The Warriner School

Online Safety & Cyber Bullying

2017—2018

Word Search!

				t	i	m	e					
s											b	
o											u	
c		c	y	b	e	r					l	
i											l	
a						f					y	
l							u					
								n				
		m	e	d	i	a						

Find these words;

Social

Media

cyber

Bully

Fun

time

Word Scrambles!

Satimagrn

paps

Cilaso

True or False

Watching too much screens will make your eyes go square

True False

Social media stops you from being outside

True False

Word Scrambles: 1.Instagram
2.Apps 3.Social

True or False: 1.False 2.True

Stranger Danger

The perfect leaflet for discovering the advantages and disadvantages of social media.

For more information;

Email: Info@StrangerDanger.co.uk

Tel: 07895 554 238

ADDITIONAL INFORMATION

The four main social media apps

Facebook

Instagram

Snapchat

WhatsApp

Do's

... Be responsible

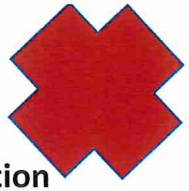
... Block or remove friends who are being horrible, It is okay to say no to any 'Friend' requests.

...Accept friend requests from people you know, not anyone you don't know.

...Trust your instincts, if something does not look right, then it probably isn't.

...Watch your language, you don't want to be known as a rude person, do you? reputation is everything.

Don'ts



... Post your private information online, Information on your whereabouts and personal details have no place on the Internet

... Spread false information or rumours .

...'Friend' anyone you don't know, this could get you into trouble.

...Put any pictures or messages online that you will regret, anyone will be able to see it, it will be stuck online forever.

...Don't share your password, with anyone.

...tag or use face recognition, unless you know none of your friends will ever, ever, ever post a photo without asking you first?!

Online Safety

If you are on social media or internet chat rooms, you need to be careful, especially with people you don't know. On social media, anyone can see your posts and find out information about you that you feel is private. Here are some tips to help you stay safe online.

1. Make your accounts private, so that only your friends can see them.

2. Don't ever arrange to meet up with anyone on the internet.

3. If you are being cyber bullied or you see others being cyber bullied, report it.

4. Remember that once you post something, it is on the internet forever. Be sensible.

6. Don't share any personal information on social media

5. Don't share private information or pictures with people you don't know.

Internet Safety

This is for all of the parents and guardians to help you keep the internet a fun but safe place for your child to be so you know they will not come across any problems when they are using any type of social media.

The first thing about social media is the age restrictions they are there for a reason, to keep people safe. Many things can be posted on the internet that can effect or make younger viewers feel sad.

Here are some points to keep your child safe.

, Never put your real name online.
, Never put any private information online about yourself or your friends.
, Only follow people you know.
, Never meet up with someone you don't actually know in person.

Stranger danger

Tips for bullying

, Always tell an adult you can trust.
, save the message but don't retaliate
, if it is someone you don't know who is saying rude comments block and report them so it wont happen again.

Remember!

Every good website should have a block and report area so your child can be safe.

Always put your childs account settings to private.

If there are age restrictions always make sure you look into the website first, they could be inappropriate.

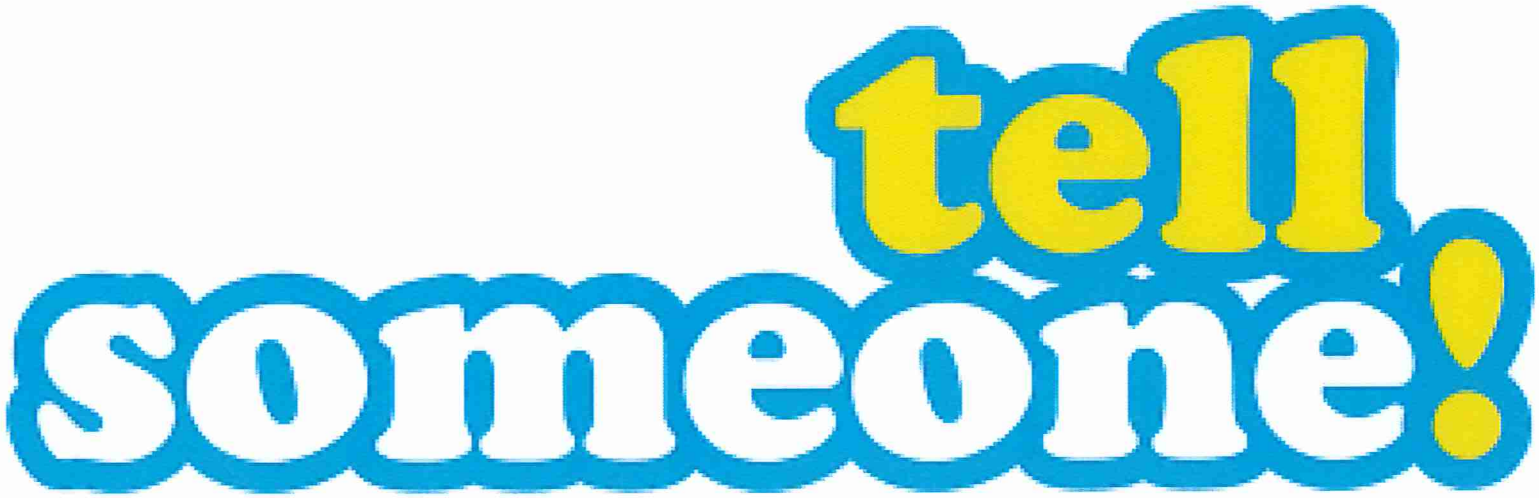
And last but not least have fun!!!

