KIDS ON THE WEB

CHILD'S PLAY?

PANDA SECURITY | *One step ahead.*

KIDS ON THE WEB
CHILD'S PLAY?

The amount of new malware (viruses, spyware and other malicious code) that appeared in 2007 increased tenfold with respect to the previous year. Moreover, cyber-crooks have found new tools such as instant messaging (programs like MSN Messenger or Yahoo! Messenger, etc.), file-sharing programs (like eMule or Kazaa) and blogs as a new way to infect users and steal their confidential data.

In other words, the risks of the Internet are increasing and children, as they have the least instruction, are also the most vulnerable.

Below, we will explain some of the main Internet threats to which children are exposed, and also look at how best they can be protected. Much of the onus of protection falls on parents and tutors, who must be able to control what children do on the Internet, instructing them in how to enjoy new technologies in a safe and responsible way.

Significant data: Children and the Internet

According to data from Save the Children, more than 13 million children in Europe have frequent access to the Net. They usually access the Web for the first time before the age of 10.

According to a study carried out in 2004 by Kleiner and Lewis, 90 percent of children in the USA between the ages of six and ten, regularly access the Internet. In 2006, a study by the American Psychological Association (APA) put the number of American children that regularly surf the Web, enter chatrooms or use IM at between 75 and 90 percent.

Data compiled in the EU tells a similar story. The Euro-barometer reveals that 64 percent of children in Denmark, Holland and the UK are Internet users; in Sweden the figure is 63 percent, in Finland 62 percent and in Estonia 60 percent. With the exceptions of Greece (15%), Cyprus (20%), Slovakia (30%) and Portugal (31%), the picture is similar across the rest of the EU.

In absolute terms, and according to data from Save the Children, more than 13 million children in Europe have frequent access to *the Net*: four million are under 12 years old and nine million are between 12 and 17. The United Kingdom tops the ranking of children that use the Internet.

With respect to the risks, some 49 percent of children surveyed by Save the Children claimed to have come across Internet content that scared or worried them.

In short, the Internet is a part of children's daily lives. They spend many hours connected to the Net, either at school or at home. That's why parents and children alike must be aware of the risks and know how to mitigate them.

Main risks

Children and young people are exposed to a host of risks on the Internet, from infection of computers by malware to people using false identities to entice them into a physical meeting.

In this document we look at a list of the main threats and discuss how parents and children can combat them.

Instant messaging and email

Instant messaging tools use email addresses and passwords to identify users. This makes it difficult to know who is on the other side.

Instant messaging (through programs such as MSN Messenger, Yahoo! Messenger, Google Talk,…) has become a widely-used communication channel for young people. This phenomenon has not gone unnoticed by cyber-crooks, who have been quick to take it up as a main channel for their activities.

One of the most dangerous threats that children and young people using these tools face is identity spoofing (somebody pretending to be someone else to trick potential victims). In these programs users are authenticated through an email address linked to a password. So, if someone accesses the account of one of the contacts, there will be nothing that warns the targeted user that the person you are speaking to is not who they claim to be. If you have files shared with that contact, the attacker will be able to access them freely. That's why it is important not to share any confidential information (personal data, physical address, ID numbers, bank details, etc.) through insecure channels such as instant messaging.

Another far more sinister danger concerning identity spoofing is its use by pedophiles. Their strategy is to gain the confidence of young people and then arrange to meet them in person or persuade them to send compromising photographs of themselves. They try to pass themselves off as other young people, professional photographers and many other similar covers.

Education is without doubt the best way to protect young people from this particular threat. Advice such as 'don't talk to strangers', is just as sound online as it is in the non-digital world, and children should have sufficient confidence to be able to talk openly to parents or tutors if they have any doubts.

Another potential risk of instant messaging is infection by viruses or malicious code. Almost 60 percent of worms (malicious codes that can spread by themselves) detected by PandaLabs in the first six months of the year were designed to spread across instant messaging applications. Some of these are designed to capture passwords for online banks. The risk, in the case of infection, obviously affects parents as much as children, as it will be their bank details, and consequently their money, that will be in jeopardy.

There are simple measures that can be taken to prevent malicious code from reaching computers through instant messaging: Don't run any file or click any link that reaches you through this channel. At least not before checking that the person who has sent it really is who they claim to be.

KIDS ON THE WEB
CHILD'S PLAY?

The best tip against malware distributed through messaging applications is not to run any file or click any link that reaches you through this channel.

Email is another source of risk for young people. In this case there are also several threats:

- Firstly, there is spam. Very often, this kind of junk mail is used to advertise anything from online casinos to pharmaceuticals. Children are much more prone to believing the messages that these emails contain, with all the risks that this entails. They can access online casinos and become hooked on gambling, or they could buy pharmaceuticals or even drugs with serious potential health risks.

