A PARENT'S GUIDE

HOW TO

Talk to your children about the Internet

safe internet

DIGI CyberSAFE™
in partnership with Cybersecurity Malaysia

October 2015

All reasonable precautions have been taken by Digi and UNICEF Malaysia to verify the information contained in this publication as of date of release.

www.digi.com.my www.unicef.my

1
Chapter one
Introduction to the Internet

2
Chapter two
Why should I talk to my kids about the Internet?

3
Chapter three
What should I say?

4
Chapter four
Real-life stories of kids and the Internet

Foreword

If you are a Malaysian parent of a child aged 15 to 24, chances are you have a digital native living in your home.

A global study by the International Telecommunication Union in 2013 revealed that Malaysia had the world's fourth-highest proportion of 'digital natives', with almost 75 per cent of its youth in this category. Digital natives are defined as young individuals between the ages of 15 and 24, with at least five years of active Internet use.

In Malaysia, even children much younger than 15 are online every day. Many use the Internet to learn, and explore, network and socialise, to keep updated with what's happening in their world and to be entertained. More and more children are also using the Internet in creative ways to produce content, create videos and apps, and to blog.

Everywhere across the world, children are quickly finding their way online with the help of a wide array of devices, and kids and teenagers in Malaysia are no exception. A recent survey showed that in 2014, 2 in 5 Internet users in Malaysia were aged 24 and below, with 15.5 per cent aged 19 and below. Meanwhile, 31.3 per cent of Malaysian handphone users were aged 24 and below, with 12.5 per cent aged 19 and below.

As Malaysia journeys deeper into the digital age, it is clear that the children will lead the way. Yet it remains our responsibility to ensure that they stay safe online, and that their online experience is an enriching and positive one every step of the way into adulthood. As with all powerful tools, we must ensure that our children are taught to use the Internet safely and responsibly, without endangering themselves or others.

This guide is for all parents who may have questions about the Internet, usage and safety measures when their kids venture online. Where and how are our children spending their time online? How do we protect them from predators, cyberbullying and harmful and inappropriate content? What other risks do they face? What resources are available? *How do we talk to our children about the Internet?*

This book hopefully sparks that conversation.

Warmest wishes, safe surfing and happy learning.

digi unicef telenor group

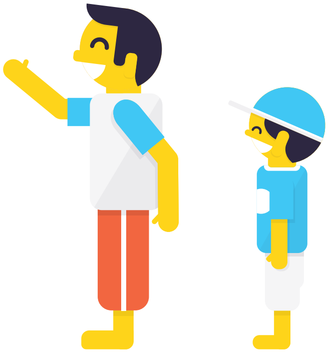
CHAPTER ONE

Introduction to the Internet

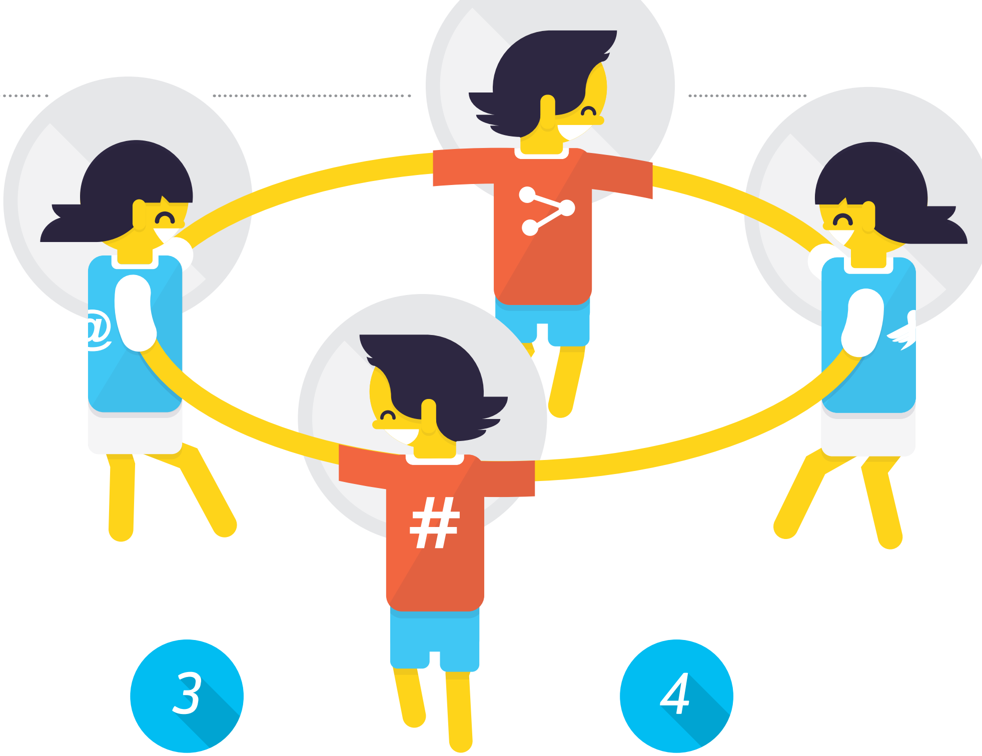
Believe it or not, once upon a time, we relied on post, radio, television, print publications, and hardbound encyclopedias to connect with the world and to research information. To connect with one another, we could only rely on the connections made within our closed circles – friends, family, and the local community around us. And then the Internet was born, and we became an interconnected global community that opened windows onto the world. Our lives were never the same again.

Some countries have had Internet for more than 20 years now, and for many of us, today the Internet feels like our friend. Linking the entire planet together, the Internet is a vast resource for connecting us all together. We can use it for all kinds of things like studying for school projects, keeping in touch with our friends, bridging the gaps between generations, learning how to make popular recipes, selling handmade wares, watching popular entertainment or getting directions when we are lost. The Internet allows us to search for job opportunities, find instructions on how to complete projects, manage our money, go shopping in other countries, research school assignments, publish our thoughts on online journals or 'blogs', and learn about all sorts of things that we never thought we could.

The Internet now makes the world a smaller place at the touch of a button.



How to use the Internet – the right way



1 Using the Internet to learn and search for information

We can now use the Internet to find information on just about anything. Really. Using search engines such as Google and Bing, we can type in a word or search phrase, and pages of indexed information on that subject pop up right in front of us. Through instructional videos on websites such as YouTube, we can learn how to cook a new recipe or how to fold a paper airplane. We can find information quickly, get weather warnings, food prices, research historical information, watch live cameras all over the world, and check out photos from places we dream of.

2 Using the Internet to connect with one another

By email, social networking, chat, social media, online forums, VoIP programs, and more, we are globally connected now more than ever, having the ability to feel connected to everyone on the planet no matter where you are. In Bangladesh and Myanmar, mobile classrooms connect qualified teachers to rural communities, and the use of video chat can connect qualified doctors to patients in remote communities. Simply put, the Internet is an amazing tool to bring together communities that otherwise would have limited access to each other.

3 Using the Internet for entertainment

TV, radio, games and the Internet were once separate things. Now, the Internet brings them all together in one powerful place. Internet entertainment can be found through YouTube, streaming media, embedded media like Windows Media Player and iTunes, online media, digital media receivers like Apple TV, Roku, Xbox, and PlayStation.

4 Using the Internet to create opportunities

Using sites like LinkedIn, Etsy, Amazon, Craigslist, Blogger and many others can create potential job opportunities, shopping and online sales opportunities, and the opportunity to publish articles in your own voice.

So now, not only is the world's information ours to access at the touch of a button, but our voices are for the world to hear at the touch of a button as well. All because of the Internet.

