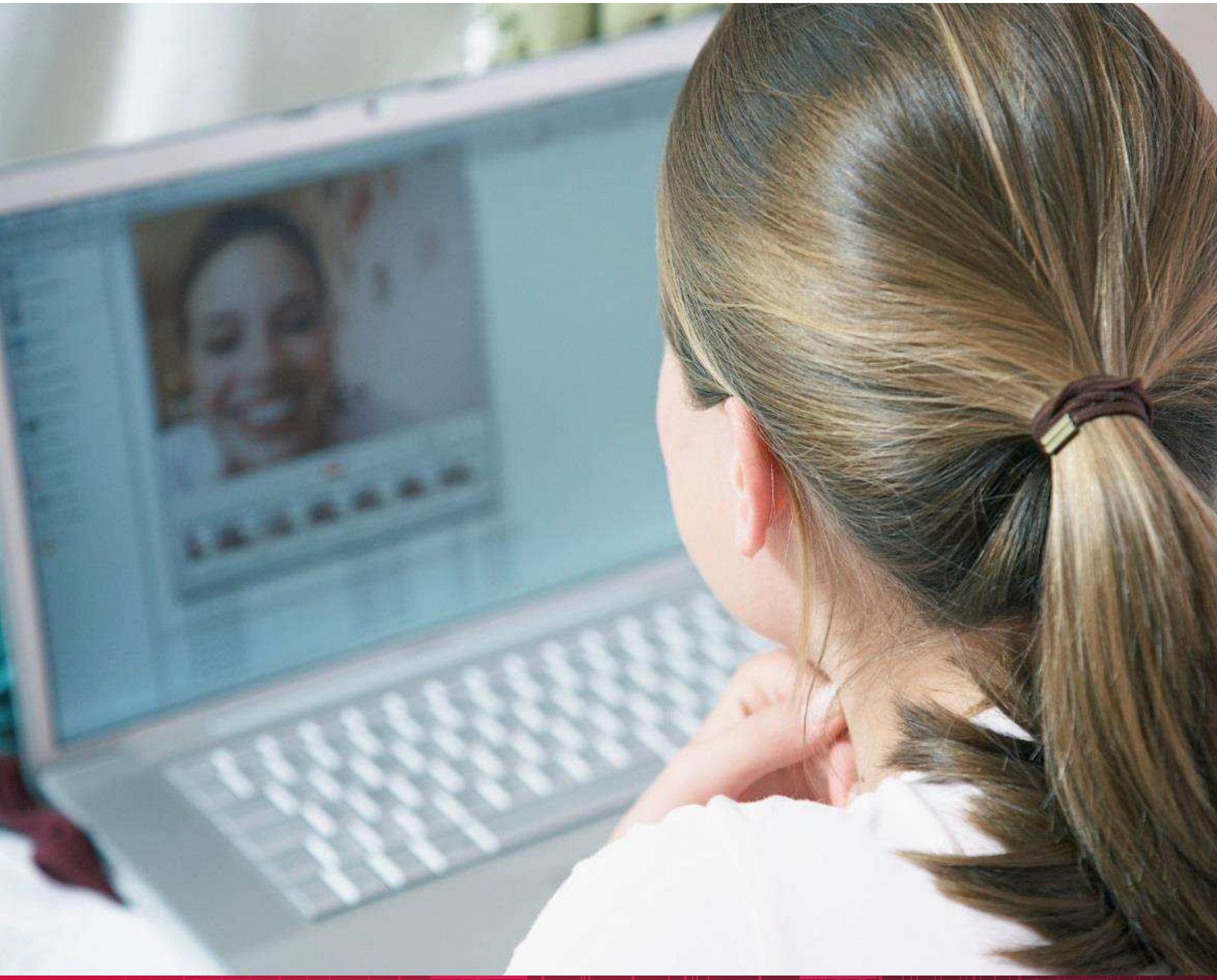
McAfee
An Intel Company

DIGITAL DECEPTION:
THE ONLINE BEHAVIOUR OF TEENS



Foreword

We love technology, and with good reason. It offers so much to the home in terms of entertainment, education, as well improving the functionality within the home. Although technology has transformed all of our lives for the better, it has also introduced the school bully into the home. Unlike before children can find no respite from their tormentor, and perhaps more worryingly has no geographical limitations of participants in the bullying of its victim. Indeed such is the ease with which children can be bullied online, this recent study found that nearly half of all parents surveyed are worried that their child may be bullied online.