HOW TO STAY SAFE WHILE USING THE INTERNET

WHAT IS INTERNET SAFETY ???

You have to stay safe while using the internet because it can be very dangerous.
The thing that makes the internet is dangerous especially for kids is that you might not know who is contacting you because you cant see if they are a 13 year old boy or a 40 year old man contacting you and this is one of the county's biggest problem as gradually more and more people start using the internet as technology starts to increase in its smartness.

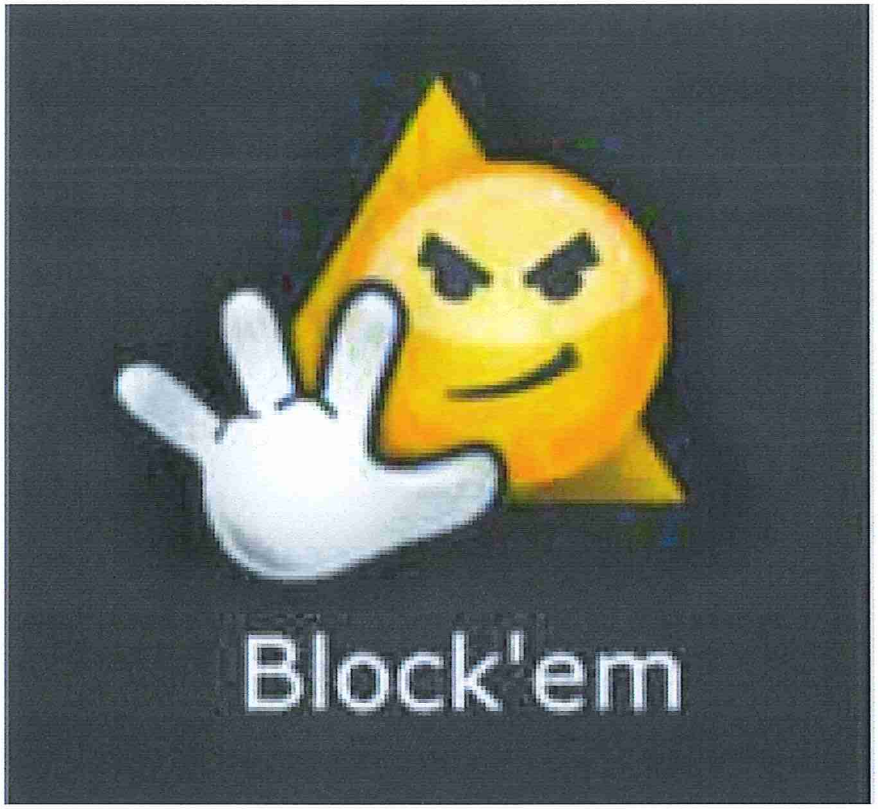
WHAT DO YOU DO IF YOUR IN A POSITION WHERE YOU DON'T KNOW WHAT TO DO????



Tell someone what is going on whether that is your parents someone at school or a friend make sure you have someone to talk to about it!!!

WHAT DO YOU DO IF SOMEONE YOU DON'T KNOW STARTS CONTACTING YOU???

Block them!!!



WHAT TO DO ???

Here are 3 rules you should use if you start worrying or feel threatened by in case you need to use them because every social media network will have these things to use to keep you and your personal details safe and secure ☺.

Zip it

Keep your personal stuff private so no one can see or know who you are.

Block it

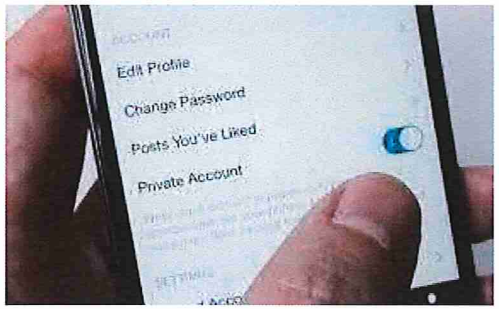
Block people you don't know or feel uncomfortable with so they cant.

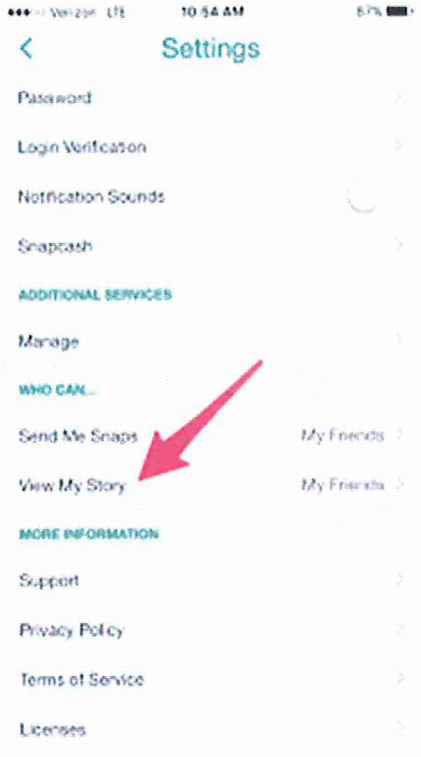
Flag it

Flag someone your unsure about and feel like they need given attention to by the website.