CHAPTER TWO

Why should I talk to my kids about the Internet?

Because knowledge is power

In a world that is constantly changing, we understand that our kids are now growing up faster than ever before. In this super-wired age, we can help to avoid pitfalls by keeping one step ahead of the exploding Internet boom. By teaching ourselves to learn the best ways to inform our children, we can protect them from some of the risks of being globally interconnected: the dangers of misusing the Internet.

Avoiding stranger danger

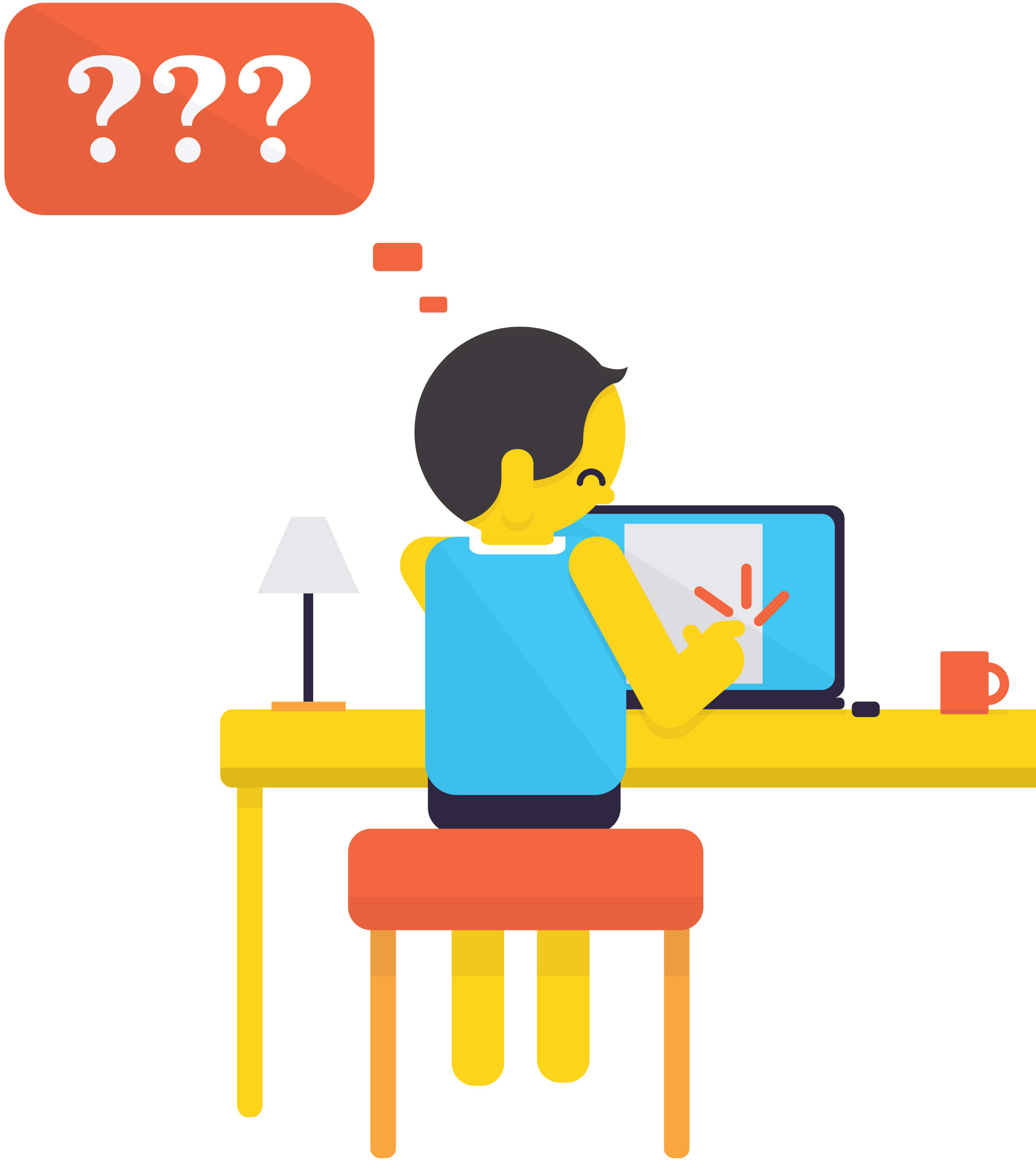
Connecting with strangers through social media networks can sometimes be risky for our children if they make the wrong connections. As there is no real way to determine whether a person's social profile is actually who they say they are, we can arm ourselves and our children with the knowledge of when an online connection or relationship turns dangerous to avoid trusting those who may be online predators.

The best way to keep track is to make sure you know who all of your children's social media connections are. The age at which a child should be allowed to have a social media profile is up to every parent to decide, but from that point on, you should have a good handle of who your kids are 'friends' with online.

If they're not relatives, if you don't know them from your kids' school, or through other families you know in your community, then they deserve a second look.

Truth: Once something goes online, it is incredibly difficult to delete

Although it may seem that we can delete online posts because they appear invisible, the posted information has already been loaded onto the Internet. Once something is online, it is online forever. In a spur-of-the-moment rant or instant post of ourselves doing something ridiculous at a party, there's no real 'undo' or 'delete' button to push. The images and text posted can turn criminal, harming others or even ourselves, as these can turn viral in a matter of seconds. Images can be misused, altered, and even shared within inappropriate networks, so it's important to think before posting. Too often, surveys about kids' and teens' attitudes about the Internet show that a majority are not concerned with the invasion of their privacy or the anonymity of the person they interact with.



DIGI CyberSAFE™ IN SCHOOLS

in partnership with Cybersecurity Malaysia

Malaysian Schoolchildren on Staying Safe Online

A National Survey Report 2014

Largest national survey on cybersafety among schoolchildren in Malaysia reveals:

40% do not know how to protect themselves online.

83% are vulnerable to online risks due to minimal protective actions taken.

2/3 below 13 years take few protective steps when online. Yet, 52% of all children feel they are safe.

70% are not concerned with the invasion of privacy or anonymity of the person they interact with.

>40% said online safety is important yet take low levels of protection. Awareness does not necessarily translate to positive action.

Children are equally exposed to online threats regardless of where they are from, contrary to common perception that those in urban cities take more protective actions.

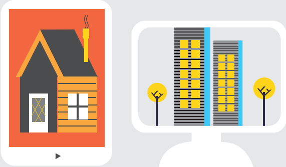
Worrying trend on cyberbullying

>70% identified themselves with various forms of online harassment, namely calling others mean names, posting improper messages and inappropriate photos.

64% feel that sending improper SMS-es, posting inappropriate photos, and pretending to be someone else are not cyberbullying.

26% have been bullied online, mostly those aged 13 to 15.

Are we doing enough to keep our children safe?



>50% go online without being supervised, while 40% claim they are not bound by any rules on cybersafety.

61% children turn to family members when encountered with negative online experiences.

6% choose to keep quiet when bullied although they have the option to report it to family members, educators and public authorities.

Families with computers in common areas of their home tend to exert more rules on cybersafety. However, this measure alone is insufficient as an increasing number of children are accessing the Internet on their mobile devices.

