ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

វិទ្យាស្ថានជាតិសង្គមកិច្ច

សុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ

ឆ្នាំ២០២៦

សុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ

អារម្ភកថា

ព្រះរាជាណាចក្រកម្ពុជា បានបោះជំហានទៅមុខក្នុងការស្តារសង្គម និងសេដ្ឋកិច្ចឡើងវិញ ដែលក្នុងពីរទសវត្សរ៍ចុងក្រោយនេះ បានសម្រេចកំណើនសេដ្ឋកិច្ច និងបានវិភាជន៍ធនធានបន្ថែមទៀតដល់វិស័យសុខាភិបាល អប់រំ សង្គមកិច្ច និងវិស័យផ្សេងៗទៀត សម្រាប់ជំរុញការអភិវឌ្ឍធនធានមនុស្ស រួមទាំងការអភិវឌ្ឍកុមារ សំដៅសម្រេចឱ្យបាននូវគោលដៅអភិវឌ្ឍន៍ប្រកបដោយចីរភាពកម្ពុជា ២០១៦-២០៣០ ដែលក្នុងនោះបានផ្តោតសំខាន់លើការអភិវឌ្ឍសុខុមាលភាពកុមារផងដែរ។ ការលើកកម្ពស់និងការការពារកុមារ គឺជាបញ្ហាអាទិភាពរបស់រាជរដ្ឋាភិបាល ដោយបានដាក់បញ្ចូលទៅក្នុងកម្មវិធីគោលនយោបាយ ជាពិសេសយុទ្ធសាស្ត្របញ្ចកោណ ដំណាក់កាលទី១ ដែលបញ្ចកោណទី១៖ ផ្តោតលើការអភិវឌ្ឍមូលធនមនុស្ស ក្នុងនោះរាជរដ្ឋាភិបាលបន្តផ្តោតលើកិច្ចការអាទិភាពមួយក្នុងចំណោមអាទិភាពទាំង៥ គឺ៖ ការពង្រឹងគុណភាពវិស័យអប់រំ កីឡា វិទ្យាសាស្ត្រ និងបច្ចេកវិទ្យា ដែលមានគោលដៅយុទ្ធសាស្ត្រផ្តោតលើការបង្កើតបរិយាកាសល្អសម្រាប់ការអប់រំ និងការបណ្តុះបណ្តាលប្រកបដោយគុណភាព និងជំនាញខ្ពស់ តាមរយៈការពង្រឹងអភិបាលកិច្ច នៃការគ្រប់គ្រងនៅតាមគ្រឹះស្ថានសិក្សា ការពង្រឹងគុណភាពនៃការបណ្តុះបណ្តាលគ្រប់កម្រិត ការបង្កើនគុណភាព និងការចូលរៀនមុខវិជ្ជាវិទ្យាសាស្ត្រ បច្ចេកវិទ្យា វិស្វកម្ម សិល្បៈ គណិតវិទ្យា និងការពង្រឹងការអប់រំកាយ និងកីឡា។

ជាមួយគ្នានេះដែរ នៅឆ្នាំ២០១៥ កម្ពុជាបានចុះហត្ថលេខាលើសេចក្តីថ្លែងការណ៍ WePROTEC នៅទីក្រុងអាប៊ុយដាប៊ី ដែលមានគោលដៅពាក់ព័ន្ធនឹងសកម្មភាពទប់ស្កាត់ការរំលោភបំពាន និងកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ ដោយអនុវត្តផ្អែកលើគំរូឆ្លើយតបថ្នាក់ជាតិ។ នៅក្នុងឆ្នាំ២០១៩ ដោយពិនិត្យឃើញនូវការរីកចម្រើនខាងបច្ចេកវិទ្យា ជាពិសេសការអភិវឌ្ឍនៃឧស្សាហកម្មឌីជីថល បានជះឥទ្ធិពលជាវិជ្ជមាន និងអវិជ្ជមានជាច្រើនមកដល់សង្គម ទើបអគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារបានធ្វើការវិភាគស្ថានភាពដំបូងស្តីពីការកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញនៅកម្ពុជា ដោយបានសិក្សាទៅលើផលប៉ះពាល់នៃបច្ចេកវិទ្យាទាំងនោះចំពោះកុមារ និងបានរកឃើញថា កុមារគឺជាជនដែលងាយប្រឈមនឹងគ្រោះថ្នាក់ពីការកេងប្រវ័ញ្ច និងរំលោភបំពានផ្លូវភេទតាមប្រព័ន្ធអ៊ីនធឺណិត។ ផ្អែកលើការវិភាគស្ថានភាពដំបូង អគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ ក៏បានរៀបចំផែនការសកម្មភាពដើម្បីបង្ការ ទប់ស្កាត់ និងឆ្លើយតបការកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ ឆ្នាំ២០២១-២០២៥។

នៅថ្ងៃទី១៧ ខែកញ្ញា ឆ្នាំ២០២៥ រាជរដ្ឋាភិបាលបានអនុម័តលើផែនការសកម្មភាពជាតិ ស្តីពីការទប់ស្កាត់ និងឆ្លើយតបចំពោះអំពើហិង្សាលើកុមារ ឆ្នាំ២០២៥-២០៣០ នៅក្នុងនោះសកម្មភាពមួយចំនួនដែលនៅសេសសល់ពីការអនុវត្តផែនការសកម្មភាពដើម្បីបង្ការ ទប់ស្កាត់ និងឆ្លើយតបការកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ ឆ្នាំ២០២១-២០២៥ ត្រូវបានដាក់បញ្ចូល និងបន្តអនុវត្ត។ ដើម្បីពង្រីកការយល់ដឹងពាក់ព័ន្ធនឹងសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញឱ្យកាន់តែទូលំទូលាយ អគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ បានសហការជាមួយវិទ្យាស្ថានជាតិសង្គមកិច្ច ក្រោមគម្រោងកម្មវិធី Swipe Safe ដែលគាំទ្រដោយអង្គការឆាលហ្វាន កម្ពុជា បានរៀបចំសៀវភៅមេរៀន និងសម្ភារៈឧបទ្ទេសសម្រាប់បណ្តុះបណ្តាលអំពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ ដែលជាម៉ូឌុលមួយនៃមុខវិជ្ជាសុខុមាលភាពកុមារ។

ការអភិវឌ្ឍសៀវភៅមេរៀននេះ បានដកស្រង់ចេញពីគំរូមេរៀនសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញរបស់អគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ ដែលបានប្រកាសដាក់ឱ្យប្រើប្រាស់ជាផ្លូវការនៅថ្ងៃទី២៦ ខែកញ្ញា ឆ្នាំ២០២៤ ក្រោមអធិបតីភាពដ៏ខ្ពង់ខ្ពស់របស់ឯកឧត្តម **ជា សុមេធី** រដ្ឋមន្ត្រីក្រសួងសង្គមកិច្ច អតីតយុទ្ធជន និងយុវនីតិសម្បទា និងជាប្រធានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ ដោយក្រុមការងារបានខិតខំដកស្រង់នូវផ្នែកពាក់ព័ន្ធនានា ដើម្បីចងក្រងសៀវភៅឱ្យស្របតាមកម្មវិធីសិក្សារបស់វិទ្យាស្ថានជាតិសង្គមកិច្ច សម្រាប់ផ្តល់ចំណេះដឹងដល់និស្សិតដែលជាអនាគតកម្លាំងសេវាសង្គម ឱ្យយល់ដឹងអំពីវិធីសាស្ត្រនៃការប្រើប្រាស់អ៊ីនធឺណិតប្រកបដោយសុវត្ថិភាព មានការទទួលខុសត្រូវ និងការការពារកុមារពីការរំលោភបំពានផ្សេងៗតាមប្រព័ន្ធអនឡាញ ជាពិសេស អាចយល់ដឹងពីការស្វែងរកជំនួយ និងការឆ្លើយតបនៅពេលប្រឈមមុខនឹងបញ្ហាតាមប្រព័ន្ធអនឡាញ។

សៀវភៅនេះ គឺជាសមិទ្ធផលនៃកិច្ចខិតខំរួមគ្នារវាងអគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ វិទ្យាស្ថានជាតិសង្គមកិច្ច និងអង្គការឆាលហ្វាន កម្ពុជា។ តាងនាមអគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ ខ្ញុំសូមថ្លែងអំណរគុណយ៉ាងជ្រាលជ្រៅចំពោះ ឯកឧត្តម លោកជំទាវ លោក លោកស្រីទាំងអស់ ដែលបានរួមចំណែកក្នុងការអភិវឌ្ឍសៀវភៅនេះឡើង។

អគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ សង្ឃឹមយ៉ាងមុតមាំថា សៀវភៅនេះនឹងក្លាយជាធនធានដ៏មានសារៈសំខាន់សម្រាប់សិស្ស និស្សិត គ្រូបង្រៀន កម្លាំងសេវាសង្គមដែលបម្រើការងារជាមួយកុមារ ជាពិសេស គឺជាការតម្រង់ទិសក្នុងការផ្តល់ការគាំទ្រដល់កុមារ និងយុវជននូវចំណេះដឹង និងជំនាញក្នុងការប្រើប្រាស់ប្រព័ន្ធអនឡាញប្រកបដោយសុវត្ថិភាព ដែលជួយពួកគេឱ្យទទួលបានអត្ថប្រយោជន៍ពីបច្ចេកវិទ្យាព័ត៌មាន និងទំនាក់ទំនង។

ថ្ងៃចន្ទ ៥កើត ខែចេត្រ ឆ្នាំម្សាញ់ សប្តស័ក ព.ស. ២៥៦៩
រាជធានីភ្នំពេញ ថ្ងៃទី ២៣ ខែមីនា ឆ្នាំ២០២៦

អគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ
អគ្គលេខាធិការ

គីម សុវណ្ណឌី

សេចក្តីថ្លែងអំណរគុណ

វិទ្យាស្ថានជាតិសង្គមកិច្ច សូមថ្លែងអំណរគុណយ៉ាងជ្រាលជ្រៅចំពោះ ឯកឧត្តម លោក លោកស្រី លោកគ្រូ អ្នកគ្រូទាំងអស់ ដែលជាតំណាងមកពីអគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ វិទ្យាស្ថានជាតិសង្គមកិច្ច និងអង្គការឆាលហ្វាន កម្ពុជា សម្រាប់ការចំណាយពេលវេលាដ៏មានតម្លៃក្នុងការចូលរួមផ្តល់នូវជាតុចូលសំខាន់ៗជាច្រើនលើខ្លឹមសារមេរៀនស្តីពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ ដែលបានរៀបចំឡើងសម្រាប់ប្រើប្រាស់បណ្តុះបណ្តាលទៅដល់និស្សិត។

សូមកោតសរសើរចំពោះ អគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ និងអង្គការឆាលហ្វាន កម្ពុជា ដែលការផ្តួចផ្តើមបង្កើតសៀវភៅមេរៀននេះ និងបានខិតខំប្រឹងប្រែងអស់ពីកម្លាំងកាយចិត្តក្នុងការអភិវឌ្ឍសៀវភៅ និងសម្ភារៈឧបទេស ស្របតាមបរិបទ ជាពិសេសមានភាពងាយស្រួលក្នុងការប្រើប្រាស់ដើម្បីបណ្តុះបណ្តាល និងការសិក្សាស្វែងយល់។ សូមអរគុណចំពោះ អង្គការឆាលហ្វាន កម្ពុជា ដែលបានឧបត្ថម្ភគាំទ្រទាំងបច្ចេកទេស និងហិរញ្ញវត្ថុ តាមរយៈគម្រោងកម្មវិធី Swipe Safe ។

សូមថ្លែងអំណរគុណយ៉ាងជ្រាលជ្រៅចំពោះឯកឧត្តមរដ្ឋមន្ត្រីក្រសួង សង្គមកិច្ច អតីតយុទ្ធជន និងយុវនីតិសម្បទា ដែលបានអនុញ្ញាតឱ្យវិទ្យាស្ថានជាតិសង្គមកិច្ច រៀបចំអភិវឌ្ឍសៀវភៅនេះឡើង ក្រោមទស្សនវិស័យលើកកម្ពស់ការអប់រំ និងកសាងមូលធនមនុស្ស ប្រកបដោយការយកចិត្តទុកដាក់ខ្ពស់ក្នុងការពង្រឹងគុណភាពវិទ្យាស្ថាន។ សៀវភៅទាំងនេះគឺជាឯកសារសំខាន់ ដែលនឹងជួយដល់និស្សិតក្នុងការសិក្សាស្វែងយល់អំពីការកេងប្រវ័ញ្ច និងរំលោភបំពានផ្លូវភេទកុមារតាមប្រព័ន្ធអនឡាញ ព្រមទាំងវិធីសាស្ត្រគាំទ្រ និងឆ្លើយតបប្រកបដោយប្រសិទ្ធភាព។

ថ្ងៃច័ន្ទ ៥កើត ខែ ចេត្រ ឆ្នាំម្សាញ់ សប្តស័ក ព.ស.២៥៦៩

រាជធានីភ្នំពេញ ថ្ងៃទី ២៣ ខែ មីនា ឆ្នាំ២០២៦

វិទ្យាស្ថានជាតិសង្គមកិច្ច

នាយក

សរ បុរីរត្ន

ក្រុមការងាររៀបរៀងសៀវភៅ

អគ្គលេខាធិការដ្ឋានក្រុមប្រឹក្សាជាតិកម្ពុជាដើម្បីកុមារ

១-	ឯកឧត្តម	**គីម សុវណ្ណឌី**	អគ្គលេខាធិការ
២-	ឯកឧត្តម	**ឈុប ឬទ្ធា**	អគ្គលេខាធិការរង
៣-	ឯកឧត្តម	**ផាន់ គីម**	អគ្គលេខាធិការរង
៤-	លោក	**មាស ទូ**	ប្រធានផ្នែកការការពារកុមារ និងពិនិត្យតាមដាន
៥-	លោក	**នូ សុខា**	ប្រធានផ្នែករដ្ឋបាល ផែនការ និងហិរញ្ញវត្ថុ
៦-	លោក	**ទ៉ូយ ចាន់ថា**	អនុប្រធានផ្នែកអប់រំ ផ្សព្វផ្សាយ និងអភិវឌ្ឍធនធានមនុស្ស
៧-	លោក	**សឿន រ័ត្តនា**	អនុប្រធានផ្នែកការការពារកុមារ និងពិនិត្យតាមដាន
៨-	លោកស្រី	**ស៊ុន សុគន្ធា**	អនុប្រធានផ្នែករដ្ឋបាល ផែនការ និងហិរញ្ញវត្ថុ
៩-	លោក	**ជា ឆារ៉ា**	អនុប្រធានផ្នែកអប់រំ ផ្សព្វផ្សាយ និងអភិវឌ្ឍធនធានមនុស្ស
១០-	កញ្ញា	**សេក សុភ័ក្រ្ត**	ប្រធានការិយាល័យពិនិត្យតាមដាន និងរបាយការណ៍
១១-	លោក	**តាត ឈុំវិចិត្រ**	ប្រធានការិយាល័យ
១២-	កញ្ញា	**ខៀវ ចន្ថា**	មន្ត្រី

វិទ្យាស្ថានជាតិសង្គមកិច្ច

១-	ឯកឧត្តម	**សរ បូរីរក្ស**	នាយក
២-	កញ្ញា	**ហៀក ម៉ូរីណា**	ប្រធានដេប៉ាតឺម៉ង់សង្គមកិច្ច
៣-	លោក	**មាស សំណាង**	អនុប្រធានដេប៉ាតឺម៉ង់សង្គមកិច្ច
៤-	លោក	**សេង វណ្ណេត**	ប្រធានការិយាល័យរដ្ឋបាល និងបុគ្គលិក
៥-	លោក	**ម៉ុត រ៉ាត់**	ប្រធានដេប៉ាតឺម៉ង់ឆ្នាំមូលដ្ឋាន
៦-	លោក	**សេង ច័ន្ទបញ្ញា**	ប្រធានការិយាល័យ
៧-	លោក	**ហ៊ាង ខៃឡាយ**	គ្រូបង្រៀន
៨-	លោកស្រី	**ពត ច័ន្ទនីភា**	គ្រូបង្រៀន
៩-	លោកស្រី	**ម៉ុយ សុម៉ាលី**	គ្រូបង្រៀន
១០-	លោក	**ស្រ៊ាន គីមស្រ៊ុន**	គ្រូបង្រៀន

