STAYING SAFE ONLINE

Content

PART 1
1 Preface

PART 2
2 Story of the Boy
14 What Went Wrong?
16 How to stay safe online: The S.M.A.R.T rule
16 - Safe
17 - Meeting
18 - Aware
19 - Reliability
20 - Tell
21 Dangers
21 - Phishing
22 - Scams
23 - Identity theft
24 - Virus
25 - Grooming
26 Values

PART 3
27 How to help your child stay safe online
31 What should you do if your child is a victim of online crimes?
32 How can you play a part as a parent?

PART 4
33 References

Preface

Our digital age has opened a wide array of doors for Internet users, giving us endless areas to explore. While there are merits to the Internet, such as easy access to information, one needs to exercise caution and responsibility when browsing the net. The Internet has made many users, especially children, vulnerable in ways that they were never before. From the more evident pop-up advertisements and phishing sites to the discreet catfishing on messaging platforms, there are many ways that one may encounter danger.

In this new digital era, it is important for us to educate children about the dangers of the Internet and how to stay safe online. This will help them to navigate their way out of online dangers while fully enjoying the benefits of the Internet.

But how much do children really understand about the dangers of the Internet? Perhaps many parents have given their children countless reminders to stay safe online, but before children can effectively practise what their parents preach, they need to first truly understand why they should. And that is due to one simple reason — the Internet is far from a safe haven.

All of us leave behind a trail of digital footprints. While small pieces of information may seem harmless, the accumulation of such information can potentially endanger us. What children need to understand is that their information can easily fall into the wrong hands and be misused by online criminals. Without truly understanding this danger, it is unlikely that children will consciously and regularly practise safe online habits.

Hence, in this book, Project Bluetick hopes to reveal the dangers of the Internet and empower all to consistently remain vigilant online.

Story of the Boy

A few hours later...

My favourite game? hmm I think it's BACMAN!

OMG same! wow, we are soooo alike! so cool haha!

Btw when will the results of the lucky draw be released?

Soon...I think a few days? just be patient!

A few days later...

Hey... I had a really bad day at school today... Can I rant to you?

Oh no :(Yeah sure! I'm always here if you need to talk.

Thanks man :)

So what happened was that

(6 Feb, 7:34 PM)

Have you had dinner?

Yeah, you?

(9 Feb, 2:11 PM)

Hey, what's up?

Nothing much, I'm just chilling.

(10 Feb 9:09 AM)

Did your Mum nag at you again today?

OMG yeah she did...

(13 Feb, 4:52 PM)

I think I passed by your school today! It looks really fancy.

So Ryan waited, and waited, and waited. And he also started growing closer and closer, beginning to confide in his new found online friend, @jameslee03...

I honestly don't get why ur parents are so strict about getting an arcadia switch... mine are cool with it....

Ya I know right! They think I'm gonna neglect my studies and game 24/7 :(

Ur parents sound so unreasonable!! why can't they just trust you... I feel bad that you have parents that don't understand you :(