MINISTRY OF EDUCATION MALAYSIA

MCMC

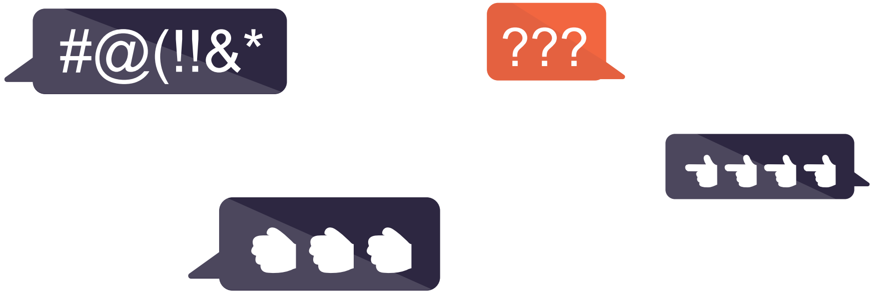
CyberSecurity MALAYSIA
An agency under MOSTI

digi

Cyberbullying

What may seem harmless online to us can actually be troublesome for others. Thinking about how we 'talk' to each other online and how we use the Internet to connect with others can help us determine between something that is cyberbullying behaviour and what is socially acceptable online.

In Malaysia, a 2014 nationwide survey, which could someday be very representative of the rest of Asia, found that half of children are unsupervised when online. And today, as many as one in four schoolchildren reported that they had been bullied online, with children aged 13 to 15 being bullied the most. Online harassment is also high – nearly three in every four kids say that they experience it. It was defined in the survey as calling other children mean names, posting improper messages and inappropriate photos. Perhaps most worrisome? Two-thirds of children feel that sending improper SMS-es, posting inappropriate photos, and pretending to be someone else is NOT cyberbullying. Cyberbullies often do not realise the consequences of their actions or that they might be cyberbullies themselves.



We in Asia can also learn from examples from across the world. A UK study in 2013 studied more than 2,000 British teens and found that seven in 10 young people between ages 13 and 22 have experienced cyberbullying. One in five of those teens consider theirs to have been extreme cases. In a 2014 survey of 10,000 youths, more than half of young people 'reported that they have experienced cyberbullying' using Facebook.

But it doesn't have to stay like this. In the USA, a 2011 Harvard School of Health study showed that schools that have anti-bullying programmes reduced bullying by half, with the worst at middle school (usually between ages 11 and 14).

And in Norway, more good news. In 2009, Telenor Norway and partners created a national programme against cyberbullying. It reached hundreds of schools and tens of thousands of students, giving kids, parents and teachers information on how to prevent cyberbullying. Results since then? Three out of every four kids who took part say that they now have what they need to know in order to avoid bullying via mobile phone and the Internet.

Goes to show what a difference simple conversations – at home and at school – can make!

Online sales fraud and identity theft of personal information

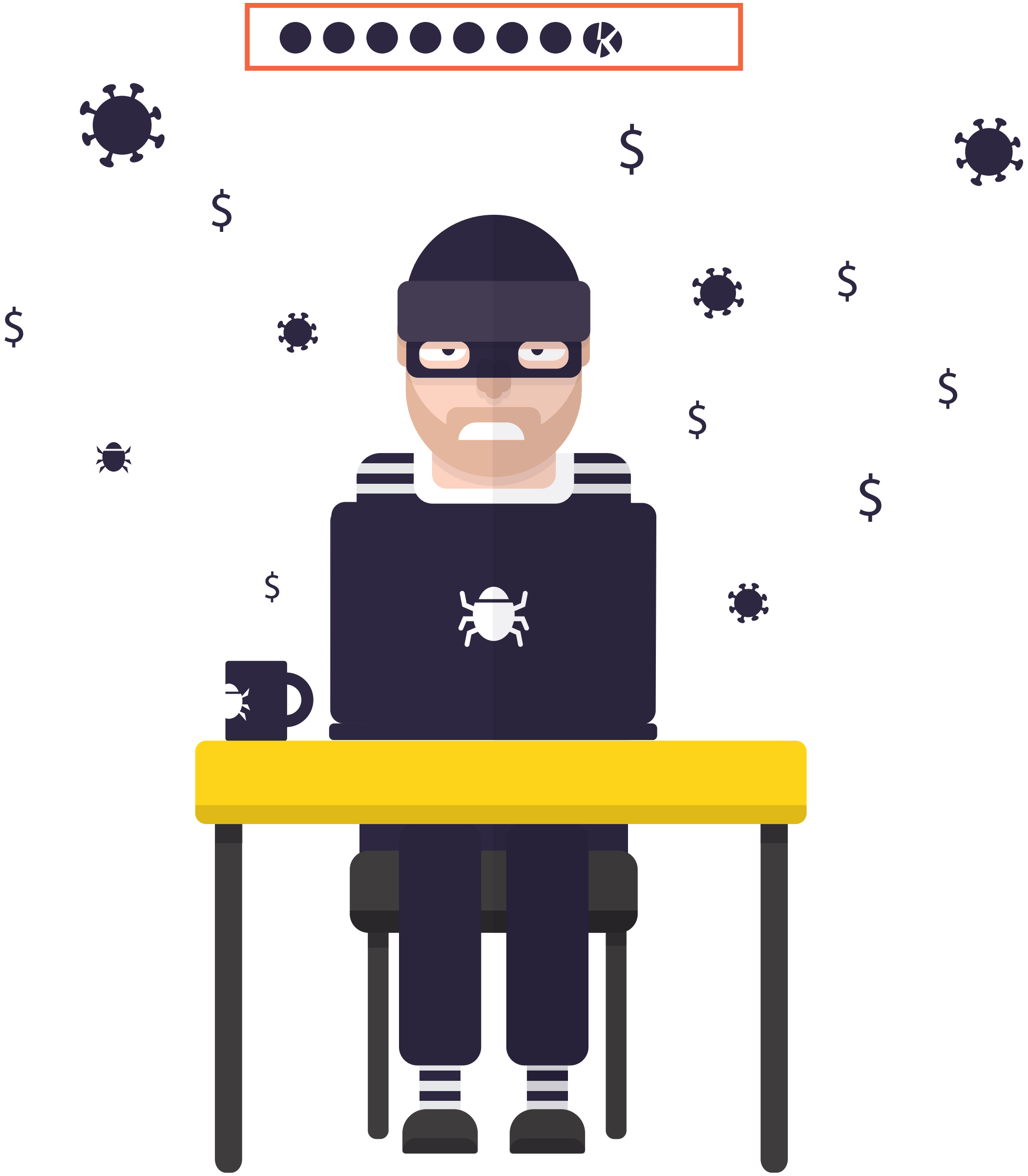
We instinctively know when something seems too good to be true, but sometimes we need a little help sorting through the mass of information. Salespeople are trained to be incredibly effective in their sales pitch, but sometimes it isn't really clear whether buying something online is acceptable or not. Teaching ourselves and our children to spot potentially fraudulent activities online can help save us from theft and unnecessary expenses, as well as spare us the headaches. Questioning where and when we share our personal information – photos, credit card and bank account numbers, and addresses – can save us from having other people falsely use our personal information.

Virus attacks and malware threats

Opening ourselves up to the vast Internet also opens us up to hackers and virus malware that can plague our computers, devices, and important files. Virus programs usually appear to be harmless links; learning how to avoid these will help keep our devices and computers healthy.

Age-inappropriate content

We get that our kids are curious beings. It's what makes them so great. But be aware that online content may be unregulated content, depending on where you live. Adult content can often be easily found by little fingers with unrestricted access, so it's a must to educate our children about what is okay and what is definitely not okay. Have a discussion with your children about accessing content, whether through the Internet, gaming, social media, or related apps that highlight alcohol and drug use, and pornography.



So, what are the popular Internet apps and websites that parents should be aware of?