HOW TO BLOCK/PRIVACY SETTINGS?

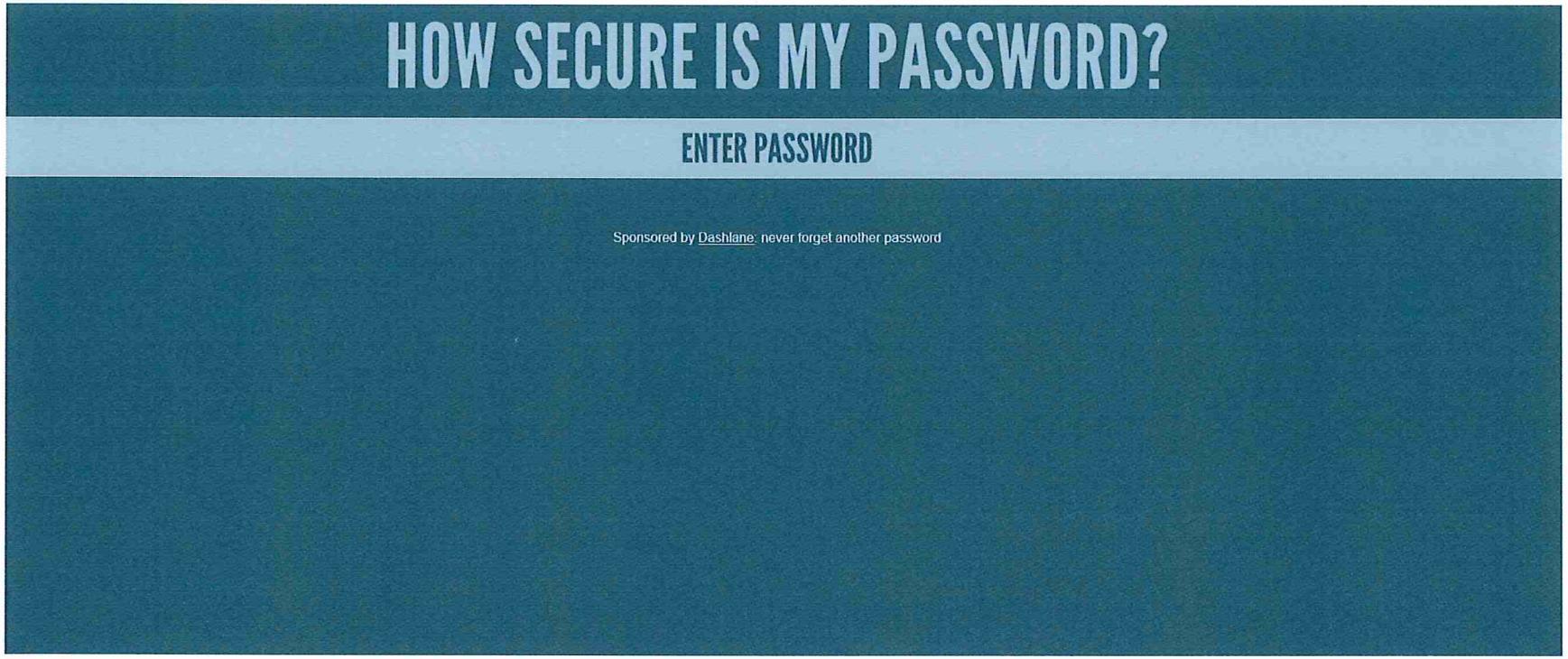
When you block someone or you want to chose who sees personal information or pictures here are some ways to do it on different social media accounts. For example Instagram you can chose if you want to be a private account(only people you let can see your pictures) or it can be an open account(anyone can see your pictures).





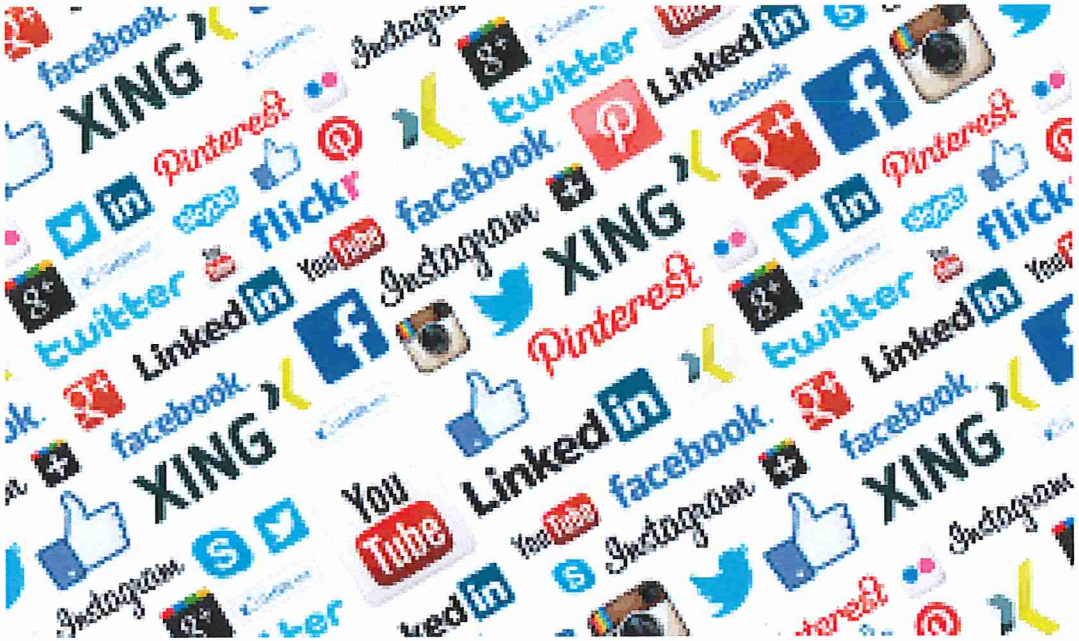
IF YOU WANT TO FIND OUT HOW SECURE YOUR PASSWORD IS GO ONTO THE LINK BELLOW!!!!