Equally children need to be aware of the implications of what they share online, unlike previous generations their mistakes are not forgotten, much like a digital tattoo. This Digital Tattoo acts as a permanent reminder of late night indiscretions, and overzealous tweets that are almost impossible to remove. With a quarter of children spending up to six hours a day on the internet, and over half away from their parents' watchful eye there appears to be no control over what children do online, or who they interact with.

Providing an effective response demands the use of both education and technology. Although we clearly understand the need for such controls, many parents not only turn a blind eye to what their children does online, but unwittingly encourage their participation in social networks despite being underage. Moreover, only 19% of parents are implementing parental controls on all internet related devices, and 1 in 3 parents admits to not having any discussion with their child about the risks online.

Understanding the best way to address these threats is a collaborative effort. Over 50% of parents surveyed in 'Digital Deception: The Online Behaviour of Teens' believe online safety should be taught in all schools, and whilst this would certainly help (note: the McAfee Online Safety for Kids programme has taught 150,000 children worldwide to date) the internet is fast becoming a life skill and should be part of the continuous education, and parental support to protect children when online. This collaborative effort also extends to the voluntary sector, and private industry and is why McAfee has partnered with the Anti-Bullying Alliance to help parents, children, and school teachers alike to understand the digital divide and the dangers of cyber-bullying. We believe that this report will be the start of a national debate to prevent cyber-bullying by bringing together all those with a responsibility, we believe that the issues in raised in this report are not only solvable, but achievable.

Luke Roberts, National Co-ordinator of the Anti-Bullying Alliance
Raj Samani, EMEA CTO, McAfee

Introduction

When it comes to their personal lives, it's well established that pre-teens and teens are very cautious about how much they reveal to their parents and usually keep their cards close to their chest. This can lead to surprise, disbelief and upset when parents discover children have been victim to internet dangers such as cyber-bullying. With the proliferation of smartphones and tablets used on the move, it has become much easier for children to chat to friends and browse websites away from the prying eyes of mum and dad,

Today's younger generations are considered to be 'digital natives' having been brought up with the internet from birth. As a result, they often know more about the digital world than their predecessors. This is often painfully evident when it comes to parental understanding on best practice for internet safety. Yet, despite their digital proficiency most young people have not developed the maturity, awareness and foresight to safeguard their personal information and avoid online issues. Parents, teachers and the industry therefore have a duty to work together to ensure young children don't befall the dangers of the online world.

This report reflects on the research undertaken by McAfee and the Anti-Bullying Alliance, part of leading children's charity the National Children's Bureau, to better understand pre-teen and teen behaviour online, the risks they're exposing themselves to, and to help parents work more effectively with schools and the industry to create a more open path to online safety awareness.

Research methodology

The survey was conducted by Atomik Research across October and November 2013. The survey polled 1012 UK children (between the ages of 10 and 17) and 1013 UK parents (with at least one child aged between 10 and 17.)

Online Behaviour

Anyone whose children use the internet often feels caught in a technology paradox. On the one hand, they know how important it is for children to experience new technologies and the wonderful benefits they offer. On the other hand, parents are afraid of the dangers in cyberspace. In many cases, kids are more technologically advanced than adults, so some parents may feel intimidated and refrain from enforcing rules that are imperative to protect their children as they surf and socialise online.

However when we looked at the online behaviour of pre-teens and teens, it became apparent that the digital divide is only increasing between parents and their children and that this continues to be cause for concern.

A quarter of children spend between four to six hours online every day and much of this internet usage take place away from the watchful eye of a parent. Currently more than half (53%) go online in their own room, nearly the same amount (43%) on a games console and two-thirds (66%) also use their smartphone for internet access.

When it comes to the top concerns from parents, it's clear that internet safety is front of mind for the majority of parents. Only 11% of parents believe their child is safe online, with parents most worried that their child might be approached by a stranger online (54%), followed by their child being cyber-bullied (45%) and their child sharing their contact information (45%). Yet despite these grave concerns and their best intentions to protect their children, a third (32%) admitted to not having had a conversation with their child about staying safe online, suggesting many parents don't know where to start.