Facebook

Considered the largest social networking site on the Internet, Facebook's global reach enables its users to share posts, images, notes, and even purchase some items online. Facebook is a great way to keep up with friends and family, and the ability to connect to those around the world makes using the app rewarding. Despite the fact that users must be at least 13 to open a Facebook account, many young kids have accounts and are active. Besides being aware of their kids' activities on FB, parents should talk to them about risks and the importance of privacy settings, and reporting unwelcome friend requests.

Twitter

Twitter is a microblogging site where users, known fondly as 'tweeples', post brief messages – known as tweets – that are no longer than 140 characters. Tweeples can also follow other users' tweets. It's popular with teens who enjoy tweeting about celebrity news as well as tidbits about their own personal lives. Parents should be aware that even though tweets can be kept private, many teens have public accounts, and public tweets are the norm for them. Talk to them about what they post and how quickly a post can spread. Updates appear immediately, and even though tweets can be quickly deleted, someone may already have read – and even screen-captured – it, so kids should be careful not to tweet in the heat of the moment. The right settings can ensure that tweets go out only to friends, but even within a circle of friends, there is potential for problems to arise.

Instagram

The app that everyone is using might actually be promoting a toxic mix of narcissism and insecurity for your kids. Most of the photos posted on Instagram are selfies – images of the user taken by friends or by themselves. 'Followers' of the user can view, 'like' the image or video, and leave a comment. The latter can get terribly explicit and mean, since teens are posting photos of themselves in swimsuits, underwear, or even full on nudity. All of these are related to self-esteem problems, and are taken in the hope that their photo will garner 'likes' and positive comments from friends and strangers.

YouTube

YouTube is not only the best-known site for watching and sharing videos, it is also one of the most popular sites on the Internet. From corporate training videos to cat videos to performances by amateur pop stars, you – and your kids – can find virtually anything on YouTube. To upload videos, you must be at least 13 – the minimum age for creating a Google account, as stipulated by the Children's Online Privacy Protection Act in the US. YouTube guidelines prohibit sex, nudity, gore, harassment, illegal acts, hate speech and other inappropriate content, but a video can technically meet these guidelines yet still be provocative and unsuitable for minors. Parents should therefore be mindful of children possibly viewing or posting unsuitable material. With guidance, YouTube can be an enriching space for education and entertainment. YouTube Kids is an app specially designed for younger children.

WhatsApp

WhatsApp is a widely used mobile messaging app that allows smartphone users to exchange text messages via the Internet, without incurring SMS charges. Besides text messages, users can exchange images, videos and audio clips; you can also make phone calls with WhatsApp. Messaging can be one-to-one, or in group chats. WhatsApp is both incredibly helpful and fun, but being a tool for communication, it can just as easily be used to exchange inappropriate content, and it can expose young users to unwanted contact. WhatsApp itself says that it is not intended for users below the age of 16, but it is popular even with younger teens. Once you sign up, it automatically connects you to the other WhatsApp users in your address book, and encourages you to add new friends.

Snapchat

This photo and video messaging app allows users to post content that only lasts for a maximum of 10 seconds before it is deleted. Because of the temporary nature of each snap, the app has been said to be a popular medium for posting questionable content, including sexting. Snapchat is hugely popular with youngsters, many of whom use it for innocent fun, but parents should still educate their children about the dangers of getting carried away when posting snaps. Many users also mistakenly believe their images cannot be saved or sent virally, and parents should warn children that nothing completely disappears from the Internet. Parents can also check out the Snapchat Safety Center on the website for tips.

Waze

Waze is the world's largest community-based traffic and navigation app. Malaysia has nearly 1.5 million users, making it the biggest Waze community in the Asia-Pacific region and one of the top 15 largest Waze communities out of nearly 200 countries. Many drivers use Waze simply to get directions to go from one point to another. It is also possible to contribute more detailed information to the community. In doing so, however, your kids may inadvertently share information about their location and routes with others.

Foursquare

Foursquare is a 'local search' app that gives users information about businesses and services (such as restaurants, shops, hotels, banks and petrol stations) that are close to their current location. The app can offer personalised recommendations to suit users' tastes, based on their usage history and other data. You can also follow other users to get their tips. Swarm is a companion app to Foursquare that offers location sharing and social networking aspects. This app allows users to share their location with friends, and to see where their friends are. Users must therefore be careful in accepting friend requests in a network. Most users are typically not well acquainted with all their friends in a social network. Kids can also unwittingly share their location with a public audience and expose themselves to risk.

LINE

As a mobile messaging app, Line is similar to WhatsApp in that users can exchange text messages, video and voice. Line, however, also integrates social media elements and offers features that are especially appealing to teenagers, such as a selection of thousands of fun stickers and emojis, as well as games. Many of these features need to be purchased, and kids can easily get carried away and overspend at the Line Store. There is also Line Play, an avatar-based social network which offers the possibility of virtually hanging out and partying with over 20 million new friends. As with other social networks, kids should be reminded that online identities can be misleading if not downright fraudulent. Line exemplifies how young people today communicate and socialise (in 2014 the company estimated that more than 1.8 billion Line stickers were sent and received every day) and parents' guidance can help to ensure this remains a healthy form of expression for the new generation.

Tinder

Tinder is a dating app, intended for adult users to pursue the possibility of romantic matches with other users who are in the same location. In reality, it is often used for casual sexual encounters. It is also possible for children to access the app, and in doing so, stumble across profile pictures that are meant for the more mature. The geo-location and anonymity features of Tinder could also enable harassment and make stalking easier for online predators. Unlike social media apps that are built on networks of friends, Tinder is based on the idea of sharing your profile and images of yourself with strangers, and potentially meeting them, often on the spur of the moment. Parents should warn their children that this app is meant only for adults, and children who experiment with it are at risk of being targeted by predators and scammers.

Vine

A video-sharing app that limits videos to six seconds or less, Vine has become a platform that contains sexual images, drug use, nudity and inappropriate language, but then again, Vine also contains videos of puppies, kittens and babies as well. If your kids are on Vine, their connections will determine which of these things they might see.

Online games

Many of the same dangers confronting young users of social media – such as predators, cyberbullying, inappropriate content, and Internet addiction – are also present in the world of online gaming. Parents should be aware of the nature of the online games their children play, and the fact that many games feature sexual and violent content. While many movies and other entertainment contain similarly inappropriate content, online games have the added element of role playing that can potentially leave a greater negative impact on children's behaviour in the real world. Online relationships with other players can also lead to problems.

CHAPTER THREE

What should I say?

It isn't easy to be a parent today, as the social media revolution isn't fizzling out. To use the Internet and its apps responsibly, we've rounded up some tips and tricks for starting the conversation with kids.

Start the conversation

You know your children best. Sit down with them and discuss the benefits of the Internet – from learning to social networking to providing entertainment to creating opportunities. Together, discover the ways in which the Internet will broaden their horizons. In the same conversation, have a realistic plan for avoiding misuse of the Internet. Use the language best suited to your relationship to create a safe, open dialogue.

If your children already use the Internet, find out what sites and apps they are using, how these apps work, and whether they have had any challenges with them (like contact with strangers and cyberbullying). Let your children know that if someone is making them feel uncomfortable or if someone is saying harmful or hurtful things to or against them online, your kids won't get in trouble with you. They should feel comfortable in telling you about any negative online experience they have and know that you will find ways to help them.

Get familiar with Internet etiquette

Just like there are social rules within our local communities, there are basic online rules that we should follow. The most important thing to ask ourselves – 'should I really be posting this?' and 'will someone be hurt or offended by this post?' Taking 10 or 30 seconds to review what we post online and the repercussions of such posts are part of our social responsibility.

