Article
53

សុវត្ថិភាពកុមារលើប្រព័ន្ធអនឡាញ

ហានិភ័យដែលកើតឡើងលើកុមារតាមប្រព័ន្ធអ៊ីនធឺណិត គឺជាបញ្ហាប្រឈមសកលមួយ ដែលទាមទារវិធីសាស្ត្ររួម និងការឆ្លើយតបជាសកលក្នុងកិច្ចសហប្រតិបត្តិការអន្តរជាតិ និងការសម្របសម្រួលថ្នាក់ជាតិ ដើម្បីការពារកុមារពីហានិភ័យតាមអ៊ីនធឺណិត និងគ្រោះថ្នាក់ដែលអាចកើតមាន ព្រមទាំងផ្តល់សិទ្ធិឱ្យពួកគេទទួលបានអត្ថប្រយោជន៍ពេញលេញពីការប្រើប្រាស់អ៊ីនធឺណិត។ សព្វថ្ងៃនេះ កុមារកំពុងធំធាត់ឡើង និងរស់នៅក្នុងពិភពឌីជីថល ដែលបង្ហាញឱ្យឃើញថាពួកគេអាចងាយនឹងរងហានិភ័យពីប្រព័ន្ធអ៊ីនធឺណិត ជាក់ស្តែងយោងតាមរបាយការណ៍របស់វិទ្យាស្ថានសិក្សាកុមារអាហ្វ្រិកបង្ហាញថា **១៣-១៩%** នៃកុមារដែលភាគច្រើនមានអាយុចន្លោះពី ១២ ទៅ ១៦ឆ្នាំ ធ្លាប់មានបទពិសោធន៍ត្រូវបានសុំសេវាផ្លូវភេទតាមអ៊ីនធឺណិត។ សម្រាប់កម្ពុជា តាមរយៈរបាយការណ៍របស់អង្គការមូលនិធិសម្រាប់កុមារអន្តរជាតិរបស់អង្គការសហប្រជាជាតិ (UNICEF) ឆ្នាំ២០២០ ក៏បានបង្ហាញថា យុវជនកម្ពុជាដែលមានអាយុចន្លោះពី **១៥ឆ្នាំ** ដល់ **២៥ឆ្នាំ** ប្រមាណ **៨៥,៧%** កំពុងជួបបញ្ហា Cyberbullying ដោយសារការប្រើប្រាស់បច្ចេកវិទ្យា និងអ៊ីនធឺណិត។ លើសពីនេះ នៅក្នុងរបាយការណ៍ស្រាវជ្រាវរបស់ "Cambodia Education" បង្ហាញពីស្ថិតិនៃផលប៉ះពាល់កើតឡើងដោយអំពើ Cyberbullying ដូចខាងក្រោម៖

- កុមារ និងយុវជនកម្ពុជាប្រមាណ **១៦០ ០០០នាក់** បានបោះបង់ការសិក្សា
- ក្នុងនោះមានយុវជនថ្នាក់វិទ្យាល័យ ប្រមាណ **១៤%** បានព្យាយាមធ្វើអត្តឃាត
- ការចាកចេញពីផ្ទះ ចូលរួមក្នុងសង្គមងងឹត ពេស្យាចារ និងអំពើល្មើសច្បាប់ផ្សេងៗ
- លើសពីនេះ មានផលប៉ះពាល់ជាច្រើនទៀត ដែលកើតឡើងដោយអំពើ Cyberbullying នេះ។

ដើម្បីចូលរួមប្រយុទ្ធប្រឆាំងអំពើរុករកកូនឆាឆៅដូចបានរៀបរាប់ខាងលើ ក្រៅពីស្ថាប័នមានសមត្ថកិច្ចរបស់រាជរដ្ឋាភិបាល អាណាព្យាបាល គណៈគ្រប់គ្រងសាលា និងគ្រូបង្រៀន គឺជាបុគ្គលសំខាន់ ដែលទាមទារឱ្យមានការចូលរួមប្រយុទ្ធប្រឆាំងអំពើរុករកកូនឆាឆៅមកលើកុមារ និងយុវជនដែលជាធនធានមនុស្សសម្រាប់សង្គមជាតិ។ ខាងក្រោមនេះជាអាយុ និងដំណាក់កាលវិវត្តរបស់កុមារ៖

- **០-៥ឆ្នាំ វ័យមុនរៀនអក្សរ និងពេលរៀនអក្សរដំបូង៖** ការវិវត្តសំខាន់ៗ មានការសិក្សាតិចតួចណាស់ស្តីពីការយល់ដឹងរបស់កុមារអំពីបរិស្ថានឌីជីថលនៅក្នុងចន្លោះអាយុនេះ ជាពិសេសចំពោះក្មេងតូចអាយុ ០-៣ឆ្នាំ។ ប៉ុន្តែភស្តុតាងខ្លះបានបង្ហាញថា កុមារជាច្រើនមានវត្តមានលើប្រព័ន្ធអនឡាញតាំងពីក្មេងតែការយល់ និងការដឹងអំពីហានិភ័យលើប្រព័ន្ធអនឡាញចំពោះកុមារនៅក្នុងចន្លោះអាយុនេះ

មានកម្រិតតិចតួចណាស់។ នៅអាយុ ៣-៥ឆ្នាំ កុមារចាប់ផ្តើមអភិវឌ្ឍន៍សមត្ថភាពក្នុងការចេះយកចិត្តគេដាក់ចិត្តខ្លួនឯង ហើយងាយនឹងលង់ជាមួយរូបរាងខាងក្រៅណាស់។ ពួកគេកំពុងតែអភិវឌ្ឍន៍មិត្តភាព ទោះបីជាសម្ពាធពីដៃគូមានកម្រិតទាបក៏ដោយ ក៏ការណែនាំ ឬឥទ្ធិពលពីឪពុកម្តាយ និងគ្រួសារ គឺជាគន្លឹះសំខាន់។

- **៦-៩ឆ្នាំ វ័យចូលរៀនបឋមសិក្សា៖** កុមារនៅក្នុងចន្លោះអាយុនេះ ក៏មិនទាន់មានឧបករណ៍បច្ចេកវិទ្យាផ្ទាល់ខ្លួនសម្រាប់ប្រើប្រាស់ទេ (ដូចជា កុំព្យូទ័រ) ប៉ុន្តែជាទូទៅគេប្រើឧបករណ៍របស់ឪពុកម្តាយ។ ប្រដាប់ប្រដាលេង ដែលមានភ្ជាប់សេវាអ៊ីនធឺណិតជាទីពេញនិយមសម្រាប់ពួកគេ។ ជារឿយៗពួកគេចូលចិត្តលេងហ្គេមអនឡាញ សកម្មភាពដែលមានភាពច្នៃប្រឌិត និងការផ្សាយវីដេអូផ្ទាល់។ កុមារអាចនឹងសាកល្បងប្រើប្រាស់បណ្តាញសង្គម ទាំងតាមរយៈហ្គេមអនឡាញ គណនី បណ្តាញសង្គមរបស់ឪពុកម្តាយ ឬតាមរយៈការបង្កើតគណនីបណ្តាញសង្គមផ្ទាល់ខ្លួន។ ពួកគេអាចភ្ជាប់ទំនាក់ទំនង និងទទួលរងឥទ្ធិពលពីអ្នកថតវីដេអូ តាមប្រព័ន្ធអនឡាញ (Vlogger) ជាពិសេសអ្នកដែលស្ថិតនៅក្នុងចន្លោះអាយុស្រដៀងគ្នា។