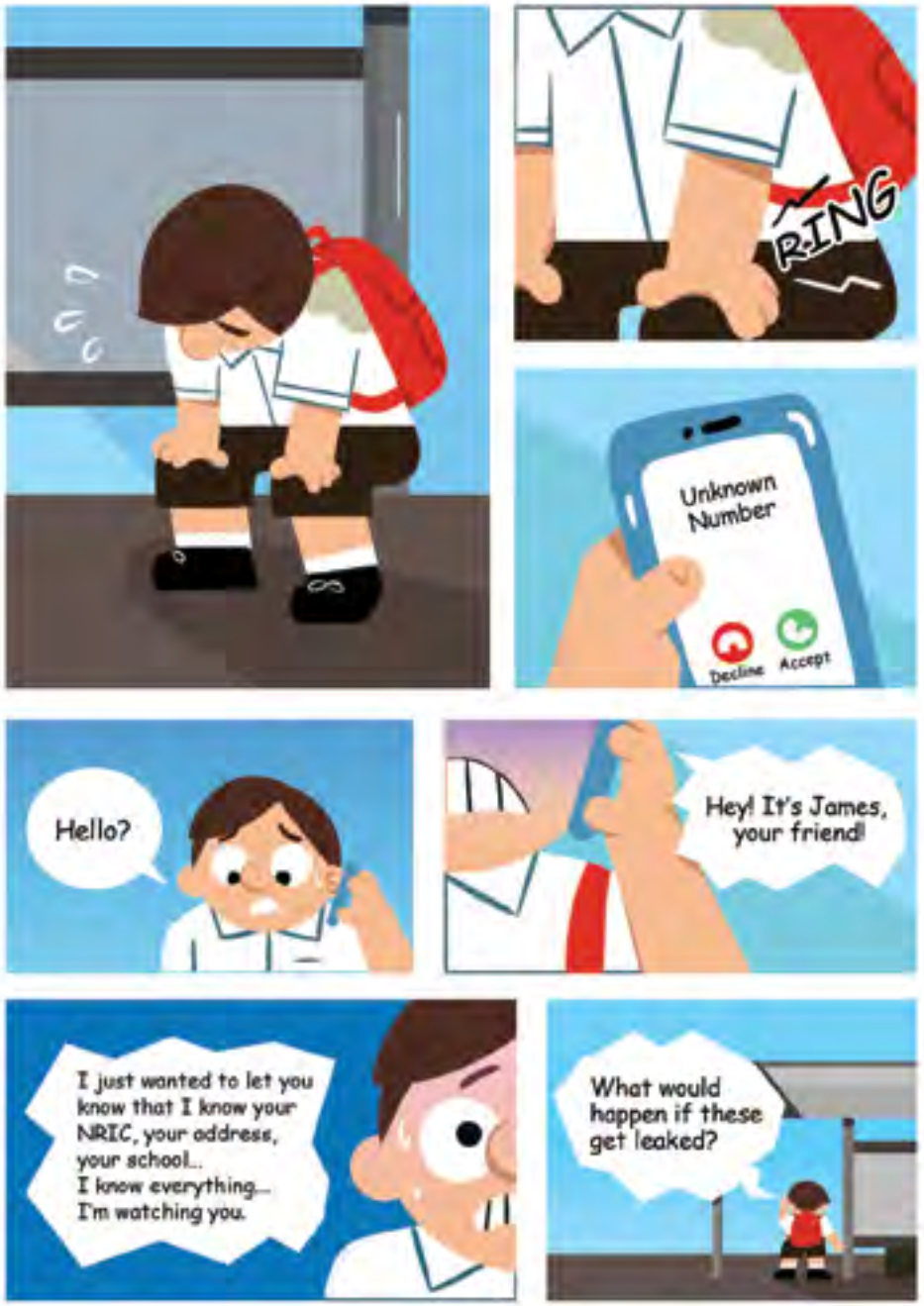
Ugh yea :(thanks for listening to me rant...i'm glad I have you as a friend :D

No problem! I'm here for u bro :)

@jameslee03:
Active now
Oh ya! I just remembered... do you know when the lucky draw results will be out?
Probably in a few more days! don't worry man, just be patient :)
After three weeks...
9: 38
Sunday, 27 January
Arcadia Switch
Dear Ryan,
Congratulations! You have won...
OMG DUDE I won the lucky draw. Thank you for sending me the link. I can't believe it...
YAY I'M SO HAPPY FOR YOU!!! NOW WE CAN PLAY GAMES ON THE SWITCH TOGETHER!!!
I know the host of the lucky draw so I can help u get the game and pass it to you tomorrow or something!
Do you want to meet up at George Park after school? around 3pm?
Sure! thanks bro! let's hang afterwards :D I can't wait to see you in real life!
Me too! I'm excited!!

George Park
3: 10
Monday, 28 January
I wonder where James is?
There aren't any photos of him on his Quickgram page so I don't know how he looks like. But he mentioned before that he's around my age!
Hi Ryan!
Um, who are you? How do you know my name?
Oh, I'm James! Your friend from Quickgram!
What?!
You're.....you're not James! Besides, where's my Arcadia Switch?

Oh, for some reason I didn't receive the game. I'm sorry... but you'll still stay and chat with me right?
NO WAY! YOU LIAR!
Come on! We're still friends, aren't we? I thought we had a special connection!


RING
Unknown Number
Decline
Accept
Hello?
Hey! It's James, your friend!
I just wanted to let you know that I know your NRIC, your address, your school... I know everything... I'm watching you.
What would happen if these get leaked?

Fishing for information about the child

Now that there is a potential victim, groomers need to know more about the potential victim.

Instead of asking for information directly which would raise alarms in the victim, groomers will gently fish for information like age, name, location, school, etc.