- Next, there are false job offers. While this may not represent a serious threat to young children, it could be a danger to adolescents. These messages normally include what seem to be fantastic job offers. They promise large salaries in exchange for little or no effort. All that is needed is the number of a bank account to which money will be sent, and then, in exchange for a commission, the recipient is asked to forward this money to another account. It seems too good to be true, and any sensible adult would be suspicious. However, a young person looking for easy money could easily fall into the trap. They would then become unwitting accomplices to a crime, as the aim of these transfers is to launder money from criminal activity.

- Another risk is that of viruses and malware entering computers. Malicious code distributed through these messages often aim to trick users into clicking a link or downloading a file (which causes the infection) using a wide range of enticing subjects: movie trailers, erotic photos, game downloads, etc. This technique is known as social engineering. Many adults are taken in by these techniques, so it's easy to see how children might take the bait.

The best way to protect young people against these threats is to **encourage them to be suspicious of emails from unknown sources**. They should be aware that much of what is written in these messages is false and that they should never run files or click on links in these types of emails.

The risks of file-sharing programs (Emule, Kazaa, etc.)

File-sharing across P2P networks is another major source of infections. A lot of malicious codes –generally worms- are copied in folders of these programs with enticing names (names of movies, programs, etc.) in an attempt to encourage other users to download the files and run them on their computers.

This is, to all intents and purposes, another variation of social engineering: the file names could be deliberately aimed at children or young people, who without knowing it, will be allowing malicious software into their computers.

That's why children should know which files they can download and which they should avoid. It is also a good idea to **scan any such file with a security solution** before opening it for the first time. If there is an error message or a dialog box asking for a license or codec to be downloaded, you should start to be suspicious, as the file almost certainly contains viruses or malware.

Social networks and blogs

Social networking sites (such as MySpace or Facebook) are widely used for sharing photos and videos, meeting and chatting with people, etc. along with blogs. A common component of these pages is the need to create a personal profile in order to access them. These profiles often contain data such as name, age, etc.

Many malicious codes copy themselves to the most visited web pages to be downloaded and run by users.

Children should be reminded, generally, that it is not necessary to give this information, and that simply an email address and name (which could be false) will do. They should not be giving out data such as their age, address, and in particular, photographs of themselves.

Many young people now use blogs as a kind of personal diary. As such, these online journals frequently contain far more information than is advisable. It is particularly important to avoid publishing any data that could identify the user as a young person, or that could reveal their address or place of study, etc.

Similarly, on certain social networks, such as MySpace, it is possible to share files with other users. Children should pay particular attention to what they share and who they give permission to view this information. There is no problem in, say, posting photographs, provided they are protected with a password which is only distributed among friends and family.

Parents should know about these new services as well as how they operate and what the risks are. They should also be able to instruct their children on how to use these tools safely and correctly.

KIDS ON THE WEB
CHILD'S PLAY?

Smartphone features like Bluetooth and Internet access are making cell phones vulnerable to attacks.

Cell phones with Internet: a new risk

According to a report by Frost & Sullivan, the increasing sophistication of cell phones will turn them into one of cyber-crooks' main targets over the next few years. According to the study, technologies like Bluetooth (allowing wireless file-sharing between devices) and fast Internet access are making these devices vulnerable to attacks.

Cell phones are now widely used by children and adolescents. The risks, therefore, that they face in this respect are similar to those commented above concerning PCs.

Firstly, instant messaging services for mobile devices are now widespread. Children can enter chatrooms from wherever they are, and the risks are the same as those detailed previously: identity theft, predators, malware infections, etc.

Spam is also beginning to hit mobile phones. SMS messages advertising all types of products and services have now been around for a few years. Many of these adverts are related to pornography. This means, that it is not just through their computers that children are exposed to this type of content, but also on their cell phones.

Parents therefore should also be controlling what children are doing with their phones. To this end, it is advisable, in the case of young children, to give them cell phones that don't include functions that could be a source of risk, and in the case of older children, advise them on how they should use their phones. Remind them that they should not answer messages from dubious sources or arrange to meet strangers.

The risk of infection

We have seen in previous sections the different ways in which young users can infect their computers (links in emails or instant messaging, infected P2P downloads…). There are numerous dangers of having malicious code running on a system.

Firstly, as mentioned above, if children share a computer with their parents, they run the risk of infecting the PC with banker Trojans or other similar malware that could steal bank details when adults use the computer.

But malware is not just a threat to adults. It also carries risks for the children themselves. For example, adware could easily enter a computer. This type of malicious code is used to display banners, pop-ups and other adverts on infected computers. For adults, this tends to be more annoying than anything else (although watch out, because some also download Trojans onto infected systems), but the risk is greater for children and young people, as some display adverts linking to web pages with pornographic content. So children can find themselves with pornography on their own PCs, without even having looked for it

If youngsters share computers with their parents, there is a risk that careless behavior may lead to computer infection.