We like to follow the idea that if a post isn't something we would share with our family, it's probably a good idea not to share it online either.

Create rules yet realise that you can't monitor your children's moves online at all times

Create general online rules to keep your children safe and smart. Make a rule that your children must ask your permission before downloading any apps on their mobile device so that you're aware of them. When your children want to join social media platforms, set the profile security settings together to choose the ones you're most comfortable with.

Advise your children not to share passwords with anyone

This includes best friends and boyfriends or girlfriends. Sharing passwords could potentially damage your child's online identity, and it's best to keep these for their own personal use.

Setting age limits on your children's smartphones, laptops, tablets and desktops

As parents, you can usually set age limits on your children's smartphones, laptops, tablets and desktops, disabling their ability to download or buy particular apps and programs. As software and hardware upgrade at lightning speed, and with wearable technology making its way onto the scene, parents should familiarise themselves with user manuals to be able to understand how they work, thereby creating a safe environment for their children.

Important questions to ask your kids about the Internet

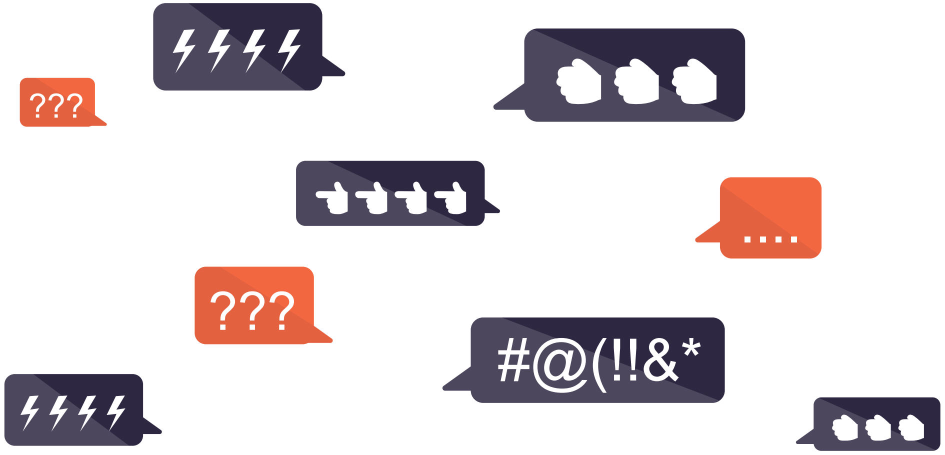
For parents whose children are already wired in the Internet community, here is a list of good questions to ask your children about their usage†

Q1

General tech use

1. What is your favourite website? What do you do on these sites?
2. What websites are your friends into these days?
3. Are you ever contacted by someone online that you don't know? If yes, what did they want? What did you do? How did you respond?
4. Have you ever received a text message from someone that made you upset? How did you respond?
5. How do you keep yourself safe online?
6. Do you get concerned that people will read what others have written about you online that is not true but think it's true?
7. Do you ever talk to anyone online that isn't in your school?

† Source: Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D., 'Cyberbullying Prevention: Questions Parents Should Ask Their Children About Technology', August 2013



Q2

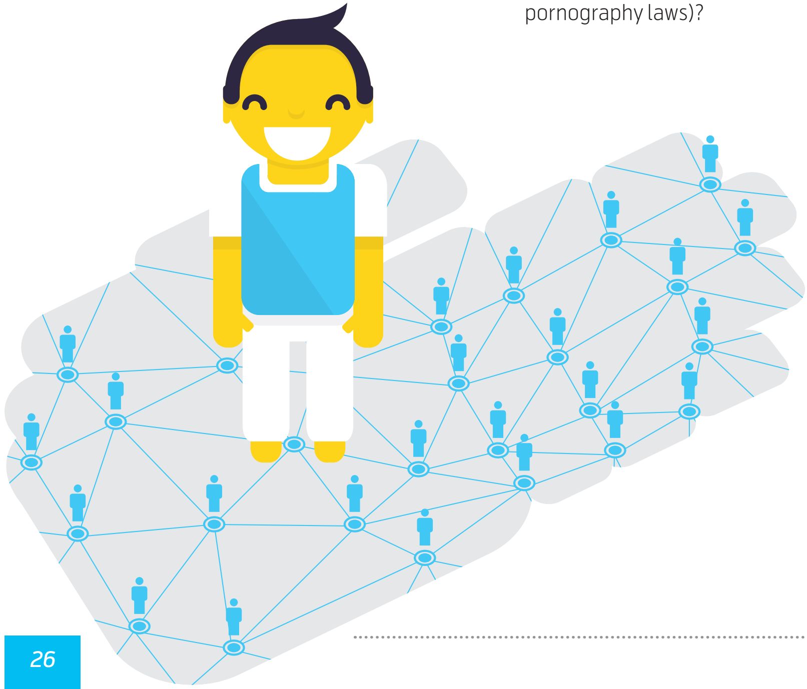
Cyberbullying

1. Do you ever argue or post hurtful updates on your Instagram, Facebook, Twitter or other social media sites? Why?
2. Have you ever had to delete a post or comment on your page that was written by someone else?
3. Does cyberbullying happen a lot? Would you feel comfortable telling me if you were being cyberbullied?
4. Do you think your school takes cyberbullying seriously?
5. Have you ever had to contact a teacher or someone else at school because of a cyber-threat? If so, did they do something about it and did it help?
6. Does your school have a way to anonymously report bullying and cyberbullying?
7. Do you feel like your friends would be supportive of you if you told them you were being cyberbullied?
8. Do you ever get verbally attacked during online games?
9. Have you ever had to leave an online game because someone was bothering you online?
10. Have rumours ever started about you in school, based on something said online?
11. Did you ever find out who started the rumour? What did you do when you found out?
12. Have you ever blocked somebody online because you felt harassed? If so, did that make it stop?

Q3

Sexting

1. Do you send pictures through text? Do you receive pictures? If so, from who?
2. Are kids in school taking a lot of pictures with their mobile phone cameras? What do they do with them?
3. Do you ever Skype or FaceTime with friends?
4. Do you use Snapchat? Can you explain to me how it works? Do you think pictures are really completely gone?
5. Have you ever had anyone do or say anything inappropriate on Skype or Snapchat?
6. Do you know what sexting is? Has any adult at school ever talked with you about sexting?
7. Has a stranger ever sent you explicit texts? What did you do with these texts?
8. Has a friend ever sent you explicit or offensive texts or pictures?
9. Do you know about the consequences that can result if you send inappropriate pictures (child pornography laws)?



Q4

Safe online social networking

1. What social networking site do you use most frequently? How many friends or followers do you have?
2. What kind of people are you meeting on Instagram and Facebook? Are you connecting with people that you know? Or are you meeting people around the world?
3. Do you get a lot of friend or follow requests from strangers? If so, how are you handling that?
4. Do you use Twitter? What for? Who do you follow and who follows you?
5. Do you know how to use the privacy settings on Instagram, Facebook, and Twitter?
6. Do you have them set so that only those you accept as friends can see what you post? How do you know who can see your information?
7. What kind of personal information are you posting online? Have you ever posted your full name? Age? School? Phone number? Current location?
8. Have you ever been tagged in a picture in a way that made you upset?
9. Do you know how to edit your privacy settings so that if somebody wants to tag you in a post or photo, you have to approve it?
10. Do you know how to un-tag yourself in pictures?
11. Do you feel like social networking sites should be used to vent your frustrations? Do your friends vent on social media? Do people comment? What do they say?
12. What kind of videos are you watching on YouTube? Do you ever post videos?
13. Have you ever reported inappropriate videos that you have seen on YouTube? Or any other website?
14. Does anyone else know your password or passcode for any site or social media app? What about for your computer or mobile phone?