Establishing trust with the child

How do groomers establish trust so quickly with their victim? Simple. They are quick to identify similarities in interests, experience, possessions, even illness, to say, "Look, we are so alike. No wonder we click. We are best buddies." That helps to draw their victim closer to them.

Threatening to spill the beans

Grooming is a psychological game. After establishing that the victim is completely isolated and dependent on the groomers, they would then threaten, either seriously or jokingly, to tell the secret to their victim's parents. Out of fear, their victim will toe the line and play by their rules.

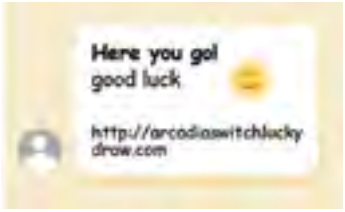
Ryan, what is going on? You can tell us... are you being groomed?
I... I'm fine! Everything's okay!
Please, son.
I know when you're lying son...it's okay, you can tell me anything.
You know we'll stick by you no matter what right?
We are here for you.
I...I... I'm so sorry...

Why don't we start from the beginning? You can tell us everything.
We will get through this together.
Together, Ryan and his parents went over the details of his experience and reported it to the police.
Months later
42-year old woman convicted of identity theft, scamming, and grooming of a minor, amongst other cyber crimes
Teens create awareness videos with fictitious story to educate public: tinyurl.com/pbtwebseries
The End
*Project Lipstick has also created a webseries in the perspective of a girl being groomed and falling prey to an online 'predator'. Visit tinyurl.com/pbtwebseries to watch it!

What Went Wrong?

1. Ryan shared too much personal information: country, age, school, pictures of self, friends, and family. He also allowed strangers to follow his account ("Will follow back").

2. Ryan talked to a stranger online and clicked on a link sent by "James" without much thought.



3. Ryan filled in his personal information on a suspicious lucky draw website (website had many advertisements and promised process to be free).

4. "James" constantly asked Ryan seemingly harmless questions about his personal life so as to accumulate more information about him.

5. "James" tried to drive a wedge between Ryan and his family by constantly criticising them. Doing so also encouraged Ryan to trust "James" instead of his family.

6. Ryan agreed to meet up with "James" in real life without considering the dangers of it.

How to stay safe online: The S.M.A.R.T. rule

S.M.A.R.T. — SAFE

Be careful about the amount of personal information you reveal to strangers as well as on your own online profile, such as:

1. Name
2. Email
3. Phone number
4. Home address
5. Details of friends and family members
6. Schedules
7. School

And any other information that may possibly be harmful.

Such information given out may not seem to be able to do much harm, but the accumulation of them can be dangerous.

S.M.A.R.T. — MEETING

: Meeting someone you have only (just) met online can be dangerous. However, if you really want to do so, we advise you to bring along a trusted adult, and never a friend. If unable to do so, do inform your parent/guardian of the time and place of the meeting and who you are meeting with.

S.M.A.R.T. — AWARE

Never accept and open emails, direct messages or files from people you do not know or trust as they can be very dangerous and may contain viruses or nasty messages.

S.M.A.R.T. — RELIABILITY

Not everything that is portrayed online is what it actually is. Always be on guard and remain careful when conversing with people you do not know.

A lot of information on the Internet can be untrue - always be extra careful if you see things that are too good to be true.

S.M.A.R.T. — TELL

It is important that the moment your conversation with someone online makes you uncomfortable or worried, you should not hesitate to inform a parent or a trusted adult to prevent the situation from getting worse.

Internet Dangers

DANGER: Phishing

Definition:

Phishing is a method cyber criminals use to illegally obtain your personal and financial information (such as your login details, and your parents' bank account numbers and credit card numbers).

Dangers:

After cyber criminals steal your sensitive information, they may use it against you. For example, they may use your parents' credit card details to purchase goods online.

Red Flags:

- The website is not secure. Its URL does not begin with "https" and there is no closed lock icon near the address bar.
- The website requests for confidential information. Most organisations will never ask for your personal information to be sent over the Internet, such as your NRIC, address, birthday and phone number. If you receive a message asking for your personal information, clarify with your parents before providing the information.
- The link is not what it appears to be. The cyber criminal may use a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n'.

DANGER: Scams

Definition:

Scams are dishonest activities that take money or other goods from an unsuspecting person. Online scams are more concerned with stealing money, property and information.

Dangers:

People with ill intentions can use information you provide when they are attempting to scam you. They may sell your information to others or use your parent's credit card.