- **១០-១២ឆ្នាំ វ័យអន្តរកាល៖** នេះគឺជាចន្លោះអាយុដែលសកម្មភាពរបស់កុមារនៅលើប្រព័ន្ធអនឡាញមានការផ្លាស់ប្តូរជាខ្លាំង។ ក្នុងឆ្នាំអន្តរកាលចន្លោះពីថ្នាក់បឋមសិក្សាទៅវិទ្យាល័យកុមារអាចមានឱកាសទទួលបានឧបករណ៍ប្រើប្រាស់ផ្ទាល់ខ្លួន ភាគច្រើនជាទូរសព្ទស្មាតហ្វូន។ កុមារនៅក្នុងចន្លោះអាយុនេះ ងាយរងសម្ពាធពីដៃគូ និងអ្នកមានឥទ្ធិពលលើប្រព័ន្ធអនឡាញ និងការកើនឡើងនៃឥរិយាបថប្រថុយប្រថាន។ កុមារវ័យនេះនិយមចូលចិត្តលេងហ្គេមអនឡាញ មើលវីដេអូ និងតន្ត្រីផ្សាយផ្ទាល់។ កុមារអាចមានអារម្មណ៍ថា មានសម្ពាធពេលលេងហ្គេមជាមួយមិត្តភក្តិ និងមានអារម្មណ៍ថាខ្លាចគេមិនទទួលស្គាល់ឬរាប់អាន។

- **១៣-១៥ឆ្នាំ វ័យជំទង់៖** នៅក្នុងចន្លោះអាយុនេះ កុមារមានតម្រូវការបង្កើតអត្តសញ្ញាណដើម្បីទំនាក់ទំនងជាមួយក្រុមមិត្តភក្តិរបស់ពួកគេ។ តម្រូវការនេះធ្វើឱ្យកុមារកាន់តែចង់បានឯករាជភាព និងស្វ័យភាពខ្ពស់ជាងមុន។ ពួកគេអាចមិនស្តាប់បង្គាប់ ឬចាប់ផ្តើមរំកិលខ្លួនឆ្ងាយពីគុណតម្លៃដែលដាក់ចេញដោយឪពុកម្តាយ ហើយព្យាយាមគេចពីកំហិត និងលក្ខខណ្ឌនៃការប្រើប្រាស់ផ្សេងៗរបស់ឪពុកម្តាយ និងប្រព័ន្ធអនឡាញ។ ពួកគេនិយមប្រើប្រាស់នូវកម្មវិធីទាំងឡាយដែលឪពុក ម្តាយមិនចេះប្រើ ឬមិនធ្លាប់ប្រើប្រាស់ ដោយសារតែកម្មវិធីទាំងនោះប្រើប្រាស់ភាសាដែលឪពុកម្តាយមិនយល់។ ការប្រើប្រាស់មុខងារ និងកម្មវិធីបណ្តាញសង្គមផ្សេងៗមានការរីកសាយភាយយ៉ាងទូលំទូលាយ ហើយការលេងហ្គេម វីដេអូនិងតន្ត្រីផ្សាយផ្ទាល់ នៅតែពេញនិយម។ កុមារអាចព្យាយាមធ្វើត្រាប់តាម "អ្នកមានឥទ្ធិពល" ឬអ្នកថតវីដេអូសកម្មភាពនៅលើប្រព័ន្ធអនឡាញ ក្នុងដំណាក់កាលនៃការវិវត្តនេះ។

- **១៦-១៧ ឆ្នាំ អាយុពេញវ័យ៖** ក្នុងវ័យនេះ កុមារភាគច្រើនមានជំនាញលើប្រព័ន្ធអនឡាញ យុទ្ធសាស្ត្រសម្របខ្លួន និងភាពធន់បានយ៉ាងពេញលេញ។ ប៉ុន្តែពួកគេនៅត្រូវការអភិវឌ្ឍ ផ្នែកបញ្ញា ស្មារតី ភាពអត់ធន់ បទពិសោធន៍ និងការវាយតម្លៃទៅលើផលវិបាករយៈពេលវែងអំពីសកម្មភាពលើប្រព័ន្ធអនឡាញ។

ចំណេះដឹង និងសមត្ថភាពបច្ចេកទេសអាចនឹងមានការអភិវឌ្ឍល្អប្រសើរជាងចំណេះដឹងផ្នែកអារម្មណ៍ ឬសមត្ថភាពរបស់ពួកគេក្នុងការគ្រប់គ្រងទំនាក់ទំនងដ៏ស្មុគស្មាញរបស់ខ្លួន។ សមត្ថភាពក្នុងការគិតគូររយៈពេលវែង កំពុងតែវិវត្ត ហេតុនេះពួកគេអាចនៅមានទំនោរទៅរកការប្រព្រឹត្តិយ៉ាងប្រថុយប្រថាន ឬឥរិយាបទតាមទំនើងចិត្ត ព្រមទាំងងាយទទួលឥទ្ធិពលពីប្រព័ន្ធផ្តល់រង្វាន់។

I. ប្រភេទនៃការគំរាមកំហែងលើប្រព័ន្ធអនឡាញសម្រាប់កុមារ

នាយុគសម័យឌីជីថល ប្រព័ន្ធអនឡាញអាចជាកន្លែងដែលមនុស្សអាចធ្វើការទំនាក់ទំនង ក៏ដូចជាទាញយកប្រយោជន៍ជាអតិបរមាពីប្រព័ន្ធនេះសម្រាប់ការប្រកបអាជីវកម្មជាដើម។ យ៉ាងណាមិញ ប្រព័ន្ធអនឡាញក៏ជាកន្លែងដែលអាចឱ្យអ្នកប្រើប្រាស់ងាយរងហានិភ័យពីការបោកប្រាស់តាមប្រព័ន្ធអ៊ីនធឺណិត ជាពិសេសកុមារ ប្រសិនបើពួកគេមិនមានការយល់ដឹងពីរបៀបនៃការប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថលឱ្យបានត្រឹមត្រូវ និងមិនមានវិធានការត្រឹមត្រូវពីអាណាព្យាបាល។ មិនខុសពីអ្នកប្រើប្រាស់ទូទៅ កុមារក៏អាចជួបប្រទះនូវការគំរាមកំហែងសំខាន់មួយចំនួនលើប្រព័ន្ធអនឡាញដូចខាងក្រោម៖