CHAPTER FOUR

Real-life stories of kids and the Internet

If you're asking yourself, 'how does my family fit into the Internet universe?' here are some answers. Families and young people in Malaysia, Myanmar, India and Thailand tell their stories from first-hand experiences on how the Internet has become a powerful tool in their lives, the challenges they have faced, and the lessons they've learned.

Mariammah Subramaniam

Malaysia

Insurance agent and mother of four Mariammah Subramaniam grew up in a home with no electricity, let alone the Internet. Her three older children are now adults, but her youngest, Cathryn Anila, is still only 15. How does Mariammah keep Cathryn safe online?

Mariammah's decision early on to embrace the Internet herself has enabled her to be comfortable talking to Cathryn about online safety. It was Mariammah who opened a Facebook account for her daughter, as a birthday present. She wanted to allow Cathryn the fun of social media, but she also took care to highlight the risks, as well as paint the big picture about social media being a powerful tool: 'I told her to use it for the benefit of mankind. I asked her to pick something she was passionate about, and use this online space for something good.'

Mariammah and her husband have chosen education, trust and empowerment over rigid restrictions. They work at developing their daughter's sense of moral responsibility, rather than telling her what to do.

Is this enough in this day and age, when a single click can so quickly lead to lasting consequences? Mariammah acknowledges the risk, but she believes ever harsher policing won't solve the problem. 'That click can happen anytime, anywhere. Today I can be sitting beside her and guiding her, but tomorrow she may be alone. How will she make the decision then?'

Besides her own moral compass, Cathryn also has friends who look out for each other. Internet safety is now an issue close to the hearts of both mother and daughter. Mariammah conducts sessions on online safety for the neighbourhood children. 'I speak to them about being careful online, now and for the future. Prospective employers will likely do an online search to gauge their standard and character.' Cathryn, for her part, has found her passion. She has been involved in Internet safety campaigns, and now aspires to be a child rights lawyer.

Nitipong Boon-long

Thailand

Nitipong Boon-long is a 45 year-old father of two tween boys, ages 9 and 12. Mr. Boon-long's family is fortunate to have three mobile phones and four iPads in the home, which results in heavy Internet usage for his family 'all day long whenever possible.' He feels the most important use of the Internet is for 'knowledge and games.' Mr. Boon-long's boys are heavily engaged in popular online games such as Fifa15 and Minecraft, with tablet use being the device of choice within the home.

Mr. Boon-long considers his family's biggest concerns for Internet safety to be 'hacking private information and billing fraud,' which can be rampant within gaming environments. As most of the boys' Internet use is within the home, Mr. Boon-long has the ability to monitor usage, however, it is not possible to be at home with the boys all of the time.

Boon-long says that parents can empower their families to learn about when NOT to click. In many gaming environments, pop-up ads and top-up schemes entice younger users with hard-to-believe offers, many through seemingly 'safe' and 'cute' images. Educating younger users to not click without adult permission will reduce the risk of hackers, disabling fraudulent activity. Additionally, many devices, apps, and programs sometimes have settings to prevent users from 'clicking' on fraudulent banners and ads. Parents would benefit from reading user manuals and getting acquainted with games to prevent identity theft.

Sudhir Jain

India

Sudhir Jain is a 44 year-old finance professional, and father of two teenagers. His 16 year-old daughter Shreya, and 14 year-old son Shreyansh, are millennial kids who were exposed to the digital world at a very young age. With four mobile devices at home, Sudhir's family is constantly connected to the Internet. The usage is varied – from online payments, ticket bookings, school projects, online shopping, games and social media. There is no aspect of their daily activity that is not touched by the Internet. Sudhir's children love to play Pacman, Candy Crush, Angry Birds, Temple Run and Subway Surfer on the devices.

Sudhir's family reflects the way Internet is consumed in India; the majority of traffic is driven by applications like Facebook, WhatsApp, YouTube, Instagram and ask.fm. Other popular apps include Hungama for music and Truecaller.

Sudhir feels that the biggest Internet concerns for his family are phishing emails, defamatory messages and the threat of malware viruses. These threats are especially harmful for children who are accessing Internet through smartphones, gaming consoles and tablets, spending as much as two to three hours per day online.

Sudhir has attended an Internet safety workshop – Uninor WebWise – in his children's school and likes to frequently research the topic to keep himself updated on risks and cyberthreats.

As a parent of teens, Sudhir, and parents like himself, have to be extra cautious in finding a balance between giving their children space, and educating them on the safety aspects. Sudhir feels it is important to make children aware of online 'stranger danger,' and teach them about appropriate Internet behaviour. It is also important to protect kids from cyberbullying and exposure to sexual predators. He feels that children should use the Internet under the supervision of adults and should be guided to use it judiciously.

Arkar Min Aung & Wai Yan Min Htay

Myanmar

Wai Yan is a young doctor from Yangon, fresh out of medical school and his peer, Arkar, also from Yangon, is a software developer who is now working on ways to give more Myanmar kids access to online education.

Explains Arkar, 'For people who have never experienced the Internet, I would say that it is something that will connect them with everything and everyone in the world. I would tell them that the Internet is where we are able to experience things by asking what we want to know rather than just consuming whatever the TV and radio provide. I would also tell them that by having a phone or a computer which is connected to the Internet, they will be able to see, not just hear, their children or relatives who are working or living far away from them. It's really wonderful when you think about it.'

Wai Yan says that the Internet is a completely different 'animal' nowadays – just a few short years after he first got online. The most obvious difference, he tells us, is that with mobile phones and wireless Internet, you can get online from anywhere and in essence, you can 'be anyone'. On social media channels, you can hide behind fake profiles and surf the lives of others. You can spread fake information and also be victimised by fake information. A story he tells from his work in disease prevention in villages between Thailand and Myanmar is eye-opening. 'Villagers at one point refused to take the vaccines we were providing them against Filariasis because they had read on social media that this was poison and would kill them,' Wai Yan explains. 'Of course it's completely untrue. And that's only one example. The tip of the iceberg.'

Wai Yan says that what we all need to remember is to not believe everything we read on the Internet, or believe people we are chatting with online whom we have not yet met in real life. The Internet can – and is mostly used – for great things. He became a youth participant at the Telenor Youth Summit and travelled to Oslo because he found the chance to apply while on the Internet. Without the Internet, he would have never had this opportunity. Such things are more common than we realise, he says.

Wai Yan and Arkar both agree that supervisors and parents should take an active interest in how their kids use the Internet. Some parents are ignorant and think that nothing big can happen to their kids by using the Internet – good or bad. It is important for parents to be curious and encouraging, but also to inform themselves about both the bright side and the dark side of the Internet. Parents should make their kids feel comfortable to talk to them when they encounter unsuitable material on the Internet too.

If parents can guide their kids in a positive way on how to use the Internet, kids will be able to benefit from the Internet more than they ever dreamed, Arkar and Wai Yan say.

So, how do we continue to educate ourselves on safe Internet practices?

The reality is that with the rapidly-changing speed of the Internet, there is no one house of information available to track your kids' online usage. What we can do, however, is continue to keep an open communication with our children to ensure they feel safe in sharing knowledge with us, and to report if something doesn't seem quite right.