Risky Behaviour

- One in ten (10%) teens has been approached online by an adult they did not know
- More than a third (32%) were asked to do inappropriate things (like sending pictures of themselves) so they deleted them from their contacts list, yet nearly a quarter (21%) did send pictures which they now regret
- 18% have looked up answers to a test or exam online
- 14% have looked up porn and 12% have looked up violent video clips on YouTube or Facebook with 9% saying they did so because they felt pressured by friends
- 35% have posted their email address online, 32% a photo of themselves, 31% a description of what they look like and 27% the name of their school

It's important for parents to remember that even though their child may be more technologically advanced than they are, young people often lack the maturity and understanding needed to address internet-related issues. Without parental supervision and moral guidance on what constitutes right and wrong behaviour online, children are far more susceptible to entertaining requests from strangers, over-sharing online, and experiencing cyber-bullying as either the victim or the perpetrator.

The truth about cyber-bullying

Our research revealed that children need help and guidance when it comes to navigating what is and isn't appropriate behaviour online. Many of the children surveyed were unaware of the types of behaviour that amounts to cyber-bullying, suggesting that the number (16%) of children who admitted to being recipients of mean or cruel behaviour may actually be higher.

Nearly a quarter (22%) of children said they had witnessed mean or cruel behaviour directed at a classmate or friend online (with 84% of that abuse on Facebook and 9% on Twitter). Only 23% of children who had directed a comment with cruel or abusive language to someone online considered it 'mean' to the person it was directed at, and just 9% consider that behaviour to be cyber-bullying. In addition, 15% said that if someone was upset by a mean comment they had directed at them online, they would think they were 'over-reacting', with a quarter (24%) saying they would be 'shocked' to have their comments perceived as cruel; displaying a real need for education about what online bullying actually is.

When it comes to parents' knowledge of cyber-bullying, 38% of parents think that their children may have been bullied online (with 9% stating that they know this for certain) and a third (33%) believe that their children may be the bullies themselves (6% have been made aware that their child has been a bully). Further reinforcing the need for greater interest and involvement from parents surrounding online activity is the fact that only a third (36%) of children who received mean or cruel behaviour online told their parents.

Cyber-bullying, the facts

- 16% said they had been the recipients of mean or cruel behaviour online
- 22% of children said they had witnessed mean or cruel behaviour directed at a classmate or friend online (with 84% of that abuse on Facebook and 9% on Twitter)
- Only 36% of children who received mean or cruel behaviour online told their parents
- Only 23% of children who have directed a comment with cruel / abusive language to someone online consider it mean to the person it was directed at, and only 9% considered it cyber-bullying
- 15% of children said that if someone was upset by a mean comment they directed at them online, they would think they were over-reacting
- 24% said they would be 'shocked' to have their comments perceived as cruel

Parents need support

Children's use of the internet is only increasing thanks in part to the growing range of internet-connected devices becoming commonplace in teenage life. Parents need to take an active role when it comes to internet safety and must get involved in their kids' online lives. To do this, they need to feel empowered with the right knowledge and tools at their disposal to make sure their children know how to act and how to react to what they see and experience on the web.

Installing parental controls across all devices – smartphones, tablets, PCs – is one of the first steps in helping to ensure children can use the internet safely, no matter where they are. Only 19% of the parents surveyed have done this, with the research suggesting a lack of technology knowledge could be a reason behind this. Nearly a third (32%) of parents admitted that better parental personal knowledge of the internet and social networks would make them feel better equipped to keep their kids safe online, with 1 in 6 (18%) parents saying that that their own knowledge of the internet and social media platforms is not adequate to match the online behaviours of their child.

Without adequate knowledge of technology, parents may be unintentionally exposing their children to the dangers of internet. Almost half (46%) of parents have set up their child's social networking site and 45% of parents with children under the age of 13 have set up a Facebook account for their child, despite the age restriction. Parents may not fully understand the implications of this. Underage children who are active on social networking sites may not have developed the resilience and rational thinking of older teens and are likely to be more at risk of cyber-bullying amongst other internet-related issues. Open and clear dialogue is a must for all parents, as more than one in eight of children (13%) also admitted to lying about their age to get around age restrictions on social networking sites.

Digital Deception

- 13% of children have lied about their age to get around restrictions their parents had placed on the internet
- 19% of children have lied about their online activities to their parents
- 21% of parents claim that their child is not a member of any social networks, but *all children* said that they were a member of a social network; (3% joining before they were 10, and 40% before they were 13)

The need for education

With today's teens being the first generation to grow up immersed in a cyber-world, we've established that parents require more support to help keep them up to date with rapidly changing technology and to understand how they can keep their children safe online. More than half (53%) of parents put the onus on education, saying that knowing their child is learning about e-safety in school would make them feel better equipped to help keep their child stay safe online.