អង្គការឆាលហ្វាន កម្ពុជា

១-	លោកស្រី	**ហ៊ុន បូរមី**	នាយិកាប្រចាំប្រទេស អង្គការឆាលហ្វាន កម្ពុជា
២-	លោក	**អេង ហុក**	ប្រធានកម្មវិធីកិច្ចការពារកុមារ
៣-	លោកស្រី	**អ៊ុំម ស្រីថា**	មន្ត្រីសម្របសម្រួលការកសាងសមត្ថភាពកិច្ចការពារកុមារ

មាតិកា

១. សេចក្ដីផ្ដើម ១
២. កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ ៣
២.១. ការសិក្សាស្រាវជ្រាវស្ដីពីការប្រើប្រាស់ប្រព័ន្ធអនឡាញរបស់កុមារ ៣
២.១.១. ការសិក្សាស្រាវជ្រាវជាសាកល និងក្នុងតំបន់អំពីការប្រើប្រាស់អ៊ីនធឺណិតរបស់កុមារ ៣
២.១.២. ការយល់ឃើញផ្សេងគ្នារវាងមនុស្សពេញវ័យ និងកុមារចំពោះអ៊ីនធឺណិត ៦
២.២. ការបញ្ចូលការកេងប្រវ័ញ្ច និងរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញទៅក្នុងកិច្ចការពារកុមារ ៧
២.២.១. គោលនយោបាយកិច្ចការពារកុមារ ៧
២.២.២. អ្នកពាក់ព័ន្ធនឹងកិច្ចការពារកុមារអហ្វឡាញ ៧
២.២.៣. កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ ៨
៣. ធាតុផ្សំសំខាន់ៗនៃអ៊ីនធឺណិត ១១
៣.១. អ៊ីនធឺណិតនិងទំនាក់ទំនងក្នុងសង្គម ១១
៣.២. អត្ថប្រយោជន៍នៃការប្រើប្រាស់អ៊ីនធឺណិត ១១
៣.៣. អំពីធាតុផ្សំនៃអ៊ីនធឺណិត ១២
៣.៣.១. ធាតុផ្សំ "សាធារណៈ" ១២
៣.៣.២. ធាតុផ្សំ "អចិន្ត្រៃយ៍" ១៣
៣.៣.៣. ធាតុផ្សំ "ការផ្សារភ្ជាប់" ១៣
៣.៣.៤. ធាតុផ្សំ "អនាមិកភាព" ១៤
៣.៣.៥. ធាតុផ្សំ "ប្រភពព័ត៌មាន" ១៥
៣.៣.៦. ធាតុផ្សំ "ការគោរព" ១៦
៤. មុខងារសុវត្ថិភាពនៃថ្នាលកម្មវិធី ១៧
៤.១. ការណែនាំអំពីមុខងារសុវត្ថិភាពនៃថ្នាលកម្មវិធី ១៧
៤.២. ការកំណត់ឯកជនភាព និងដែនកំណត់ (Privacy settings and limits) ១៨
៤.២.១. ការកំណត់ឯកជនភាព Facebook នៅលើប្រព័ន្ធប្រតិបត្តិការ Android ១៨
៤.២.២. ការកំណត់ឯកជនភាព Telegram នៅលើប្រព័ន្ធប្រតិបត្តិការ Android ១៩
៤.៣. ការរុករកដោយសុវត្ថិភាព (SafeSearch) ២០
៤.៤. ការរឹតបន្តឹងនៅលើ Youtube ២០
៤.៥. ការរាំងខ្ទប់នៅលើកម្មវិធី Facebook, Telegram, TikTok និង Instagram ២១
៤.៦. ការរាយការណ៍នៅលើកម្មវិធី Facebook, Telegram, TikTok និង Instagram ២២
៤.៧. ការកំណត់លើទីតាំងដែលកំពុងស្ថិតនៅ (Live location settings) ២៤
៤.៨. ការប្រមូលវត្ថុតាង ២៥
៥. ការអភិវឌ្ឍជំនាញកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ ២៧
៥.១. ប្រភេទហានិភ័យតាមប្រព័ន្ធអនឡាញ ២៧

៥.២. ការកេងប្រវ័ញ្ច និងរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ ២៨
៥.២.១. ការលួងលោមកុមារតាមប្រព័ន្ធអនឡាញ (Child Online Grooming) ៣០
៥.២.២. រូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ (Child Sexual Abuse Material-CSAM) ៣២
៥.២.៣. ការគំរាមពាក់ព័ន្ធសកម្មភាពផ្លូវភេទ (Sextortion) ៣២
៥.២.៤. ការផ្សាយផ្ទាល់នៃការរំលោភបំពានផ្លូវភេទលើកុមារ (Live online child sexual exploitation) ៣៣
៥.២.៥. ការផ្ញើសារបែបផ្លូវភេទ (Sexting) ៣៣
៥.៣. ការរុកកួនតាមប្រព័ន្ធអនឡាញ (Cyberbully) ៣៤
៥.៤. ការប្រឈមនឹងមាតិកាមិនសមរម្យតាមប្រព័ន្ធអនឡាញ ៣៥
៥.៥. បាតដៃសុវត្ថិភាព ៣៧
៥.៦. ការជួយឪពុកម្តាយក្នុងការពិភាក្សាអំពីសុវត្ថិភាពតាមប្រព័ន្ធអនឡាញ ៣៨
៥.៦.១. កិច្ចព្រមព្រៀងស្តីពីការប្រើប្រាស់អនឡាញនៅផ្ទះ ៣៨
៥.៦.២. ការពិភាក្សាអំពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ ៣៩
៥.៧. គន្លឹះឆ្លើយតបទៅនឹងបញ្ហាធ្ងន់ធ្ងរតាមប្រព័ន្ធអនឡាញ ៤០
៥.៨. ការគាំទ្រចំពោះការលាតត្រដាងបញ្ហារបស់កុមារ ៤១
៦. គន្លឹះសុវត្ថិភាពសម្រាប់កុមារតាមប្រព័ន្ធអនឡាញ ៤៤
៦.១. គន្លឹះគេចចេញពីជនទុច្ចរិតតាមប្រព័ន្ធអនឡាញ ៤៤
៦.២. ផែនការសុវត្ថិភាពសម្រាប់កុមារ ៤៥
៦.៣. កេរ្តិ៍ឈ្មោះតាមប្រព័ន្ធអនឡាញ ៤៥
៦.៤. ការទទួលខុសត្រូវតាមប្រព័ន្ធអនឡាញ ៤៦
៦.៥. ព័ត៌មានតាមប្រព័ន្ធអនឡាញ ៤៧
៦.៦. ការចែករំលែកព័ត៌មានតាមប្រព័ន្ធអនឡាញ ៤៧
៦.៧. ការរុកកួនតាមប្រព័ន្ធអនឡាញ ៤៨
៦.៨. ការលួងលោមតាមប្រព័ន្ធអនឡាញ ៤៩
៦.៩. តើខ្ញុំនិយាយជាមួយនរណាតាមប្រព័ន្ធអនឡាញ? ៥០
៦.១០. អ្នកបោកប្រាស់ និងអ្នកលួចគណនីតាមប្រព័ន្ធអនឡាញ ៥០
៦.១០. មាតិកាមានលក្ខណៈប្រមាថ និងបង្កគ្រោះថ្នាក់ ៥២
៦.១១. ការចំណាយពេលច្រើនពេកតាមប្រព័ន្ធអនឡាញ ៥២
៦.១២. ហ្គេមអនឡាញ ៥៣
៦.១៣. ការរាយការណ៍ ៥៤
៧. សង្ខេប ៥៦
សំណួរ ៥៨
ឧបសម្ព័ន្ធ១ ៖ ការណែនាំអនុវត្តមុខងារសុវត្ថិភាពលើថ្នាលកម្មវិធី ៥៩
ឧបសម្ព័ន្ធ២ ៖ កម្មវិធីអេបអប់រំស្តីពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ ៧៧

១. សេចក្តីផ្តើម

ការរីកចម្រើនផ្នែកបច្ចេកវិទ្យាឌីជីថលបាននាំមកនូវកាលានុវត្តភាពការងារ នយោបាយ សេដ្ឋកិច្ច និងសង្គម ព្រមទាំងបានលើកកម្ពស់គុណភាពជីវិត ការងារ បង្កើនទំនាក់ទំនង និងកិច្ចសហការល្អជាមួយបណ្តាប្រទេសនានា ក្នុងតំបន់ និងជុំវិញពិភពលោកថែមទៀតផង។ ជាមួយគ្នានេះដែរ ប្រព័ន្ធអ៊ីនធឺណិតនិងទំនើបកម្មនៃឧបករណ៍ឌីជីថល បានក្លាយជាមធ្យោបាយងាយស្រួលសម្រាប់ជនខិលខូចនៅទូទាំងពិភពលោកប្រើប្រាស់ដើម្បីរំលោភបំពាននិងកេងប្រវ័ញ្ចផ្លូវភេទ។ កុមារនិងយុវជនបានក្លាយជាគោលដៅរបស់ជនខិលខូចក្នុងការអូសទាញឱ្យប្រព្រឹត្ត ឬទទួលរងការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទតាមប្រព័ន្ធអនឡាញ។ ការប្រឈមនឹងគ្រោះថ្នាក់តាមប្រព័ន្ធអនឡាញអាចមានផលប៉ះពាល់ធ្ងន់ធ្ងរ និងយូរអង្វែង ទៅលើសុខភាព ផ្លូវចិត្ត ការអភិវឌ្ឍអារម្មណ៍ និងសុខុមាលភាពរបស់កុមារ។ បច្ចុប្បន្ន ដោយសារតែភាពអនាមិក និងវិសាលភាពដ៏ធំធេងនៃការប្រើប្រាស់អ៊ីនធឺណិតជុំវិញពិភពលោក បានជួយសម្រួលដល់ការកើនឡើងនៃឧក្រិដ្ឋកម្មដ៏អាក្រក់ចំពោះកុមារ ដូចជាការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ។ ក្រៅពីនេះ កុមារក៏អាចប្រឈមនឹងបញ្ហាជាច្រើនទៀតដូចជា ការរុកកួនតាមអនឡាញ ការលួងលោមតាមអនឡាញ ការទទួលបានព័ត៌មានមិនពិត និងការរំលោភលើឯកជនភាព។ ម្យ៉ាងវិញទៀត បច្ចេកវិទ្យាឌីជីថលបន្តវិវត្តយ៉ាងឆាប់រហ័ស ជាពិសេស ការកើនឡើងនៃបញ្ញាសិប្បនិម្មិត (AI) បានធ្វើឱ្យទិដ្ឋភាពនៃគ្រោះថ្នាក់ និងហានិភ័យអនឡាញមានការផ្លាស់ប្តូរយ៉ាងលឿនឥតឈប់ឈរ។ ហេតុនេះ ការការពារកុមារតាមប្រព័ន្ធអនឡាញនៅតែជាបញ្ហាប្រឈម ដែលកំពុងអនុវត្តបន្ត និងជាបន្ទាន់ ដោយទាមទារនូវការច្នៃប្រឌិត កិច្ចសហប្រតិបត្តិការអន្តរជាតិ និងការប្តេជ្ញាចិត្តរួមគ្នាពីគ្រប់វិស័យពាក់ព័ន្ធ។

ដើម្បីដោះស្រាយបញ្ហាប្រឈម ដែលពាក់ព័ន្ធនឹងកុមារតាមប្រព័ន្ធអនឡាញ មានលិខិតុបករណ៍អន្តរជាតិ និងលិខិតបទដ្ឋានគតិយុត្តជាច្រើន ត្រូវបានកសាងឡើងដើម្បីគាំទ្រ និងគាំពារចំពោះកុមារ។ ក្នុងនោះរួមមាន អនុសញ្ញាស្តីពីសិទ្ធិកុមារ ពិធីសារបន្ថែម ច្បាប់ គោលនយោបាយ ផែនការ និងលិខិតបទដ្ឋានគតិយុត្តនានា ដែលផ្តោតលើការការពារកុមារពីការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទតាមប្រព័ន្ធអនឡាញ ដោយបានដាក់ចេញនូវវិធានការបង្ការ ទប់ស្កាត់ និងឆ្លើយតបជាច្រើនដូចជា បទប្បញ្ញត្តិនានា ដែលដាក់បន្ទុកលើអ្នកផ្តល់សេវាអ៊ីនធឺណិត (ISPs) ឱ្យអនុវត្តវិធានការសុវត្ថិភាពសម្រាប់កុមារ។ ការអប់រំ និងការលើកកម្ពស់ចំណេះដឹង តាមរយៈការលើកកម្ពស់អក្ខរកម្មឌីជីថល និងពលរដ្ឋឌីជីថល ដោយបង្រៀនកុមារអំពីរបៀបប្រើប្រាស់បច្ចេកវិទ្យាដោយការទទួលខុសត្រូវ របៀបកំណត់ហានិភ័យ និងរបៀបឆ្លើយតបនៅពេលពួកគេជួបបញ្ហា។ ដំណោះស្រាយបច្ចេកទេសរួមមាន ការកំណត់របស់អ្នកប្រើប្រាស់ (User Settings) ការគ្រប់គ្រងដោយឪពុកម្តាយ (Parental Controls) ការច្រោះ ឬត្រងខ្លឹមសារ (Content Filter) ការបង្កើតឯកជនភាព និងការរាយការណ៍លើថ្នាលកម្មវិធី (Platform Reporting)។ល។

បច្ចុប្បន្នអ៊ីនធឺណិតបានរួមចំណែកយ៉ាងសំខាន់ក្នុងការអប់រំ។ ការភ្ជាប់ទំនាក់ទំនងយ៉ាងទូលំទូលាយនៅក្នុងពិភពលោកនាពេលបច្ចុប្បន្ននេះ បានរំលេចឱ្យឃើញថា អ៊ីនធឺណិតគឺជា **ប្រកផ្លូវឆ្ពោះទៅកាន់ឱកាសដោយ**

គ្មានទីបញ្ចប់ រាប់តាំងពីការចែករំលែកគំនិតច្នៃប្រឌិតនៅលើប្រព័ន្ធផ្សព្វផ្សាយសង្គមរហូតដល់ការប្រើប្រាស់ពិភពនិម្មិតអនឡាញ (Virtual Reality)។ តែទន្ទឹមនេះ វាក៏ជាទិដ្ឋភាពដែលពោរពេញទៅដោយហានិភ័យលាក់កំបាំងសម្រាប់កុមារផងដែរ។ ដើម្បីបំបែកនូវភាពមន្ទិលនៃអ៊ីនធឺណិតឱ្យមានភាពងាយស្រួលក្នុងការសិក្សាទស្សនទានអ៊ីនធឺណិតត្រូវបានបង្កើតឡើងក្នុងគោលគំនិតដ៏សាមញ្ញ និងមានប្រសិទ្ធភាពសម្រាប់អនុវត្តក្នុងពិភពអនឡាញប្រកបដោយសុវត្ថិភាព និងការទទួលខុសត្រូវ។ ទស្សនទាននេះហៅថា **"ធាតុផ្សំទាំងប្រាំមួយ"** ដែលផ្តល់សិទ្ធិអំណាចដល់អ្នកប្រើប្រាស់ឱ្យគិតពិចារណា ការពារខ្លួន និងជំរុញឱ្យមានអន្តរកម្មវិជ្ជមាន។ សម្រាប់អ្នកសិក្សា អ្នកអប់រំ កុមារ និងក្រុមគ្រួសារត្រូវយល់អំពីគោលគំនិតទាំងនេះ ដើម្បីជួយដល់មនុស្សជំនាន់ក្រោយឱ្យមានជំនាញការពារខ្លួនតាមប្រព័ន្ធអនឡាញ។