- https://howsecureismypassword.net/



AGE RESTRICTIONS

- ***Snapchat:13+***
- ***Instagram:13+***
- ***Facebook:13+***
- ***Twitter:13+***
- ***YouTube: 12+***
- ***WhatsApp:13+***
- ***Vine: 16+***
- ***Pinterest:13+***
- ***Messenger: 13+***



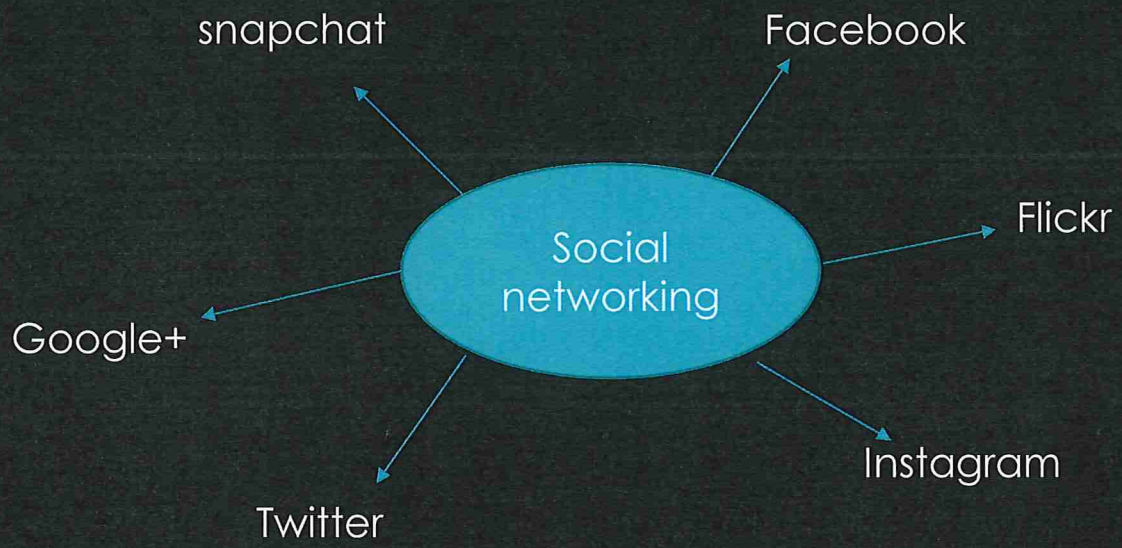
REMEMBER TO STAY SAFE WHILE USING THE INTERNET AND THANKS FOR WATCHING☺!!!

Stay Safe On The

Social networking and internet safety presentation

Mind map


LinkedIn
foursquare
LIVEJOURNAL
vimeo
YouTube
facebook
my Blogger
twitter
flickr
tumblr.
Like
Behance

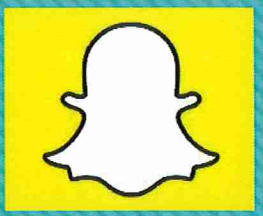

snapchat
Facebook
Flickr
Social networking
Google+
Instagram
Twitter

Facebook

- Keep account on private so only people you have friended can see you profile and photos you have shared
- Don't put personal information on your profile e.g. phone number, email, address school etc.
- Don't post inappropriate photos
- Use good long passwords that are hard to crack
- Facebook is an American online social media and social networking service based in Menlo Park, California. The Facebook website was launched on February 4th 2004 by Mark Zuckerberg.
- Be careful with what you share. Things like your home address, your family members, and your birthday are all easy pickings for identity thieves. It's harder to retract information than to simply not share at all.

•Be careful what is in the background of your photos e.g. Credit card, house number, and open laptop etc

Snapchat



•Enjoy fast and fun mobile conversation! Snap a photo or a video, add a caption and send it to a friend. They'll view it, laugh, and then the Snap disappears from the screen.

•One of the most important aspects of using this app is to make sure you limit pictures to your friends and people you can trust. When you allow people who aren't your friends to send you pictures or receive the ones you send, though, you are putting yourself at risk for receiving pictures that can get you in trouble. The safest thing to do is limit the use of this app to your closest friends.

•On snapchat people can find your location by looking on 'snap maps'. By putting it on ghost mode nobody will be able to see where you are and you will be safe.

Flickr

•Flickr is an image- and video-hosting website and web services suite that was created by Ludicorp in 2004 and acquired by Yahoo on 20 March 2005.

