E-Safety

INFORMATION BOOKLET

Contents:

Does your organisation in the Forth Valley need some input for Internet Safety? Contact the partnership for information on presentations to youth groups, schools, parents, professionals, carers, or indeed any group who would benefit from this. centralesafety@scotland.pnn.police.uk

CEOP Training for professionals? Contact Stewart Kerr, Fiona Murphy, or Bryan Mackie on 101 or the above email address for information about arranging CEOP Thinkuknow Introduction Training.

POLICE SCOTLAND
Keeping people safe
FORTH VALLEY DIVISION

Introducing the Central E~Safety Partnership

Internet Safety is a developing sphere for specialists within crime prevention. Two significant police investigations in recent years within the former Central Scotland Police area indicated limited knowledge and skill base for parents and guardians relating to protecting their children online. Whilst any crime prevention strategy should highlight the significant contribution that the internet has to offer children, parents, carers and practitioners, there is a message which requires to be relayed to ensure all can learn and enjoy the Internet safely.

The **Central E-safety Partnership** was created in response to this need, reporting to the Stirling Community Planning Partnership and driven by the Stirling Interventions Unit. An action plan was devised whereby members of the partnership would engage with communities to deliver practical and consistent Esafety advice and information. This was extended to encompass other identified agencies such as teaching staff within Primary and Secondary Education, both public and private. Care Organisations such as “Stirling Young Carers” “Aspire Adult Learning Team” and “Life Choices” program (skill based learning program for teenagers out with mainstream education) as well as staff, volunteers & young adults from Action In Mind (formerly Stirling & District Association for Mental Health). The logo (above) was designed by two primary school pupils as part of a competition and depicts several landmarks in the Forth Valley area where the partnership operate.

The aim of the partnership is: To promote the safe use of the internet and digital technology to reduce online crime and risk of harm to children, young people, adults, and vulnerable groups. This fits with local authority strategic objectives (Smarter, Safer, Stronger) and with National Outcomes.

It is perhaps particularly relevant to raise awareness of safety online when considering some recent high profile national media reporting of online bullying, grooming and blackmailing cases, some of which are very close to home for us.

The E-Safety Partnership is currently comprised of the Community Planning Officer and Schools Liaison Officer from the Interventions Unit at Stirling Police (both are Police Officers & CEOP Ambassadors) and representatives from Stirling Council Child Protection, Youth Services, Libraries and Education/ICT, Stirling & Falkirk Foster Care coordinators and Central Scotland Rape Crisis Youth Project. The action plan was produced in recognition of the Scottish Action Plan on Child Internet Safety and Responsible Use. Recent additions are staff from the Adult Learning Team, Trading Standards and technical staff from two mobile phone outlets.

One of the priorities in the action plan included advice and guidance to parents at the point of sale relating to insecure wi-fi and security of personal information. This has led to continued partnership working with the private sector after initial campaigns. Computer retailers have designated specific areas within their stores for displays of information from the E-Safety Partnership.

This has proved to be highly successful having received positive feedback from both public and staff alike. The Partnership has also secured the cooperation of an independent computer retailer within the city centre of Stirling who is currently providing technical information and advice to customers along with E-Safety Partnership material. With other commercial partners this further extends outlets of E-Safety material. The partnership has engaged with all who have been supportive of this work and identified the need to include mobile device users in the delivery of the on-line safety message.

The information supplied to retailers and at events includes CEOP (Child Exploitation and On-line Protection Centre) videos for continuous display in addition to booklets, leaflets and advice packs prepared by the Partnership.

We have hosted events in Stirling and Falkirk with drop-in sessions at premises of large employers and Education Centres and we plan to continue this.

The Partnership has also recognised that youth groups such as the Scout and Guide Associations have training programmes that include awareness of technology, personal and community safety through their training and badge work. The partnership delivers talks to groups of Scouts, Cubs, Guides, Brownies and Boys Brigade who expressed interest in help with their badge-work and training programmes.

The 2013 Safer Internet Day saw the Partnership working with Beaconhurst School in Bridge of Allan, where some of their pupils presented a play on Internet Safety called “Caught In The Net” to other high school drama groups in the area. The play was written by a pupil and staff member from Beaconhurst School. “Caught in the Net” has its own page on Facebook that you can visit (and like!). This drama was taken to The Edinburgh Fringe this year, and formed part of the opening of the two Esafety Seminars at Alloa Town Hall on Wed 20th November 2013.