Cyberbullying

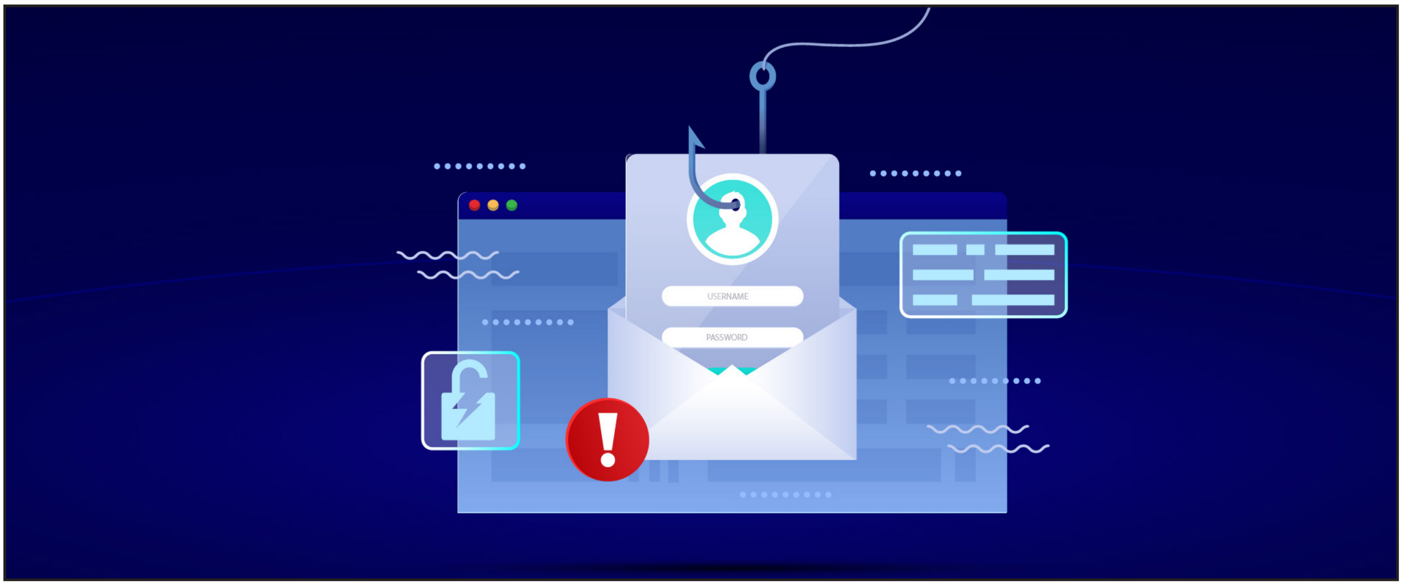
តាមរយៈការរីកចម្រើនយ៉ាងឆាប់រហ័សនៃបច្ចេកវិទ្យាឌីជីថល ក៏ដូចជាបណ្តាញសង្គម បានធ្វើឱ្យ Cyberbullying មានការកើនឡើងផងដែរ។ Cyberbullying សំដៅដល់ការប្រើប្រាស់បច្ចេកវិទ្យាដើម្បីបំពាន ឬដើម្បីវាយប្រហារធ្វើទុកបុកម្នេញលើបុគ្គល តាមរយៈការបង្ហាញខ្លឹមសារអវិជ្ជមាន មិនពិត គ្រោះថ្នាក់ អាកប្បកិរិយាមិនល្អ ការបន្លាច បញ្ចេញកំហឹង ឬធ្វើឱ្យនរណាម្នាក់ខ្មាសគេជាដើម ហើយសកម្មភាពទាំងអស់នេះច្រើនកើតមានឡើងនៅតាមបណ្តាញសង្គម, ក្នុង Chat និងក្នុងហ្គេមអនឡាញជាដើម។ យោងតាមការសិក្សារបស់អង្គការសុខភាពពិភពលោក WHO បានបង្ហាញថា ទិន្នន័យចុងក្រោយពីឆ្នាំ២០១៨ ដល់ឆ្នាំ២០២២ បង្ហាញពីការកើនឡើងទាក់ទងនឹង Cyberbullying ដោយក្មេងប្រុសដែលជួបប្រទះបញ្ហានេះបានកើនឡើងពី **១១%** ទៅ **១៤%** និងក្មេងស្រីពី **៧%** ទៅ **៩%**។

ការកេងប្រវ័ញ្ច និងការរំលោភបំពានតាមប្រព័ន្ធអនឡាញ

ការគំរាមកំហែងបែបនេះ រួមបញ្ចូលការលួងលោម, រូបភាពមិនសមរម្យរបស់កុមារ ដែលត្រូវបានថតដោយការបង្ខំ ការគំរាមកំហែង ការបោកបញ្ឆោត ការបញ្ចុះបញ្ចូល ឬតាមរយៈការចែករំលែកតាមដៃគូ និងប្រើប្រាស់កុមារនៅក្នុងសំឡេង ឬរូបភាពនៃការរំលោភបំពានលើកុមារ។ ការចូលមើល ឬចែករំលែកបន្តនូវរូបភាពសម្ភារៈរំលោភបំពានផ្លូវភេទទាំងនោះ ម្តងហើយម្តងទៀត បង្កើតជាការរំលោភលើសិទ្ធិកុមារ។

ការបោកបញ្ឆោត

ការបោកបញ្ឆោត (phishing) គឺជាការវាយប្រហារសាយប័រមួយ ដែលជនខិលខូចក្លែងបន្លំធ្វើពុតជាតួអង្គណាម្នាក់ ដើម្បីបញ្ឆោតមនុស្សឱ្យប្រគល់ព័ត៌មានរសើបដល់ខ្លួន ដែលមាន ដូចជា ពាក្យសម្ងាត់ លេខកាតឥណទាន ឬទិន្នន័យផ្ទាល់ខ្លួនផ្សេងទៀត ដែលអាចប្រើជាបន្តបន្ទាប់ដើម្បីលួចចូលប្រព័ន្ធកុំព្យូទ័រ លួចប្រើអត្តសញ្ញាណ និងសកម្មភាពទុច្ចរិតផ្សេងៗ។ អ្នកប្រើប្រាស់ ជាពិសេសកុមារងាយនឹងរងការវាយប្រហារបែបនេះ ដោយហេតុថាពួកគេមានបទពិសោធន៍តិចនៅក្នុងពិភពឌីជីថល, ទំនោរក្នុងការជឿទុកចិត្ត និងភាពធ្វេសប្រហែសក្នុងការគិតគូរវែងឆ្ងាយ។ កុមារអាចមិនសូវដឹងពីសារ ឬតំណគួរឱ្យសង្ស័យ ដែលអាចឱ្យពួកគេចុចតំណនោះដោយមិនស្ទាក់ស្ទើរ។



ការជួញដូរមនុស្ស

ការជួញដូរកុមារ គឺជាការរំលោភសិទ្ធិកុមារយ៉ាងធ្ងន់ធ្ងរ ដែលពាក់ព័ន្ធនឹងការដឹកជញ្ជូនខុសច្បាប់ ការជ្រើសរើស ឬការកេងប្រវ័ញ្ចលើអនីតិជនសម្រាប់គោលបំណង ដូចជា ពលកម្មដោយបង្ខំ ការកេងប្រវ័ញ្ចផ្លូវភេទ ឬសកម្មភាពខុសច្បាប់។ អ្នកជួញដូរជារឿយៗប្រើឧបាយកល និងការបោកបញ្ឆោត ដើម្បីទទួលបានការជឿទុកចិត្តពីកុមារដែលងាយរងគ្រោះ ជួនកាលធ្វើពុតជាផ្តល់ឱ្យនូវជីវិតប្រសើរជាងមុន ឱកាស ឬផ្លូវចេញពីភាពក្រីក្រ។ នាពេលបច្ចុប្បន្ននេះ ការកើនឡើងនៃអ៊ីនធឺណិតក៏បានធ្វើឱ្យកាន់តែងាយស្រួលសម្រាប់អ្នកជួញដូរក្នុងការកេងប្រវ័ញ្ចលើកុមារ ដោយប្រើថ្នាលអនឡាញ ប្រព័ន្ធផ្សព្វផ្សាយសង្គម និងបណ្តាញហ្គេម ដើម្បីបង្កើតទំនាក់ទំនង ទទួលបានទំនុកចិត្ត និងចុងក្រោយបង្ខិតបង្ខំកុមារឱ្យស្ថិតក្នុងស្ថានភាពគ្រោះថ្នាក់។ កុមារទាំងនេះច្រើនតែទទួលរងការរំលោភបំពានផ្លូវកាយ ផ្លូវចិត្ត និងផ្លូវចិត្ត ដោយមានឱកាសតិចតួចក្នុងការរត់គេចខ្លួន។ ដូច្នេះ ការប្រយុទ្ធប្រឆាំងនឹងការជួញដូរកុមារតម្រូវឱ្យមានក្របខ័ណ្ឌច្បាប់រឹងមាំ ការយល់ដឹង និងការប្រុងប្រយ័ត្នពីអាជ្ញាធរ និងសាធារណៈជន ដើម្បីការពារកុមារពីការកេងប្រវ័ញ្ច និងធានាសុវត្ថិភាពរបស់ពួកគេទាំងក្រៅបណ្តាញ និងអ៊ីនធឺណិត។