សៀវភៅនេះ ត្រូវបានរៀបចំផ្នែកៗដើម្បីងាយស្រួលយល់ និងរំលេចពីគោលបំណងច្បាស់លាស់។ ដើម្បីផ្តល់ចំណេះដឹងជាមូលដ្ឋានអំពីអ៊ីនធឺណិត ដោយផ្តោតលើគោលគំនិតសំខាន់ៗទាំង៦ ដែលហៅថា **"ធាតុផ្សំទាំងប្រាំមួយ"** ដែលជាការបង្ហាញពីឫសគល់នៃបញ្ហា ហានិភ័យ អត្ថប្រយោជន៍ និងការការពារកុមារតាមប្រព័ន្ធអនឡាញ។ ទន្ទឹមនេះ ក៏មានការណែនាំអំពីការកំណត់សុវត្ថិភាពលើថ្នាលកម្មវិធី (ដូចជា Facebook, Instagram, TikTok និង YouTube) ដែលជា**ខ្សែការពារដំបូង** សម្រាប់ប្រើប្រាស់ក្នុងការផ្លាស់ប្តូរតាមបំណងលើថ្នាលកម្មវិធីដោយរាប់ចាប់ពីការគ្រប់គ្រងឯកជនភាពរហូតដល់ការច្រោះ(Filter)ខ្លឹមសារ។ ក្រៅពីនេះ ក៏មានការបង្កើនសមត្ថភាពសម្រាប់អ្នកផ្តល់សេវាសង្គមកិច្ចក្នុងការការពារកុមារតាមប្រព័ន្ធអនឡាញផងដែរ តាមរយៈការផ្តល់នូវវិធីសាស្ត្រនានា ដើម្បីឆ្លើយតបនឹងការកើនឡើងនៃករណីការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ (Online Child Sexual Exploitation and Abuse - OCSEA) ដោយផ្តោតលើការផ្តល់ចំណេះដឹង ជំនាញ និងយុទ្ធសាស្ត្រជាក់ស្តែងសម្រាប់ការវាយតម្លៃហានិភ័យ អន្តរាគមន៍ ការផ្តល់សេវាឆ្លើយតប និងការអប់រំក្រុមគ្រួសារ។

> សុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ គឺចាប់ផ្តើមដោយ**ការយល់ដឹង ការណែនាំ** និង**ការការពារទុកជាមុន**។ ការបញ្ឈប់កុមារពីការចូលប្រើប្រាស់អ៊ីនធឺណិតមិនមែនជាដំណោះស្រាយទេ ប៉ុន្តែការណែនាំពួកគេឱ្យប្រើប្រាស់អ៊ីនធឺណិតដោយឈ្លាសវៃទើបជាគន្លឹះសំខាន់សម្រាប់យើង។ ការបង្រៀនឱ្យ**គិតល្អិតល្អន់** (Critical thinking) ស្វែងយល់ពីគន្លឹះនៃការការពារខ្លួន ការទទួលខុសត្រូវតាមប្រព័ន្ធអនឡាញ និងការវាយតម្លៃព័ត៌មាន (ក្លែងបន្លំ បោកប្រាស់) ដើម្បីបង្កើតភាពធន់ទប់ទល់នឹងការគំរាមកំហែងតាមប្រព័ន្ធអនឡាញនានាចំពោះកុមារ ដែលកំពុងតែវិវត្តឥតឈប់ឈរ។

២. កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ

២.១. ការសិក្សាស្រាវជ្រាវស្តីពីការប្រើប្រាស់ប្រព័ន្ធអនឡាញរបស់កុមារ

បច្ចុប្បន្ននេះ កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញត្រូវបានបង្កើនការយកចិត្តទុកដាក់យ៉ាងខ្លាំង តាមរយៈការសិក្សាស្រាវជ្រាវ និងប្រមូលភស្តុតាងជាក់លាក់ជាច្រើនបានបង្ហាញថា ការប្រើប្រាស់ប្រព័ន្ធអនឡាញរបស់កុមារក្នុងប្រទេសកំពុងអភិវឌ្ឍន៍បាននឹងកំពុងកើនឡើងគួរឱ្យកត់សម្គាល់។ ថ្មីៗនេះ តាមរយៈការសិក្សាស្រាវជ្រាវប្រកបដោយគុណវុឌ្ឍិ បានបង្ហាញយ៉ាងច្បាស់អំពីសកម្មភាព និងវិធីសាស្ត្រ ដែលត្រូវអនុវត្ត ដើម្បីការពារកុមារតាមប្រព័ន្ធអនឡាញ។

២.១.១. ការសិក្សាស្រាវជ្រាវជាសាកល និងក្នុងតំបន់អំពីការប្រើប្រាស់អ៊ីនធឺណិតរបស់កុមារ

នៅឆ្នាំ២០២២ អង្គការឆាលហ្វាន អង្គការភ្លែនអន្តរជាតិ និងសាកលវិទ្យាល័យវេស្ទើនស៊ីដនី បានធ្វើការសិក្សាស្រាវជ្រាវនៅប្រទេសគោលដៅមួយចំនួនក្នុងតំបន់អាស៊ី និងប៉ាស៊ីហ្វិក ពាក់ព័ន្ធនឹងសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ[1]។ ទន្ទឹមនោះក៏មានការសិក្សាស្រាវជ្រាវស្តីពី "ការបញ្ឈប់គ្រោះថ្នាក់ - Disrupting Harm"[2] នៅក្នុងប្រទេសចំនួន ១៣ នៃតំបន់អាស៊ីអាគ្នេយ៍ និងអាហ្វ្រិក ដែលបានផ្តល់នូវការយល់ដឹងយ៉ាងស៊ីជម្រៅផងដែរ។

តាមរយៈការស្រាវជ្រាវទៅលើកុមារនៅបណ្តាប្រទេសក្នុងតំបន់អាស៊ី និងប៉ាស៊ីហ្វិក បានបង្ហាញថា៖

- កុមារប្រើប្រាស់បច្ចេកវិទ្យាច្រើនជាងឪពុកម្តាយ អាណាព្យាបាល និងអ្នកថែទាំរបស់ពួកគេ ហើយពួកគេភាគច្រើនប្រើប្រាស់អ៊ីនធឺណិតនៅផ្ទះ សាលារៀន ឬទីសាធារណៈ។ល។
- ទូរសព្ទឆ្លាត និងថ្នាលកម្មវិធី គឺជាផ្នែកមួយនៃជីវិតប្រចាំថ្ងៃ និងកំណត់ពីរបៀបដែលកុមារមានទំនាក់ទំនងជាមួយគ្នា។
- កុមារមានចំណេះដឹង និងជំនាញអំពីប្រព័ន្ធអនឡាញជាងមនុស្សពេញវ័យ ឪពុកម្តាយ អាណាព្យាបាល និងអ្នកថែទាំ។
- ឪពុកម្តាយ អាណាព្យាបាល និងអ្នកថែទាំ មានលទ្ធភាពតិចតួចក្នុងការផ្តល់ដំបូន្មានអំពីការប្រើប្រាស់បច្ចេកវិទ្យាដល់កុមារ។

តាមរយៈការស្រាវជ្រាវជាសាកល និងក្នុងតំបន់បានរកឃើញនូវភាពខុសគ្នាមួយចំនួន នៃបទពិសោធរបស់កុមារនៅលើអ៊ីនធឺណិត ដោយផ្អែកលើយេនឌ័រ ពិការភាព ឬលក្ខណៈផ្សេងៗទៀត ក្នុងនោះរួមមាន៖

- ការប្រើប្រាស់ប្រព័ន្ធអនឡាញរបស់កុមារា និងកុមារី មានកម្រិតជំនាញប្រហាក់ប្រហែលគ្នា តែពេលខ្លះកុមារីមានជំនាញខ្ពស់ជាងកុមារាលើផ្នែកសុវត្ថិភាពឌីជីថល និងភាពធន់នឹងឌីជីថល[3]។

[1] www.childfund.org.au/swipe-safe-program/

[2] www.end-violence.org/disrupting-harm

[3] UNESCO, Digital Kids Asia Pacific, 2019; Swipe Safe Vietnam Gender Analysis

- ទាំងកុមារា និងកុមារីប្រើប្រាស់អ៊ីនធឺណិតក្នុងសកម្មភាពដូចគ្នា ដូចជាការកម្សាន្ត សកម្មភាពសង្គម និងការស្វែងរកព័ត៌មាន។ តែទន្ទឹមនេះ ក៏មានភាពខុសគ្នារវាងសកម្មភាពរបស់កុមារា និងកុមារីនៅលើប្រព័ន្ធអនឡាញផងដែរពាក់ព័ន្ធនឹងផ្នត់គំនិតយេនឌ័រ ដូចជា កុមារីចំណាយពេលច្រើនតាមប្រព័ន្ធអនឡាញ ដើម្បីទិញរបស់របរនៅលើបណ្តាញផ្សព្វផ្សាយសង្គម ចំណែកកុមារាចំណាយពេលច្រើនលើការលេងហ្គេមអនឡាញ[4]។
- បច្ចេកវិទ្យាឌីជីថលបានផ្តល់ការគាំទ្រយ៉ាងទូលំទូលាយលើបរិយាបន្ន និងឱកាសក្នុងការចូលរួមរបស់កុមារមានពិការភាព ដែលអាចឱ្យពួកគេចូលប្រើប្រាស់ព័ត៌មានលើបណ្តាញសង្គម និងការកម្សាន្ត ពេលខ្លះស្ថិតក្នុងជំហរ "សមភាព" ជាមួយអ្នកប្រើប្រាស់ដទៃទៀតផងដែរ ប៉ុន្តែពេលខ្លះពួកគេបានជ្រើសរើសយកការបិទបាំង ឬមិនបិទបាំងពិការភាពរបស់គេនៅលើប្រព័ន្ធអនឡាញ។ ទោះជាបែបនេះក្តី កុមារមានពិការភាពអាចប្រឈមនឹងរបាំងក្នុងការចូលប្រើប្រាស់អ៊ីនធឺណិត ដោយសារបញ្ហារាងកាយ និងការគិតបែបអវិជ្ជមានរបស់ឪពុកម្តាយ ដែលយល់ថាកុមារមានពិការភាពរៀនមិនចេះ ងាយរងគ្រោះ ឬងាយត្រូវបានគេរុកកួនតាមប្រព័ន្ធអនឡាញ[5]។
- កុមារា និងកុមារីជាច្រើនមានបទពិសោធអំពីហានិភ័យតាមប្រព័ន្ធអនឡាញដូចគ្នា តែខ្លះទៀតក៏ខុសគ្នាដែរ។ ឧទាហរណ៍ កុមារីទទួលសំណើធ្វើជាមិត្តជាច្រើនពីមនុស្សដែលពួកគេមិនស្គាល់ ភាគច្រើនទទួលនូវសារបែបផ្លូវភេទ ការលួងលោម និងរងការរុកកួនលើរូបរាងច្រើនជាងកុមារា។ ដោយឡែក កុមារាចូលចិត្តចូលរួមច្រើនក្នុងទង្វើហានិភ័យតាមប្រព័ន្ធអនឡាញ ដូចជា ផ្ញើនូវព័ត៌មានផ្ទាល់ខ្លួន មើលរូបភាព-សម្ភារៈបែបផ្លូវភេទ និងទាញយកដោយខុសច្បាប់។
- កុមារមានពិការភាពក៏ប្រឈមនឹងហានិភ័យនៅលើប្រព័ន្ធអនឡាញដូចកុមារដទៃទៀតដែរ ប៉ុន្តែពួកគេអាចប្រឈមនឹងហានិភ័យលើសពីគេ។ ឧទាហរណ៍ ប្រសិនបើពិការភាពរបស់ពួកគេត្រូវបានបើកបង្ហាញ ឬត្រូវបានកំណត់ កុមារអាចប្រឈមនឹងការមិនយកចិត្តទុកដាក់ ការមើលងាយ ឬការរុកកួន ហើយក៏អាចត្រូវប្រឈមនឹងហានិភ័យជាក់លាក់ផងដែរ ចំពោះពិការភាពរបស់ពួកគេ ដូចជា កុមារខ្សោយគំហើញមានការពិបាកក្នុងការកំណត់រូបភាពរបស់ខ្លួន នៅពេលមានការបង្ហោះដោយមិនមានការយល់ព្រម។

ការសិក្សាស្រាវជ្រាវក៏បានរកឃើញផងដែរថា៖

- កុមារបានបង្ហាញពីហានិភ័យជាច្រើនទាក់ទងនឹងបទពិសោធ នៃជីវិតតាមប្រព័ន្ធអនឡាញរបស់ពួកគេ ដូចជា៖
    - ហានិភ័យនៃមាតិកា (ការរុកកួន សកម្មភាពហិង្សា ការមើលឃើញរូបភាពអាសអាភាស និងការរំលោភបំពានតាមប្រព័ន្ធអនឡាញ)
    - ហានិភ័យនៃសុវត្ថិភាព (ការឆបោក មនុស្សចម្លែក ការរក្សាការសម្ងាត់ផ្ទាល់ខ្លួន)
    - ហានិភ័យសុខភាព (ផ្លូវកាយ ផ្លូវចិត្ត)

[4] UNICEF, Girls' Digital Literacy in the East Asia and Pacific Region, 2023
[5] Council of Europe, Report on children with disabilities in the digital environment, 2019

- កុមារមានទំនុកចិត្តខ្ពស់ក្នុងការរក្សាសុវត្ថិភាពខ្លួនតាមប្រព័ន្ធអនឡាញ ប៉ុន្តែរបៀបការពារខ្លួននៅមានកម្រិតនៅឡើយ
- កុមារបានលើកឡើងថា ពួកគេចង់ពិភាក្សាជាមួយឪពុកម្តាយ អាណាព្យាបាល ឬអ្នកថែទាំអំពីសុវត្ថិភាពតាមប្រព័ន្ធអនឡាញ ដើម្បីទទួលបានដំបូន្មាន និងការណែនាំល្អៗ
- ការឆ្លើយតបទៅនឹងបញ្ហានៅលើប្រព័ន្ធអនឡាញរបស់កុមារពីមនុស្សពេញវ័យ ភាគច្រើនគឺផ្តល់ត្រឹមតែកម្រិតអ្វីដែលគេបានដឹង និងហាមឃាត់មិនឱ្យកុមារប្រើប្រាស់អ៊ីនធឺណិត។ ទង្វើនេះមិនអាចបញ្ឈប់បញ្ហាបានទេ ប៉ុន្តែបានធ្វើឱ្យកុមារមានអារម្មណ៍ឯកា និងអាចកាត់ផ្តាច់នូវការគាំទ្រ ឬការជួយពីមិត្តភក្តិរបស់ពួកគេ។

លទ្ធផលនៃការស្រាវជ្រាវស្តីពី "ការបញ្ឈប់គ្រោះថ្នាក់ - Disrupting Harm" ក្នុងប្រទេសចំនួន ១៣ នៅអាស៊ីអាគ្នេយ៍ និងអាហ្វ្រិក បានបង្ហាញថា៖

- មួយភាគបី នៃកុមាររងគ្រោះពីការរំលោភបំពានតាមប្រព័ន្ធអនឡាញមិនបានប្រាប់នរណាម្នាក់ពីអ្វី ដែលពួកគេបានជួបប្រទះនោះទេ
- ប្រសិនបើគេនិយាយ គឺនិយាយជាមួយមិត្តភក្តិ ឪពុកម្តាយ ឬបងប្អូនបង្កើត
- កុមារស្ទើរតែទាំងអស់ មិនរាយការណ៍ទៅយន្តការផ្លូវការទេ លុះត្រាតែមានការជួយជ្រោមជ្រែងដោយផ្ទាល់ពីសមាជិកគ្រួសារ។ មានកុមារប្រមាណ ០-៣%ប៉ុណ្ណោះ ដែលបានរាយការណ៍។
- បណ្តាញទូរសព្ទជំនួយ និងប្រព័ន្ធកិច្ចការពារកុមារមិនមែនជាជម្រើសដំបូង នៃការរកជំនួយរបស់ពួកគេទេ
- ពួកគេបាននិយាយថា ពួកគេមិនដឹងថាតើត្រូវរកជំនួយពីអ្នកណា?
- ពួកគេមានអារម្មណ៍អាម៉ាស់ និងបន្ទោសខ្លួនឯងចំពោះអ្វីដែលជនទុច្ចរិតបានប្រព្រឹត្តមកលើ។