The Partnership will as usual be participating in the 2014 Safer Internet Day with an event to raise awareness in the community of online safety.

The Central E-Safety Partnership actively seeks other organisations, groups and employers across Forth Valley to engage and deliver the E-Safety message to all. The below named can also be contacted to arrange CEOP training courses locally for those who are involved professionally with young people.

Our work continues…

Follow us and ‘Like’ us on

http://www.facebook.com/centralesafety

Contact with Central E-Safety Partnership can be made via
Stewart Kerr or Fiona Murphy - call 101 (Police Scotland - Forth Valley Division)

Top Tips - Online Safety

Following the success of internet safety seminars in Stirling, we feel it is important to give a quick guide to some of the simple measures you can take to protect your family on-line.

Look at your computer system at home and take the following steps:

1. Make sure you connection to the internet is secure. If you use wi-fi make sure it is secured so that only people with your password or key number can access it (never give this out to people outwith your home). If you do not know how to do this contact you internet service provider and they will talk you through how to do that as every system is slightly different.
2. Most computers come with a built in firewall. Make sure this is switched on. To do this you normally have to click on the start button and then on the control panel. If the firewall icon does not appear there then it should be found within the security centre within the control panel.
3. Ensure you have installed an anti-virus system. There are many such as Norton and McAfee. Systems like these and others will help to prevent attacks on your PC and many include a system that alerts you as to whether or not a web site you are visiting has been previously checked to make sure it is safe.

The next step is to set up controls on your internet.

1. Ensure your pop-up blocker is turned on. This can be done via the TOOLS tab which is normally on the top right hand side of the screen on your internet page. This will stop unwanted and un-checked adverts popping up onto the screen. Once it is turned on go back into tools and click on pop-up blocker settings. If set to medium it should prevent most pop ups from appearing on your screen while still allowing new internet pages to pop up when you click on a link.
2. In the same way you did the pop up blocker, go back in and turn on your phishing filter. This filter helps to avoid scams that create fake web site. Such sites ask for personal information including bank details or offer corrupted downloads.
3. Again go back into the tools bar and click on the internet options, then on to cookies. Make sure the security settings are raised for this area also.

The next issue is how to protect yourself and children when surfing online.

There are various steps you can take. It is not about spying on your children, it is about protecting them and encouraging them to use the internet safely.

1. Keep the computer in an open area, e.g, the living room so that you check what sites they are on from time to time.

2. Check the browsing history. This is usually in the same tab as you favourites. If the history has been deleted then there may be an issue. You can often check deleted history by clicking on the search button in the history section, type the letter C in the search box and then hit return. This should bring up all the sites visited along with a date, time and number of times visited. If the search history has been deleted then you may wish to speak with your child to find out why.
3. If your children are using social networking then ask them to make you a friend on their page so that you can see what's going on. Again nothing intrusive is needed but it is a way on encouraging them to be responsible.
4. Make sure both you and your children know what the CEOP button looks like (link to CEOP website is at the end of this article) and know where to find it on social network sites and chat sites.
5. On chat sites like MSN etc, go into message setting and tick the `Automatically keep a history of my conversations` button in the message history section. This will mean you can go in later and check what has been said. To do this make sure your child gives you access (eg passwords)
6. Again on the same types of chat facilities go into the Privacy Options sections and click on Private. This means only friends can get access and reduces the risk of strangers getting in.
7. On sites such as facebook, bebo, myspace etc make sure your privacy settings are set. This is normally done by clicking on account, then privacy settings then custom. We recommend you always tick friends only, as the friends of friends option would give access to strangers.
8. Use your own personal e-mail for the social network site(s) so that you get alerts about online conversations
9. Talk to your children about the contacts/friends they have on their pages. If they do not actually know the person then encourage your children to delete them. This should reduce the risk to them talking to strangers.
10. Make sure that nobody other than yourself is paying for online gaming for your children on Xbox or P3S. If you have concerns about who they are talking to, then an option could be to remove the headsets so that they cannot have unrestricted chat.
11. Make sure you and your children always sign out of any networking site once you have finished going online
12. Talk to your children and make sure they know never to give our their personal details such as names, dates of birth, addresses, phone number etc.
13. If they have a mobile phone contact the provider and have restrictions put in place for both internet and the types of numbers they can call.
14. If you do see anything that gives you cause for concern then report by clicking the CEOP report now button or in an emergency by calling 999.