II. ដំណោះស្រាយបច្ចេកវិទ្យា

នៅក្នុងទិដ្ឋភាពនៃការវិវត្តឥតឈប់ឈរនៃពិភពឌីជីថលនាពេលបច្ចុប្បន្ននេះ បច្ចេកវិទ្យាបានក្លាយជាអាវុធមុខពីរ ដែលមានសមត្ថភាពអាចជំរុញ និងបង្កើតរឿងល្អៗដល់កុមារ ប៉ុន្តែក៏អាចបង្កជាហានិភ័យដល់កុមារផងដែរ ប្រសិនបើមិនមានការគ្រប់គ្រងឱ្យបានហ្មត់ចត់។ ជាក់ស្តែង ឧបករណ៍ឌីជីថលមួយចំនួន អាចប្រើប្រាស់ដើម្បីជាជំនួយក្នុងការគ្រប់គ្រងការប្រើប្រាស់ប្រចាំថ្ងៃរបស់កុមារ ទាំងការគ្រប់គ្រងលើមាតិកា និងកំណត់ការចូលប្រើប្រាស់នានា ដែលអាចបង្កគ្រោះថ្នាក់ដល់កុមារ។ សព្វថ្ងៃនេះ យើងមានឧបករណ៍ឌីជីថលសំខាន់ៗមួយចំនួន ដើម្បីឱ្យអាណាព្យាបាលអាចគ្រប់គ្រងលើការប្រើប្រាស់របស់កុមារបាន ដូចជា៖

ឧបករណ៍គ្រប់គ្រងដោយអាណាព្យាបាល (Parent Control Tools)

ឧបករណ៍ឌីជីថលសម្រាប់ការគ្រប់គ្រងកុមារអនុញ្ញាតឱ្យឪពុកម្តាយ ឬអាណាព្យាបាល ធ្វើការតាមដានសកម្មភាពលើអ៊ីនធឺណិតរបស់កូនពួកគេ រួមទាំងផ្តល់នូវជម្រើសក្នុងការទប់ស្កាត់ ឬគ្រប់គ្រងលើខ្លឹមសារឌីជីថលនៅលើកម្មវិធី និងគេហទំព័រជាក់លាក់ណាមួយបានទៀតផង។ ឧបករណ៍ឌីជីថលប្រភេទនេះ អនុញ្ញាតឱ្យអាណាព្យាបាលបង្កើតគណនីគ្រួសាររួម ដើម្បីផ្តល់ភាពងាយស្រួលដល់គ្រួសារក្នុងការគ្រប់គ្រងតាមពេលវេលាជាក់ស្តែង ជាពិសេសការការពារដោយសម្ងាត់។ បច្ចុប្បន្ននេះ ក្រុមហ៊ុនជាច្រើនបានបង្កើតនូវថ្នាលការពារផ្សេងៗ ដែលផ្តល់ឱ្យនូវមុខងារជាច្រើនសម្រាប់អាណាព្យាបាលឱ្យកាន់តែមានជម្រើសក្នុងការគ្រប់គ្រងកូនៗរបស់ពួកគេ។ ជាក់ស្តែង ដូចជា៖

- **Qustodio**

  កម្មវិធីនេះ បច្ចុប្បន្នគឺមានចំនួនអ្នកប្រើប្រាស់ច្រើនជាងគេ ដែលកម្មវិធីនេះផ្តល់ជូនការគ្រប់គ្រង និងការរក្សាសុវត្ថិភាពបានយ៉ាងល្អ។ Qustodio មានសមត្ថភាពក្នុងការទប់ស្កាត់ និងកំណត់មាតិកាមិនសមរម្យ ហ្គេម និងកម្មវិធីតាមដានប្រព័ន្ធផ្សព្វផ្សាយសង្គម គ្រប់គ្រងពេលវេលាអេក្រង់ និងតាមដានទីតាំងផងដែរ។

- **Net Nanny**

  កម្មវិធីនេះត្រូវបានប្រើប្រាស់សម្រាប់ការផ្តល់ការគាំទ្រលើមូលដ្ឋានការពារសំខាន់ៗ ដូចជាការគ្រប់គ្រងដោយមាតាបិតា, ការគ្រប់គ្រងពេលវេលាលើអេក្រង់, ការប្រើប្រាស់អ៊ីនធឺណិត, សមត្ថភាពក្នុងការទប់ស្កាត់កម្មវិធី និងគេហទំព័រ ដោយផ្តោតសំខាន់លើការទប់ស្កាត់រូបភាព និងមាតិកាអាសអាភាស។ Net Nanny ធ្វើការជូនដំណឹងអំពីសកម្មភាពលើអ៊ីនធឺណិតប្រចាំថ្ងៃ ដែលអាចតាមដានយ៉ាងរហ័ស និងងាយស្រួល។

ការកំណត់ឯកជនភាព និងសុវត្ថិភាព

ការកំណត់ឯកជនភាព និងសុវត្ថិភាពនៅលើប្រព័ន្ធផ្សព្វផ្សាយសង្គម និងកម្រងព័ត៌មានអនឡាញ

ផ្តល់នូវវិធីសាស្ត្រ និងវិធានការសំខាន់បំផុតមួយ ដើម្បីបង្ការ និងប្រឆាំងលើហានិភ័យដែលអាចកើតមានឡើងលើកុមារតាមប្រព័ន្ធអ៊ីនធឺណិត។ ជាក់ស្តែង ការកំណត់ប្រវត្តិរូបរបស់ក្មេងក្នុងទម្រង់ឯកជន (Private Mode), ការធានាការប្រើប្រាស់ដោយពាក្យសម្ងាត់ និងការកំណត់ឱ្យមានការយល់ព្រមជាមុនសម្រាប់សំណើគ្រប់ប្រភេទ បានរួមចំណែកយ៉ាងសំខាន់ក្នុងការធ្វើឱ្យសុវត្ថិភាពកុមារនៅលើប្រព័ន្ធអ៊ីនធឺណិតកាន់តែប្រសើរជាងមុន។ បន្ថែមពីនេះ យើងក៏អាចប្រើប្រាស់ Google SafeSearch បន្ថែមដើម្បីជាជំនួយក្នុងការការពារកុមារនៅពេលដែលពួកគេធ្វើការស្វែងរក (Browse) អ្វីមួយនៅលើអ៊ីនធឺណិត ដែលមុខងារនេះនឹងបន្ថែមស្រទាប់ការពារពីលើអ្វីដែលយើងមានស្រាប់។

តួនាទីរបស់ AI ក្នុងសុវត្ថិភាពអនឡាញ

AI បម្រើតួនាទីសំខាន់ពីរក្នុងការរក្សាកុមារឱ្យមានសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត ដូចជាការការពារ និងការអប់រំ។ តួនាទីទាំងនេះ មិនត្រឹមតែការពារកុមារពីការគំរាមកំហែងប៉ុណ្ណោះទេ ថែមទាំងបង្រៀនពួកគេនូវអាកប្បកិរិយាប្រកបដោយការទទួលខុសត្រូវលើអ៊ីនធឺណិតផងដែរ។