តាមរយៈរបកគំហើញ នៃការស្រាវជ្រាវអាចជួយឱ្យយើងដឹងថា យើងត្រូវធ្វើការកែទម្រង់នូវវិធីសាស្ត្រក្នុងការដោះស្រាយបញ្ហាកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញនៅក្នុងសហគមន៍។ មានព័ត៌មានជាច្រើនអំពីកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ ផ្តល់ដល់ឪពុកម្តាយ អ្នកថែទាំកុមារឱ្យទាក់ទងបណ្តាញជំនួយកុមារ ឬសេវាគាំពារសង្គម ដែលនាំឱ្យមនុស្សភាគច្រើនគិតថា "**សេវាទាំងនោះអាចដោះស្រាយបញ្ហានេះបាន**" ប៉ុន្តែនេះមិនមែនជាដំណោះស្រាយជាក់ស្តែងទេ។ បញ្ហាទាំងនេះ មិនអាចដោះស្រាយបានក្នុងវិស័យតែមួយនោះទេ តែត្រូវដោះស្រាយដោយអន្តរវិស័យ ដូចជា ការប្រឹក្សាយោបល់ និងការទទួលបានជំនួយផ្នែកច្បាប់។ល។ កុមារដែលរងផលប៉ះពាល់ពីការរំលោភបំពានតាមប្រព័ន្ធអនឡាញ ត្រូវការកិច្ចគាំទ្រជាច្រើន ដើម្បីជួយពួកគេ ជាពិសេសពីអ្នកដែលជិតស្និទ្ធជាមួយពួកគេ ដូចជា គ្រួសារជាដើម។

២.១.២. ការយល់ឃើញផ្សេងគ្នារវាងមនុស្សពេញវ័យ និងកុមារចំពោះអ៊ីនធឺណិត

តាមការស្រាវជ្រាវបានរកឃើញថា ទស្សនៈ ឬការយល់ឃើញអំពីអ៊ីនធឺណិតរបស់កុមារ និងមនុស្សពេញវ័យ គឺមានភាពខុសគ្នា៖

- បទពិសោធក្នុងការប្រើប្រាស់អ៊ីនធឺណិតរបស់កុមារ និងមនុស្សពេញវ័យ គឺមានភាពផ្សេងគ្នា
- មនុស្សពេញវ័យភាគច្រើនតែងគិតអំពីការរស់នៅដែលមានលក្ខណៈសាមញ្ញ (មិនរញ៉េរញ៉ៃ ឬស្មុគស្មាញ) មុនពេលមានអ៊ីនធឺណិត ឬប្រើប្រាស់អ៊ីនធឺណិត
- ចំពោះកុមារ ការប្រើប្រាស់អ៊ីនធឺណិតបានក្លាយជាផ្នែកមួយដ៏សំខាន់ក្នុងជីវិតប្រចាំថ្ងៃរបស់ពួកគេ
- មនុស្សពេញវ័យបានយល់ដឹងពីការវិវឌ្ឍនៃអ៊ីនធឺណិត ទន្ទឹមនោះ ពួកគេក៏មានការយល់ដឹងពីនិយាម (ច្បាប់ទម្លាប់) សីលធម៌ដែលមាននៅក្នុងសង្គមជាក់ស្តែង និងអាចផ្សារភ្ជាប់ការយល់ដឹងទាំងនេះជាមួយទំនាក់ទំនងថ្មី (អនឡាញ) នាពេលបច្ចុប្បន្ន
- ទន្ទឹមនឹងការប្រើប្រាស់ប្រព័ន្ធអនឡាញ កុមារនៅតែបន្តរៀនអំពីនិយាម សីលធម៌ នៅក្នុងសង្គមជាក់ស្តែង។ ពួកគេត្រូវតែរៀនរឿងទាំងពីរនេះ ក្នុងពេលតែមួយ។

ទោះស្ថិតក្នុងស្ថានភាពបែបនេះក្តី ដរាបណាអ៊ីនធឺណិតនៅតែត្រូវបានបន្តប្រើប្រាស់ ការងាររបស់យើងដែលជាអ្នកផ្តល់សេវាសង្គមកិច្ច គឺត្រូវជួយកុមារឱ្យមានសុវត្ថិភាពនៅតាមប្រព័ន្ធអនឡាញ តាមដែលអាចធ្វើទៅបាន។ ចំណុចចុងក្រោយនៃការសិក្សាស្រាវជ្រាវបានបង្ហាញថា មធ្យោបាយដ៏មានប្រសិទ្ធភាព គឺការលើកទឹកចិត្តឱ្យមានការប្រាស្រ័យទាក់ទងគ្នាល្អ ចំពោះកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ ដោយធានាថា ការលើកឡើងពីកង្វល់របស់កុមារនឹងមិនត្រូវទទួលរងការដាក់ទណ្ឌកម្ម ដូចជា ការស្តីបន្ទោស ការវាយដំ ការហាមឃាត់មិនឱ្យប្រើទូរសព្ទវៃឆ្លាត ឬអ៊ីនធឺណិតឡើយ។

ការសិក្សាស្រាវជ្រាវបង្ហាញថា កុមារភ័យខ្លាចចំពោះការកាត់ផ្តាច់ការប្រើប្រាស់អ៊ីនធឺណិត ប្រសិនបើមានអ្វីមួយខុសប្រក្រតី។ ដូច្នេះ ពួកគេមិនហ៊ានប្រាប់ពីកង្វល់របស់ពួកគេទៅនរណាម្នាក់ឡើយ។ តាមការសិក្សាស្រាវជ្រាវនេះក៏បង្ហាញថា ការហាមឃាត់ការប្រើប្រាស់អ៊ីនធឺណិតអាចនឹង៖

- កាត់ផ្តាច់ទំនាក់ទំនងរបស់ពួកគេពីមិត្តភក្តិ និងអ្នកជួយគាំទ្រ
- ធ្វើឱ្យមានការលំបាកប្រមូលវត្ថុតាង និងពិនិត្យតាមដានបញ្ហា
- ធ្វើឱ្យកុមារធ្លាក់ទឹកចិត្ត និងបាត់បង់អំណាច តាមរយៈការដកហូតមធ្យោបាយធ្វើសកម្មភាពរបស់ពួកគេ។ ឧទាហរណ៍ ការរាំងខ្ទប់ (Block) ឬការរាយការណ៍ (Report) នៅលើថ្នាលកម្មវិធីផ្សេងៗ។

ការពិភាក្សា និងសកម្មភាពរបស់មនុស្សពេញវ័យដើរតួជា "ដៃគូសុវត្ថិភាពតាមប្រពន្ធ័អនឡាញ" គឺជាផ្នែកដ៏សំខាន់មួយនៃភាពជោគជ័យ ក្នុងការដោះស្រាយបញ្ហាសុវត្ថិភាពកុមារតាមអនឡាញ។

២.២. ការបញ្ចូលការគេចប្រវ័ញ្ច និងរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញនៅក្នុងកិច្ចការពារកុមារ

២.២.១. គោលនយោបាយកិច្ចការពារកុមារ

"កិច្ចការពារកុមារ" នៅតែបន្តពង្រីកវិសាលភាពក្នុងប្រទេសកំពុងអភិវឌ្ឍន៍។ ការសិក្សាអំពីជំនាញនេះនឹងបង្កើនមូលធនមនុស្ស និងកម្លាំងការងារ ដើម្បីកសាងប្រព័ន្ធកិច្ចការពារកុមារ។ ប្រព័ន្ធទាំងនេះនឹងបន្តវិវឌ្ឍដោយគុណភាព និងការផ្តល់សេវាផ្សេងៗ កាន់តែប្រសើរឡើងពីមួយថ្ងៃទៅមួយថ្ងៃ។ ភាពជោគជ័យនៃការពង្រឹងប្រព័ន្ធកិច្ចការពារកុមារ គឺអាស្រ័យលើការលះបង់ខ្ពស់របស់យើងក្នុងការគាំទ្រកុមារ។ នៅក្នុងវិស័យកិច្ចការពារកុមារមានបញ្ហាជាច្រើនកំពុងប្រែប្រួលឥតឈប់ឈរ។ ដូច្នេះ អ្នកផ្តល់សេវាសង្គមកិច្ចក៏ត្រូវមានជំនាញទូទៅជាច្រើនទៀតផងដែរ ពិសេសជំនាញឆ្លើយតបទៅនឹងតម្រូវការជាក់លាក់របស់កុមារ។ កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ គឺជាប្រធានបទថ្មីដែលមនុស្សគ្រប់គ្នាចង់ដឹង។

រាជរដ្ឋាភិបាលកម្ពុជាបានដាក់ចេញនូវច្បាប់ គោលនយោបាយជាតិ ផែនការយុទ្ធសាស្ត្រជាតិ ផែនការសកម្មភាពជាតិ និងយន្តការជាច្រើន ដែលពាក់ព័ន្ធនឹងកិច្ចការពារកុមារ ក្នុងគោលបំណងសំខាន់ៗ រួមមាន៖

- ផ្តោតលើឧត្តមប្រយោជន៍របស់កុមារ ដែលជាបុគ្គលមានអាយុក្រោម ១៨ឆ្នាំ
- ផ្តោតលើកិច្ចការពារកុមារពីអំពើហិង្សា ការកេងប្រវ័ញ្ច ការរំលោភបំពាន និងការមិនអើពើ
- ផ្តោតលើសកម្មភាពបង្ការ ទប់ស្កាត់ និងការឆ្លើយតប។

ក្នុងនោះក៏មានដាក់ចេញនូវសកម្មភាពសំខាន់ៗមួយចំនួនផងដែរ រួមមាន៖

- ការពង្រឹងយន្តការការពារកុមារតាមសហគមន៍ ដែលជាការការពារ និងឆ្លើយតបនឹងហានិភ័យ
- ការពង្រឹងប្រព័ន្ធកិច្ចការពារកុមាររបស់រាជរដ្ឋាភិបាល និងអង្គការមិនមែនរដ្ឋាភិបាលនានា។

២.២.២. អ្នកពាក់ព័ន្ធនឹងកិច្ចការពារកុមារអហ្វឡាញ

កិច្ចការពារកុមារ គឺជាការទទួលខុសត្រូវរបស់យើងទាំងអស់គ្នា ដែលរាប់ចាប់ពីគ្រួសារ មិត្តភក្តិ សាលារៀន។ល។ ភាគីពាក់ព័ន្ធទាំងអស់ រួមមាន ក្រុមផ្សេងៗនៅក្នុងសង្គម ដូចមានបង្ហាញក្នុងរូបដ្យាក្រាមគំរូវិភាគបែបមជ្ឈដ្ឋាន។ ចំណុចសំខាន់នៃកិច្ចគាំទ្រ ឬការផ្តល់ជំនួយដល់កុមារ ដោយផ្អែកលើគំរូវិភាគបែបមជ្ឈដ្ឋាន គឺក្រុមនៅក្នុងរង្វង់ខាងក្នុង រួមមាន ក្រុមគ្រួសារ សាច់ញាតិ និងមិត្តភក្តិ។ ដោយឡែកក្រុមនៅក្នុងរង្វង់ខាងក្រៅ ដែលជាអ្នកផ្តល់សេវាសង្គមកិច្ច ត្រូវផ្តោតលើកិច្ចគាំទ្រ និងពង្រឹងសមត្ថភាព ចំណេះដឹងអ្នកនៅរង្វង់ខាងក្នុង។

២.២.៣. កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ

នៅពេលនិយាយអំពីកិច្ចការពារកុមារ គំរូនៃកិច្ចអន្តរាគមន៍តាមប្រព័ន្ធអនឡាញនិងអហ្វឡាញ គឺមិនមានភាពខុសគ្នាទេ ហើយលក្ខណៈពិសេសនៃកិច្ចអន្តរាគមន៍ទាំងអស់នេះ គឺនៅដដែល ដោយហេតុផលថា៖

- ផ្ដល់កិច្ចការពារចំពោះកុមារ ដែលត្រូវបានកំណត់និយមន័យដូចគ្នា
- កិច្ចការពារកុមារ គឺការពារកុមារពីហានិភ័យដូចគ្នា ដូចជាអំពើហិង្សា ការកេងប្រវ័ញ្ច ការរំលោភបំពាន និងការមិនអើពើ
- ផ្ដោតលើការបង្ការ ទប់ស្កាត់ និងឆ្លើយតប ដែលជាគន្លឹះសំខាន់
- ពង្រឹងយន្តការដោះស្រាយទាំងផ្លូវការ (អាជ្ញាធរ...) និងក្រៅផ្លូវការ (ឪពុកម្ដាយ ក្រុមយុវជន អ្នកស្ម័គ្រចិត្ត...) ដើម្បីជួយការពារកុមារពីហានិភ័យ
- មានយន្តការល្អដែលអាចកំណត់បញ្ហានៅដំណាក់កាលដំបូង មុនពេលរីករាលដាលធ្ងន់ធ្ងរ។

"កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ" មានគំរូអន្តរាគមន៍ដូចគ្នានឹងអហ្វឡាញដែរ ហើយកិច្ចការនេះក៏ទើបតែមានសន្ទុះឡើងខ្លាំងនៅក្នុងជីវិតនាសម័យបច្ចេកវិទ្យាទំនើបនេះដែរ។

អនឡាញគឺជាផ្នែកសំខាន់មួយនៃទំនាក់ទំនងប្រចាំថ្ងៃ ទាំងនៅក្នុងគ្រួសារ សាលារៀន កន្លែងការងារ និងសង្គម។ ឧទាហរណ៍ យើងប្រើប្រាស់បច្ចេកវិទ្យាដើម្បីធ្វើការពីផ្ទះ ឬកុមាររៀនតាមប្រព័ន្ធអនឡាញ។ ដូច្នេះការបង្ការ ទប់ស្កាត់ និងឆ្លើយតបចំពោះរឿងនេះ គឺត្រូវការចាំបាច់ណាស់នូវកិច្ចអន្តរាគមន៍ពីអ្នកផ្តល់សេវាសង្គមកិច្ច ដែលពេលខ្លះតម្រូវឱ្យអ្នកផ្តល់សេវាសង្គមកិច្ចប្រើបច្ចេកវិទ្យា ដើម្បីធ្វើអន្តរាគមន៍។

តាមការស្រាវជ្រាវក៏បានបង្ហាញនូវកង្វល់មួយចំនួន ចំពោះកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញផងដែរ ដូចជា៖

- កង្វល់ទី១៖ កុមារមិនមានអារម្មណ៍ល្អក្នុងការសុំជំនួយពីមនុស្សពេញវ័យ ដែលពួកគេជឿទុកចិត្ត ដើម្បីដោះស្រាយបញ្ហាជួបប្រទះតាមប្រព័ន្ធអនឡាញទេ។
- កង្វល់ទី២៖ គំរូវិភាគបែបមជ្ឈដ្ឋានបង្ហាញថា កិច្ចអន្តរាគមន៍ទប់ស្កាត់ និងការឆ្លើយតបដំបូងចំពោះបញ្ហានៃកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ គឺគ្រួសារ និងមិត្តភក្តិរបស់ពួកគេ។

កង្វល់ទាំងពីរនេះ ទាមទារឱ្យមានការដោះស្រាយ។

ការស្រាវជ្រាវក៏បានបង្ហាញដែរថា ការពិភាក្សាអំពីបញ្ហាជាមួយកុមារ គឺជាកិច្ចការសំខាន់ដែលយើងទាំងអស់គ្នាត្រូវធ្វើ និងលើកទឹកចិត្តឱ្យអនុវត្ត៖

- លើកទឹកចិត្តឱ្យបង្កើតនូវទំនាក់ទំនងល្អប្រសើរក្នុងគ្រួសារ បងប្អូន និងមិត្តភក្តិ ដោយឱ្យលើកបញ្ហា ឬការបារម្ភផ្សេងៗបានទាន់ពេលវេលា ទើបអាចជួយទប់ស្កាត់មិនឱ្យក្លាយជាបញ្ហាធំបាន។
- ពង្រឹង និងផ្តល់កិច្ចគាំទ្រដល់គ្រួសារ មិត្តភក្តិ អំពីជំនាញ និងចំណេះដឹងក្នុងការផ្តល់កិច្ចគាំទ្របឋមដល់កុមារ ដែលទទួលរងផលប៉ះពាល់ និងរបៀបឆ្លើយតប និងកិច្ចគាំទ្រផ្សេងទៀត។

