure any transactions you make only take place across secure web pages which can be identified by a padlock sign in your browser address bar and the website address includes https. The 's' stands for 'secure'.

9 BE CAREFUL WHAT LINKS YOU CLICK ON – Double check before clicking links in an email, IM or on your social network to make sure the message is from someone you know. Cybercriminals have been known to hack into your friends email accounts to send emails claiming they are in trouble and asking you to transfer them money. Don't believe it if it sounds suspicious or offers something unrealistic.

10 MAKE SURE YOUR SECURITY SOFTWARE IS UP TO DATE – Security software is now available on all types of devices; mobile phones, tablets and PCs. Make sure you have the latest security software on your devices to stay protected at all times.