

Children, parents and the Internet

In today's world, the Internet is becoming an increasingly dangerous place for children and young adults. Many parents are calling for protection of their children while they surf online, and there are differing opinions as to how best to achieve this.



There is a significant amount of unwanted and dangerous content on the Internet. As parents you need to understand the dangers this content can pose to your young children, tweens and teens surfing the web. People with criminal and fraudulent intent are using the Internet in increasingly sophisticated ways, often exploiting the naivety of children. As a leading provider of security solutions, with more than 80 million active users worldwide, AVG knows how important it is for parents to better understand the dangers online — so let's explore them in a very straightforward way.

Below are some important ways to protect children online.

- 1) Malware.** Malware is defined as harmful content like viruses, worms, rootkits and Trojans, that lie dormant on your computer after you have visited an infected website or downloaded an infected file. They live on your computer without you being aware of them and when activated, send spam, gather information, or are used for targeted attacks on others computers. Malware infected computers can be used to store and distribute pornography. You can protect your family by using up to date anti-virus, anti-spyware and anti-rootkit software with a firewall.
- 2) Illegal content.** This type of content includes copyrighted work and work that is published without the author's permission. While copyright laws differ from country to country, the awareness and enforcement in this area is very weak. While there is no perfect solution, using a two-way firewall that blocks peer-to-peer sharing, the common way for illegal content to be distributed, is an excellent first step.
- 3) Misrepresentation online.** On many community sites, such as FaceBook and MySpace, there are opportunities for people to misrepresent who they really are. A sexual predator could easily establish a false identity and masquerade as a young girl online to gain the trust of your children. The only solution here is to trust, but verify. Using common sense and examining the profile photo is a good start to identifying online predators.
- 4) Pornography.** Pornographic content is mostly unwelcome, although not illegal. The only exception to this is child pornography. Protecting your children from child pornography requires a filter for advertising programs such as Adblock (plug-in for Firefox) or AdMuncher. These programs filter web pages with words and phrases that are offensive and block them.

What are the issues with protecting children online?

Kids generally don't want to have their online behaviour monitored. While they are okay with protection from malware, their technical savvy is generally much higher than that of their parents. Even if the parents use parental controls, children today will likely know how to disable them.

The Internet pornography industry is a huge business and the managers of this industry are doing what they need to protect it. To date, nobody has been able to filter unwanted content based on the actual pictures themselves.

While some children are naive about who they are talking to online, parents can also be naive about the perils of the Internet. The only way to safeguard children is to be circumspect. You need to educate yourself and your children about trickery on the Internet, just as you educate them about how to safely cross a road.

How to avoid trickery online

Only trust websites you can verify to be legitimate. It is easy to make an authentic looking website, so don't be fooled by clever fakes.

Nobody should request your personal details via e-mail or online chat. Anyone who does is either a crook, or an incompetent marketer. Either way, you should ignore them.

If it seems too good to be true, then it probably is. It's highly unlikely that you've won a lottery that you never bought a ticket for, or are about to inherit millions of dollars from family you've never heard of. And while you may think these scams are obvious, they continue to be used by criminals because enough people fall into their trap and hand over significant amounts of money every day. You need to exercise caution at all times.

The bad guys will go to a lot of trouble and take their time, to be genuine and build trust because it helps them to get what they want. They will carefully, over time, obtain more and more sensitive information about you. Then they will either use this information to steal your money, or use your good reputation to help them defraud other people.



What does AVG recommend?

Essential protection: Parents should ensure the home computers have anti-virus, anti-spyware and firewall protection, at a bare minimum. A product such as **AVG Anti-Virus plus Firewall 8.0** is a good, affordable solution. This will enable you to block malware and peer-to-peer nets with illegal content.

Safe search and surf protection: The LinkScanner safe search and safe surf protection built in to all AVG commercial products provides the best protection available from online threats. Web pages known to be bad are highlighted when you search so that you know not to visit them. Plus the web pages of all links you click as you browse the web outside of search engines are quickly scanned for threats in real-time, before you actually visit them.

Spam protection: "Spam" is the term used to describe junk e-mail (which often includes unpleasant content and malicious malware in attached files). Because spam e-mail and attached malware has increased to such intrusive levels, you need to protect your family from spam. The **AVG Internet Security 8.0** full suite solution provides comprehensive protection against all online threats, including spam e-mail.

Backup protection: Data loss is an important topic that nobody worries about until it happens to them. A backup of the documents, photos and other files that you can't easily reproduce is important. Ideally the second copy is kept physically separate to also protect against fire, flood or theft. **Carbonite Online PC Backup** is a very cost effective, set and forget solution.

Update, update, update: It is especially important to keep the operating system software that runs the computer, security software that protects your computer and software you use to access the Internet, up-to-date. Indeed, the more regularly all of your software is updated, the safer you are. It is ideal to have your software set to update automatically. Any software that is not up-to-date is potentially vulnerable.

There are no radical technology solutions, so using parental controls and being aware of what your children are doing online is the first line of defence for children. Awareness of the problem is the first step to a solution.

Lloyd Borrett, AVG (AU/NZ) and

Zdeněk Breitenbacher, AVG Technologies, 2008

Tough on threats. Easy on you.
avg.com.au