មានបញ្ហាខ្លះនៅក្នុងបរិបទអហ្វឡាញ និងអនឡាញ បង្ហាញនូវសកម្មភាពដូចគ្នា ប៉ុន្តែមានប្រតិកម្មខុសគ្នា។ ឧទាហរណ៍ "ឥទ្ធិពលនៃគ្រួសារ" នៅក្នុងជីវិតពិតរាល់ទំនាក់ទំនងរបស់យើងជាមួយមនុស្សទូទៅ តែងត្រូវបានដាក់កម្រិតតឹងរឹង ប៉ុន្តែនៅពេលយើងប្រើជីវិតតាមប្រព័ន្ធអនឡាញ យើងអាចមានទំនាក់ទំនងជាមួយមនុស្សជាច្រើនគ្រប់ទីកន្លែងជុំវិញពិភពលោក។ ដើម្បីយល់ដឹងពីរឿងរ៉ាវទាំងអស់នេះ កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញតម្រូវឱ្យយើងរៀនជំនាញ និងចំណេះដឹងថ្មីៗមួយចំនួន ដើម្បីប្រើប្រាស់ និងផ្សារភ្ជាប់ជីវិតតាមប្រព័ន្ធអនឡាញជាមួយកុមារ។ ជំនាញថ្មីៗ ដែលកម្លាំងសេវាសង្គមត្រូវដឹង រួមមាន៖

- បង្កើនការយល់ដឹង និងភាពស៊ាំជាមួយបច្ចេកវិទ្យា ការប្រើប្រាស់ឧបករណ៍ឌីជីថល ថ្នាលកម្មវិធី និងហ្គេមអនឡាញ។
- ការប្រើប្រាស់ឧបករណ៍បច្ចេកវិទ្យាផ្សេងៗ ដូចជាទូរសព្ទវៃឆ្លាត ថេបប្លេត ឬកុំព្យូទ័រជាដើម។
- ស្គាល់ពីថ្នាលកម្មវិធី និងមុខងាររបស់វា (ឧទាហរណ៍ ចេះប្រើ Facebook និងដឹងពីមុខងារសុវត្ថិភាពរបស់ Facebook)។

ចំណេះដឹងថ្មីៗ រួមមាន៖

- យល់ដឹងពីភាពខុសគ្នានៃការរំលោភបំពាន ការកេងប្រវ័ញ្ច និងបញ្ហាផ្សេងទៀតតាមអនឡាញ
- យល់ដឹងពីផលប៉ះពាល់នៃបញ្ហាតាមប្រព័ន្ធអនឡាញមួយចំនួន ដែលខុសពីបញ្ហាអហ្វឡាញ តែបញ្ហាតាមប្រព័ន្ធអនឡាញមួយចំនួនទៀតអាចមានផលប៉ះពាល់ដូចគ្នានឹងបញ្ហាអហ្វឡាញដែរ
- យល់ដឹងពីការប្រែប្រួលនៃអាកប្បកិរិយារបស់កុមារ និងសញ្ញាណទូទៅនៃបញ្ហាតាមអនឡាញ
- យល់ពីរបៀបឆ្លើយតបសមស្រប ចំពោះបញ្ហាតាមប្រព័ន្ធអនឡាញ ដោយ ប្រើប្រាស់ជំនាញដែលមានស្រាប់ក្នុងជីវិតជាក់ស្តែង និងដឹងពីរបៀបច្នៃប្រឌិតជំនាញទាំងនោះ ដើម្បីដោះស្រាយបញ្ហាតាមប្រព័ន្ធអនឡាញ។

មធ្យោបាយនៃការការពារកុមារតាមប្រព័ន្ធអនឡាញ គឺជាការរៀន និងអនុវត្តនូវអ្វីដែលថ្មី ប៉ុន្តែត្រូវចងចាំថា គោលការណ៍មូលដ្ឋានសម្រាប់កិច្ចការពារកុមារ គឺអនុវត្តដូចគ្នា។ ការសិក្សាអំពីកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញនេះ គឺគ្រាន់តែជាការពង្រឹង និងបន្ថែមចំណេះដឹងថ្មីមួយចំនួនទៀតប៉ុណ្ណោះ លើមេរៀនកិច្ចការពារកុមារទូទៅ។ ដើម្បីឱ្យកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញអនុវត្តមានប្រសិទ្ធភាព គឺទាមទារឱ្យមានកិច្ចសហការគ្នារវាងក្រសួង ស្ថាប័នពាក់ព័ន្ធ អង្គការ សង្គមស៊ីវិល និងវិស័យឯកជន ក្នុងការគាំទ្រ និងពង្រឹងយន្តការផ្លូវការ និងក្រៅផ្លូវការនៅតាមសហគមន៍ឱ្យបានកាន់តែប្រសើរឡើងក្នុងការបង្ការ ទប់ស្កាត់ និងឆ្លើយតប។

៣. ធាតុផ្សំសំខាន់ៗនៃអ៊ីនធឺណិត

៣.១. អ៊ីនធឺណិតនិងទំនាក់ទំនងក្នុងសង្គម

ការប្រាស្រ័យទាក់ទងគ្នានៅក្នុងជីវិតប្រចាំថ្ងៃ មិនថានៅក្នុងគ្រួសារ កន្លែងសិក្សា កន្លែងធ្វើការ ឬការបង្ហាញអំពីចំណង់ចំណូលចិត្តផ្សេងៗ... ទង្វើទាំងនេះគឺជា "ទំនាក់ទំនងសង្គម" សកម្មភាពទាំងនេះក៏មាននៅតាមប្រព័ន្ធអនឡាញផងដែរ ដោយគ្រាន់តែខុសគ្នាត្រង់ថា អ្វីដែលយើងកំពុងធ្វើនេះគឺ "នៅក្នុងជីវិតពិត"។ ការធ្វើទំនាក់ទំនងសង្គមនៅក្នុងជីវិតពិត(អហ្វឡាញ) និងតាមប្រព័ន្ធអនឡាញមានលក្ខណៈស្រដៀងគ្នា ប៉ុន្តែវាមានចំណុចខុសគ្នាមួយចំនួន។ ដូច្នេះ បើយើងយល់ច្បាស់អំពីរបៀបនៃការប្រព្រឹត្តនៅក្នុងជីវិតពិត យើងក៏អាចប្រើសកម្មភាពទាំងនោះជាត្រីវិស័យសម្រាប់សកម្មភាពនៅតាមប្រព័ន្ធអនឡាញផងដែរ។

បច្ចុប្បន្ននេះ ការផ្សារភ្ជាប់ទំនាក់ទំនងមានការកើនឡើងយ៉ាងខ្លាំង ជាពិសេសទំនាក់ទំនងតាមប្រព័ន្ធអនឡាញ ដែលបានបង្កើតឡើងតាមរយៈថ្នាលកម្មវិធី (Platform) ដូចជា ប្រព័ន្ធផ្សព្វផ្សាយសង្គម (Social Media) កម្មវិធីណាត់ជួប (Dating App) ឬសហគមន៍និម្មិត (Virtual Community) ដោយពឹងផ្អែកលើអត្ថបទ រូបភាព សារសម្លេង និងវីដេអូ ។ ដោយឡែក ទំនាក់ទំនងនៅក្នុងជីវិតពិត គឺជាសកម្មភាពកើតឡើងដោយការជួបមុខគ្នាផ្ទាល់ ទំនាក់ទំនងដោយអារម្មណ៍ពិតៗ ដូចជា ភាសា កាយវិការ និងសំឡេង។ នៅទូទាំងពិភពលោក ទំនាក់ទំនងសង្គមនៅក្នុងជីវិតពិត និងតាមប្រព័ន្ធអនឡាញបានក្លាយជារឿងស្រពិចស្រពិល ដែលកំពុងជះឥទ្ធិពលដល់សុខភាពផ្លូវចិត្ត និងជំនាញចិត្តសង្គម។ ការយល់ដឹងអំពីទំនាក់ទំនងសង្គមនៅក្នុងជីវិតពិត និងតាមប្រព័ន្ធអនឡាញ គឺជាគន្លឹះដ៏សំខាន់សម្រាប់យើងគ្រប់គ្នា។

៣.២. អត្ថប្រយោជន៍នៃការប្រើប្រាស់អ៊ីនធឺណិត

ការយល់ដឹងអំពីទ្រឹស្តីរបស់អ៊ីនធឺណិតនឹងជួយឱ្យយើងមើលឃើញពីអត្ថប្រយោជន៍នៃការប្រើប្រាស់ និងការស្វែងយល់ពីហានិភ័យនានាតាមប្រព័ន្ធអនឡាញ។ ការបង្ហាញពីភាពវិជ្ជមាននៃអ៊ីនធឺណិតនេះ មានគោលបំណងដើម្បីឱ្យគ្រប់គ្នាបានដឹង ជាពិសេសមនុស្សពេញវ័យ ដែលភាគច្រើនតែងគិតអវិជ្ជមានចំពោះអ៊ីនធឺណិត និងការប្រើប្រាស់អ៊ីនធឺណិតរបស់កុមារ ដើម្បីជាមូលដ្ឋានសម្រាប់ការថ្លឹងថ្លែង និងពិចារណាបញ្ហានេះឱ្យបានគ្រប់ជ្រុងជ្រោយ។ ការប្រើប្រាស់អ៊ីនធឺណិត ឬការចូលរួមក្នុងពិភពអនឡាញរបស់កុមារគឺជារឿងវិជ្ជមាន ទន្ទឹមនេះ ការរស់នៅប្រចាំថ្ងៃរបស់យើងភាគច្រើនក៏កំពុងស្ថិតនៅជាមួយអ៊ីនធឺណិតផងដែរ តែយើងមិនបានកត់សម្គាល់លើចំណុចនេះទេ។ ប្រសិនបើយើងមិនទទួលស្គាល់ថា នេះគឺជាការពិតទេ នោះកុមារនឹងមើលឃើញថា យើងកំពុងគេចចេញពីការពិត។

អ៊ីនធឺណិត ឬអនឡាញផ្តល់អត្ថប្រយោជន៍ជាច្រើនដែលមិនអាចកាត់ថ្លៃបាន ក្នុងនោះរួមមាន៖

- **ការទទួលបានព័ត៌មាន៖** យើងអាចទទួលបាននូវព័ត៌មានយ៉ាងទូលំទូលាយពីគ្រប់ទិសទី។
- **ទំនាក់ទំនងជាមួយអ្នកដទៃ៖** អ៊ីនធឺណិតគឺជាស្ពានជួយភ្ជាប់ទំនាក់ទំនងជាមួយមិត្តភក្តិ គ្រួសារ និងសហគមន៍ ដែលមានចំណាប់អារម្មណ៍ដូចគ្នា ទោះបីជានៅឆ្ងាយពីគ្នាយ៉ាងណាក៏ដោយ។

- **ការកម្សាន្ត និងភាពសប្បាយរីករាយ៖** ពិភពអនឡាញក៏ជាប្រភពនៃភាពសប្បាយរីករាយ និងការកម្សាន្តផងដែរ តាមរយៈហ្គេម វីដេអូ តន្ត្រី និងសិល្បៈជាច្រើនទម្រង់ផ្សេងទៀត។
- **ការបង្កើតមិត្តភក្តិ៖** យើងអាចបង្កើតមិត្តភក្តិថ្មីៗនៅទូទាំងពិភពលោក ដែលជួយពង្រីកការយល់ដឹង និងផ្លាស់ប្តូរវប្បធម៌គ្នាទៅវិញទៅមក។
- **ឱកាសរៀនសូត្រ និងការអប់រំ៖** អ៊ីនធឺណិតបានផ្តល់ឱកាសសិក្សារៀនសូត្រ និងការអប់រំគ្មានដែនកំណត់ តាមរយៈវគ្គសិក្សាអនឡាញ និងឯកសារសិក្សាជាច្រើន។
- **ការបង្ហាញអំពីខ្លួនឯង និងភាពច្នៃប្រឌិត៖** ថ្នាលកម្មវិធីអនឡាញជាច្រើនផ្តល់ឱកាសឱ្យយើងបង្ហាញពីទេពកោសល្យ គំនិតច្នៃប្រឌិត និងអត្តសញ្ញាណរបស់ខ្លួនទៅកាន់ពិភពលោក។
- **ការពង្រឹងជំនាញបច្ចេកវិទ្យាឌីជីថល៖** ការប្រើប្រាស់ឧបករណ៍ និងកម្មវិធីផ្សេងៗនៅលើប្រព័ន្ធអនឡាញជាប្រចាំ ជួយបង្កើនជំនាញឌីជីថល ដែលជាតម្រូវការចាំបាច់ក្នុងយុគសម័យបច្ចុប្បន្ន។
- **ឱកាសការងារ៖** ជំនាញដែលទទួលបានពីពិភពអនឡាញ ដូចជាការធ្វើទីផ្សារឌីជីថល ការសរសេរកូដ ឬការរចនាក្រាហ្វិក អាចបើកផ្លូវទៅរកឱកាសការងារថ្មីៗ និងអាជីពនាពេលអនាគត។
- **ការបង្កើតសហគមន៍គាំទ្រ៖** ជាពិសេសសម្រាប់ក្រុមដែលប្រឈមការរើសអើង ដូចជាកុមារមានពិការភាព ឬកុមារនៃក្រុមចម្រុះភេទ (LGBTIQ+) អនឡាញអាចជាកន្លែងសុវត្ថិភាពមួយសម្រាប់ពួកគេក្នុងការស្វែងរកការគាំទ្រ និងការកសាងទំនាក់ទំនងក្នុងក្រុមផ្ទាល់។

៣.៣. អំពីធាតុផ្សំនៃអ៊ីនធឺណិត

អ៊ីនធឺណិតមានធាតុផ្សំសំខាន់ៗចំនួន៦ រួមមាន៖ សាធារណៈ អចិន្ត្រៃយ៍ ការផ្សារភ្ជាប់ អនាមិកភាព ប្រភពនៃព័ត៌មាន និងការគោរព។ ធាតុទាំងនេះនឹងជួយយើងឱ្យយល់កាន់តែច្បាស់អំពីអ៊ីនធឺណិត និងទិដ្ឋភាពទូទៅនៃការសិក្សារបស់យើង និងអាចប្រើប្រាស់ប្រកបដោយសុវត្ថិភាព។ ការយល់ដឹងអំពីធាតុផ្សំសំខាន់ៗទាំងនេះ គឺជាចំណុចចាប់ផ្តើមដ៏ចាំបាច់។ ធាតុផ្សំទាំងនេះគឺជាទិដ្ឋភាពទូទៅដែលនឹងជួយឱ្យយើងយល់ពីលក្ខណៈ និងសក្តានុពលរបស់អ៊ីនធឺណិត។

៣.៣.១. ធាតុផ្សំ "សាធារណៈ"

បច្ចុប្បន្ននេះ មនុស្សស្ទើរតែគ្រប់គ្នាសុទ្ធតែអាចប្រើប្រាស់អ៊ីនធឺណិត។ អ្វីៗគ្រប់យ៉ាងដែលយើងធ្វើតាមប្រព័ន្ធអនឡាញគឺមានលក្ខណៈជាសាធារណៈ។ បុគ្គលដែលមានទូរសព្ទវៃឆ្លាត ឬកុំព្យូទ័រគឺសុទ្ធតែអាចប្រើប្រាស់អ៊ីនធឺណិត បានគ្រប់ពេលវេលា។ យើងអាចបង្ហោះ (Post) ដាក់បញ្ចូល (Upload) ឬទាញយក (Download) អ្វីៗពីបណ្តាញអ៊ីនធឺណិតយកមកប្រើប្រាស់បាន។ ប៉ុន្តែត្រូវចងចាំថា អ្វីៗគ្រប់យ៉ាងនៅលើអ៊ីនធឺណិតគឺជា "សាធារណៈ" បើកចំហ និងមិនមានការរារាំងទប់ស្កាត់ទេ។ នៅពេលដែលយើងប្រើប្រាស់អ៊ីនធឺណិត គឺយើងចាប់ផ្តើមមានវត្តមាននៅលើប្រព័ន្ធអនឡាញ ហើយអ្នកផ្សេងអាចស្វែងរកព័ត៌មាន និងអ្វីដែលយើងបានធ្វើនៅតាមប្រព័ន្ធអនឡាញដោយងាយ។ ឧទាហរណ៍ យើងរុករកព័ត៌មានអ្វីមួយតាមប្រព័ន្ធអនឡាញដោយប្រើកម្មវិធី Google ហើយកំណត់ត្រានៃចំនួនលទ្ធផលដែលបានរកឃើញនឹងបង្ហាញនៅខាងក្រោមប្រអប់ស្វែងរក "លទ្ធផល

