Cyp networking internet use buying

Cyp 3. 3 – 7. 2 Describe ways of reducing risk to children and young people from: Social networking, internet use, buying online and using a mobile phone. There are many ways to reduce the risks to children and young people using these technologies: Educate your children – Be clear about the kind of personal information your children should not divulge over the Internet, including their names, addresses, and phone numbers. Teach your children what to do if a stranger approaches them online. Monitoring software will allow you to monitor, chats, emails, website visits, and internet searches so you can keep informed silently.

Specifically, tell children to cut off communication with any person they don’t know and to notify you immediately. Educate your child how to be focuse on the smat rules: S: Safe Keep safe by being careful not to give out personal information when you’re chatting or posting online. Personal information includes your email address, phone number and password. M: Meeting Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents’ or carers’ permission and even then only when they can be present.

Remember online friends are still strangers even if you have been talking to them for a long time. A: Accepting Accepting emails, IM messages, or opening files, pictures or texts from people you don’t know or trust can lead to problems – they may contain viruses or nasty messages. R: Reliable Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it’s best to only chat to your real world friends and family.

T: Tell Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online. Make the Internet a family activity – Maybe more important than anything else, keep your computers in a central part of the house; that way you can stay involved and keep an eye on what your children are doing. Talk often – The most important online safety strategy, regardless of the technology involved, is to maintain an open dialogue with your child about their digital lives.

Set ground rules for using mobile phones (as with any technology) – and have penalties for if they are abused – but try not to impose fear in your child that their phones will be taken away from them if they do encounter problems. If problems do occur, talk through the issues in a calm and rational way, and try to help your child devise sensible self-protection strategies should they encounter problems again in the future. Use inbuilt tools and services – Mobile operators take safety issues very seriously, and there are a number of pan-European and international initiatives to make mobile use safer for children and young people.

These predominantly focus on awareness raising and self-regulation within the industry. Mobile operators are providing an increasing range of tools to help parents manage their children’s mobile phone use. These may be features of the handsets themselves (there are many handsets appearing on the market that are specifically designed for younger users), or may be applied to the account, such as parental control filters. Such content restrictions are typically set to the highest level of protection by default.

Be a good role model – Try to be a good role model in your own mobile phone use. If your child sees that you adopt safe and responsible behaviour when using mobile technology, they may be more inclined to follow your lead! Have some daily downtime – Consider having a central point in the home where all mobile phones are kept for charging overnight. Aside from making sure that phones are always charged – essential in case of emergencies – it will also ensure that the phone owner gets some ‘ downtime’, without disturbance from the constant ‘ ping’ of text messages or emails.

Talk with other parents: it’s likely that they are dealing with similar issues too. Sharing views and experiences might help you to formulate ideas about what’s right for your family. Filters – The most important task of filters for the protection of minors is to provide a reliable barrier preventing access to content that the parents see as inappropriate or harmful, dangerous or morally damaging to the development of minors. Ideally, at the same time, content suitable for children and young people should not be affected.

Filtering in the context of parental control also concerns outgoing streams, for instance to avoid that young children disclose their names, address, school name or parents’ credit card number. This type of filtering is particularly important for young users and there is free software (freeware) available to deal exclusively with that issue. What kind of filters are available? Recommended lists with content suitable for childrenSo-called “ walled gardens” or “ white lists” are lists of selected content, which only permit the user to surf to these selected websites.

Blacklists of Internet addresses with content relevant to the protection of minorsFilter systems based on blacklists take the opposite approach. They permit access to all Internet content and attempt to filter out morally damaging or dangerous content. However, editing the entire Internet is impossible, so the blacklisting of Internet content will probably never catch up with developments in Internet content Blocking websites according to a list of forbidden wordsThe simplest filter systems block Internet content using a list of forbidden words.

These keyword lists are easy to produce and simple to maintain, but some websites providing unwanted content make sure that they do not make reference to words common in the black lists. Filtering based on automatically classified contentsThe second generation of automatic classification systems evaluate the complete text contained in a website. They use statistical methods familiar, for instance from spam filters. Self-classification by the providersProviders use a list of questions to describe what can be seen on their websites (e. g. naked breasts, killing of people).

This description is inserted into the source code for the website or saved on the web server in a standardised form so that filter systems can evaluate the classification and block all content, which does not conform to the user’s settings. Currently the effectiveness of the filters using labelling is still very low because only a few providers have taken the trouble to classify their pages themselves. Combinations of filtering methodsThe basic approaches to filtering are now combined in many ways in order to increase their effectiveness but also to permit age-differentiated access.

Labelling – Labelling is also one precondition for effective filtering. It can be done by users or by providers or automatic. Sites are labelled in order to protect minors, increase public trust and use of online transactions, and also to comply with legal standards. When labelling website content (by editorial or provider), a code is written into the webpage html code, thereby detailing its contents so that the page can be rated. This rating – which in most cases is invisible on the page itself, details the nature of the content and is detected by filtering mechanisms, which will subsequently either block or load the page.