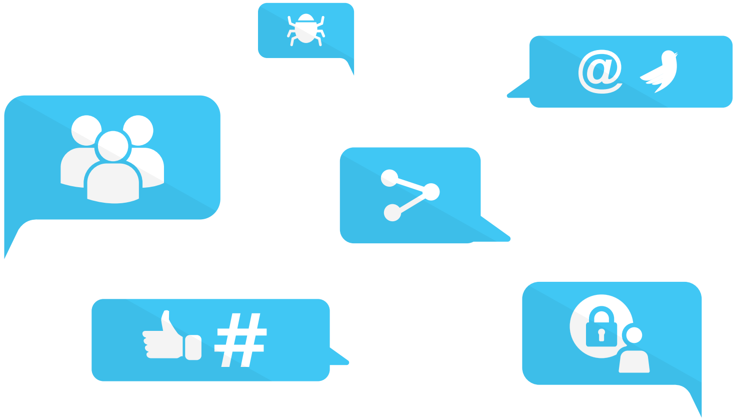
For those who have children kitted out with smartphones, there are apps available for parents who wish to track their children's location, like Life 360, available free on Android and iOS. TimeAway is a free Android tool that enables parents to place blocks, set app limits, track your child's location, and schedule usage time on your child's smartphone. Free app MamaBear on Android and iOS helps parents keep track of social media activity, manage app usage, and geo-locates your child with alerts when they arrive and depart destinations. You can also be alerted when your child adds contacts, uses words that are restricted or uploads and tags images on social media.

The ultimate but high-priced Internet monitoring software is mSpy, available for all devices and computers worldwide. Boasting more than a million users around the globe, mSpy is spyware for your kids, tracking their web history, images, videos, email, SMS, keystrokes and more with a 256 bit encryption. In lieu of this fancy app, good old fashioned conversations and cooperation with your kids to share their devices and their history will work too.

Conclusion

For the millions of first-time users and young children, the Internet opens the doors to fantastic vaults of information and learning... but also to risks of online theft, fraud, bullying, abuse and malware. We're all responsible for making sure our kids are equipped not just with the means to access the Internet, but with the right information to stay safe while learning and communicating on the Internet.

It may seem a bit overwhelming to all of us because our kids today are mostly getting on the Internet with mobile phones – much harder to supervise and monitor all the time. Our kids' safety while being 'online' on their phones is built by the conversations and trust that we have with them. That's how they develop their life skills and grow their resilience in the online world. In combination with everything that we've read in this book, here are a few simple rules to leave you with.



Limit how much time your kids spend online

Give your kids a set amount of free online time to chat, play games or get on social sites, but after that, limit their computer or mobile phone use to homework or productive activities.

Keep talking and learning together with your children

Talk about and ask questions about technology with each other. Communicate openly and try to keep the tone positive and trusting. It's important that your kids know that they can talk to you – about good things and about bad things, like when they make a mistake on the Internet or visit a site that they shouldn't have. It's important that they aren't punished too harshly when they make a mistake because you don't want them to not tell you about it the next time.

Share Internet information and stay close

Have them show you their favourite websites and other Internet services and make sure you have information for any accounts that they have online. Do not allow your kids to share their passwords with anyone else but you. When your kids are on the Internet, try to keep a central area of your home for Internet use only so that your children are at least nearby when they're online.

Find out more about your local resources

In many countries there are help lines that you can contact to report computer or Internet-related incidents such as security problems, offensive content online, and so on. There are also help lines specially to assist children in need of protection or guidance. *(For resources in Malaysia, see page 41 of this publication.)*

The bottom line? Set rules, critique content and openly communicate with your kids. Keeping kids safe means setting guidelines and having critical and non-judgmental discussions about Internet behaviour. If your children feel comfortable with these conversations, they will be more likely to let you know when they run into a problem online – like a bully or a bad website or a questionable online personality. These are some of the keys to a safe and enriching online world.

GLOSSARY & FURTHER READING

Internet vocabulary

Algorithm

Mathematical calculations based on procedural steps to process data and produce systematic reasoning. Example: Facebook's algorithm helps users to discover content that is relevant to the user's preferences and history. The Facebook algorithm also understands how a user likes to 'be' on Facebook to show information relevant to the user.

App

Short for 'application software', and app is a computer program used on mobile devices such as smartphones and tablets. Example: Google Maps is an interactive map app that uses GPS (global positioning system) technology to help users with locations and directions.

Blog

Typically an informal, conversational website or web page authored by an individual or group. Example: suitcasesandstrollers.com, a travel blog written by Singapore mum blogger Aimee Chan.

Chatroom

A place on the Internet that offers immediate, interactive communication with users.

Cyberbullying

Bullying behaviour that occurs online, via chatrooms, social media, and email. Cyberbullying is usually threatening and intimidating, and considered dangerous communication between Internet users.

Embedded media

Media files and players that are included in web pages, such as GIF animation, video clips, and audio players.

Hacker

An Internet user who uses electronic data to gain access to other users' data. Hackers can often gain access to personal information such as bank accounts and user profiles to perform identity theft.

Online predator

Someone who uses the Internet to locate someone in a harmful way, especially someone who uses the Internet to lure children into danger.

Platform

In hardware and software, a framework that enables particular applications to run.

Search engine

A program on the Internet that provides search capabilities for users, usually by keywords and characters, to find information on the World Wide Web.

Selfie

When one takes a photograph of himself or herself, this is called a 'selfie'. Usually, selfies are taken with a user's own smartphone and shared through social media.

Social media

Apps and websites where users interact in social networking on the Internet, with content sharing capabilities. Popular examples are Twitter, LinkedIn, and Facebook.

Social profile

Within social networks, a user's profile is that user's identity, usually containing information about the user's location, name, preferences, marital status, gender, and the like.

Social wall

In social media, a social wall is a section of a user's profile where other users can write messages, share links and photos.

Streaming media

Media, like a video, a song, or even a football game that you watch online, when sent to your computer or mobile phone in a continuous stream of data over the Internet.

Viral

Rapid spreading of information and content through social networks, websites, and email on the Internet.

Virus malware

Dangerous software programs on the Internet that spread rapidly, usually in the form of spyware (software that spies on computers to extract personal data).

VoIP programs

Voice over Internet protocol software (and sometimes hardware) that enables telephone calls by Internet transmission.

Further reading

'5 Ways to Protect Girls from Online Bullying'. SheKnows. 5 Jan. 2012.

'Cyber Bullying Statistics'. BullyingStatistics.org. n.d. Web. 2013.

'Children Online'. AACAP.org. American Academy of Child & Adolescent Psychology. n.d. Web. 2014.

'Children and Video Games: Playing with Violence'. AACAP.org. American Academy of Child & Adolescent Psychology. n.d. Web 2011.

'Cyberbullying & Social Media'. MeganMeierFoundation.org. n.d. Web. 2014.

'Enough is Enough'. InternetSafety101.org. n.d. Web. 2014.

'e-Safety Education'. iSAFE.org. n.d. Web. 2014.

'Facebook Community Standards'. Facebook.com. n.d. Web. 2014.

'Make it Happy: Flood the Internet with Positivity'. DoSomething.org. n.d. Web.

'NetSmartz 411'. Netsmarts411.org. National Center for Missing & Exploited Children. n.d. Web. 2014.

'Online Abuse'. Twitter.com. Twitter.com Support and Help Desk. n.d. Web. 2014.

'Predators 101'. InternetSafety101.org. n.d. Web. 2014.

'Share Aware: Help Your Child Stay Safe on Social Networks'. NSPCC.org.uk. n.d. Web. 2014.