Red Flags:

- You do not know the sender of the email and the email has links or attachments (most commonly .exe files)
- Email subject and contents do not match
- Email contains request for you to forward the message to more people, sometimes offering money for you to do so
- Emails or advertisements contain urgent offers (e.g. "Buy NOW") or offers that are too good to be true (e.g. "You just won an iPhone from a lucky draw!")

Scams can seem genuine at first because scammers can pose as people you know, such as family members or friends. However, you must remain vigilant and ensure that you do not click on any link or attachment that will enable scammers to have access to your information. If you are unsure, ask your parents to help you check the source of the email and ask the sender if they actually sent the email to you.

DANGER: Identity Theft

Definition:

Identity theft is when someone "steals" your name and personal information in order to commit crimes such as taking over your accounts or buying things online.

Dangers:

You could be mistaken for committing crimes and be held accountable for paying for things that you did not buy.

Red Flags:

- Seeing your name or your photo in accounts that do not belong to you is an indication that someone else is using your name and pretending to be you.
- Receiving summons/letters/warnings/charges for things that you did not do/buy. This shows that someone else is making use of your account to do/buy things.

DANGER: Virus

Definition:

Viruses are softwares that copy and paste its own codes into the computer programs, causing the programs to become corrupted or become unusable.

Dangers:

It can steal information about your activity on your computer, which can potentially be used against you.

Red Flags:

- If many people received the same email from you after you have clicked on a link, your computer would very likely have been infected.
- In many cases, viruses cause a decrease in performance of the device you are using. For example, your computer may load much slower than normal due to viruses in it.
- If your files/applications suddenly begin to crash very often or can no longer be opened, it is also likely that it was corrupted by the virus (the virus inserts its own code between the files or applications, preventing them from functioning normally).

DANGER: Grooming

Definition:

Sexual grooming is an action taken by an adult to form a trusting relationship with a child — through acts of friendship and emotional support — with the intent of later establishing sexual contact with the child. The adult manipulates the child into a situation where the child may be more readily abused and simultaneously less likely to disclose. This action may be performed either online or offline, and in most cases, both.

Dangers:

Groomers may attempt to manipulate and brainwash you with words or gifts in order to gain your fullest trust. Groomers may even try to isolate you from your friends and families so that you will fully depend on them. If the situation escalates, the groomer may even be able to convince or coerce you into doing activities that may harm you, and use threats or charms to ensure that you do not leave the relationship.

Red Flags:

- When someone online appears to be particularly interested in your personal information and fishes for it in bite-sized pieces in ways that appears unsuspecting. These include your everyday schedule, interests, places you like to frequent and so on. This person may want to learn more information from you so as to piece together a more complete profile in order to build a stronger relationship with you to take advantage of you, or even to stalk and observe you.
- People you meet online who use flattery too often with you, give you gifts for no particular reason, express excessive sympathy, use intimidation to control you, or give sudden declarations of devotion and love. They may be trying to establish control and power over you.
- Someone who makes you feel pressured to do something, even though you are not fully comfortable with it. This person may have harmful intentions.

Values

1. Responsibility:
   We must always be responsible when uploading or posting any information online since this information can be used against you. It is up to you to take charge of your actions and stay safe online.

2. Respect:
   Always respect yourselves and others. If someone online is making you uncomfortable, do not be afraid to block them. However, be careful not to be rude when speaking to others because there is a real person behind every online account. You could hurt their feelings if you are not careful with your words and actions.

3. Supportive:
   Remember to look out for one another and help someone if you think they need some support. Never feel ashamed or shy to ask for help when needed.

4. Alert:
   Stay alert online and be discerning. It is important to be able to pick up red flags when using the Internet to prevent becoming a victim of online crimes.

5. Stay updated:
   Ensure that your computer and antivirus software is always updated such that people with harmful intentions are unable to use your information. You can remind your parents to help you check your software if you do not know how to. Also, remember to stay updated by being informed of the latest online scams — you can ask your parents about this too.

Remember that you play the most important part in taking responsibility for your own safety and behaviours. But at the same time, remember that if someone does hack into your accounts, use your information maliciously or otherwise harm you online, you should not blame yourself. The fault lies on the shoulders of the perpetrator, not yours. You did not ask to be targeted.

How will you protect yourself online? You can continue to discuss this question with your parents or your peers!