១. ការសម្របសម្រួលមាតិកា

ក្បួនដោះស្រាយ AI អាចរកឃើញ និងទប់ស្កាត់នូវខ្លឹមសារដែលបង្កគ្រោះថ្នាក់ រួមទាំងរូបភាព និងវីដេអូមិនសមរម្យ និងការនិយាយមិនល្អ។ AI ត្រូវបានកំណត់នៅលើថ្នាលបណ្តាញផ្សព្វផ្សាយសង្គម និងម៉ាស៊ីនស្វែងរក ដើម្បីផ្តល់ភាពងាយស្រួលសម្រាប់កុមារ ដែលមានតម្រូវការសម្រាប់ការប្រើប្រាស់បច្ចេកវិទ្យា និងធ្វើឱ្យមាតិកានៅលើថ្នាលទាំងនោះវិជ្ជមានផងដែរ។

២. ការស្វែងរកការគំរាមកំហែងតាមអ៊ីនធឺណិត

ឧបករណ៍ AI ត្រួតពិនិត្យការសន្ទនាតាមអ៊ីនធឺណិតហើយពិនិត្យមើលសញ្ញានៃការគំរាមកំហែង។ ក្បួនដោះស្រាយម៉ាស៊ីនសិក្សាអាចវិភាគលំនាំនៅក្នុងអត្ថបទ កំណត់អត្តសញ្ញាណការគំរាមកំហែងដែលអាចកើតមានមុនពេលបញ្ហានោះកើនឡើង។

៣. ការជូនដំណឹងផ្ទាល់ខ្លួន

AI ផ្តល់ជូនមាតាបិតានូវការដាស់តឿនតាមតម្រូវការ អំពីសកម្មភាពអនឡាញរបស់កូនពួកគេ។ ការណ៍នេះ អាចធានាបានថាមាតាបិតាទទួលបានព័ត៌មានអំពីហានិភ័យនានាដែលអាចកើតមានបានគ្រប់ពេលវេលា និងគ្រប់ទីកន្លែង។

III. អត្ថប្រយោជន៍នៃសុវត្ថិភាពតាមប្រព័ន្ធអនឡាញសម្រាប់កុមារ

ការធានាសុវត្ថិភាពរបស់កុមារតាមអ៊ីនធឺណិត គឺជាផ្នែកសំខាន់មួយក្នុងការចិញ្ចឹមបីបាច់ និងការផ្តល់ឱ្យនូវចំណេះដឹងផ្នែកឌីជីថលដល់ពួកគេ និងការពារពួកគេពីការគំរាមកំហែងផ្សេងៗតាមអ៊ីនធឺណិត។ នៅពេលដែលវិធានការសុវត្ថិភាពអ៊ីនធឺណិតត្រូវបានដាក់ឱ្យដំណើរការ កុមារនឹងកាន់តែ

មានឱកាសទទួលបានការអប់រំ និងឱកាសចូលរួមសកម្មភាពសង្គមជាច្រើន ដែលពិភពឌីជីថលផ្តល់ជូន ខណៈពេលដែលនៅតែត្រូវបានការពារពីហានិភ័យ។ ទាំងនេះជាអត្ថប្រយោជន៍លម្អិតមួយចំនួននៃសុវត្ថិភាពតាមប្រព័ន្ធអនឡាញសម្រាប់កុមារៈ

- **ជួយកុមារពីការគំរាមកំហែងនានា**

ការធានាសុវត្ថិភាពរបស់កុមារតាមប្រព័ន្ធអនឡាញពិតជារឿងសំខាន់ ក្នុងការការពារកុមារពីការវាយប្រហារនានាដែលបាននិងកំពុងកើតមានឡើងនៅក្នុងសង្គមនាពេលបច្ចុប្បន្ន រួមមាន Cyberbullying, កាត់បន្ថយហានិភ័យនៃការលួចអត្តសញ្ញាណ និងការក្លែងបន្លំ, ការពារការកេងប្រវ័ញ្ច និងការរំលោភបំពានតាមប្រព័ន្ធអនឡាញ ក៏ដូចជាកាត់បន្ថយហានិភ័យដែលកុមារអាចត្រូវបានជួញដូរផងដែរ។ ក្នុងនោះ វិធានការសុវត្ថិភាពអ៊ីនធឺណិត ដូចជា ការបង្រៀនកុមារអំពីទម្លាប់នៃការស្វែងរកដោយសុវត្ថិភាព ការការពារពាក្យសម្ងាត់ និងសារៈសំខាន់នៃការមិនចែករំលែកព័ត៌មានលម្អិតផ្ទាល់ខ្លួននៅលើអ៊ីនធឺណិត អាចកាត់បន្ថយហានិភ័យក្នុងការក្លាយខ្លួនជាជនរងគ្រោះពីការវាយប្រហារខាងលើ។

- **ជួយលើកកម្ពស់ឥរិយាបថល្អតាមប្រព័ន្ធអ៊ីនធឺណិត**

ការអប់រំអំពីសុវត្ថិភាពអ៊ីនធឺណិតជួយជំរុញឱ្យមានការយល់ដឹងអំពីការទទួលខុសត្រូវ និងការគោរពនៅពេលកុមារធ្វើអន្តរកម្មលើអ៊ីនធឺណិត។ នៅពេលដែលកុមារយល់ដឹងអំពីហានិភ័យនៃការប្រើប្រាស់ឧបករណ៍ឌីជីថលលើសកម្រិត, ដឹងពីសារៈសំខាន់នៃការប្រព្រឹត្តចំពោះអ្នកដទៃដោយចិត្តល្អ និងផលវិបាកនៃសកម្មភាពអនឡាញរបស់ពួកគេ ពួកគេទំនងជាចូលរួមក្រោមអាកប្បកិរិយាវិជ្ជមាន និងចូលរួមជួយស្ថាបនាអាកប្បកិរិយាតាមប្រព័ន្ធអ៊ីនធឺណិត។ វិធានការសុវត្ថិភាពអ៊ីនធឺណិតជួយកុមារបង្កើតវិធីសាស្ត្រប្រកបដោយតុល្យភាពចំពោះការប្រើប្រាស់បច្ចេកវិទ្យា និងលើកទឹកចិត្តដល់ទម្លាប់ដែលនាំឱ្យមានសុខភាពល្អ ដូចជា ការសម្រាក កំណត់ពេលវេលាចំណាយលើអ៊ីនធឺណិត និងជៀសវាងការប៉ះពាល់នឹងឥទ្ធិពលអវិជ្ជមានជាដើម។