•Flickr offers geotagging, which shows the locations of your public photos on a map. This means that for each photo you take geotags will show the location where each picture was taken. If you geotag your hometown hangouts on public photos, it's possible to disclose more information than intended. To prevent this, change the location privacy for your photos, or create a geofence (a location with special privacy settings for private places, such as your home or your child's school).

•The Flickr staff works with the community to ensure an enjoyable experience for all. If you see something you feel violates the Terms of Service or the Community Guidelines then report it.

•The Flickr community is ever growing. As you upload content, be sure to know which privacy settings you have selected and how visible the content will be to the general public. you can choose whether you want just your friends to see your post or everyone.

Instagram

- Keep account on private so only people you have friended can see you profile and photos you have shared
- Don't put personal information on your profile e.g. phone number, email, address school etc.
- Don't post inappropriate photos
- Use good long passwords that are hard to crack
- If someone is sharing photos or videos that make you uncomfortable, you can unfollow or block them. You can also report something that you feel violates our Community Guidelines right from the app.

•Make sure your email account is secure. Anyone who can read your email can probably also access your Instagram account. Change the passwords for all of your email accounts and make sure that no two are the same. Log out of Instagram when you use a computer or phone you share with other people.

Twitter

Twitter is an online news and social networking service where users post and interact with messages, known as "tweets." These messages were originally restricted to 140 characters, but on November 7, 2017, the limit was doubled to 280 characters for all languages except Japanese, Korean and Chinese. Registered users can post tweets, but those who are unregistered can only read them.

Twitter, Inc. is based in San Francisco, California, United States, and has more than 25 offices around the world.

There are a number of signs that indicate that your Twitter account is compromised. Some of these signs are:

-You have been notified that you have sent direct messages that you didn't

-You get answers to tweets you don't remember sending

-You follow, or stop following, accounts you don't remember

-You receive non-requested or strange security notifications

-The appearance of your profile has changed, but you didn't do it.

If you see these signs, revoke the authorization of unknown apps (previous tip) and change your password immediately. And remember you can always use a password manager.

Google+

•Google Plus is an internet based social network that is owned and operated by Google. The service, Google's fourth foray into social networking.

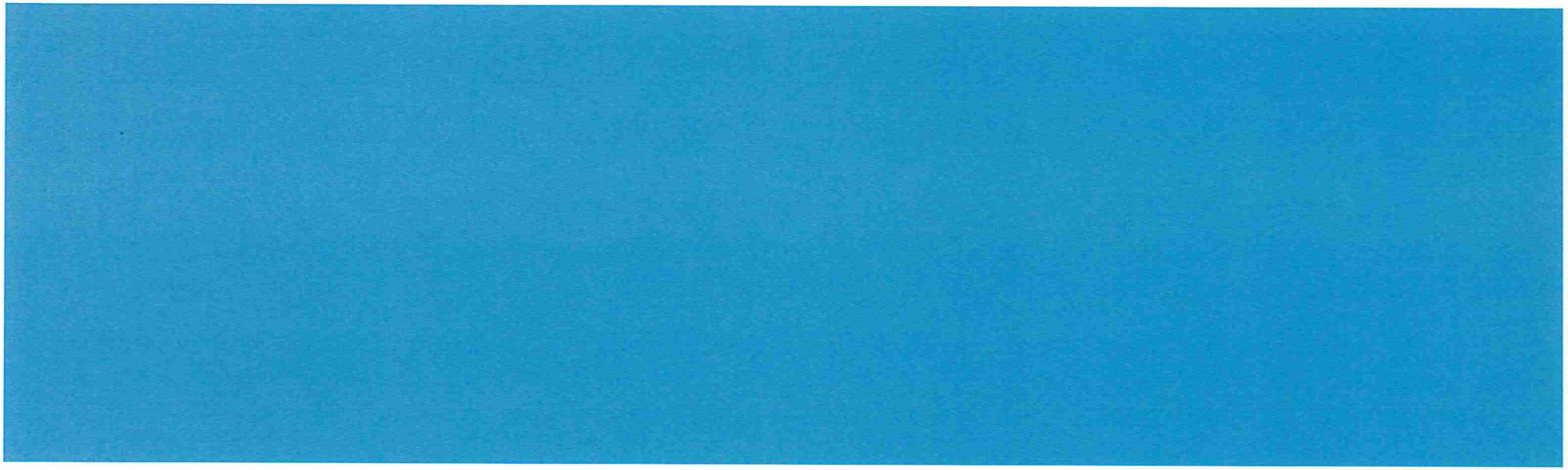
•The "+" is the social networking piece it adds to all of Google's other services, including Web search, Gmail, and YouTube – which makes the complete package even more attractive to young people.

•Identity thieves love personal details such as where you went to school, where you have worked, etc. These details are a gold mine for them. If you make the information available for the whole world to see, you are just asking for them to use it to steal your identity. It's best to restrict access to most of these details.

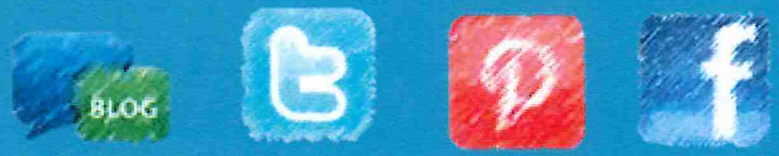
•If you use a public computer always remember to sign out as anyone could take your personal information.