How to help your child stay safe online

If a child is being groomed they may:

- Be very secretive, including about where they are going and what they are doing
- Go to unusual places to meet friends
- Have new things that they cannot or will not explain
- Become very withdrawn and anxious
- Receive messages such as:
  - You are the love of my life
  - I feel sorry that your parents do not seem to understand you
  - You can tell me anything, you know
  - If you don't do what I want, I'll do something bad to you/to myself

* Please note that this list is not exhaustive and the individual descriptive behaviour is not to be taken in isolation.

How to help your child stay safe online

1 Change your computer settings

- To prevent or minimise attack by viruses, ensure that your home computer has the firewall turned on. This will prevent unauthorised applications, programs and services from accepting incoming connections. Remember to disable downloads from the Internet from untrusted websites. This can be done in system preferences using a Macbook, or the Internet options in the control panel for a Windows computer.
- Download anti-virus software in computers.
- For your child to be safe from scams, help your child download softwares or extensions that block advertisements. These can be found on the Chrome Web Store, Internet Explorer and Safari. These softwares ensure that scam adverts and all untrusted websites will be blocked.
- Keep your computer software up to date to ensure that all the bugs are fixed and cannot be exploited by hackers to get your information.
- Adjust any parental controls in system preferences to ensure that your child cannot venture to any unauthorised websites.

2 Keep an eye on your children

Place the computer in a family area of the home (such as the living room, rather than their bedroom). This way, you can monitor your child's Internet activities and what he posts online and who he is in contact with (so that you'll know if your child starts receiving inappropriate messages from an online predator or his/her peers)

- Not allowing your child to have his/her own computer, but rather allowing him to use a shared family computer, which he is not permitted to modify or upload data onto without your permission. This way, you can monitor and manage your child's Internet activities (an Internet content filter is most

useful in this area, as it will enable you to restrict what content is viewed and downloaded) even after he has logged off from the computer, and you can also more easily manage the amount of time he spends online.

- For younger children, consider not availing the password for downloads of apps as that will prevent the unfettered installation of apps. For teenagers, ensure that your child has a strong password with at least one number, symbol and capital letter, such that others with malicious intent cannot easily retrieve their personal information.
- Curate the apps or mobile applications to ensure that it does not contain unsavoury or age-inappropriate content.

3 Constantly remind your children about staying safe online

- Remind your children not to use open Wi-Fi, especially at cafes, airports and public spaces in general. They should only use the Wi-Fi if there is a password and is encrypted. This will ensure that your data cannot be used by any trained malicious individuals.
- Remind your children not to open any links or attachments in emails without knowing what they could be and ensuring that the website or programme is safe. Discretion must always be observed, even if the email is sent by a friend or family member as hackers sometimes pose as others when sending out viruses.
- Remind your child about the importance of online discernment- that not everything they see or read on the Internet is true. You could educate them about the importance of applying critical thinking and analysis to find out whether the information is true or whether the source is reliable. Many emails or websites claim that we have won prizes and use the information we provide to exploit netizens.
- Remind your child to review their privacy and security settings on social media such as Facebook or Instagram. Make sure that their account is private such that strangers on the Internet cannot access anything they share, and teach them not to accept friend requests from people they do not know.
- Remind your children never to give out too much personal information online such as their full name, address, phone number, birthdate, school and schedules. In the digital age, we are prone to sharing details from our lives online but we should only do so with people we are comfortable with, and never with a stranger we have just met online.

- Educate your child on the common red flags of cyber crimes. For instance, red flags that indicate a message is a scam include:
  a. Spelling errors and poor grammar in the message
  b. Feigned sense of urgency (e.g. your account will be deleted in 24 hours)
  c. Sender's email address is spoofed
- Remind your children that safety is a right and a responsibility. They do not have to subject themselves to disrespectful language, images and/or behaviours online. At the same time, they should exercise care in the use of mobile device messaging – once sent, the message cannot be clawed back. This is especially because of how contexts of a message can be misread or misinterpreted.

4 Most importantly, be good role models

- Actions speak louder than words. The example set by parents for their children through their actions is very important. This is because young children often follow in their parents' footsteps, and of course, if parents do not practice what they preach, then it would not appeal to the children to heed their advice. Hence, it is crucial that parents lead by example for their children to learn and follow, so that children can effectively cultivate safe online habits from a young age.
- Inculcation of positive values at home is also important. Such values include respect and responsibility for self and others. We need to educate our young to take ownership of their own safety whether it is online or offline.
- Reduce screen time habits to include other activities like cycling, going for outings or other interests to create more parent-child bonding time.
- Speak to your children about this topic, and help cultivate an environment that encourages your children to confide in you should such they fall victim to such crimes.

