

# SCAMS

Internet fraud often consists of scams that con-artists have been using for years — only now they have a new medium and new victims to exploit.

Here are some tips to help you:

- Shop on-line only with companies you know or have friends who have used them regularly before.
- Never give anyone your bank account number, passwords or other personal information that isn't absolutely needed to complete a transaction.
- Never click on any links that are contained in emails from people you don't know.
- Never give out your Internet password or account passwords. Never. Change your passwords often and be creative!
- Never to enter an area that charges for services without asking your parents first.

*Home computers are being called upon to perform many new functions, including the consumption of homework formerly eaten by the dog.*

Doug Larson

# CYBERJARGONS

- Drive-by Download/ Trojan: Software that installs on your computer without your knowledge when you visit certain websites. Some can collect personal information from your computer such as passwords.
- Parental Controls: Tools that allow parents to prevent their children from accessing certain Internet content that they might find inappropriate.
- Phishing: An email or Internet site trying to get personal information or a response to hook you into a scam.
- Digital Footprints: The information we leave behind on sites we use.
- POS (Parent Over Shoulder).

# MOBILE DEVICE TIPS

- Texting: Work out the balance between trust and a semi-regular chat about text use, bullying issues etc.
- Party: With texting a mass of people can suddenly arrive. Unsupervised teen parties are not safe.
- With many of these devices, what can be done on a computer can be done on a mobile.
- Put an ICE (International Contact in Emergency) number in your address book.



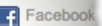
One of the biggest challenges that parents face!

# CYBERSAFE TIPS FOR PARENTS & CHILDREN

## One in four teens cyber-bullied

Alice Neville

10:00 AM Sunday Oct 4, 2009



As a British teen cyber-bully is jailed, experts here say the phenomenon is widespread in New Zealand.

... is serving a three-month sentence in a young offenders' institute after being found guilty of harassment on Facebook.

## FILTERING AND SAFETY SOFTWARE

Remember, all software is never perfect!

- Internet based filtering: i.e. Watchdog (screens sites in various categories, they update... you use, speed not affected)
- Filtering software you install: purchase and download, they update via the web like a virus filter. Consumer NZ 2008 Recommended: Integard and Netnanny 5 (commercial) and Parent Control Bar (Freeware)
- Buttons: Buttons like those found at [hectorsworld.com](http://hectorsworld.com) can be pressed to blank the screen when inappropriate material is seen.

Teach children about exploitation, pornography, downloading, hate literature, excessive violence, and other issues that concern you, so they know how to respond when they see this material. The best tool a child has for screening material found on the Internet is his or her brain.

Creative original work is vastly more valuable than copy and paste. Many schools now screen essays and projects for plagiarised content.. encourage the creative attitude and correct quoting techniques.

“The kids seem to know so much more than me.. where can I start?”

### 10 + 1 FREE HOT TIPS

1. Know that many children-teens will attempt to explore. This does not reflect on you, it is how you handle prevention and problems that are important.
2. Realise that prevention is better than cure. Time spent NOW will save larger problems developing later. Respect and trust are to be built. It is about instilling a sense of values and citizenship.
3. Discuss monitoring and safe-use expectations with your child. Make it O.K. to tell and communicate.
4. Place computers or use devices in open areas or leave the bedroom door open. Remember that cellphones, ipod and other devices can go on the web. Be consistent in your boundaries.
5. Install a safety button, use Internet filtering or accountability software (See Hectors World).
6. Screening/filtering software is never perfect.
7. Regularly check your child's Internet history by saying, “Tell me about some of the great sites you have visited recently.” Look through their history with them. If it's not there, be suspicious. Check that search preferences set to strict or moderate filter.
8. Keep your Firewall, Internet Virus and Spyware checkers up-to-date (less crucial for Mac users). See reviews for these at: <http://www.cnet.com/topic-reviews/antivirus.html>
9. Keep your browser (Internet Explorer, Firefox, Safari) and Operating System (Windows, MacOSX) up to date with the latest patches.
10. Discuss the school's Cyber-Safety policy with your child.
11. Know your children's friends and their parents.

## GREAT LINKS

Use these sites to help you find out further information, free security software or to discuss issues with your child.

[WWW.HECTORSWORLD.COM](http://WWW.HECTORSWORLD.COM)

A N.Z. site with animation, activities and information on a wide range of issues. Year 3 and above.

[NETSAFE.ORG.NZ](http://NETSAFE.ORG.NZ)

A New Zealand based site with information focusing on issues within N.Z. They produce [Hector's World](http://hectorsworld.com).

[HTTPS://WWW.COMMONSENSEMEDIA.ORG/PARENT-CONCERNS](https://www.common sense media.org/parent-concerns)

A great resource with a range of information.

[HTTP://WWW.NETLINGO.COM/](http://www.netlingo.com/)

Catch up on the online lingo

**Credit Card Watch:** Make sure you understand about apps that have incremental purchasing options. Do you really want to spend \$1000's on software?

Explore with your children about safety and privacy settings on social networking sites like Facebook (older kids), Club Penguin, Habbo or MoshiMonsters etc.

This work by Medbury School is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-nc-sa/3.0/).