

HOW YOU CAN PLAY AN ACTIVE ROLE IN KEEPING YOUR CHILDREN SAFE ONLINE

– AN ARTICLE BY CYBER SECURITY AGENCY OF SINGAPORE (CSA)

Did you know that a 2020 study from Google revealed that children in Singapore tend to overshare information about themselves on social media?

KEY FINDINGS FROM THE GOOGLE STUDY¹

- **42 per cent** of the respondents surveyed said that their children had **overshared information** such as personal data, compared with 31 per cent in 2019
- Around 35 per cent said their children had received unwanted attention from strangers online, **14 per cent reported that their children had encountered scams** and 12 per cent shared that their children had experienced being hacked.

While the Internet offers an entertaining and educational experience for children, there are some common unsafe practices that can leave them susceptible to dangers online, such as:

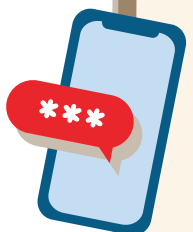
1. Oversharing personal information on social media, which could lead to privacy issues as the information could be inappropriately used eg. passwords used to hack into accounts for social media impersonation.
2. Clicking on suspicious links on websites and emails, which could result in children falling victim to phishing scams.
3. Downloading games or apps from unofficial sources which could lead to devices being infected with malicious software.
4. Setting weak passwords for online accounts which could result in hacked accounts.
5. Performing online transactions using unsecured Wi-Fi networks which could lead to information theft.

CHILDREN ARE SPENDING MORE TIME ONLINE

Findings² revealed that Singaporeans, including children, spent more time online due to the pandemic – with an average of 3.6 hours daily pre-pandemic to about 4.1 hours post-pandemic. The study also found that as children had to switch to home-based learning due to the pandemic, the house rules to access the Internet for educational, social and entertainment purposes were relaxed.

¹ More than half of S'pore children encountered inappropriate content in 2020: Google
<https://www.todayonline.com/singapore/more-half-spore-children-encountered-inappropriate-content-2020-google>

² Google Survey: Rising concerns about children's online wellbeing amid increased encounters of cyber threats in 2020
<https://www.betterinternet.sg/-/media/Research/Google-2020-COVID-Survey/Media-Release-Google-Survey-Rising-concerns-about-childrens-online-wellbeing-amid-increased-encount.pdf>



CHILDREN CAN BE VULNERABLE TO ONLINE DANGERS

With children in Singapore being among the youngest in the world to go online³, they can be more susceptible to online dangers. As such, it becomes even more important to keep our children safe in the age of the Internet. **Christopher Anthony**, Deputy Director from the Critical Information Infrastructure Division at **CSA**, shares what he did when his 15-year-old daughter received a phishing message and dishes out tips on how he keeps his daughter safe online.

Q: WHAT DID YOU DO WHEN YOUR DAUGHTER ENCOUNTERED A PHISHING EMAIL?

A: My daughter received a phishing message on WhatsApp purportedly from Amazon which requested her to log in to a given link to change the delivery date and time, failing which the item which she purportedly had bought would be delayed in delivery. My daughter's immediate reaction was one of puzzlement because she did not make any purchase from Amazon and hence was not expecting a delivery. She informed me about the WhatsApp message, and I advised her to delete it immediately. I also affirmed her correct reaction not to immediately act on the instructions.

Q: WHAT ARE THE STEPS YOU TAKE TO ENSURE YOUR DAUGHTER STAYS SAFE ONLINE?

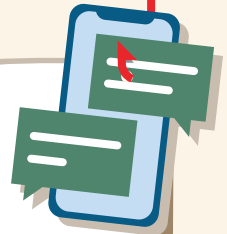
A: Firstly, I ensure that all the devices used at home are **installed with anti-virus software** and that **automatic updates are turned on**. I have not installed any parental controls on my daughter's laptop because I feel that it is important to teach her about online dangers and how she can keep herself safe online.

I have shared with my daughter that free public Wi-Fi is not always safe and that she needs to exercise caution when she connects to public Wi-Fi.

My daughter is also able to identify the signs of a phishing email just like in the case of the phishing message she received on WhatsApp, and she does not click on strange links. I have also taught my daughter not to pick up calls from unknown numbers and delete spam emails without even looking at them. It is **very important for parents to teach their children how to be safe online as it will go a long way in changing the way they navigate the Internet**.

Q: WHAT CAN YOU DO WHEN YOUR CHILD HAS UNKNOWINGLY DOWNLOADED MALICIOUS SOFTWARE?

A: The first thing that parents should do is to check with their child if he or she had shared any personal information like login credentials to their online accounts or their banking details. If the child had shared such information on websites, then the next step parents should take is to immediately notify the bank, change all their passwords and thereafter scan their devices with an anti-virus software to detect and remove any unauthorised installations or malware residing in their devices.





Q: HOW IMPORTANT IS IT FOR PARENTS TO HAVE AN OPEN AND HONEST CONVERSATION WITH THEIR CHILDREN?

A: It is **important for parents to show their child that they are able to abide by the rules that they have established for their children as children tend to follow what they see instead of what they are told.** For example, parents should not download apps from unofficial sources. Also, parents should explain to their children that at times they may be tempted to click on a phishing link thinking that there are good deals available. If something sounds too good to be true, it usually is. Parents should encourage their children not to be afraid to tell the truth and to confide in them. **By starting a conversation with your child early and having open and honest conversations, you can help your child develop a strong foundation to use the Internet safely and responsibly.** For most of us, our parents did not teach us about cybersecurity because it is a concept unfamiliar to them. As parents, we are not digital natives either, so we need to equip ourselves with the latest cyber hygiene practices because the dangers in cyberspace evolve very quickly. And we need to impart this knowledge to our children to keep them safe from cyber criminals.



³ <https://www.todayonline.com/singapore/sporean-children-get-first-internet-device-age-8-among-youngest-worldwide-google>

USEFUL RESOURCES

CSA has produced a series of videos titled 'Get Cyber Safe' which follows the adventures of two siblings, Kayden and Kayla as they navigate dangers in cyberspace. You can use these videos to educate your children on how they can protect themselves with good cyber hygiene practices.



Episode 1

<https://youtu.be/KvD0RNHUbos>



Episode 2

<https://youtu.be/W30Z7F83RBk>



Episode 3

<https://youtu.be/gEb6q6cM7kk>

OTHER USEFUL RESOURCES



Useful resources for students

<https://www.csa.gov.sg/Programmes/sq-cyber-safe-students/about-sq-cyber-safe-students>



Useful articles for parents

<https://www.csa.gov.sg/gosafeonline/Go-Safe-For-Me/For-Parents>



Visit Scam Alert website

(www.scamalert.sg) for information on scams