ប្រមាណ ១៦,៦០០,០០០ ដោយប្រើរយៈពេលត្រឹមតែ ០.៦២វិនាទី” (**ចំណាំ** ការបង្ហាញអំពីចំនួនលទ្ធផលនៃការរុករកមានតែនៅលើកុំព្យូទ័រប៉ុណ្ណោះ តែត្រូវចុចលើ Tool)។

យើងអាចរកឃើញព័ត៌មានជាច្រើនអំពីបុគ្គលណាម្នាក់ ហើយពេលខ្លះព័ត៌មានផ្ទាល់ខ្លួនរបស់យើងក៏អាចរកឃើញតាមប្រព័ន្ធអនឡាញផងដែរ ដូច្នេះយើងត្រូវប្រុងប្រយ័ត្នចំពោះព័ត៌មានដែលយើងចែករំលែក។ សូមសាកល្បងប្រើកម្មវិធី Google ឬ Gemini ឬឆាត AI ផ្សេងទៀត។ល។ ដើម្បីរុករកព័ត៌មានផ្ទាល់ខ្លួនរបស់យើង។ លទ្ធផលបង្ហាញអាចមានចំនួនតិច ឬច្រើន ប៉ុន្តែក្នុងនោះក៏អាចមានព័ត៌មានមួយចំនួនទៀតមិនបង្ហាញទេ។ សូមបញ្ជាក់ថា រូបថត និងមតិមួយចំនួនដែលអ្នកបានបង្ហោះនៅក្នុងថ្នាលកម្មវិធីបណ្តាញទំនាក់ទំនងសង្គម ដូចជា X (Twitter), TikTok, Instagram និង Facebook ក៏អាចនឹងរកឃើញផងដែរ។

ចំពោះកុមារ ដើម្បីគេចចេញពីការរុករកឃើញនៅលើអនឡាញ ត្រូវជ្រើសយកការកំណត់**ឯកជនភាព**នៅលើប្រូហ្វាល (Profile) របស់ពួកគេនៅលើថ្នាលកម្មវិធី ប៉ុន្តែពួកគេក៏នៅតែត្រូវប្រុងប្រយ័ត្នផងដែរ ព្រោះមិនមានការការពារល្អឥតខ្ចោះទេ។ ឧទាហរណ៍ មិត្តភ័ក្តិរបស់ពួកគេអាចថតចម្លងអេក្រង់ (Screen shot) នូវព័ត៌មានដែលពួកគេចែករំលែក ហើយផ្ញើទៅឱ្យមនុស្សដទៃផ្សេងទៀត។

៣.៣.២. ធាតុផ្សំ “អចិន្ត្រៃយ៍”

ធាតុផ្សំ **“អចិន្ត្រៃយ៍”** មានទំនាក់ទំនងយ៉ាងជិតស្និទ្ធជាមួយធាតុផ្សំ **“សាធារណៈ”**។ យើងត្រូវដឹងថា អ្វីៗគ្រប់យ៉ាងដែលយើងបង្ហោះតាមប្រព័ន្ធអនឡាញអាចមានវត្តមានជារៀងរហូត។ ទោះបីយើងលុបចេញពីប្រូហ្វាល (Profile) របស់យើង ដែលមិនអាចមើលឃើញជាសាធារណៈក៏ដោយ ក៏មាតិកាទាំងនោះអាចបន្តមាននៅក្នុងទិន្នដ្ឋានរបស់ក្រុមហ៊ុនដដែល។ ក្រុមហ៊ុនដែលដំណើរការថ្នាលកម្មវិធីបច្ចេកវិទ្យានឹងរក្សាទុកទិន្នន័យ ដែលយើងបានបង្កើតទាំងអស់នៅក្នុង **“ម៉ាស៊ីនមេ”** ដ៏ធំរបស់គេ។ **ម៉ាស៊ីនមេ** គឺដូចជាបណ្ណាសារដ៏ធំសម្រាប់ផ្ទុកទិន្នន័យទាំងអស់ ដែលយើងចែករំលែក និងបង្ហោះតាមប្រព័ន្ធអនឡាញ។ **ម៉ាស៊ីនមេ**ស្ថិតនៅទីតាំងដែលមានសុវត្ថិភាពជុំវិញពិភពលោក ប៉ុន្តែយើងត្រូវដឹងថា ទិន្នន័យគឺជាកម្មសិទ្ធិរបស់ក្រុមហ៊ុនទាំងនោះ ហើយបន្តមាននៅក្នុងទិន្នដ្ឋានរបស់ពួកគេ។ អ្នកប្រើប្រាស់មិនអាចគ្រប់គ្រងលើទិន្នន័យទាំងនោះបានទេ។

ត្រូវចាំថា មតិយោបល់(Comment) រូបភាព(Photo) ឬការបង្ហោះ(Post) របស់យើង នៅតែបន្តមានក្នុងទិន្នដ្ឋានរបស់ក្រុមហ៊ុន ទោះបីជាត្រូវបានលុបចេញពីសាធារណៈក៏ដោយ។ យើងអាចសាកល្បងប្រើទូរសព្ទឆ្លាតបើកគណនី Facebook ផ្ទាល់ខ្លួន ដើម្បីស្វែងរកព័ត៌មានចាស់ៗ ឬកម្រងអនុស្សាវរីយ៍ (Memories)។ រកមើលការបង្ហោះព័ត៌មានចាស់ៗរបស់យើង។ ការពន្យល់ខាងលើនេះ គឺគ្រាន់តែជាការបង្ហាញគោលគំនិត ដើម្បីបញ្ជាក់ថាអ្វីៗតាមប្រព័ន្ធអនឡាញអាចមានវត្តមានជារៀងរហូត ព្រោះទិន្នន័យត្រូវបានរក្សាទុកដោយក្រុមហ៊ុនដំណើរការបច្ចេកវិទ្យាថ្នាលកម្មវិធី នៅក្នុងទិន្នដ្ឋានដែលមានសុវត្ថិភាព និងនិរន្តរភាពរបស់គេ។

៣.៣.៣. ធាតុផ្សំ “ការផ្សារភ្ជាប់”

ធាតុផ្សំ **“ការផ្សារភ្ជាប់”** អ៊ីនធឺណិតអាចឱ្យយើងភ្ជាប់ទំនាក់ទំនងជាមួយមនុស្សជុំវិញពិភពលោក ប៉ុន្តែមិនមែនមនុស្សគ្រប់គ្នាសុទ្ធតែគួរឱ្យទុកចិត្តនោះទេ។ សូមចងចាំថា ការផ្សារភ្ជាប់ពិតជាមានអត្ថប្រយោជន៍។ ឧទាហរណ៍ យើងអាចភ្ជាប់ទំនាក់ទំនងជាមួយមិត្តភក្តិ ឬក្រុមគ្រួសារដែលរស់នៅក្នុងភូមិ និងទីកន្លែងផ្សេងទៀត

ជុំវិញពិភពលោក។ ប៉ុន្តែទន្ទឹមនេះ យើងក៏អាចភ្ជាប់ទំនាក់ទំនងជាមួយជនទុច្ចរិត និងជនដែលមានបំណងអាក្រក់ផងដែរ។

អ៊ីនធឺណិតគឺជា "ប្រព័ន្ធកុំព្យូទ័រពិភពលោកដែលអាចឱ្យមនុស្សចែករំលែកព័ត៌មាន និងទាក់ទងគ្នាទៅវិញទៅមក។" បណ្តាញទំនាក់ទំនងទូទាំងពិភពលោក World Wide Web (www) ដែលយើងឃើញនៅដើមអាសយដ្ឋានគេហទំព័រនានា វាអនុញ្ញាតឱ្យមនុស្សគ្រប់គ្នាអាចចែករំលែកព័ត៌មាន និងទាក់ទងគ្នាបានភ្លាមៗ។ តំណភ្ជាប់ (Hyperlinks) គឺជាមូលដ្ឋានគ្រឹះដែលផ្សារភ្ជាប់ទំព័រព័ត៌មានរាប់លាន បង្កើតបានជាបណ្ណាល័យចំណេះដឹង និងការកម្សាន្តដ៏សម្បូរបែប។ សម្រាប់កុមារ ការតភ្ជាប់តាមប្រព័ន្ធអនឡាញអាចផ្តល់ឱកាសដ៏អស្ចារ្យ ប៉ុន្តែវាក៏ភ្ជាប់មកជាមួយហានិភ័យផងដែរ ជាពិសេស នៅពេលដែលពួកគេអាចប្រាស្រ័យទាក់ទងជាមួយមនុស្សដែលមិនស្គាល់ និងមិនគួរឱ្យទុកចិត្ត។ ទោះជាបែបនេះក្តី យើងមិនគួរផ្តោតតែលើគ្រោះថ្នាក់ពេកនោះទេ ព្រោះកុមារភាគច្រើនបានទទួលនូវបទពិសោធវិជ្ជមានពីពិភពអនឡាញ។ វាបានជួយដល់កុមារក្នុងការកសាង និងរក្សាមិត្តភាពដ៏រឹងមាំប្រកបដោយការគាំទ្រ ដែលយើងអាចមើលឃើញយ៉ាងច្បាស់ក្នុងអំឡុងពេលការរាតត្បាតនៃជំងឺកូវីដ-១៩ ដែលប្រព័ន្ធអនឡាញបានក្លាយជាឧបករណ៍ដ៏សំខាន់ និងមិនអាចខ្វះបានសម្រាប់ទំនាក់ទំនងសង្គមរបស់ពួកគេ។

ក្នុងនាមជាអាណាព្យាបាល ឬមនុស្សពេញវ័យ យើងអាចដើរតួជា "ដៃគូសុវត្ថិភាព" របស់កុមារនៅលើប្រព័ន្ធអនឡាញ។ តួនាទីរបស់យើងគឺជួយតម្រង់ទិស និងបង្រៀនពួកគេឱ្យយល់ដឹងពីរបៀបការពារហានិភ័យនានា កុំឱ្យក្លាយទៅជាគ្រោះថ្នាក់ពិតប្រាកដ។ មធ្យោបាយការពារកុមារប្រកបដោយប្រសិទ្ធភាព មិនមែនជាការតាមដានរាល់សកម្មភាពរបស់ពួកគេនោះទេ ព្រោះវាស្ទើរតែមិនអាចទៅរួចឡើយ។ វិធីសាស្ត្រដែលប្រសើរនោះគឺការកសាងទំនុកចិត្តតាមរយៈការពិភាក្សាដោយបើកចំហជាប្រចាំ។ យើងគួរពិភាក្សាជាមួយកុមារអំពីមនុស្សដែលពួកគេគួរទាក់ទង ពេលវេលានៃការប្រើប្រាស់អ៊ីនធឺណិត និងបទពិសោធផ្សេងៗ ដែលពួកគេជួបប្រទះតាមប្រព័ន្ធអនឡាញ។

៣.៣.៤. ធាតុផ្សំ "អនាមិកភាព"

ជាតុផ្សំ "អនាមិកភាព" អ្នកប្រើប្រាស់ប្រព័ន្ធអនឡាញមួយចំនួនអាចលាក់បាំងអត្តសញ្ញាណរបស់ពួកគេ។ យើងមិនអាចដឹងប្រាកដ ១០០% ថាអ្នកដែលយើងកំពុងនិយាយជាមួយ ឬអ្នកដែលកំពុងមើលខ្លឹមសារមាតិការបស់យើងតាមប្រព័ន្ធអនឡាញជានរណានោះទេ។ ការប្រាស្រ័យទាក់ទងគ្នាតាមរយៈប្រព័ន្ធអនឡាញមិនដូចជាការជួបជជែកគ្នាផ្ទាល់ទេ។ យើងមិនអាចដឹង ឬឃើញច្បាស់អំពីអ្នកនៅម្ខាងទៀតបាន ដូចការធ្វើទំនាក់ទំនងក្នុងជីវិតពិតនោះទេ។ ជនទុច្ចរិតប្រើប្រាស់ប្រព័ន្ធអនឡាញ ហើយក្លែងបន្លំខ្លួនជាមនុស្សផ្សេង ដើម្បីបោកបញ្ឆោត ឬបង្ខំកុមារឱ្យចែករំលែករូបភាព និងវីដេអូបែបផ្លូវភេទ។ យើងត្រូវបង្រៀនកុមារកុំឱ្យឆាប់ជឿទុកចិត្តលើទំនាក់ទំនងថ្មីលឿនពេក។ កុមារមួយចំនួនអាចធ្លាប់ដឹងរឿងនេះ ប៉ុន្តែការជួយរំលឹកពួកគេបន្ថែមទៀត គឺកាន់តែប្រសើរ។ យើងមិនអាចស្គាល់អត្តសញ្ញាណរបស់នរណាម្នាក់តាមប្រព័ន្ធអនឡាញ១០០% បានទេ។ មានដំបូន្មានសំខាន់មួយ ដែលយើងអាចផ្តល់ឱ្យកុមារ គឺឱ្យពួកគេធ្វើតាមសតិសម្បជញ្ញៈរបស់ពួកគេ។ ដំបូន្មាននេះក៏ដូចគ្នា

នឹងអ្វីដែលយើងប្រាប់ពួកគេនៅក្នុងជីវិតពិតដែរ។ ជារឿយៗប្រសិនបើមានអ្វីមួយមិនប្រក្រតី បញ្ហានោះអាចនឹងកើតឡើងពិតមែន។

ការបង្ហាញពីគោលបំណងនៃធាតុផ្សំនេះ មិនមែនដើម្បីឱ្យយើងឈប់ប្រើប្រាស់អ៊ីនធឺណិតនោះទេ ប៉ុន្តែជាការបង្រៀនកុមារឱ្យចេះគិតពិចារណា និងប្រុងប្រយ័ត្នចំពោះមនុស្សដែលពួកគេមិនស្គាល់ ហើយបានទាក់ទងតាមប្រព័ន្ធអនឡាញ។ ត្រូវចងចាំថា មិនមែនគ្រប់ហានិភ័យទាំងអស់សុទ្ធតែអាចជៀសវាងបាននោះទេ។ រឿងដែលសំខាន់បំផុតគឺត្រូវ**គិតឱ្យបានហ្មត់ចត់ និងកុំឆាប់ជឿទុកចិត្តគេពេក**។ ហានិភ័យអាចមកពីមនុស្សដែលកុមារមិនស្គាល់ ពេលខ្លះក៏អាចមកពីមនុស្សដែលកុមារស្គាល់នៅក្នុងសហគមន៍ផងដែរ។

៣.៣.៩. ធាតុផ្សំ "ប្រភពព័ត៌មាន"

ធាតុផ្សំ **"ប្រភពព័ត៌មាន"** គឺជាការពណ៌នាអំពីព័ត៌មានផ្សេងៗ ដែលមាននៅតាមប្រព័ន្ធអនឡាញ។ ដោយសារប្រព័ន្ធអ៊ីនធឺណិតជាលំហសាធារណៈដែលមានផ្ទុកព័ត៌មានច្រើន ហេតុនេះ អ៊ីនធឺណិតអាចឱ្យយើងទាញយកព័ត៌មាន ដែលមានផលជាវិជ្ជមានបានយ៉ាងច្រើន។ ជាទូទៅ យើងអាចស្វែងរកព័ត៌មានបានស្ទើរតែទាំងអស់តាមតម្រូវការ។ ប៉ុន្តែទន្ទឹមនេះ ប្រភពព័ត៌មានក៏បង្កើតបញ្ហាផងដែរ ព្រោះយើងពិបាកក្នុងការកំណត់ឱ្យដឹងថា តើអ្វីជាការពិតត្រឹមត្រូវ និងអាចទុកចិត្តបាន។