What should you do if your child is a victim of online crimes?

If your child is a victim of cyber crimes, take legal action:

- Do not delete the email or data evidence from the computer.
- Note down the date/time of the crime that happened.
- Keep a log of all online sessions or print them out.
- If this is a phishing case, save any email your child may have received
- Seek the police's assistance immediately at the nearest Neighbourhood Police Centre

Should your child require assistance, you may wish to reach out to organisations that can provide help regarding cyber wellness issues, such as TOUCH Cyber Wellness, Help123 or Fei Yue Community Services.

Organisations that can offer help

* TOUCH Cyber Wellness – for help on a range of cyber wellness issues
  Phone: 1800 377 2252 | Email: cyberwellness@touch.org.sg

* Fei Yue Community Services – for practical and emotional guidance for youth
  Phone: 6422 1599 | Email: project180@fycs.org
  Offers online counselling services for secondary school aged children:
  www.ec2.sg

* Help123 – hotline for youth cyber wellness issues
  Phone: 1800 6123 123 | Email: hello@help123.sg

* Tinkle Friend – hotline for primary-school aged children
  Phone: 1800 2744 788

* AWARE's SACC (Sexual Assault Crisis Centre) – for counselling, legal advice for sexual harassment and assault, and assistance in courts and police cases
  Phone: 6779 0282 | Email: sacc@aware.org.sg

How can you help other parents?

Other than educating your children on the dangers of the Internet and how to stay safe online, you can also play a part by passing this knowledge on to other parents. To cultivate a safer online community, it is paramount for this message to be as widespread as possible. If everyone plays their part by practising safer online habits, there will be a decrease in cyber crimes in time to come.

References

* 12 Tips to Proactively Protect Your Identity. (n.d.). Retrieved January 15, 2019, from https://www.amfam.com/resources/articles/money-matters/identity-protection
* Athow, D. (2019, January 02). The best antivirus software of 2019. Retrieved January 15, 2019, from https://www.itproportal.com/guides/the-best-antivirus-software/
* Australian Competition and Consumer Commission. (2018, May 08). Protect yourself from scams. Retrieved January 15, 2019, from https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams
* Australian Competition and Consumer Commission. (2018, January 04). Online shopping scams. Retrieved January 15, 2019, from https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams
* Benton, B. (2018, December 21). Infected! 10 Tips How To Prevent Malware On Your Computer. Retrieved January 15, 2019, from https://www.autodesk.com/redshift/10-tips-on-how-to-prevent-malware-from-infecting-your-computer/
* Bolton, N. (2019, January 10). List of the Effects of Computer Viruses. Retrieved January 15, 2019, from https://itstillworks.com/list-effects-computer-viruses-2857.html
* Collier, A. (n.d.). SafeKids.com. Retrieved January 15, 2019, from http://www.safekids.com/how-to-recognize-grooming-2/
* Cyber Tip - Spot Signs Of Phishing. (2018, April 23). Retrieved January 15, 2019, from https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/spot-signs-of-phishing
* Doell, L. (2013, January 18). 8 Tips to Protect Your Computer From Viruses and Malware. Retrieved January 15, 2019, from https://www.moneytalksnews.com/8-ways-to-protect-your-computer-from-scams-and-viruses/
* Keeping our Children Safe on the Internet. (2017, June 1). Retrieved January 15, 2019, from https://www.csa.gov.sg/gosafeonline/go-safe-for-me/for-parents/children-and-the-internet-keeping-our-kids-safe
* KIDSMART. (n.d.). Retrieved January 15, 2019, from http://www.kidsmart.org.uk/beingsmart/