- **ជួយកសាងសមត្ថភាពអក្ខរកម្មឌីជីថល និងទំនួលខុសត្រូវ**

ការបង្រៀនកុមារអំពីសុវត្ថិភាពអ៊ីនធឺណិតមិនត្រឹមតែជួយការពារពួកគេពីគ្រោះថ្នាក់ប៉ុណ្ណោះទេ ប៉ុន្តែថែមទាំងផ្តល់ឱ្យពួកគេនូវជំនាញអក្ខរកម្មឌីជីថលសំខាន់ៗផងដែរ។ តាមរយៈការយល់ដឹងអំពីរបៀបស្រាវជ្រាវលើអ៊ីនធឺណិតប្រកបដោយសុវត្ថិភាព កុមារអាចដឹងពីរបៀបប្រើប្រាស់អ៊ីនធឺណិតជាឧបករណ៍សម្រាប់គោលបំណងអប់រំ ទំនាក់ទំនងសង្គម និងការកម្សាន្ត។ ចំណេះដឹងទាំងនេះអាចឱ្យពួកគេធ្វើការសម្រេចចិត្តប្រកប ដោយការយល់ដឹង មិនថាជាការការពារឯកជនភាពរបស់ពួកគេ ការកំណត់អត្តសញ្ញាណប្រភពព័ត៌មានដែលអាចទុកចិត្តបាន ឬដឹងពីរបៀបរាយការណ៍អំពីអាកប្បកិរិយាដែលបង្កគ្រោះថ្នាក់។ ក្នុងរយៈពេលវែង ការអប់រំសុវត្ថិភាពអ៊ីនធឺណិតអាចលើកកម្ពស់ភាពជាពលរដ្ឋឌីជីថលប្រកបដោយការទទួលខុសត្រូវ ដោយបំពាក់ឱ្យកុមារនូវជំនាញក្នុងការប្រើប្រាស់បច្ចេកវិទ្យាប្រកបដោយក្រមសីលធម៌ និងការទទួលខុសត្រូវ។

អន្តរកម្មសង្គមដែលមានសុវត្ថិភាពជាងមុន

កុមារកាន់តែច្រើនប្រើប្រាស់អ៊ីនធឺណិតសម្រាប់ទំនាក់ទំនងសង្គម មិនថាតាមរយៈប្រព័ន្ធផ្សព្វផ្សាយសង្គម ហ្គេមអនឡាញ ឬការហៅជាវីដេអូនោះទេ។ សុវត្ថិភាពអ៊ីនធឺណិតអនុញ្ញាតឱ្យកុមារបង្កើតមិត្តភាព ទំនាក់ទំនងជាមួយមិត្តភក្តិ និងចូលរួមក្នុងសកម្មភាពសង្គមក្នុងបរិយាកាសសុវត្ថិភាព។ តាមរយៈការបង្រៀនកុមារអំពីគ្រោះថ្នាក់នៃការចែករំលែកព័ត៌មានផ្ទាល់ខ្លួនហួសហេតុ ឬការធ្វើអន្តរកម្មជាមួយមនុស្សចម្លែក ពួកគេអាចចូលរួមក្នុងបទពិសោធន៍សង្គមអនឡាញប្រកបដោយសុវត្ថិភាព។ លើសពីនេះ ការគ្រប់គ្រងដោយមាតាបិតាអាចជួយតាមដាន និងគ្រប់គ្រងអន្តរកម្មសង្គមរបស់ពួកគេ ដោយធានាថាពួកគេភ្ជាប់ទំនាក់ទំនងជាមួយបុគ្គលដែលគួរឱ្យទុកចិត្ត និងជៀសវាងសកម្មភាពដែលបង្កគ្រោះថ្នាក់។

ការគាំទ្រសម្រាប់ការរៀនសូត្រ និងការអភិវឌ្ឍ

អ៊ីនធឺណិតផ្តល់នូវធនធានអប់រំដ៏អស្ចារ្យមួយ ដែលអាចគាំទ្រដល់ការលូតលាស់ និងការអភិវឌ្ឍនៃការសិក្សារបស់កុមារ។ ចាប់ពីការបង្រៀនតាមអ៊ីនធឺណិត និងកម្មវិធីអប់រំ រហូតដល់ដំណើរកម្សាន្តនិម្មិត និងល្បែងសិក្សាបែបអន្តរកម្ម អ៊ីនធឺណិតផ្តល់ឱ្យនូវឧបករណ៍ដ៏មានតម្លៃសម្រាប់កុមារដើម្បីពង្រីកចំណេះដឹងរបស់ពួកគេ។ តាមរយៈការអនុវត្តសុវត្ថិភាពអ៊ីនធឺណិត កុមារអាចចូលប្រើប្រាស់ធនធានទាំងនេះដោយមិនមានការរំខានដោយមាតិកាមិនសមរម្យ ឬជួបប្រទះគ្រោះថ្នាក់នៅលើអ៊ីនធឺណិត ដែលនេះបង្កើតបានជាទីតាំងសុវត្ថិភាពសម្រាប់កុមារដើម្បីស្វែងយល់ពីចំណាប់អារម្មណ៍របស់ពួកគេ រៀនជំនាញថ្មីៗ និងរីកចម្រើនផ្នែកសិក្សា។

IV. តួនាទីរបស់មាតាបិតា អ្នកអបរំ និងរដ្ឋាភិបាលក្នុងការការពារសុវត្ថិភាពអ៊ីនធឺណិត

តួនាទីរបស់អាណាព្យាបាល

ឪពុកម្តាយដើរតួនាទីយ៉ាងសំខាន់ក្នុងការរៀបចំបរិយាកាសឌីជីថលដែលមានសុវត្ថិភាពនៅផ្ទះ និងការពារកូនរបស់ពួកគេពីការគំរាមកំហែងនានាតាមប្រព័ន្ធអ៊ីនធឺណិត។ សុវត្ថិភាពតាមប្រព័ន្ធអ៊ីនធឺណិតមិនគ្រាន់តែជាការគ្រប់គ្រងដោយមាតាបិតាប៉ុណ្ណោះទេ ប៉ុន្តែគឺជាការកសាងទំនាក់ទំនងនៃការជឿទុកចិត្ត ការអប់រំកុមារ និងជំរុញអាកប្បកិរិយាប្រកបដោយការទទួលខុសត្រូវលើអ៊ីនធឺណិត។ អាណាព្យាបាលត្រូវប្រាកដថាកូនរបស់ខ្លួនដឹងអំពីសារៈសំខាន់នៃឯកជនភាព និងសារៈសំខាន់នៃការរក្សាព័ត៌មានរបស់ពួកគេឱ្យមានសុវត្ថិភាពនៅលើអ៊ីនធឺណិត។ បន្ថែមពីនេះ អាណាព្យាបាលគួរគប្បីធ្វើការណែនាំកូនៗរបស់ខ្លួនទាក់ទងនឹងការផ្តល់ព័ត៌មានផ្ទាល់ខ្លួន ដូចជា ឈ្មោះ អាសយដ្ឋាន លេខទូរសព្ទ ឬឈ្មោះសាលាដល់អ្នកមិនស្គាល់នៅលើអ៊ីនធឺណិត។ អាណាព្យាបាល ក៏គួរគប្បីកំណត់លើការប្រើប្រាស់របស់កូនៗ ទាំងលើមាតិកា, ហ្គេម និងការស្វែងរក (Browse) នៅលើគេហទំព័រនានា ដើម្បីអាចគ្រប់គ្រងលើពេលវេលាប្រើប្រាស់ ព្រមទាំងការពារពីការលួចទិន្នន័យផងដែរ។