While this list is by no means exhaustive and not everyone will take every measure, by taking some simple steps we can reduce the risks to our young people. The internet can be a fantastic tool but like the real world the virtual world has dangers and parents can take measure to help protect their children.

For Parents: Help your teens stay safe (Info from Facebook Safety)

For years, teenagers spent much of their free time talking to friends on the phone. Today's teens aren't so different. They just have more ways to communicate.

What's my teen doing on Facebook?
Just like adults, teens use Facebook to connect with friends — through chat, personal messages and sharing photos, videos, links and other kinds of information. They use Facebook to announce achievements, wish each other a happy birthday and plan social events — like going to the cinema or to a friend's house.

Who Can See My Teen's Timeline?
We maintain added protections and security settings for teenagers (age 13-17) to ensure that their timelines and posts are not shown in public search results. Only Facebook friends, friends of friends, and networks (such as their school) can see what a teenager posts. Similarly, if a teenager shares their location using the Places tool, only their Facebook friends can see it. Encourage your children to use the View As tool (in the top right corner of their timeline page) to see what their timeline looks like to the public. They can also see how it appears to a specific person by typing a name into the field & pressing the enter key.

Start a conversation
Parents don't need to be social media experts in order to ask questions and begin an ongoing dialogue with teens. Have conversations about safety and technology early and often, in the same way that you talk to your kids about being safe at school, in the car, on public transportation or playing sport.
One of the best ways to begin a conversation is to ask your teens why services like Facebook are important to them. You might also ask them to show you how to set up your own Facebook timeline, so you can see what it's all about. Discuss what's appropriate information to share online—and what isn't. Ask them about privacy settings and suggest that you go over them together, regularly. Set ground rules and enforce them.

Learn from your teen
Today's teens have grown up with the internet, mobile phones and text messaging. Most don't distinguish between being online or off. New technology has always been a part of their lives, so when we write it off as trivial or a waste of time, we criticise a big part of their social interaction. You probably know this already, but unless you're really on top of social media, your teenager probably knows more about it than you do. That's OK. Don't be afraid to ask your child to show you the ropes!
It's about respect
It's also important to talk about the Golden Rule: treating others the way you want to be treated. This also applies to using new technologies. Make sure your teenagers know where to go for support if someone ever harasses them. Help them understand how to make

responsible and safe choices about what they post—because anything they put online can be misinterpreted or taken out of context.

Once You're on Facebook...

If you have a Facebook timeline, and have friended your child, try to respect the same boundaries you use offline. Let your relationship dictate how you interact. For example, whether you join a conversation among your child's friends or if you post on their wall. Think of social media as a get-together at one of your child's friends' houses. You can give permission for your teen to attend, and even though you won't be there to monitor their behaviour, you trust your teen to have good judgment around peers and other parents. It's all about balancing your teen's growing independence and need for privacy with your safety concerns.

See our Tools page for more information and resources for parenting on the web.

Learn the lingo

Friends? Friends of friends? Like? Poke? Wall? Learn what all these terms mean in the Facebook Help Centre.

Tips for parents

1. It can be tough to keep up with technology. Don't be afraid to ask your kids to explain it to you.
2. If you're not already on Facebook, consider joining. That way you'll understand what it's all about!
3. Create a Facebook group for your family so you will have a private space to share photos and keep in touch.
4. Teach your teens the online safety basics so they can keep their Facebook timeline (and other online accounts) private and safe.
5. Talk about technology safety just like you talk about safety while driving and playing sports.

Start a Conversation with Your Teen -

1. Do you feel like you can tell me if you ever have a problem at school or online?
2. Help me understand why Facebook is important to you.
3. Can you help me set up a Facebook timeline?
4. Who are your friends on Facebook?
5. I want to be your friend on Facebook. Would that be OK with you? What would make it OK?

Source: http://www.facebook.com/safety
http://www.facebook.com/safety/groups/parents/

WHAT IS MY ONLINE REPUTATION?

