

YOUTH CHARTER



You have the right to explore the internet but remember that you cannot trust everything that you see or read on the internet.

Could this be YOU?

Ahmed has received a surprise email saying : “Your details have been safely received. Please confirm by clicking on the link below. You could win a digital camera.”

Ahmed realises that this is a scam. He knows that the email is automatically sent to thousands of email addresses and that replying will send information about an active email address which could result in loads more spam email. He ignores the email, deletes it and tells his friends and his teacher about it in case they receive it too and don't know what to do.

Top Tips

Another example is a pop up web page that says you have “won a prize” or “your computer is infected with viruses”. Pop-ups appear when certain links are triggered (either by clicking, pressing a key or mouse over functions), they can also be set to appear when a page loads in your browser, when you exit a page and multiple pop-ups can bet triggered - common on pornography Web sites.

Their practical purpose is intended to carry useful information about the Web site you are visiting, however, the concept (like so many things) has been entirely abused and pop-ups generally carry advertising or pornography. Most Internet users find them annoying and many Webmasters are phasing them out. As more people are using pop-up blockers, the information the pop-up windows carry is not being viewed. There are also accessibility issues - opening a link in a new browser window, for instance, not only registers as a pop-up in most pop-up blockers but also breaks the browsers back link and creates many issues for Internet users with disabilities.



Then there are the security aspects. Pop ups are very often triggered by cookies or spyware already resident on machines.

Don't click or download anything that you're not sure of, Another recent example is a virus in Facebook, which was sent my one of your friends, when you follow the link it asks you to download the latest Flash player, this is a virus it then infects your computer and spreads it to your Facebook friends!

With so many techniques for gathering email addresses, it's unlikely you'll ever be able to cut spam out altogether. But there are measures you can take, to minimise the chances of spammers getting hold of your email address. Here are just a few.

- Only give your email address to people you know and trust.
- Try setting up a separate email account to use when shopping online or registering with websites or forums.
- If a web site asks for your email address, read their terms of use and privacy policy so you know how they'll use it.
- Keep an eye out for a check box which lets you opt-out of future marketing messages.
- Never respond to a spam email, as this will let spammers know you're there – delete it immediately instead.
- Don't advertise your email address by posting it on your personal site, forums or chat rooms – spammers are constantly trawling the internet on the look out for exactly that.

Make sure you have a updated AntiVirus Software on your machine to keep it protected.

http://www.wiredsafety.org/safety/email_safety/index.html

<http://www.safe2read.com/>

http://kidshealth.org/parent/positive/family/net_safety.html