Michele Borba, EdD. SheKnows. *'Bullies in Cyberspace'.* 14 Oct. 2008. Web.

Collier, Anne. *'Social Media Literacy in an App'.* ConnectSafely.org. 16 Jan. 2015. Web.

LeClerc Greer, Katie. *'The Age Old Device Debate'.* iKeepSafe.org. 9 Jun. 2014. Web.

Captain Marlowe. *'Be Aware Before You Share'.* iKeepSafe.org. 10 Dec. 2014. Web.

Martin, Amanda. HoneyKidsAsia. *'Online Safety for Kids'.* 21 Feb. 2014. Web.

McKay, Tiernan. SheKnows. *'Can You Steer Your Kids Away From Facebook?'.* 22 Mar. 2012. Web.

Offenbacher, Taryn. SharedHope.org. '*5 Scary Statistics About Internet Safety'.* 7 Aug. 2013. Web.

Perets, Abbi. SheKnows. *'Cyberbullies'* 5 Jan. 2014. Web.

Prabhu, Trisha. Google Science Fair 2014.*'Rethink: An Effective Way to Prevent Cyberbullying'.* Web.

Useful contacts

Cyber999

Computer security incidents may be reported to Cyber999 via the following ways:

1. Online Form at https://www.mycert.org.my/online_form/index.html
2. Email to cyber999@cybersecurity.my
3. SMS to 15888 using the following format: CYBER999 REPORT (email)(complaint) to 15888. Each SMS will be charged at RM0.15 per message.
4. Phone Call – Office Hours: 1-300-88-2999 / 24x7 (Emergency): +6019 - 266 5850. Calls to MyCERT and the Cyber999 Hotline are monitored during business hours (9:00 AM – 6:00 PM).
5. Cyber999 Mobile Apps on App Store or Google Play

Communications & Multimedia Consumer Forum of Malaysia (www.cfm.org.my)

Report consumer-related issues or problems relating to Internet service providers via:

1. Hotline: 1800-182-222
2. Email to aduan@cfm.org.my
3. Online Complaints Portal (CoP) at www.complaint.cfm.org.my

Communications & Multimedia Content Forum of Malaysia (www.cmcf.my)

Report offensive content such as pornography, violence and inappropriate SMS (containing lies, scams or obscenities) via:

1. Hotline : 1800-882-623
2. Email to secretariat@cmcf.org.my
3. Online Complaints Portal (CoP) at http://www.cmcf.my/online-form-online-content

Malaysian Communication and Multimedia Commission (aduan.skmm.gov.my)

You can lodge a report with MCMC as a last resort.

1. Hotline: 1800-188-030
2. Email to aduanskmm@cmc.gov.my

Childline Malaysia

A national 24-hour hotline for children and adults to call to report abuse, bullying, neglect, etc.

1. Hotline: 15999 (Calls via Digi are free.)
2. Website: http://stopchildabuse.unicef.my/protect_reportAbuse.html

Useful contacts

Protect and Save the Children

Refer issues regarding the protection of children from sexual abuse and exploitation via:

1. Phone: 03-7957 4344
2. Email: protect@psthechildren.org.my

Befrienders

The Befrienders provide confidential befriending 24 hours a day, 7 days a week. Contact them via:

1. Hotlines: 03-7956 8144 & 03-7956 8145 (24 hours a day)
2. Email: sam@befrienders.org.my
3. Or call to make an appointment

WEBSITES

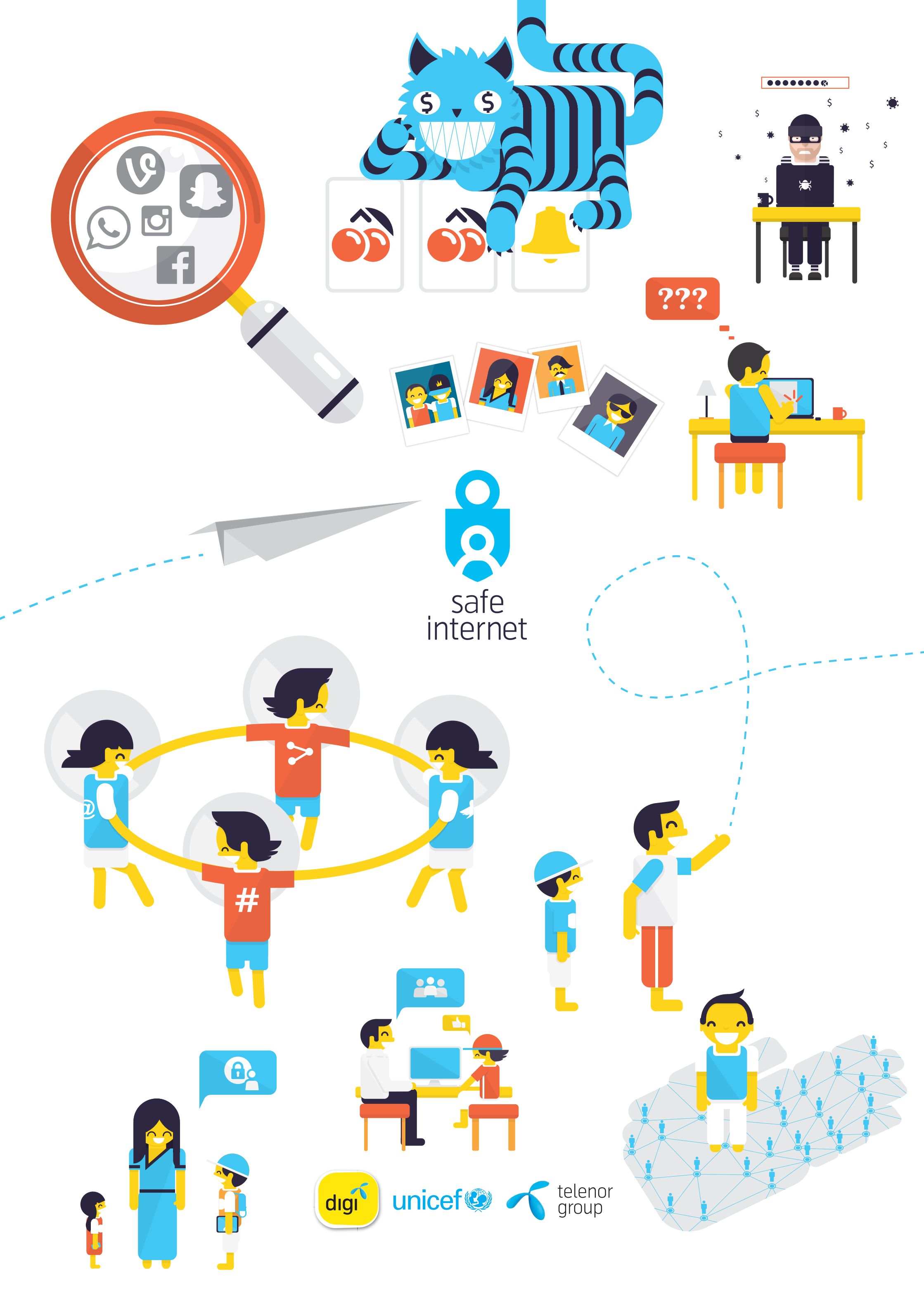
Digi Cybersafe
www.digi.cybersafe.my
www.digi.com.my/digicybersafe

Klik Dengan Bijak
www.klikdenganbijak.my

P.S. the Children
www.psthechildren.org.my

Stop Child Abuse
http://stopchildabuse.unicef.my

UNICEF
www.unicef.org/malaysia



safe
internet

digi unicef telenor group