តួនាទីរបស់អ្នកអប់រំ

អ្នកអប់រំដើរតួនាទីយ៉ាងសំខាន់ក្នុងការការពារសុវត្ថិភាពលើអ៊ីនធឺណិតរបស់កុមារ ដោយដើរតួនាទីជាអ្នកណែនាំ និងអ្នកការពារនៅក្នុងពិភពឌីជីថល។ នៅពេលដែលបច្ចេកវិទ្យាកាន់តែជ្រៀតចូលយ៉ាងជ្រៅនៅក្នុងការអប់រំ បានធ្វើឱ្យការប្រើប្រាស់អ៊ីនធឺណិតក្លាយជាកត្តាសំខាន់សម្រាប់គ្រូបង្រៀនក្នុងការអប់រំសិស្ស ដែលនេះទាមទារចាំបាច់នូវការប្រើប្រាស់អ៊ីនធឺណិតប្រកបដោយការទទួលខុសត្រូវ។ ទាំងនេះរួមបញ្ចូលទាំងការបង្រៀនជំនាញអក្ខរកម្មឌីជីថល ដូចជា ការកំណត់អត្តសញ្ញាណប្រភពដែលអាចជឿទុកចិត្តបាន ការការពារព័ត៌មានផ្ទាល់ខ្លួន និងការយល់ដឹងពីផលវិបាកនៃការចែករំលែកខ្លឹមសារលើអ៊ីនធឺណិត។ អ្នកអប់រំក៏ជួយលើកកម្ពស់ការយល់ដឹងអំពីគ្រោះថ្នាក់តាមអ៊ីនធឺណិតដែលអាចកើតមាន រួមទាំងការគំរាមកំហែងតាមអ៊ីនធឺណិត ការប៉ះពាល់នៃខ្លឹមសារមិនសមរម្យ និងការប្រមាញ់តាមអ៊ីនធឺណិតផងដែរ។ តាមរយៈការបង្កើតបរិយាកាសសិក្សាប្រកបដោយសុវត្ថិភាព និងមានភាពគាំទ្រ គ្រូបង្រៀនក៏គួរតែលើកទឹកចិត្តសិស្សឱ្យព្យាយាមនិយាយដោយបើកចំហអំពីបទពិសោធន៍តាមអ៊ីនធឺណិតរបស់ពួកគេ ក្នុងគោលបំណងនៃការកំណត់សម្គាល់របៀបប្រើប្រាស់របស់ក្មេងៗ។ ពួកគេក៏ត្រូវតែអនុវត្តគោលការណ៍សាលាស្ដីពីការប្រើប្រាស់អ៊ីនធឺណិតឱ្យបានប្រសើរផងដែរ តាមរយៈការតាមដានសកម្មភាពលើអ៊ីនធឺណិតរបស់សិស្សក្នុងអំឡុងពេលម៉ោងសិក្សា និងរាយការណ៍ពីអាកប្បកិរិយា ឬឧប្បត្តិហេតុគួរឱ្យសង្ស័យណាមួយ។ បន្ថែមពីលើការងារផ្ទាល់របស់ពួកគេជាមួយសិស្ស អ្នកអប់រំចាំបាច់ត្រូវសហការជាមួយឪពុកម្ដាយ និងអាណាព្យាបាល ដើម្បីពង្រីកការអនុវត្តសុវត្ថិភាពតាមអ៊ីនធឺណិតក្រៅពីថ្នាក់រៀន។ បន្ថែមពីនេះ គ្រូបង្រៀនត្រូវមានឥរិយាបថឌីជីថលវិជ្ជមាន ដោយបង្ហាញពីរបៀបចូលរួមដោយការគោរព និងដោយសុវត្ថិភាពក្នុងប្រព័ន្ធអ៊ីនធឺណិត ដែលរួមបញ្ចូលគ្នានៃការអប់រំ ការត្រួតពិនិត្យ និងការសហការ។ អ្នកអប់រំដើរតួនាទីយ៉ាងសំខាន់ក្នុងការជួយកុមារឱ្យអភិវឌ្ឍន៍ចំណេះដឹង និងជំនាញដែលត្រូវការ ដើម្បីអាចប្រើប្រាស់ប្រព័ន្ធអ៊ីនធឺណិតប្រកបដោយសុវត្ថិភាព និងការទទួលខុសត្រូវ។

តួនាទីរបស់រដ្ឋាភិបាល

រដ្ឋាភិបាលដើរតួនាទីគឺជាផ្នែកមួយមិនអាចខ្វះបាននៅក្នុងការការពារសុវត្ថិភាពរបស់កុមារតាមប្រព័ន្ធអ៊ីនធឺណិត តាមរយៈបង្កើតយុទ្ធសាស្ត្រ និងអនុវត្តច្បាប់ដែលការពារការកេងប្រវ័ញ្ច ការគំរាមកំហែងនានាតាមអ៊ីនធឺណិត និងការបង្ហារមាតិកាខ្លឹមសារដែលបង្កគ្រោះថ្នាក់។ រដ្ឋាភិបាលបង្កើតបទប្បញ្ញត្តិ ដែលទាមទារឱ្យថ្នាលបណ្ដាញផ្សព្វផ្សាយសង្គម និងគេហទំព័រនានា អនុវត្តវិធានការការពារកុមារ ដូចជា ការផ្ទៀងផ្ទាត់អាយុ និងការសម្របសម្រួលខ្លឹមសារជាដើម។ បន្ថែមពីនេះ រដ្ឋាភិបាលក៏ដើរតួនាទីជាអ្នកគាំទ្រយុទ្ធនាការផ្សព្វផ្សាយការយល់ដឹងជាសាធារណៈ និងផ្ដល់មូលនិធិដល់កម្មវិធីអប់រំ ដើម្បីបង្រៀនទាក់ទងនឹងសុវត្ថិភាពឌីជីថលនៅក្នុងសាលារៀនផងដែរ។ ទន្ទឹមនេះ ភ្នាក់ងារអនុវត្តច្បាប់ធ្វើការស៊ើបអង្កេត និងលុបបំបាត់ឧក្រិដ្ឋកម្មតាមប្រព័ន្ធអ៊ីនធឺណិតដែលពាក់ព័ន្ធនឹងកុមារ ព្រមទាំងធ្វើការជាមួយដៃគូ ដូចជា អង្គការអន្តរជាតិ ដើម្បីជួយដោះស្រាយការគំរាមកំហែង

ជាសកល។ តាមរយៈច្បាប់ ការអប់រំ និងការអនុវត្ត រដ្ឋាភិបាលផ្តល់នូវក្របខ័ណ្ឌដែលជួយធានាបាននូវបរិយាកាសអនឡាញដែលមានសុវត្ថិភាពជាងមុនសម្រាប់កុមារ។ ជាក់ស្តែង សម្រាប់ប្រទេសកម្ពុជា តាមរយៈក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ បានដើរតួនាទីក្នុងការផ្តល់ការគាំទ្របច្ចេកទេសដល់ក្រុមហ៊ុនខ្នាតតូច និងធុរកិច្ចថ្មីឌីជីថល អំពីការយល់ដឹងស្តីពីសិទ្ធិកុមារ និងទំនួលខុសត្រូវលើកិច្ចការពារកុមារ។ ក្នុងរយៈពេលប៉ុន្មានឆ្នាំចុងក្រោយនេះ ក្រសួងបានយកចិត្តទុកខ្លាំងចំពោះតួនាទីរបស់សាលារៀនក្នុងការរក្សាសុវត្ថិភាពរបស់សិស្ស។