បច្ចុប្បន្ន នរណាក៏អាចសរសេរ និងបង្ហោះ **"ព័ត៌មានមិនពិត"** តាមប្រព័ន្ធអនឡាញ បានយ៉ាងងាយស្រួលដែរ។ ប្រសិនបើព័ត៌មាននោះត្រូវបានចែករំលែកតៗគ្នាជាច្រើនដង វានឹងក្លាយជាព័ត៌មានដែល**ពេញនិយម** ហើយមនុស្សជាច្រើនអាចនឹងជឿជាក់ថា វាជាការពិត។ ការរុករកព័ត៌មានតម្រូវឱ្យយើងគិតដោយប្រុងប្រយ័ត្នអំពីប្រភពដែលយើងបានរកឃើញ ឬទទួលបាន។ លទ្ធផលដែលបង្ហាញនៅពេលរុករកតាមប្រព័ន្ធអនឡាញមិនមែនមានន័យថាជាការពិតទាំងអស់នោះទេ ជាទូទៅ លទ្ធផលនៃការស្វែងរកគឺផ្អែកលើ **"ប្រជាប្រិយភាព ឬពេញនិយមបំផុត"** ជាជាង **"ភាពត្រឹមត្រូវ"**។ ភាពជឿនលឿននៃបច្ចេកវិទ្យា ដូចជា បញ្ញាសិប្បនិម្មិត(AI) បានធ្វើឱ្យបញ្ហានេះកាន់តែស្មុគស្មាញ។ មាតិកាក្លែងក្លាយមិនត្រឹមតែជាអត្ថបទនោះទេ ប៉ុន្តែបច្ចុប្បន្នមានរួមបញ្ចូលទាំងរូបភាព រូបថត វីដេអូ និងតន្ត្រីផងដែរ។ ឧទាហរណ៍ AI អាចបង្កើតបទចម្រៀងដែលក្លែងបន្លំសម្លេងដូចទៅនឹងតារាចម្រៀងល្បីៗបានយ៉ាងល្អឥតខ្ចោះ។

ទោះជាយ៉ាងណាក៏ដោយ សូមចងចាំថា នៅពេលដែលការក្លែងបន្លំកាន់តែមានភាពប៉ិនប្រសប់ឡើង ទង្វើដែលសំខាន់បំផុតគឺត្រូវគិតឱ្យបានល្អិតល្អន់ដើម្បីវាយតម្លៃព័ត៌មាន និងមិនត្រូវឆាប់ជឿលឿនពេកនោះទេ។ មុននឹងយើងចែករំលែក (Share) អ្វីមួយទៅអ្នកដទៃ ត្រូវគិតឱ្យបានហ្មត់ចត់ បើមិនដូច្នោះទេ យើងអាចនឹងត្រូវបានគេគិតថា **ឆោតល្ងង់** ព្រោះបើអ្វីដែលបានចែករំលែកនោះជារឿងមិនពិត វាអាចនាំមកនូវផលវិបាកដល់ខ្លួនយើងទៀតផង។ យើងត្រូវណែនាំដល់កុមារឱ្យចេះគិតពិចារណាបានដិតដល់ ចំពោះព័ត៌មានដែលពួកគេមើលឃើញនៅលើអ៊ីនធឺណិត។ ពួកគេត្រូវចេះសួរថា តើព័ត៌មាននេះមានប្រភពមកពីណា? ហើយត្រូវព្យាយាមវាយតម្លៃថា ពិតឬមិនពិត មុននឹងសម្រេចចិត្តបង្ហោះ ឬចែករំលែកបន្តទៅអ្នកដទៃទៀត។

៣.៣.៦. ធាតុផ្សំ "ការគោរព"

ធាតុផ្សំ "ការគោរព" គឺជាកត្តាសំខាន់បំផុតមួយក្នុងការប្រាស្រ័យទាក់ទងតាមប្រព័ន្ធអនឡាញ។ នៅពេលយើងទាក់ទងគ្នាតាមរយៈអេក្រង់ យើងអាចភ្លេចថាយើងកំពុងភ្ជាប់ទំនាក់ទំនងជាមួយមនុស្សពិតប្រាកដ។ ការមិនបានឃើញប្រតិកម្មផ្ទាល់ ឬកាយវិការរបស់អ្នកដទៃ អាចធ្វើឱ្យការប្រាស្រ័យទាក់ទងគ្នាបាត់បង់លក្ខណៈធម្មជាតិនៃទំនាក់ទំនង។ ជាទូទៅ នៅក្នុងការផ្សាយផ្ទាល់ (Live) ការផ្ញើសារ (Message) ឬការជជែកជាក្រុម (Group chat) យើងមិនអាចមើលឃើញប្រតិកម្មតបភ្លាមៗរបស់អ្នកដទៃបានទេ ដែលអាចនាំឱ្យយើងមិនខ្វល់ពីអារម្មណ៍របស់ពួកគេដោយអចេតនា។ បើមិនប្រុងប្រយ័ត្នទេ ការនិយាយរបស់យើងអាចក្លាយទៅជាការរុកគួន ឬជាពាក្យសម្ដីស្អប់ខ្ពើម (ឧទាហរណ៍ ការជេរប្រមាថ ភាសាអសុរោះ ការប្រកាន់ពូជសាសន៍ ភេទ)។ ទង្វើទាំងនេះអាចផ្ដល់ផលអវិជ្ជមានដល់ជនរងគ្រោះ និងអាចធ្វើឱ្យអ្នកប្រព្រឹត្តមានបញ្ហាធ្ងន់ធ្ងរផងដែរ។ ដូច្នេះ មុននឹងបង្ហោះខ្លឹមសារអ្វីមួយដែលពាក់ព័ន្ធនឹងនរណាម្នាក់ យើងគួរតែសួរខ្លួនឯងថា "តើយើងហ៊ាននិយាយពាក្យទាំងនេះនៅចំពោះមុខគេផ្ទាល់ដែរឬទេ?"។

ការគោរព គឺជាការទទួលខុសត្រូវចំពោះសកម្មភាពរបស់យើងតាមប្រព័ន្ធអនឡាញ និងជារឿងចាំបាច់។ មនុស្សជាច្រើនយល់ថា ការបញ្ចេញមតិតាមប្រព័ន្ធអនឡាញគឺងាយស្រួលជាងការនិយាយទល់មុខគ្នា ព្រោះពួកគេមិនស្គាល់គ្នា និងគិតថាខ្លួនឯងអនាមិក។ ពួកគេមិនអាចមើលឃើញប្រតិកម្ម ឬភាសាកាយវិការរបស់យើងទេ ដែលធ្វើឱ្យគេមិនសូវខ្វល់ពីអារម្មណ៍អ្នកដទៃ។ ទោះបីជាការនិយាយអ្វីដែលមិនល្អតាមប្រព័ន្ធអនឡាញមានភាពងាយស្រួលក៏ដោយ យើងត្រូវចងចាំថាផលវិបាកនៅតែអាចកើតមាន។ អ្នកផ្សេងទៀតអាចវិនិច្ឆ័យអាកប្បកិរិយារបស់យើង ហើយយើងអាចនឹងមានបញ្ហាដោយសារទង្វើទាំងនោះ។ នៅក្នុងបរិបទនៃការលេងហ្គេមអនឡាញក៏ដូចគ្នាដែរ យើងត្រូវតែចងចាំពីរបៀបដែលយើងនិយាយជាមួយអ្នកលេងដទៃទៀត និងត្រូវប្រុងប្រយ័ត្នចំពោះពាក្យសម្ដីមិនសមរម្យ។ ការប្រកាន់ខ្ជាប់នូវ "ការគោរព" គឺជាគន្លឹះដើម្បីកសាងទំនាក់ទំនងល្អតាមប្រព័ន្ធអនឡាញ។

៤. មុខងារសុវត្ថិភាពនៃថ្នាលកម្មវិធី

៤.១. ការណែនាំអំពីមុខងារសុវត្ថិភាពនៃថ្នាលកម្មវិធី

សព្វថ្ងៃនេះ គ្រប់ថ្នាលកម្មវិធីទាំងអស់សុទ្ធតែមានមុខងារសុវត្ថិភាពដែលអាចប្រើបាន។ ប៉ុន្តែមុខងារទាំងនោះមិនត្រូវបានបើកឱ្យដំណើរការទេ ដោយគ្រប់ថ្នាលកម្មវិធីតែងតែរក្សាឱ្យនៅតាមលំនាំដើមទាំងអស់។ ថ្នាលកម្មវិធីចង់ឱ្យការប្រើប្រាស់ស្ថិតលើការកំណត់មុខងារបើកចំហជាសាធារណៈ (Public) ដែលអាចឱ្យមានការចូលរួមប្រើប្រាស់ និងចរាចរកាន់តែច្រើន។ ជាទូទៅនៅពេលនរណាម្នាក់ចុះឈ្មោះបង្កើតគណនីថ្មីប្រើប្រាស់ក្នុងថ្នាលកម្មវិធីមួយ វានឹងកំណត់អ្នកប្រើប្រាស់ថ្មីនោះក្នុងទម្រង់ជាសាធារណៈ អ្នកប្រើប្រាស់ត្រូវតែជ្រើសរើសមុខងារសុវត្ថិភាព ដើម្បីធ្វើឱ្យប្រូហ្វាល (Profile) មានលក្ខណៈឯកជនភាព។ កម្លាំងសេវាសង្គមត្រូវយល់ដឹង និងមានតួនាទីសំខាន់ក្នុងការអប់រំបន្តទៅដល់កុមារ ឪពុកម្ដាយ អាណាព្យាបាល និងអ្នកថែទាំឱ្យយល់ថា នៅលើគ្រប់ថ្នាលកម្មវិធីទាំងអស់ គឺសុទ្ធតែមានមុខងារសុវត្ថិភាព ដែលអាចដំណើរការបាន។ ទោះយើងគិតថា មិនអាចការពារហានិភ័យបានទាំងស្រុងក៏ដោយ តែការកំណត់ឯកជនភាព (Privacy) និងប្រើប្រាស់មុខងារសុវត្ថិភាពក្នុងថ្នាលកម្មវិធីមានអត្ថប្រយោជន៍ក្នុងការបង្ការ ទប់ស្កាត់បញ្ហាបានច្រើនសម្រាប់កុមារ។

> តាមបទពិសោធនៃការអនុវត្តកម្មវិធីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញនាពេលកន្លងមក បានបង្ហាញថាកុមារមានការយល់ដឹងតិចតួចអំពីមុខងារសុវត្ថិភាពនៃថ្នាលកម្មវិធី និងមានការទុកចិត្តខ្លាំងទៅលើមនុស្សពេញវ័យពេកដែលជាហេតុបណ្ដាលឱ្យមានបញ្ហាមិនល្អកើតឡើង។ វិធីសាស្ត្រដ៏ល្អសម្រាប់កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ គឺជាការបង្ការ និងទប់ស្កាត់បញ្ហាមិនឱ្យកើតឡើងតាំងពីដំបូង។

មុខងារសុវត្ថិភាពនៃថ្នាលកម្មវិធីមួយចំនួន អាចមានប្រយោជន៍ក្នុងការបង្ការ ទប់ស្កាត់បញ្ហាដូចជា៖

- **ការមើលឃើញឯកជនភាព (Privacy visibility)៖** នៅពេលដំឡើងថ្នាលកម្មវិធីភាគច្រើនបើកជាសាធារណៈ (Public) តាមលំនាំដើម ប៉ុន្តែអ្នកមានជម្រើស ដើម្បីកំណត់លទ្ធភាពមើលឃើញជាឯកជនភាព (Privacy) ឬចាក់សោរប្រូហ្វាល (Lock profile)។ សម្រាប់កុមារអាចកំណត់យកតែមិត្តភក្តិ ឬលេខទំនាក់ទំនងដែលបានអនុញ្ញាតិទើបឱ្យឃើញប្រូហ្វាល(Profile) របស់ពួកគេ។
- **ការកម្រិតលើមតិយោបល់ (Moderate comments)៖** អ្នកអាចដាក់កម្រិត ចំពោះការបញ្ចេញមតិរបស់នរណាម្នាក់លើខ្លឹមសាររបស់អ្នក។ ថ្នាលកម្មវិធីមួយចំនួន ក៏អនុញ្ញាតឱ្យអ្នកពិនិត្យមើលការបង្ហោះ ឬមតិយោបល់ ឬខ្លឹមសាររបស់អ្នក មុនពេលត្រូវបានបង្ហោះជាសាធារណៈផងដែរ។
- **ការច្រោះការឆបោក ឬមាតិកាដែលមិនសមរម្យ (Filter spam or inappropriate content)៖** នៅលើថ្នាលកម្មវិធីមួយចំនួន យើងអាចកំណត់លើការបញ្ចេញមតិយោបល់ដោយស្វ័យប្រវត្តិ ចំពោះមាតិកាមិនសមរម្យ ឬសារប្រមាថមាក់ងាយ។ ការដាក់កម្រិតលើការផ្ដល់មតិយោបល់ ផ្ដោតចំពោះតែគណនីដែលកំពុងតាមដានអ្នកតែប៉ុណ្ណោះ។

- កំណត់ការផ្ញើសារផ្ទាល់ និងសារសន្ទនា (Limiting direct messages and chat)៖ ថ្នាលកម្មវិធីភាគច្រើនឥឡូវនេះ អាចឱ្យអ្នកជ្រើសរើសកំណត់ការទទួលសារពីគណនី ដែលអ្នកបានទទួលជាមិត្តតែប៉ុណ្ណោះ។ នេះក៏ជាការកំណត់មួយ ដែលអ្នកគួរតែបើកប៊ូតុងជម្រើសនេះ។

យើងនឹងលើកយកមកបង្ហាញនូវដំណើរការនៃមុខងារទូទៅរបស់ថ្នាលកម្មវិធីមួយចំនួន ដូចជា៖ TikTok, Instagram, Facebook, Telegram ដោយផ្តោតលើការរុករកដោយសុវត្ថិភាព (Safe search) ការរាំងខ្ទប់ (Block) ការរាយការណ៍ (Report) និងការលាក់បាំង (Hidden) ដែលមុខងារទាំងនេះមានសារៈសំខាន់ ដើម្បីជួយបង្ការ ទប់ស្កាត់ និងឆ្លើយតបតាមប្រព័ន្ធអនឡាញ។ ជាទូទៅ ថ្នាលកម្មវិធីភាគច្រើនប្រើពាក្យពេចន៍ស្រដៀងគ្នាដូចជា បញ្ជីមុខងារ (Menu) និងជម្រើស (Options)។ មុខងារទាំងនេះភាគច្រើនខុសប្លែកគ្នាតែខាងក្រៅ និងទីតាំង ដែលត្រូវរកតែប៉ុណ្ណោះ។ **សូមបញ្ជាក់ថា** ដំណើរការនៃការប្រើប្រាស់មុខងារសុវត្ថិភាពនៃថ្នាលកម្មវិធីនឹងមានការប្រែប្រួលពីមួយជំនាន់ទៅមួយជំនាន់ អាស្រ័យលើការធ្វើបច្ចុប្បន្នភាពរបស់ថ្នាលកម្មវិធី។

៤.២. ការកំណត់ឯកជនភាព និងដែនកំណត់ (Privacy settings and limits)

ការកំណត់ឯកជនភាព និងដែនកំណត់ គឺជាការគ្រប់គ្រងលើរាល់ការមើលឃើញ ការបង្ហោះ ការផ្សាយ ការភ្ជាប់ និងការស្វែងរកប្រូហ្វាល។ យើងអាចកំណត់ថាបុគ្គលណាម្នាក់អាចមើលឃើញ ឬមើលមិនឃើញបញ្ជីមិត្តរបស់យើង ការបង្ហោះ ការផ្សាយ ការភ្ជាប់ និងការស្វែងរកអ្នកតាមអ៊ីមែល ឬលេខទូរសព្ទបាន។