KIDS ON THE WEB
CHILD'S PLAY?

Practical tips for parents

1 **Speak to your children:** The starting point for protecting your children is to speak to them. You must know what pages they view, with whom they speak, what they like to see, etc. You wouldn't let them leave the house without knowing where they're going and with whom, so you shouldn't let them access the Internet without knowing what they are doing.

2 **Learn yourself, and pass the knowledge on to your children:** For many parents the Internet is still an unknown world. Some use it for looking for information, reading the newspaper or downloading music, films and other files, but for many, the services and pages that their children are using are completely unknown. For this reason it is very important to be aware of the tools that the Net offers children, and to know what the risks are and how to avoid them. Once you have done this, you can then advise your children on how to enjoy the Internet safely .

3 **Set firm rules for using the Internet:** You should establish clear and firm rules on how they use the Internet, with timetables, maximum online time, etc. Make sure they abide by the rules, especially with regard to using the Web at night. Another aspect to consider is the location of computers in the house; if you have just one PC for the whole family, it should be in a family room and not in the child's bedroom.

4 **Forbid children from giving out confidential information:** You must instruct your children not to give out data such as their name, address or photos across the Internet. Advise them to use false names or nicks in forums and show them how to create secure passwords (mixing upper and lower-case letters) to prevent cyber-crooks or other malicious users from accessing their email or messaging accounts.

5 **Teach your children to be wary of appearances:** Appearances can deceive on the Internet. We have seen how malicious code can disguise itself as codecs or movie trailers, how pedophiles can pretend to be someone else in order to establish contact with children or how messages that seem to come from a known contact can be infected. Therefore on the Web, things are not always what they seem to be. Teach your children to be wary and not to do anything that could jeopardize their security or privacy.

6 **Install an effective security solution:** To protect your children from malicious code, the best strategy is to have an up-to-date and effective security solution. Panda offers solutions for home users that don't just eliminate malware, they also block web pages that could infect computers, filter spam and, in the case of Panda Internet Security, include a parental control feature that lets you decide which pages your children can see.

KIDS ON THE WEB
CHILD'S PLAY?

Practical tips for children

1 **Don't click on links:** When you are chatting through instant messaging or you receive an email, never click directly on any links. If the message or email comes directly from someone you know, then type the address in the browser. If you don't know the person that it has come from, the best thing is to ignore it. Even if you type in the address, you may still end up on a malicious web page that drops malware onto your computer.

2 **Don't download or run files from dubious sources:** No doubt you have often received instant messages inviting you to download a photo, a song or a video. Sometimes, this file could have been sent not by the contact, but by a malicious program that has infected their computer and which is trying to spread to other users. Just in case, the best thing to do is ask your contacts if they have really sent something. If they haven't, let them know that they are infected so they can delete the file and advise their other contracts.

3 **Don't talk to strangers:** In chatrooms or on instant messaging, you can never really be sure who you are talking to. Especially in online communities, where people have never met in real life. Never make friends with strangers, and under no circumstances should you ever arrange to meet them in real life.

4 **Don't give out confidential information across the Internet:** Never send private information (your details, your address, etc.) via email or instant messaging, and never publish this kind of information in a blog or on a forum. You should also take care when you create profiles for services such as FaceBook or Myspace. You should never include confidential information such as your age or your address. It is also advisable not to use your real name, but a false name or nick.

5 **Beware of tempting job offers:** Generally, nobody gives anything away for nothing. On the Internet, if something seems too good to be true, it probably is. So if you receive fantastic job offers from unknown users, just ignore them.

6 **Don't run suspicious files:** If your security solution tells you that a file could or does contain malware, don't open the file. Just delete it.

7 **Speak to your parents or teachers:** If you have any questions about any of this, if you see something suspicious or you receive offensive or dangerous emails, speak to an adult. They will be able to advise you.

Practical tips for teachers

Teachers also have an important role to play in showing young people the correct way to use new technologies, above all, as computers are now commonplace in the classroom. That's why we have outlined a series of recommendations to follow:

1. **Find out:** Look up and study information about Internet threats. Find out what they are and their consequences, and how you can impart this information to children.

2. **Design an IT security education plan:** As young people learn about how to handle computers and the Internet, they should also be learning about potential dangers. This way, you will be ensuring they can keep themselves safe right from the start. It is best to draw up a plan to follow, preparing what you will tell them and finding any documentation you need.

3. **Make your explanations enjoyable and practical:** A good way to teach these concepts is to use practical examples. You can demonstrate some of the dangers of the Internet by showing your kids some of the effects they have. Find news stories relating to real cases.

4. **Teach them how to protect themselves:** During practical classes, show children how to configure an antivirus and create secure passwords, explain how to shop online securely, etc.

PANDA SECURITY