we're in IT together…

ONLINE SAFETY

Messaging, eMail, Vlogging and Sexting

www.eitts.co.uk

Contents

THE RISKS

People online are not necessarily who they say they are or seem to be.

Somebody persuading you to download and run a virus-infected piece of software.

Eavesdropping on your conversations. There is no guarantee of privacy as conversations are not encrypted and can be saved for use offline.

IM software may be vulnerable to virus or other attack.

Online chat rooms – accessible through instant messaging – can be undesirable places.

HOW TO USE IM SAFELY

- Never give out passwords, credit card information or other private data.
- Block strangers. If your software allows it, set up the system so that only people on your 'allow' list can contact you.
- Be very wary of disclosing any private information to a stranger you meet via instant messaging. Even apparently innocent information like the name of your employer can be used against you by fraudsters.
- Never click on links that you receive through instant messaging from people that you do not know and trust, and that you have never met in real life.
- Leave your online profile blank, or where you have to enter data to use the system, enter fictitious data.
- Do not use your system or email password to log on to an IM system.
- IM is not encrypted, so do not use it to transmit information such as credit card numbers or other sensitive information.
- Disable automatic downloads.
- Verify information you receive on IM elsewhere. In particular, check any security 'advice' you get.
- Keep your IM software up to date.
- Do not let children use instant messaging chat rooms unsupervised.

Contents

WHAT SORT OF EMAIL?

- Spam (Scam)
- Phishing

Don't get hooked by an email scam!

USING EMAIL SAFELY

- Do not open emails which you suspect as being scams.
- Do not forward emails which you suspect as being scams.
- Do not open attachments from unknown sources.
- **If in doubt, contact the person or organisation the email claims to have been sent by ... better safe than sorry.**
- Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email.
- Do not respond to emails from unknown sources.
- Do not make purchases or charity donations in response to spam email.
- Don’t click on ‘remove’ or reply to unwanted email.
- Check junk mail folders regularly in case a legitimate email gets through by mistake.

- When sending emails to multiple recipients, list their addresses in the 'BCC' (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving phishing or spam emails.
- Similarly, delete all addresses of previous parties in the email string, before forwarding or replying.
- If you are suspicious of an email, you can check if it is on a list of known spam and scam emails that some internet security vendors such as McAfee and Symantec feature on their websites.
- Most Microsoft and other email clients come with spam filtering as standard. Ensure yours is switched on.
- Most spam and junk filters can be set to allow email to be received from trusted sources, and blocked from untrusted sources.
- When choosing a webmail account such as gmail, Hotmail and Yahoo! Mail, make sure you select one that includes spam filtering and that it remains switched on.
- Most internet security packages include spam blocking. Ensure that yours is up to date and has this feature switched on.

Contents

WHAT THE HECK IS V-LOGGING?

https://www.youtube.com/user/SHAYTARDS

Concerns for Parents

- If your child is creating a Vlog, anyone with Internet access can see what they have posted. If your child is oversharing overly-personal or otherwise inappropriate content, your child could become a target for online predators, spam, cyberstalking, and identity theft.
- For older children and teens, Vlogs can become the perfect forum for cyberbullying.

How Can I Keep My Child Safe?

- Talk with your child about the wide audience a blog might have. Discuss safety guidelines your child will follow, such as never posting full names, email addresses, ages, or phone numbers on a blog. Decide if your child will be allowed to post pictures or videos. Once you have agreed upon a set of reasonable rules, be sure to keep tabs on your child by visiting his or her blog often.
- You may want to consider limiting your child to a "closed" or "whitelisted" blog. This means that you can grant a select group of Internet users access to your blog while keeping the blog's contents hidden from anyone else on the web.
- Be sure that your child is not saying unkind or derogatory things about others on a blog--even if it is only in joking. Doing so constitutes cyberbullying and can escalate into a serious issue.

Contents

WHAT ARE THE DANGERS OF SEXTING?

- It's not Harmless
- It's illegal
- No control of images and how they are shared
- Vulnerable to blackmail, bullying and harm

HOW TO TALK TO YOUR CHILD ABOUT SEXTING

Think about the best way of starting the conversation

You know your child best and your approach should be based on your child and your parenting style.

When you give your child their first mobile phone, outline your expectations and explain the rules of having the phone. Monitor how younger children can use their phone – for example, set up controls so that only you can authorise the apps that your child downloads.

Ask your child what they feel is acceptable to send to people and then ask if they would be happy for you, a stranger or other children to see that photo. If the answer is 'no', explain that the image or message is probably not appropriate to send.

Make sure your child is comfortable saying no, that they know their body is private and that being asked to 'sext' is inappropriate.

HOW TO TALK TO YOUR CHILD ABOUT SEXTING

Explain the risks of sexting

Tell your child what can happen when things go wrong. Don't accuse your child of 'sexting', but do explain the dangers.

You may find it easiest to use real-life examples, such as television programmes or news stories, to help you explain the risks. You can also look at ChildLine's advice about 'sexting' together.

Ask them if they would want something private shown to the world. Explain that photos are easy to forward and can be copied.

Talk about whether your child thinks that the person who sends a request is likely to be asking other people to do the same.

If children are sending images to their friends, they may see it as less of a risk than sending them to strangers. Use examples of when friends or partners have had a falling-out and what might happen to the images if this happens.

HOW TO TALK TO YOUR CHILD ABOUT SEXTING

Reassure your child you will be supportive and understanding
Let your child know that you are always there for support if they feel pressured by anyone.

Tell your child to come to you if someone asks them to 'sext' or if they receive an explicit message.

Let them know that you won't be angry with them but just want to make sure they are safe and happy.

we're in IT together…

THANK YOU FOR WATCHING

www.eitts.co.uk