•Most operating systems will let you know you when it's time to upgrade – don't ignore these messages. Old versions of software can sometimes have security problems that criminals can use to easily get to your data.

SOCIAL NETWORKING



WHAT IS A SOCIAL NETWORK?



- A social network is the use of websites and applications to interact with other users, or to find people with similar interests to someone.
- It is a platform where you can build social relations or networks with other people.
- Examples of social networking sites are: *-Facebook,-Instagram,-Snapchat,-Twitter, -WhatsApp,-Google+,-Flickr and -LinkedIn.*

- However, social media platforms can be a way for people to find information about you. Anyone you are friends with can access your personal information your posts.
- This can be dangerous because someone you don't know could access all your personal information and be stalking you but you wouldn't know it.

SOME OF THE SOCIAL NETWORKING PLATFORMS...

- **Twitter-** This is one of the fastest-growing networks. You follow people you know or are interested in, they follow you, you exchange brief text-only messages. If you say something interesting, someone might 're-tweet' it, which means repeating it to other people and saying who said it. So, this is a good way of getting more followers, and that's how you meet new people.

- **Facebook-** You get a page on the web and can use this for longer posts and messages. You can upload pictures, and videos. There are Facebook applications for areas for private messages and for more open discussions. You can also control who you follow. They have to be accepted my you to see you posts and information.

- **Instagram-** This is similar to Facebook in the fact that it is for longer posts and messages. You are also in control of who you follow and who follows you. Someone has to be accepted by you to see your posts and be able to message you etc. Other applications are available to download,(like Instagram layout), that help you use the app to its full potential.

- **Snapchat-** It is a video messaging app. When using the application, users can take photos, record videos, add text and drawings, and send them to a controlled list of recipients. These sent photographs and videos are known as "Snaps".

WHAT CAN GO WRONG?

- Many people think that most social media sites are safe and that your friends can't access personal information.
- This is not entirely true; if you have posted location or phone number, anyone following you can access that information.
- Also, you may accept a friend request form someone you thought was your friend but they might not be. There are cyber-criminals that can stalk you and access information about you by just a picture or a phone number.
- This is dangerous.

- Another point would be that if you posted an embarrassing picture or video that you don't want your boss or parents to see you can't just delete it.
- Once something is on the net… it doesn't leave!

HOW TO BE SAFE WHEN USING SOCIAL NETWORKS.

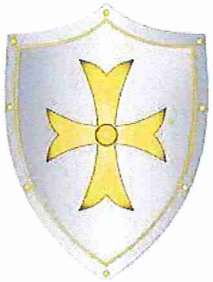
- Safety is very important when using social media platforms.
- Here are some tips on how to avoid cyber-criminals and bulling:

1. Don't accept a friend request from someone you don't know.
2. Make sure your password is secure.
3. Chose who you share posts and messages with.
4. If you are being cyber-bullied or stalked, you should block them and then make sure your privacy settings are on so that they cant see your posts.
5. You can also make sure not to share your phone number or address with anyone you don't know or who is acting suspicious.
6. Make sure to tell a responsible adult or teacher if it gets too out of hand.
7. Try to rise above bullies and block them from messaging you.
8. Be SMART…

IF IN DOUBT, THESE ARE SOME RULES TO FOLLOW:

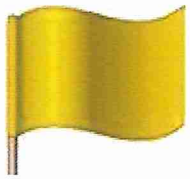
Lock it

Keep your personal information private and only accessible by people you know. Think about what you do online.



Block it

Block people who send you nasty messages or people you don't know. Don't open any unknown links or attachments.



Flag it

Tell someone you trust if anything upsets or hurts you. If someone you don't know asks you to meet offline flag it up with a responsible adult.

OR

S

Safe

Don't give out your personal information to people you don't know because it could be dangerous.

M

Meet

Meeting someone you have only met online can be dangerous. Only meet up if you know them or have your parents/carers permission and they are there.

A

Accepting

Never Accept emails or massages from people you don't know or trust as it can lead to viruses or nasty messages.

R

Reliable

If you find information on the internet it may not be true. Someone may be lying about who they are or information may be untrue. Make sure to check with many people and websites to be sure.

T

Tell

Tell a trusted adult if someone or something make you feel uncomfortable or worried. Or if someone you know is being bullied.

Social Network

What is a social network?

- A dedicated website or other application which enables users to communicate with each other by posting information, comments, messages, images, etc.

What are the social networking sites?

- Snapchat - you can now use it for a range of different tasks, including sending short videos, live video chatting, messaging, creating Bitmoji avatars, and sharing photos and videos via a chronological story that's broadcasted to all your followers
- Facebook - you can use Facebook to contact, post videos or photos
- Instagram - Instagram is a free, online photo-sharing application and social network platform. Instagram allows users to edit and upload photos and short videos through a mobile app
- Twitter - post a message, image, etc. on the social media service Twitter

Cyber Criminals

Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.

Who are they?

- Most cyber crimes are committed by individuals or small groups. However, large organized crime groups also take advantage of the Internet. These criminals find new ways to commit old crimes, treating cyber crime like a business.
- Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities.
- It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things anonymously and from any location. Many computers used in cyber attacks have actually been hacked and are being controlled by someone far away. Crime laws are different in every country, which can make things really complicated when a criminal launches an attack in another country.