Your online reputation is the perception, estimation and opinion that is formed when you are encountered online. This could be when someone visits your social networking profile, but could also be when anyone reads a comment you posted on another profile. It could also be when someone sees your online photo albums or an image with you in it, indeed any instance or reference of you that either you posted or someone else did - what your digital footprint says about you.

Your online reputation will be formed through:

- Postings by you
- Postings by others but about you or linked to you
- Postings by others pretending to be you

Who does it affect?

Everyone! Obviously it applies to those who post online, however as other people could be posting information about you, you don't even have to have been on the internet before to have an online reputation! Rory Cellan-Jones commented on a survey conducted by AVG which concluded that 23% of unborn children already have a digital footprint - **www.bbc.co.uk/blogs/thereporters/rorycellanjones/2010/10/are_parents_the_biggest_threat_to.html**

Why is online reputation important?

Many businesses and celebrities value their online identity and reputation and go to extraordinary lengths to protect it, in many cases taking legal action.

The following clip, produced by the BBC in collaboration with Garlik, outlines the types of information available online and how it can be pieced together **http://www.bbc.co.uk/learningzone/clips/5594.flv**

Your reputation should be important to you as it is a tool that others could and will use to make decisions about you. Clearly this could have a dramatic effect on your personal and professional lives, especially if your digital footprint is poor. Would you like a potential partner or employer to decide whether to see you or not purely based on your digital footprint? Media headlines regularly appear, such as **http://tinyurl.com/3bdmmhe**

What does your profile picture or avatar say about you?

Remember that the Internet never forgets…..
When you post something online it will always be there.

WHAT CAN AFFECT MY ONLINE REPUTATION?

	Comments	Photos	Films	Groups/Affiliations
Postings by you	Inappropriate comments about other people or staff at work. Comments that you have made about other people's reputation. Defamatory comments you have posted about others photos or films Inappropriate language and poor grammar Publishing misleading or fraudulent information about you or others	Nights out on the town. Prank photographs of others that have been posted without their permission. Photos that compromise the security of others that could be interpreted as bullying.	My two weeks in Ibiza or Aya Nappa. Films put up of members of staff without their permission. Re distributing content on youtube Posting content without copyright or license to do so	Sports team and other robust groups where the pressure is on to be defamatory. Gaming clans or guilds where there is online taunting and posturing Inappropriate friends or group, eg radicalisation and racial hatred etc
Postings by others but linked to you	Comments posted by children or their parents, commenting on your work or professionalism. Re-tweets of things you said in confidence. “friends” posting comments with inappropriate language on your profile	Tagging you in a photo from a staff night out		Suggesting you are a member of an inappropriate group
Postings by others pretending to be you	Someone logging into your social networking account and changing or posting information apparently on your behalf (known as FRAPE) Comments posted apparently by you but expressing extreme of defamatory views	Mistaken identity - distributing pseudo pornographic images - images made to look like you	Third party posting inappropriate films on youtube but spoofing your identity as if they were posted by you.	Suggestions that you are a member of an extremist group for example.

WHAT CAN I DO?

STRATEGIES FOR MANAGING YOUR ONLINE REPUTATION

- **Think before you post anything**
- **Understanding your digital footprint**
- Search for yourself using Google or another search provider.
- **Appropriate language and behaviour**
  Consider how others may interpret your words, especially if using abbreviations
- **Protect your passwords**
  Don't disclose and the stronger the better! **www.pctools.com/guides/password/**
- **Managing your Privacy settings, using privacy effectively**
- **Testing your privacy**
  Find out from your friends what information they can see on your profile?
- Use **http://www.reclaimprivacy.org/** to scan your profile privacy settings
- **Discussing expectations with friends**
  Are you happy to be tagged in a photo?
- **Familiarise yourself with your organisations policies and procedures**
  Make sure you know how what the rules are!

More sophisticated ways to consider amending your Digital footprint - instructions on how to do these are included in links within the **further reading section**

- Limiting your online information in Google searches
- Removing yourself from Facebook searches
- Manage your friends lists and redefining access you allow to your content
- Manage your online photos and albums
- Explore what other applications access your online profiles
- Does your physical location appear online?
- Look for photos you are 'tagged' in
- Regularly review your privacy settings and amend accordingly

When posting online consider

- **Scale** - global platforms
- **Permanency** - once it is online it is there forever
- **Audience** - public or private? friends, friends of friends or everyone?

