WHAT IF MY CHILD FALLS PREY TO A SCAM?

With technology advancements, children are increasingly using the Internet for learning and entertainment purposes, making them more vulnerable to cyber threats.

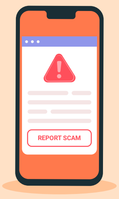
The 2023 Child Online Safety Index[1] reported that 67% of children aged 8 to 18 face at least one cyber risk, which include gaming addiction, cyberbullying, and encountering strangers online. Children may be tricked into sharing their personal information or unwittingly granting access to their online accounts, thereby becoming scam victims.

1. A worldwide index by international think-tank DQ Institute.

IF YOUR CHILD IS A VICTIM OF A PHISHING SCAM

1. Find Out More Information from Your Child

Remain calm and ask your child to recount the events. Help your child understand what made him/her fall prey to the scam.



2. Alert the Authorities

If your child has given away their personal information or lost access to an account linked to your credit card, monitor your online accounts for any suspicious activity. If you spot any unauthorised transactions, contact your bank immediately to block these transactions and file a police report.

3. Secure Accounts by Changing Your Passwords

Change the passwords for affected accounts immediately. Set a strong passphrase that is at least 12 characters long, with a mix of letters, numbers and symbols. For additional security, enable Two-Factor Authentication (2FA).

4. Run a Security Scan

Installing an anti-virus app can help to remove malware and block access to spam messages and unsafe websites. Report any suspicious activities to the Police and SingCERT.

YOUR ROLE AS A PARENT IN GUIDING YOUR CHILD TO BE CYBER SAFE

No parent would want their child to become a scam victim. Thus, it is important to take precautionary measures to protect your child from online dangers.

1. Guide Your Child to be Cyber Safe

Use CSA's four cyber tips to guide your child to be cyber safe!

1. Ensure your child uses strong passphrases and enables 2FA
2. Teach your child how to spot signs of phishing
3. Remind your child to update software promptly
4. Help your child to install ScamShield and anti-virus apps to protect their devices

2. Empower Your Child to be Safe Online

It is important to model good Internet habits for your child. Remind him/her to seek permission when downloading new applications and to refrain from sharing any personal information with strangers whom he/she met online. Warn your child about the potential dangers online and remind your child to practise the tips to be cyber safe.

CSA SINGAPORE
Cyber Security Agency of Singapore

Visit our website for more tips to keep your child cyber safe!
www.csa.gov.sg/information-for/parents-educators