V. សេចក្តីសន្និដ្ឋាន

ការវិវត្តឥតឈប់ឈរនៃពិភពឌីជីថលនាពេលបច្ចុប្បន្ននេះ បច្ចេកវិទ្យាបានក្លាយជាអាវុធមុខពីរដែលមានសមត្ថភាពក្នុងការបង្កើតរឿងល្អៗដល់កុមារ ប៉ុន្តែក៏អាចបង្កជាហានិភ័យដល់កុមារផងដែរ ប្រសិនបើមិនការគ្រប់គ្រងឱ្យបានហ្មត់ចត់។ ជាក់ស្តែង ឧបករណ៍ឌីជីថលមួយចំនួន អាចប្រើប្រាស់ដើម្បីជាជំនួយក្នុងការគ្រប់គ្រងការប្រើប្រាស់ប្រចាំថ្ងៃរបស់កុមារ ទាំងការគ្រប់គ្រងលើមាតិកា និងកំណត់ការចូលប្រើប្រាស់នានាដែលអាចបង្កគ្រោះថ្នាក់ដល់កុមារ។ យ៉ាងណាមិញ ប្រព័ន្ធអនឡាញក៏ជាកន្លែងដែលអាចឱ្យអ្នកប្រើប្រាស់ងាយរងហានិភ័យពីការបោកប្រាស់តាមប្រព័ន្ធអ៊ីនធឺណិតជាពិសេសកុមារ ប្រសិនបើពួកគេមិនមានការយល់ដឹងពីរបៀបនៃការប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថលឱ្យបានត្រឹមត្រូវ និងមិនមានវិធានការត្រឹមត្រូវពីអាណាព្យាបាល។ កុមារអាចជួបប្រទះនូវការគំរាមកំហែងសំខាន់ៗមួយចំនួនលើប្រព័ន្ធអនឡាញដូចជា Cyberbullying, ការកេងប្រវ័ញ្ច និងការរំលោភបំពានតាមប្រព័ន្ធអនឡាញ, ការបោកបញ្ឆោត និងការជួញដូរមនុស្ស ដែលទាមទារឱ្យមានការយកចិត្តទុកដាក់ពី អាណាព្យាបាល, អ្នកអប់រំ និងរដ្ឋាភិបាល ពីការគំរាមកំហែងនានាតាមប្រព័ន្ធអ៊ីនធឺណិត។ ការធានាសុវត្ថិភាពរបស់កុមារតាមអ៊ីនធឺណិត គឺជាផ្នែកសំខាន់មួយក្នុងការអភិវឌ្ឍចំណេះដឹងផ្នែកឌីជីថលរបស់ពួកគេ និងការពារពួកគេពីការគំរាមកំហែងផ្សេងៗ។ នៅពេលដែលវិធានការសុវត្ថិភាពអ៊ីនធឺណិតត្រូវបានដាក់ឱ្យដំណើរការ កុមារកាន់តែមានឱកាសទទួលបានការអប់រំ និងឱកាសចូលរួមសកម្មភាពសង្គមជាច្រើន ដែលពិភពឌីជីថលផ្តល់ជូន ខណៈពេលដែលនៅតែត្រូវបានការពារពីគ្រោះថ្នាក់៕

ឯកសារយោង

- *Child Online Protection*, ចេញផ្សាយខែមករា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៨ ខែមេសា ឆ្នាំ២០២៥,https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx
- CHILD PROTECTION, ចូលអានថ្ងៃទី២៨ ខែមេសា ឆ្នាំ២០២៥, https://institutechildstudies.org/safety-online/
- *Keeping children safe online*, ចេញផ្សាយថ្ងៃទី២៦ ខែកុម្ភៈ ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៨ ខែមេសា ឆ្នាំ២០២៥, https://eacrn.net/news/keeping-children-safe-online/
- សៀវភៅណែនាំបង្រៀន អំពី សុវត្ថិភាពកុមារលើប្រព័ន្ធអនឡាញ កម្រិតសិក្សាបឋមភូមិ របស់ក្រសួងអប់រំ យុវជន និងកីឡា, ចេញផ្សាយខែមករា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៨ ខែមេសា ឆ្នាំ២០២៥
- គោលការណ៍ណែនាំ ស្តីពី កិច្ចការពារកុមារលើប្រព័ន្ធអនឡាញសម្រាប់ក្រុមហ៊ុនបច្ចេកវិទ្យាឌីជីថលនៅកម្ពុជា, ចេញផ្សាយ ឆ្នាំ២០២៣, ចូលអានថ្ងៃទី២៨ ខែមេសា ឆ្នាំ២០២៥
- *10 Internet Safety Tools to Keep Your Kids Safe Online*, ចេញផ្សាយថ្ងៃទី១៩ ខែឧសភា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៥ ខែមេសា ឆ្នាំ២០២៥, https://theexodusroad.com/10-tools-to-keep-your-kids-safe-online/
- *Achieving Child Safety Online through Technology*, ចូលអានថ្ងៃទី២៨ ខែមេសា ឆ្នាំ២០២៥,https://ecpat.org/story/achieving-child-safety-online-through-technology/#:~:text=Parental%20Control%20Tools,accounts%20that%20are%20password%20protected.
- *Keeping Kids Safe Online with AI: Balancing Risks and Protections*, ចេញផ្សាយថ្ងៃទី១០ ខែធ្នូ ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៨ ខែមេសា ឆ្នាំ២០២៥, https://americanspcc.org/keeping-kids-safe-online-with-ai-balancing-risks-and-protections/#:~:text=AI%20tools%20monitor%20online%20conversations,potential%20threats%20before%20they%20escalate.&text=AI%20provides%20parents%20with%20tailored%20alerts%20about%20their%20child's%20online%20activity.
- *The Role of Parents in Cyber Safety: Creating a Secure Home Environment*, ចូលអានថ្ងៃទី២៩ ខែមេសា ឆ្នាំ២០២៥, https://kidssafe.lk/2024/11/13/the-role-of-parents-in-cyber-safety-creating-a-secure-home-environment/#:~:text=Restrict%20access%20to%20inappropriate%20content,from%20cyberbullying%20or%20unwanted%20attention
- *One in six school-aged children experiences cyberbullying, finds new WHO/Europe study*, ចេញផ្សាយថ្ងៃទី២៧ ខែមីនា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៩ ខែមេសា ឆ្នាំ២០២៥, https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study
- *Internet Safety for Kids: How to Protect Your Child from the Top 7 Dangers They Face Online*, ចូលអានថ្ងៃទី២៩ ខែមេសា ឆ្នាំ២០២៥, https://www.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online

- *Child and Youth Safety Online*, ចូលអានថ្ងៃទី២៩ ខែមេសា ឆ្នាំ២០២៥, https://www.un.org/en/global-issues/child-and-youth-safety-online
- *Internet Safety | The Importance of Internet Safety for Children*, ចេញផ្សាយថ្ងៃទី១៨ ខែតុលា ឆ្នាំ២០២៣, ចូលអានថ្ងៃទី២៩ ខែមេសា ឆ្នាំ២០២៥, https://www.theoldstationnursery.co.uk/journal/internet-safety-the-importance-of-internet-safety-for-children/
- *តើការបោកបញ្ឆោត (Phishing) ដំណើរការយ៉ាងដូចម្តេច?*, ចេញផ្សាយថ្ងៃទី២៤ ខែមិថុនា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៩ ខែមេសា ឆ្នាំ២០២៥, https://surl.li/rxlymr
- *គោលការណ៍ណែនាំស្តីពីកិច្ចការពារកុមារលើប្រព័ន្ធអនឡាញសម្រាប់ក្រុមហ៊ុនបច្ចេកវិទ្យាឌីជីថលនៅកម្ពុជា*, ចេញផ្សាយឆ្នាំ២០២៣, ចូលអានថ្ងៃទី២៩ ខែមេសា ឆ្នាំ២០២៥

កម្ពុជា ៤.0 - Cambodia 4.0

កម្ពុជា ៤.0 Cambodia 4.0

កម្ពុជា ៤.0 - Cambodia 4.0

កម្ពុជា ៤.0 - Cambodia 4.0

www.cambodia4point0.org

cambodia_4.0

កម្ពុជា ៤.0 - Cambodia 4.0

Cambodia 4.0 Center

កម្ពុជា 4.0 CAMBODIA

វិបុលភាព បរិយាប័ន្ន សុវត្ថិភាព

គាំទ្រដោយ

មូលនិធិ ស.អ.
CBRD FUND