Use technology to its full potential but be aware of the pitfalls and **Think before you post.**

FURTHER READING

Facebook Safety pages - **http://www.facebook.com/safety**

Facebook Safety pages for educators - **http://www.facebook.com/safety/groups/teachers/**

Cyberbullying Advice produced by Childnet and commissioned by DCSF in 2007 that builds on the 'Safe to Learn' guidance - **http://www.digizen.org/resources/cyberbullying/overview/**

Resources

Social Times Inc, Facebook Privacy Guide - **http://www.allfacebook.com/downloads/facebook-privacy.pdf**

Facebook Privacy Scanner - **http://www.reclaimprivacy.org/**

Let's Fight it Together - **http://www.digizen.org/resources/cyberbullying/films/uk/lfit-film.aspx**

Support and Advice

Childline - 08001111 - **www.childline.org.uk**

POSH - Professionals Online Safety Helpline - **www.saferinternet.org.uk/helpline**

Provided by the UK Safer Internet Centre, a helpline dedicated to supporting professionals who work with children in the UK with Online Safety related issues

helpline@saferinternet.org.uk or 0844 3814772

NASUWT - **www.nasuwt.org.uk/cyberbullying**

ATL - **http://www.atl.org.uk/publications-and-resources/factsheets/cyberbullying.asp**

Establishing your own Digital Footprint

Online tools and services that can help you to understand the extent of your online digital footprint

www.123people.co.uk

www.zoominfo.com

www.reputation.com

With thanks to **UK SAFER INTERNET CENTRE**
http://www.saferinternet.org.uk/

(Go on….visit this site and see what else there is…)

10 tips for securing your Smartphone

by Lee Munson on October 8, 2013 - **Naked Security from Sophos**

1. Always secure your smartphone with a password

One of the most basic security tips, but one which is sometimes completely overlooked! Having no access protection at all is just foolish. Swipe patterns are ok, but greasy finger-trails could reveal too much.

A four-digit PIN is an improvement but using a strong passcode is the ideal phone protection.

2. Ensure that your device locks itself automatically

If you set up password-protection on your phone but then leave it unlocked on your desk for 15 minutes, you won't have achieved very much. Most smartphones allow you to set them up to automatically lock themselves after a period of inactivity.

Make sure you choose the shortest timeout you are comfortable with. Two to five minutes is better than ten to thirty, even if it does feel slightly inconvenient.

3. Install security software

Your smartphone is a computing device and should be protected accordingly. Look for an app like Sophos Mobile Security that includes malware prevention, remote data wipe, privacy review of apps and an automatic security advisor to alert you to potential risks when you change a device setting.

If you're in charge of securing your organisation's phones and tablets, then choose a mobile device management solution like Sophos Mobile Control.

4. Only download apps from approved sources

The Google Play Store and Apple's App Store take security pretty seriously. They are very careful about what apps they make available and will withdraw apps that raise concerns after release.

Read user reviews of apps before installing them. If there are any security concerns then someone else may well have mentioned them.

5. Check your apps' permissions

Many apps require more than the basic default permissions. For instance, you can reasonably expect an SMS app to send and receive text messages just as a mapping app will request your GPS location.

But something like a calculator that needs network access or an alarm clock that wants to read your contact database should be treated with extreme caution!

6. Don't miss operating system updates

Updates to your OS often include system vulnerability patches, so it's important to install them. You might want to be advised of updates rather than having them automatically installed, as early adopters sometimes experience teething problems - but the forgetful among you may prefer that to missing updates altogether.

7. Be wary of any links you receive via email or text message

Now you can pick up email on your phone, exercise caution when clicking on links. And phishing scams are not limited to email - a text message can incite you to click on a dodgy link or ask for personal information.

Even simply replying to unknown SMS or email senders can raise the crooks' interest in you, leading to more pressure to respond.

8. Encrypt your smartphone

Even if you've secured your smartphone with a password, a thief could still plug your device into a computer and gain access to all of your personal information. Using encryption on your smartphone can help to prevent such data theft.