Things you shouldn't post

These are just some things that you shouldn't post online

Only accept request from people you know

Never give out passwords

Don't post any personal information, like where you live, email address or mobile number

Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do

Remember that not everyone online is who they say they are

Keep your privacy settings as high as possible

If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately

Think carefully about what you say before you post something online

Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it, it's not just yours anymore

Things you can do to keep safe

- Regularly change your password
- Use a strong password. The longer it is, the more secure it will be.
- Use a different password for each of your social media accounts.
- Set up your security answers. This two factor authentication is available for most social media sites.
- If you have social media apps on your phone, be sure to password protect your device.
- Be selective with friend requests. If you don't know the person, don't accept their request. It could be a fake account.
- Click links with caution. Social media accounts are regularly hacked. Look out for language or content that does not sound like something your friend would post.
- Be careful about what you share. Don't reveal sensitive personal information i.e.: home address, financial information, phone number. The more you post the easier it is to have your identity stolen.
- Become familiar with the privacy policies of the social media channels you use and customize your privacy settings to control who sees what.
- Protect your computer by installing antivirus software to safeguard. Also ensure that your browser, operating system, and software are kept up to date.
- Remember to log off when you're done.

Remember the smart thing to do

S Stay Safe - don't give out personal information to people or places you don't know.

M Don't Meet up - meeting up with someone you met online can be dangerous. Always check with an adult you trust.

A Accepting - accepting files, pictures or emails from people you don't know can cause problems.

R Reliable? - check information before you believe it. The person or website might not be telling the truth.

T Tell someone - tell an adult if someone or something makes you feel uncomfortable or worried

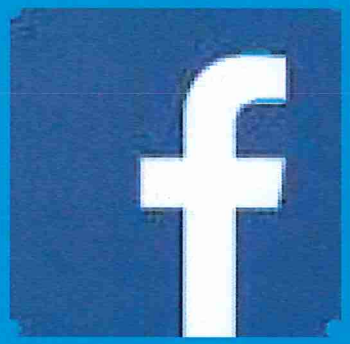
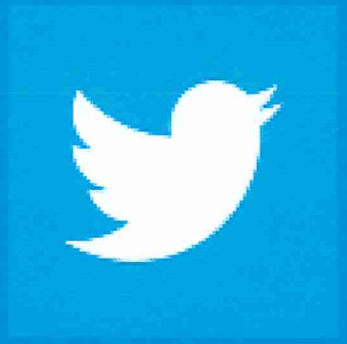
Statistics

- 29% of internet sex crime relationships started on a social media site. Further, in 26% of online sex crimes against minors perpetrators distributed information or images of the victims via social networks.
- The very nature of social networks can also lend itself to trolling, the act of intentionally posting mean or provocative messages to upset or anger other people. internet. Almost a third of people have admitted to engaging in trolling
- Cyber-bullying is also a very big problem. According to a survey, 70% of students report to having witnessed bullying online and over 40% have been victims of online bullying. The vast majority (over 80%) of respondents indicated that online bullying is easier to get away with face to face bullying.
- Nearly four in five ex-burglars have indicated that thieves look for potential opportunities. This is because 57% of people post something about their travel plans, like a photo from the airport or checking in at the hotel, telling burglars when they could break in.
- Stalking via social media is quite common. As 63% of Facebook profiles are public it is very easy for exes to check up on their former partners and their new relationships. Oftentimes, you don't know who is viewing your profile and you don't know what could happen next. Over 80% of online stalking incidents are never reported to the authorities.