* KnowBe4. (n.d.). 10 Ways To Avoid Phishing Scams. Retrieved January 15, 2019, from http://www.phishing.org/10-ways-to-avoid-phishing-scams
* KnowBe4. (n.d.). What Is Phishing? Retrieved January 15, 2019, from http://www.phishing.org/what-is-phishing
* Lab, K. (2015, July 8). Security tips for kids: Beware of viruses. Retrieved January 15, 2019, from https://www.kaspersky.com/blog/security-tips-for-kids-1/9271/
* Let's Fight Scams. (n.d.). Retrieved January 15, 2019, from https://www.scamalert.sg/
* M. (2018, September 27). Get help. Retrieved July 18, 2019, from https://www.betterinternet.sg/Resources/Get-Help"
* Need help? (n.d.). Retrieved January 15, 2019, from https://www.pandasecurity.com/usa/support/card?id=1679
* NSPCC. (n.d.). Grooming. Retrieved January 15, 2019, from https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/
* Rubenking, N. J. (2018, November 06). The Best Antivirus Protection of 2018. Retrieved January 15, 2019, from https://sea.pcmag.com/antivirus/22/the-best-antivirus-protection
* Singapore Police Force. (2010, August 25). Retrieved January 15, 2019, from https://www.facebook.com/singaporepoliceforce/posts/cybercrime-what-should-you-do-if-you-become-a-victim-what-are-some-measures-you-/152761494740918/
* Spam & Scam email. (n.d.). Retrieved January 15, 2019, from https://www.getsafeonline.org/protecting-yourself/spam-and-scam-email/
* Viruses & Spyware. (n.d.). Retrieved January 15, 2019, from https://www.getsafeonline.org/protecting-yourself/viruses-and-spyware/
* Welner, M., Dr. (2010, October 18). Child Sexual Abuse: 6 Stages of Grooming. Retrieved from http://www.oprah.com/oprahshow/child-sexual-abuse-6-stages-of-grooming/all
* Whitwam, R. (2017, May 03). Android Antivirus Apps Are Useless - Here's What to Do Instead. Retrieved January 15, 2019, from https://www.extremetech.com/computing/104827-android-antivirus-apps-are-useless-heres-what-to-do-instead

Staying Safe Online
Print edition: ISBN 978-981-14-2433-5
E-book edition: ISBN 978-981-14-2617-9
© Raffles Girls' School, 2019

Published by
Raffles Girls' School
20, Anderson Road
Singapore 259978

All rights reserved.

Layout and production by Word Image Pte Ltd
28 Sin Ming Lane #06-131 Midview City
Singapore 573972

Acknowledgements

This book is written by Project Bluetick (2019), comprising of Natasha, Thet Thet, Rou Yi and Regin. We sincerely hope that the book will be able to help educate the public on the dangers of the Internet and the importance of safer online habits. Through this, we hope to bring about a safer online community.

This book is a culmination of four years of hard work by not just the four of us, but also the remaining members of our original eight-member team. We would like to thank Kyu Min, Chia Ying, Nadine and Sun Ru for being part of this cause and for playing a part in making this book possible.

In writing this book, we would like to acknowledge and thank some important figures for their indispensable role in this journey.

Firstly, we would like to thank our illustrator, Ms Vivien Tan, for creating beautiful visuals for our book; Guidance Branch officers from the Ministry of Education, Ms Jenny Chua and Mdm Serene Tan; our principals Mrs Poh Mun See and Ms May Tan from Raffles Girls' School (Secondary); and our publisher, Word Image. This book was also written with support from the Media Literacy Council under the 2nd Better Internet Call-for-Proposal.

Last but not least, we would like to thank our mentors both past and present – Ms Norhuda, Mr Lim Shi Zhi and Mrs Marie Huang. We would like to take this opportunity to thank them for believing in us when we started this project, and for their endless guidance through this arduous (but very fulfilling) journey. Without their unwavering support for us, this would never have been possible.

Project Bluetick is actualised by a group of four students originally from Raffles Girls' School (Secondary). We have been working on increasing teenagers' capacities to practise safer online habits since 2016, primarily through conducting talks with students and parents, and creating and distributing educational materials.

We began working on this book as part of our aim to spread internet safety and improve online habits among youths in Singapore. This book serves both as a guide to help parents play a bigger role in ensuring their child's online safety, and as a child-friendly comic meant to aid children's understanding of the potential dangers online. Through this, we hope that parents and children will develop a more comprehensive understanding of online dangers. Overall, we hope that this will help children remain vigilant and responsible for their online actions, and be better equipped to protect themselves online.

If you would like to find out more about Project Bluetick and make use of materials that have been created throughout the course of our advocacy so far, do check out our website projectbluetick.weebly.com and follow our group on Instagram and Twitter @projectbluetick!

This book is written and produced by Raffles Girls' School (Secondary)

RAFFLES GIRLS'SCHOOL

with the kind support of Media Literacy Council.

MEDIA LITERACY COUNCIL

ISBN 978-981-14-2433-5

WORD IMAGE