9. Turn off automatic Wi-Fi connection

One of the great things about modern mobile phones is their ability to connect to the internet in many ways, but continually probing for wireless networks gives away information about your identity and location, and blindly connecting to unencrypted access points can let your phone leak all sorts of useful things for malicious actors to intercept and act upon.

So tell your phone to forget networks you no longer use, so as to minimise the amount of data leakage and configure your phone to automatically turn on/off wireless in certain places using a location-aware smartphone app.

10. Turn off Bluetooth and NFC when not in use

Bluetooth and NFC (near field communication) are great in terms of connectivity, allowing you to use accessories such as wireless keyboards and headsets or make payments with a wave of your smartphone.

But it does open a door for the bad guys to gain access to your device and access your data, so you should either switch these features off or put your device into "not discoverable" mode whenever possible. Also, be careful when pairing devices – never accept requests from unknown devices

MOBILE TRACKING (Find your lost / stolen device)

First thing to understand about Mobile Tracking is it only works when
1. Your location services are turned on *and*
2. When there is data connection (either cellular or WiFi)

Apple - Find My Phone FREE
For Apple devices, iPhones and iPads you have Apples Find My phone, this services must be installed on to the device and is not pre installed as most people believe and is an opt in service as you must give permission for apple to track your location. Find my phone allows you to track your phone location, lock the handset (although I'd always recommend that a passlock is on the phone in the 1st place as thieves aren't stupid and will just turn location services off), Wipe the handset, push a message through to the handset or make the handset ring often called a scream function (if you have lost it down the back of the sofa on silent).

Blackberry - Blackberry Protect FREE
Blackberry protect is a similar service to Apples find my phone which will allow you to track your phone and will also allow you to wipe the handset if worse case scenario. It is available to download from Blackberry app world although most newer devices come pre installed but you will still have to opt in and set up an account. Blackberry protect comes with the added benefit of allowing you to back up your information before you wipe the device. You can access your account through the Blackberry website, or by speaking to an 'O2 guru' who can remotely wipe your device. Blackberry protect also has a scream mode.

Samsung Android Devices FREE
Samsung provide their own service which can be set up by going to www.SamsungDive.com this service is linked to you handset via your Samsung account and allow tracking via GPS, Scream mode and a Push message and remote wipe function.

Android Devices
Lookout App FREE/£2.99 per month /£29.99 a year
Lookout is an app available on the Google PLAY store for all android devices the features as follow.
Italic text is premium service only charged at £2.99 per month or £29.99 a year. (at January 2013)

Anti-Virus, Anti-Malware, Anti-Spyware
Block phishing and malicious websites
Scan all click-to-call links
Protect your privacy with Privacy Advisor
Contacts Backup
Photo, Call History Backup
Restore Data to Existing Phone
Transfer Data to New Phone
Find Phone (Locate & Scream)
Find a phone with a dying battery
Remote Wipe
Remote Lock
Standard Support
Premium Support

Other Recommendations
It is also recommended that everyone registers their handset on www.immobilise.com where they can report their phone lost and make it available to the police nationally immediately. This also helps to simplify insurance claims.

Article prepared by: Martyn Kelly | Telefónica UK Ltd - **O2 Guru** & **Central E-Safety Partnership**

Worldwide Internet Activity in 60 seconds. (Thanks to Go-Globe.com)

Perfect Password Checklist

My Passwords:

- ☐ use letters and numbers
- ☐ use a minimum of 8 characters
- ☐ don't contain any personal information
- ☐ use characters like brackets, &, or %
- ☐ use a mixture of capitals and lower case letters
- ☐ use a sentence or a line from a song instead of just one word
- ☐ only use the first letters of that sentence
- ☐ use different languages
- ☐ will be easy for me to remember

- ☐ I have different passwords for my online accounts
- ☐ I will change my passwords again within the next 6 months

Texting, chatting and video messaging can be fun, however you need to be aware that once you send pictures or other personal details, you never know where they might end up. Always think before you send!

Do not give out personal details to people you do not know

Personal details include things like:

- your home address
- your mobile number
- pictures of you or your family and friends
- it is a good idea to use a nickname when you are on-line. Keep your real name, address, telephone number and school name a secret.

Never reply to texts from people you don't know.
If you do not know the sender it's best to delete them straight away.