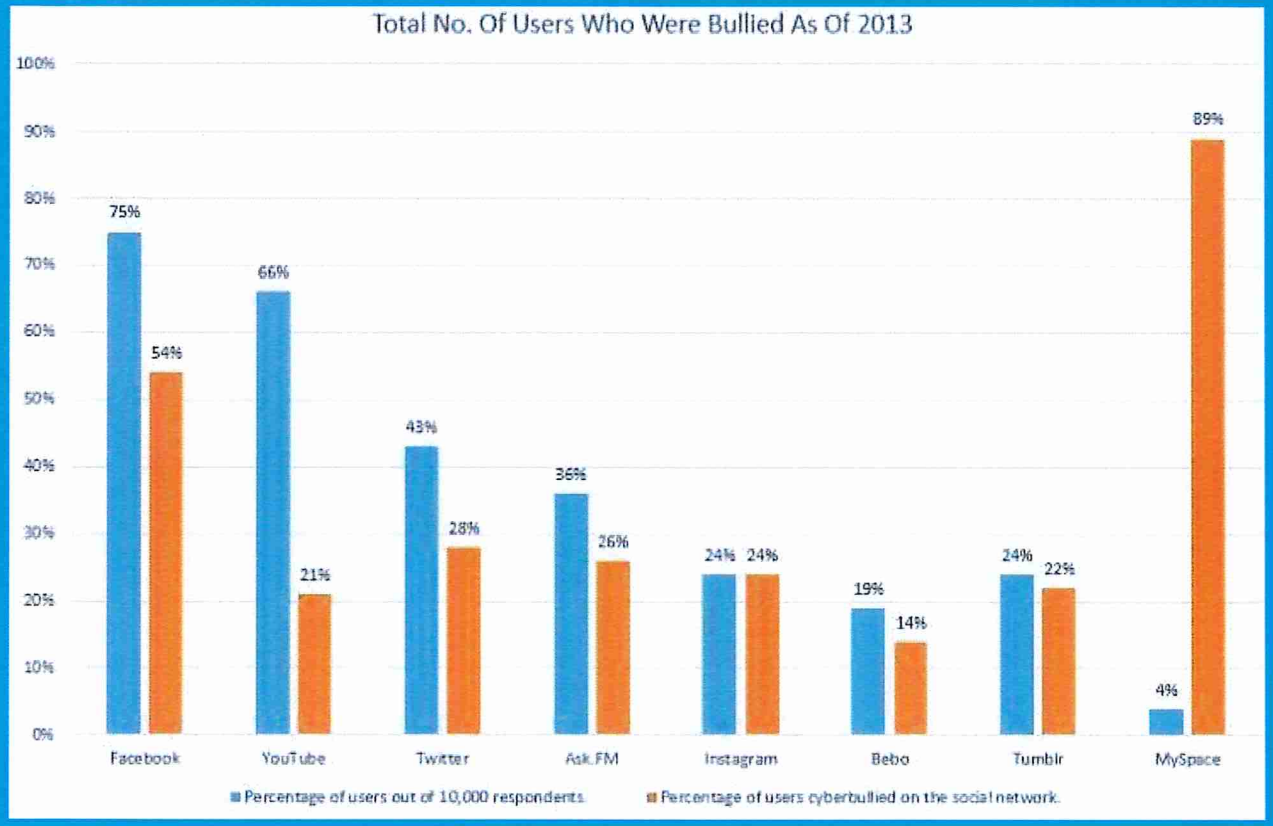
BEING SAFE ONLINE

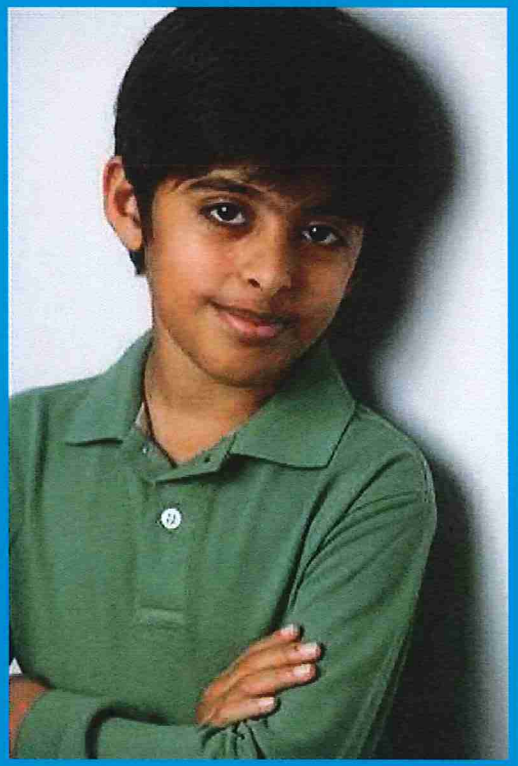
SOCIAL MEDIA

- Social media is media that allows people to connect with each other. Email allows you to connect and interact with other people, so it is "social". But given most email is just text based messaging and delivered and received on a one-to-one basis, it's a communication tool rather than media.

STATISTACS

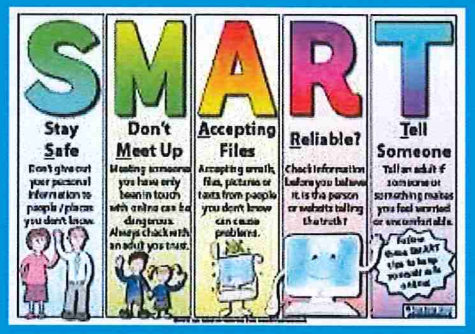


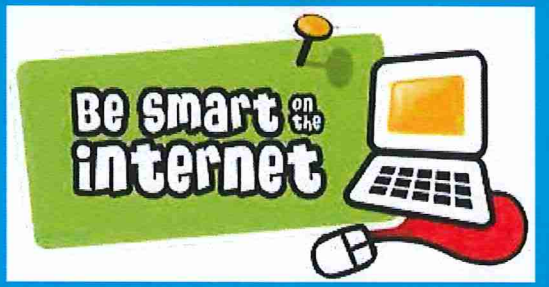


Be more like Chirag

WHAT IS INTERNET SAFETY

- Internet safety, or online safety, is the knowledge of maximizing the user's personal safety against security risks to private information and property associated with using the Internet, and the self-protection from computer crime in general.





HOW YOU CAN STAY SAFE

- 1.Create Complex Passwords.
- 2.Boost Your Network Security.
- 3.Use a Firewall.
- 4.Click Smart.
- 5.Be a Selective Sharer.
- 6.Protect Your Mobile Life.
- 7.Practice Safe Surfing & Shopping.
- 8.Keep up to date.

AGE RESTRICTIONS

- The minimum age to open an account on Facebook, Twitter, Instagram, Pinterest, Tumblr and Snapchat is 13. For Vine, Tinder and Yik Yak it's 17. YouTube requires account holders to be 18, but a 13-year-old can sign up with a parent's permission