But whilst schools and the wider industry certainly have a big part to play, parents must also work to improve their knowledge of the internet to ensure children can enjoy the great benefits of the internet safely. Parents can protect their children from online threats and realising that this is within their capability is critical. Sitting down with children and reviewing our top ten rules with them will help to ensure a worry-free experience that fosters learning and understanding.

Top 10 ways to protect your kids online

1. **Monitor your children's use of the internet**. Put the computer in a high-traffic family area and limit night time use. If your child uses the internet on their smartphone or laptop, make sure to take an interest in what they've been doing and the sites they've been visiting. Also, check out online child safety monitoring software.

2. **Work as a team to set boundaries**. Decide exactly what is okay and what is not okay together with regard to:
   a) the kinds of websites that are appropriate to visit
   b) kinds of things your children can discuss online
   c) the chat rooms, social networking sites and forums that are appropriate to participate in. Make sure to use only monitored chat rooms and make sure your children avoid ".alt" chat rooms, which focus on alternative topics that may be inappropriate for young people

3. **Together, agree upon family internet rules. We recommend the following:**
   - Never log in with user names that reveal true identity or that are provocative
   - Never reveal your passwords
   - Never reveal phone numbers or addresses
   - Never post information that reveals your identity
   - Never post inappropriate photos or ones that may reveal your identity (for example: city or school names on shirts)
   - Never share any information with strangers met online
   - Never meet face-to-face with strangers met online
   - Never open attachments from strangers

Once you have established the rules, post them next to the computer or somewhere in the house that will serve as a reminder for children.

4. **Sign an agreement for appropriate online behaviour**. Write up an agreement together so there is a clear understanding among all family members on appropriate computer use and online behaviour.

5. **Install security software.** Make sure you have robust security software that protects your computer against viruses, hackers, and spyware. It should also filter offensive content, pictures, and websites. This software should be updated frequently, as new threats are emerging daily. Software such as McAfee® LiveSafe protects against a range of devices such as smartphones, tablets and PCs to ensure online safety even on the go.

6. **Use parental controls.** All major security software providers offer parental controls. Be sure to enable them. If you are using freeware or software that doesn't have parental controls, consider purchasing software that does. Take time to learn how these controls work, and use options that filter and block inappropriate material. To completely protect your children online, use McAfee Family Protection software in addition to the parental controls in your security software. McAfee Family Protection software keeps children of all ages safe from exposure to inappropriate content, social networking risks, strangers, and other online threats. Of course, these tools have their limitations. Nothing can take the place of attentive and responsive parents who monitor their children when they are online.

7. **Remind family members that people met online are strangers**. Everyone who goes online must understand this - no matter how often you chat with online "friends," no matter how long you've been chatting, and no matter how well you think you know them, people you meet online are strangers. It is easy to lie and pretend you are someone else when you are online. Kids especially need to know that a new "friend" may really be a 40-year-old man rather than someone their own age. Social networking websites like Facebook and Twitter are an ideal way to meet new people online. Therefore, you must visit these sites and check your child's profile to ensure that inappropriate conversations are not taking place and that unacceptable photos are not being posted. You should monitor your children's instant messaging conversations to make sure they aren't being pursued online.

8. **Create strong passwords.** To create passwords that are difficult to crack, start by using at least 8 characters and then use a combination of letters, numbers, and symbols. Passwords should be changed periodically to reduce the likelihood of a particular password being compromised over time. Techniques for strong passwords:
    - Use a vanity license plate: "GR8way2B"
    - Use several small words with punctuation marks: "betty,boop$car"
    - Put punctuation in the middle of a word: "Roos%velt"
    - Use an unusual way of contracting a word: "ppcrnbll"
    - Use the first letter of each word in a phrase, with a random number: "hard to crack this password" = "htc5tp"
    - Don't share your passwords!

9. **Check your computer's security software**. Open whatever security software you are using and verify that your computer is protected by the following three core protections: anti-virus, anti-spyware, and a firewall. These core protections should be augmented by anti-spam and safe search software like McAfee SiteAdvisor® that features anti-phishing protection and safety ratings. It is also a very good idea for families to have a suite of protections on home PCs that includes parental controls, like McAfee Family Protection software, and identity theft prevention tools.

10. **Stay informed.** The more you know, the safer you will be. Check out McAfee's Security Advice Centre for easy-to-read educational material on computer and internet security. www.mcafee.com/advice

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com