Tell your parents or teacher if someone or something makes you feel uncomfortable or worried.
Never be afraid to let someone know if you feel bullied or uncomfortable about anything you've been sent or see online.

Top Tips to keep you safe:

- Do not give out your name, address or telephone number to anyone you don't know
- Do not arrange to meet anyone you don't know
- If you are not sure about something, ask an adult you trust
- Do not get involved in a 'happy slappy' activity. It is an assault on the victim & you may get into trouble.

Top Tips to keep your phone safe:
Your mobile phone may be small, but it's an expensive bit of kit, so it makes sense to take a few smart steps to avoid it getting stolen.

1. Don’t be flash with your phone. Keep it out of sight when you're not using it.
2. When you're on the phone, keep an eye on what's going on around you. If you start to feel unsafe, hang up, put your phone away and keep walking.
3. Don’t leave your mobile lying around. That's just asking for trouble.
4. If the worst happens and someone threatens you for your mobile phone its best to hand it over and tell the police. Phones can be replaced...YOU can't.

It's bad news if your phone is stolen. The good news is there are things you can do to help get it back.
1. Log on to http://www.immobilise.com/ and register your mobile with the National Mobile Phone Register, a free service, backed by the police. If your phone turns up it'll help police return it to you.
2. If you think your phone's been stolen, let the police and your mobile phone company know as soon as you can.
3. Keep a note of the make and model of your phone, plus its unique IMEI number. You'll find this 15-digit number inside the battery case, or key in *#06# and the IMEI number will appear on the screen. If your mobile turns up, this information will help the police return it to you.
4. Get a **UV pen** and write your postcode and house number inside the battery case.
5. If your phone is stolen, get it blocked by phoning 08701 123 123. This will make the handset useless, even with a new SIM card.

Helpful information can be obtained from these web-sites:

www.saferinternet.org.uk

www.iwf.org.uk
(Internet Watch Foundation - Report illegal sites)

http://www.internetmatters.org/
useful guidance for parents from BT, Talk Talk, Sky and Virgin Media

http://parents.vodafone.com/
Contains useful information and access to the on-line version of the Vodaphone Digital Parenting magazine.

http://www.ceop.police.uk/
Info from Child Exploitation Online Protection Centre.

https://www.thinkuknow.co.uk/
Part of the CEOP network with info and material available and info on courses for teachers, police, carers etc.

http://www.ecrimescotland.org.uk/
Info on Ecrime for businesses etc.

http://nakedsecurity.sophos.com/
General Information on Ecrime and Internet Safety

http://www.getsafeonline.org/
Free advice on wide range of Internet Safety matters.

http://kids.getnetwise.org/ and http://www.getnetwise.org/
Useful link to wide range of information for kids, families etc. with links to other useful web pages.

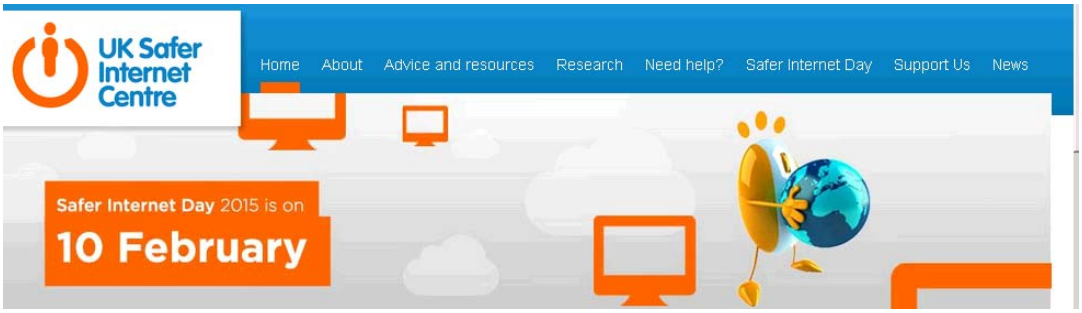
www.beatbullying.org and www.respectme.org.uk
Anti Bullying sites

www.childnet.com
Advice, Info and resources for adults and young people.

….and don't forget to visit

http://www.facebook.com/centralesafety

NOTES


UK Safer Internet Centre
Home
About
Advice and resources
Research
Need help?
Safer Internet Day
Support Us
News
Safer Internet Day 2015 is on
10 February