៤.២.១. ការកំណត់ឯកជនភាព Facebook នៅលើប្រព័ន្ធប្រតិបត្តិការ Android

- បើកកម្មវិធី Facebook ចុចលើបន្ទាត់ផ្តេកបី (☰) នៅជ្រុងស្តាំខាងលើ
- ចូលទៅកាន់ **ការកំណត់ & ឯកជនភាព** (Settings & Privacy) រំកិលចុះក្រោម រួចចុចលើ **ការកំណត់ & ឯកជនភាព** បន្ទាប់មកចុចលើការកំណត់ (Settings)។
- ប្រើឧបករណ៍ **ការពិនិត្យឯកជនភាព** (Privacy Checkup) ចុចលើ **ការពិនិត្យឯកជនភាព** និងអនុវត្តតាមលំដាប់នៃការកំណត់ឯកជនភាពសំខាន់ៗ។ អ្នកនឹងត្រូវបានណែនាំថា៖
  - តើអ្នកណាអាចមើលឃើញការចែករំលែករបស់អ្នក
  - តើគេអាចស្វែងរកអ្នកដោយរបៀបណា
  - ការកំណត់ទិន្នន័យរបស់អ្នកនៅលើ Facebook
  - ចំណង់ចំណូលចិត្តលើការផ្សាយពាណិជ្ជកម្ម។
- **កំណត់ការមើលឃើញផុសតាមបំណង** (Customize Post Visibility) នៅខាងក្រោមការ**កំណត់ឯកជនភាព** (Privacy Setting) សូមចុចលើប្រូហ្វាល និងការភ្ជាប់។ រួចធ្វើការកែតម្រូវ៖
  - តើអ្នកណាអាចឃើញការបង្ហោះនាពេលអនាគតរបស់អ្នក → កំណត់ទៅមិត្តភក្តិឬមានតែខ្ញុំ
  - កំណត់ការបង្ហោះពីមុន → ដាក់កម្រិតការបង្ហោះចាស់ៗចំពោះតែមិត្តភក្តិប៉ុណ្ណោះ
  - អ្នកណាអាចមើលរឿងរ៉ាវរបស់អ្នក → ជ្រើសរើសមិត្តភក្តិ ផ្ទាល់ខ្លួន ឬលាក់ទុក។
- កំណត់មនុស្សដែលអាចចូលមើល ស្វែងរក ឬទាក់ទងជាមួយអ្នក។ ចុចលើ របៀបដែលមនុស្សអាចស្វែងរកអ្នកនៅលើ Facebook៖

- កំណត់អ្នកដែលអាចផ្ញើសំណើសុំធ្វើជាមិត្តរបស់អ្នក
- សម្រេចចិត្តថាបុគ្គលណាអាចរកមើលឃើញអ្នក ដោយប្រើលេខទូរសព្ទ ឬអ៊ីមែលរបស់អ្នក
- បិទការភ្ជាប់ប្រព័ន្ធរុករកទៅប្រូហ្វាលរបស់អ្នក។

- គ្រប់គ្រង **ការភ្ជាប់ការបង្ហោះ** (Tag) និងកំណត់ពេលវេលា ចុចលើប្រូហ្វាល និងការភ្ជាប់ការបង្ហោះ៖
  - បើក ឬបិទដំណើរការភ្ជាប់ការបង្ហោះ (Tag) ពិនិត្យឡើងវិញ មុនពេលវាបង្ហាញនៅលើ Facebook របស់អ្នក
  - គ្រប់គ្រងអ្នកដែលអាចបង្ហោះនៅលើ Facebook របស់អ្នក
- ការរាំងខ្ទប់ទំនាក់ទំនងដែលអ្នកមិនចង់បាន ចុចលើការរាំងខ្ទប់ (Block) នៅក្រោមការកំណត់។ បន្ថែមអ្នកប្រើប្រាស់ទៅក្នុងបញ្ជីរាំងខ្ទប់របស់អ្នក ដើម្បីកុំឱ្យពួកគេប្រាស្រ័យទាក់ទងជាមួយអ្នកបាន។
- ចំណាប់ចំណូលចិត្តលើការផ្សាយពាណិជ្ជកម្ម ចូលទៅកាន់ការកំណត់ការផ្សាយពាណិជ្ជកម្ម៖
  - បិទការផ្សាយពាណិជ្ជកម្ម ដោយផ្អែកលើសកម្មភាពរបស់អ្នក
  - កំណត់ការចែករំលែកទិន្នន័យជាមួយអ្នកផ្សាយពាណិជ្ជកម្ម។

៤.២.២. ការកំណត់ឯកជនភាព Telegram នៅលើប្រព័ន្ធប្រតិបត្តិការ Android

បើកកម្មវិធី Telegram ចុចលើបន្ទាត់ផ្ដេកបី (☰) នៅជ្រុងឆ្វេងខាងលើ។ ជ្រើសរើស ការកំណត់ → បន្ទាប់មកចុចលើ **ឯកជនភាព និងសុវត្ថិភាព**។ ការកំណត់ឯកជនភាពគន្លឹះ ដើម្បីកែតម្រូវ៖

- ការមើលឃើញលេខទូរសព្ទ រួចចូលទៅកាន់ **ឯកជនភាព និងសុវត្ថិភាព** (Privacy and Security) → លេខទូរសព្ទ (Phone Number)។ ជ្រើសរើស៖
  - មនុស្សគ្រប់គ្នា (Everybody)៖ អាចមើលឃើញ។
  - បញ្ជីទំនាក់ទំនង (Contact)៖ មានតែលេខទំនាក់ទំនងដែលបានរក្សាទុកប៉ុណ្ណោះ។
  - គ្មាននរណាម្នាក់ (Nobody)៖ មិនអាចមើលឃើញទាំងស្រុង។
  - យើងក៏អាចគ្រប់គ្រងអ្នកស្វែងរកយើងតាមលេខរបស់យើងផងដែរ។
- ការឃើញ **ចុងក្រោយ និងស្ថានភាពអនឡាញ** (Last seen and online)៖ ចុចលើ **ការឃើញចុងក្រោយ និងស្ថានភាពអនឡាញ** ដោយមានជម្រើស៖
  - មនុស្សគ្រប់គ្នា (Everybody) បញ្ជីទំនាក់ទំនង (Contact) ឬគ្មាននរណាម្នាក់ (Nobody)។
  - អ្នកអាចបន្ថែមករណីលើកលែង (ឧ. អនុញ្ញាតឱ្យមនុស្សជាក់លាក់ ទោះបីជាអ្នកជ្រើសរើស "គ្មាននរណាម្នាក់")។
- រូបថតប្រូហ្វាល ចុចលើរូបថតកម្រងព័ត៌មាន រួចជ្រើសរើសអ្នកដែលអាចមើលឃើញ ដូចជា៖ អ្នករាល់គ្នា ទំនាក់ទំនងរបស់ខ្ញុំ ឬគ្មាននរណាម្នាក់។

- ការបញ្ជូនសារបន្ត (Forwarded Message) ចុចលើសារបញ្ជូនបន្ត រួចកំណត់ទៅជា គ្មាននរណាម្នាក់ ដើម្បីការពារអ្នកផ្សេងពីការបញ្ជូនសារបន្ត ដែលបានបញ្ជូនបន្តត្រឡប់ទៅប្រូហ្វាលរបស់អ្នក។
- ក្រុម និងឆានែល (Group and Channel)៖ ចុចលើក្រុម និងឆានែល រួចគ្រប់គ្រងអ្នកដែលអាចបញ្ចូលអ្នកទៅក្នុងក្រុម ដូចជា៖ មនុស្សគ្រប់គ្នា បញ្ជីទំនាក់ទំនង ឬគ្មាននរណាម្នាក់។
- ការហៅទូរសព្ទ (Call)៖ ចុចលើការហៅទូរសព្ទ រួចកំណត់អំពីអ្នកដែលអាចហៅចូលទូរសព្ទអ្នកបាន និងការភ្ជាប់ពីមិត្តភ័ក្តិដែលត្រូវបានអនុញ្ញាត។
- ការរាំងខ្ទប់អ្នកប្រើប្រាស់(Block)៖ ចុចលើ ឈ្មោះដែលត្រូវរាំងខ្ទប់ ដើម្បីទប់ស្កាត់។ អ្នកអាចបន្ថែម ឬលុបឈ្មោះអ្នកត្រូវរាំងខ្ទប់បានគ្រប់ពេល។
- ការជជែកជាលក្ខណៈឯកជន (Chat privacy)៖ ចុចលើការជជែកជាលក្ខណៈឯកជន ដែលប្រើការអ៊ិនគ្រីប (Encrypt) ពីដើមដល់ចុង ដូចខាងក្រោម៖
    - បើកការជជែក → ចុចឈ្មោះទំនាក់ទំនង → ចុចលើចំណុចគ្រាប់ → ជ្រើសរើស ចាប់ផ្តើមការជជែកជាលក្ខណៈឯកជន។
    - សារអាចលុបដោយស្វ័យប្រវត្តិ និងមិនអាចបញ្ជូនបន្តបានទេ។

៤.៣. ការរុករកដោយសុវត្ថិភាព (SafeSearch)

ការរុករកដោយសុវត្ថិភាព (SafeSearch) គឺជាឧបករណ៍ចម្រោះមាតិកាដែលបានបង្កើតឡើងនៅក្នុង Google Search។ នៅពេលបើកដំណើរការ វានឹងកាត់បន្ថយឱកាសនៃការមើលឃើញមាតិកាអាសអាភាស ឬហិង្សា (រូបភាព វីដេអូ គេហទំព័រ) ឬតំណភ្ជាប់ទៅគេហទំព័រអាសអាភាស ឬការផ្សាយពាណិជ្ជកម្មមិនសមរម្យ។ ការរុករកដោយសុវត្ថិភាពមានប្រយោជន៍ ជាពិសេសសម្រាប់កុមារ និងសិស្សានុសិស្ស។

របៀបបើកការរុករកដោយសុវត្ថិភាព នៅលើប្រព័ន្ធប្រតិបត្តិការ Android

- បើកកម្មវិធី Google ឬចូលទៅកាន់ការកំណត់ Google SafeSearch
- ចុចលើប្រូហ្វាលរបស់អ្នក → ការកំណត់ → SafeSearch
- ជ្រើសរើសអ្វីដែលអ្នកពេញចិត្ត៖ បិទ (Off) ព្រិល (Blur) ឬច្រោះ (Filter) (ជម្រើសច្រោះ គឺជាការត្រងមាតិកាដែលមិនសមរម្យចេញ)
- អ្នកក៏អាចចាក់សោរ SafeSearch ជាមួយនឹងគណនី Google Family Link ផងដែរ។

៤.៤. ការរឹតបន្តឹងនៅលើ Youtube

ការរឹតបន្តឹងនៅលើ YouTube (Restrict Mode) គឺជារបៀបដាក់កំហិតរបស់ YouTube ដូចជាការច្រោះឌីជីថលដែលជួយពិនិត្យមើលមាតិកាមិនសមរម្យ ដែលមានប្រយោជន៍សម្រាប់គ្រួសារ សាលារៀន និងកន្លែងសាធារណៈ។ ការដាក់កម្រិត គឺជាការកំណត់នូវការលាក់វីដេអូដែលទាក់ទងជាមួយខ្លឹមសារបែបរំលោភបំពានផ្លូវភេទ អំពើហិង្សា ឬរូបភាពដែលរំខាន រូបភាពអាសអាភាស ឬប្រធានបទសម្រាប់មនុស្សពេញវ័យ និងមតិយោបល់ដែលមិនសមរម្យ។ ការរឹតបន្តឹងនេះ មិនមានល្អឥតខ្ចោះទេ ដោយសារ YouTube ប្រើប្រាស់ប្រព័ន្ធ

ស្វ័យប្រវត្តិ និងរបាយការណ៍របស់អ្នកប្រើប្រាស់ ដើម្បីកំណត់អត្តសញ្ញាណខ្លឹមសារទាំងនោះ ដូច្នេះវីដេអូមួយចំនួនអាចនៅតែឆ្លងកាត់ ឬមិនត្រូវបានច្រោះចេញ។

របៀបបើកការរឹតបន្តឹង ឬដាក់កម្រិតរបស់កម្មវិធី YouTube នៅលើប្រព័ន្ធប្រតិបត្តិការ Android ៖

- ចុចលើរូបតំណាងប្រូហ្វាលរបស់អ្នកនៅជ្រុងខាងស្តាំខាងលើ
- ចូលទៅកាន់ការកំណត់ → ទូទៅ (General)
- អូសចុះក្រោម ហើយបើកការរឹតបន្តឹង (Restrict Mode)
- នៅពេលបើកឱ្យដំណើរការ YouTube នឹងព្យាយាមច្រោះចេញនូវមាតិកាដែលបានកំណត់នៅលើការរុករក ការណែនាំ និងមតិយោបល់នានា។

៤.៥. ការរាំងខ្ទប់នៅលើកម្មវិធី Facebook, Telegram, TikTok និង Instagram

ការរាំងខ្ទប់ (Block) គឺជាមុខងារសាមញ្ញមួយ ដែលប្រើដើម្បីដោះស្រាយជាមួយបុគ្គលណាម្នាក់ ឬមាតិកា ដែលធ្វើឱ្យកុមារមានអារម្មណ៍មិនល្អតាមប្រព័ន្ធអនឡាញ។ មុខងារនេះនឹងលុបគណនី ឬមាតិកាចេញភ្លាមៗមិនឱ្យមើលឃើញ។ ផ្ទាលកម្មវិធីនីមួយៗគឺសុទ្ធតែមាន "ការរាំងខ្ទប់" លើខ្លឹមសារមាតិកា និងគណនីដូចគ្នា ប៉ុន្តែរបៀបនៃការអនុវត្តអាចមានភាពខុសៗគ្នា។

ឧទាហរណ៍ ប្រសិនបើយើងរាំងខ្ទប់គណនីនៅលើកម្មវិធី Instagram, Facebook ឬ Messenger ការសន្ទនារបស់យើងទាំងពីរនឹងលែងមើលឃើញទៀតហើយ ការបង្ហោះឯកជនត្រូវបានលាក់ ប៉ុន្តែការបង្ហោះជាសាធារណៈនៅតែអាចមើលឃើញ។ នៅក្នុងកម្មវិធី Telegram, Whatsapp ឬ Line ប្រសិនបើយើងរាំងខ្ទប់នរណាម្នាក់ យើងនឹងលែងទទួលបានសាររបស់ពួកគេហើយ ប៉ុន្តែប្រវត្តិសន្ទនានៅតែអាចមើលឃើញគ្នា ហើយអ្នកម្ខាងទៀតមិនបានដឹងថាយើងរាំងខ្ទប់គេទេ។

ចូរចាំថា ពេលខ្លះគណនីដែលយើងបានរាំងខ្ទប់ គេអាចនឹងបង្កើតគណនីថ្មីជាច្រើនទៀត ដើម្បីតាមដានយើង។ តែយើងត្រូវបន្តរាំងខ្ទប់រហូតដល់ពួកគេនឿយណាយ នោះពួកគេអាចនឹងបញ្ឈប់ដោយខ្លួនឯង។ ប៉ុន្តែប្រសិនបើនៅតែមានបញ្ហា យើងអាចរាយការណ៍គណនីនោះទៅកាន់ផ្ទាលកម្មវិធី ឬទៅសមត្ថកិច្ច ដើម្បីអន្តរាគមន៍លើការបៀតបៀនប្រភេទនេះ។ ផ្ទាលកម្មវិធីអាចទប់ស្កាត់បុគ្គលនោះជាអចិន្ត្រៃយ៍មិនឱ្យទាក់ទងអ្នកបានទៀតឡើយ។

ក. របៀបរាំងខ្ទប់គណនីនៅលើ Facebook តាមទូរសព្ទវៃឆ្លាត ឬថេបប្លេត៖

- បើកកម្មវិធី Facebook
- ចុចលើប្រូហ្វាល (Profile) របស់មនុស្សដែលត្រូវរាំងខ្ទប់
- ចុចលើចំណុចចុចបី ឬគ្រាប់បីនៅផ្នែកខាងលើនៃទំព័រ
- ជ្រើសរើស "រាំងខ្ទប់" (Block)
- បញ្ជាក់នៅលើទំព័របន្ទាប់ ដោយចុច "រាំងខ្ទប់" (Block) ម្តងទៀត។

ខ. របៀបរាំងខ្ទប់គណនីនៅលើផ្ទាលកម្មវិធី Instagram៖

- បើកកម្មវិធី Instagram
- ចុចលើប្រូហ្វាល (Profile) របស់មនុស្សដែលត្រូវរាំងខ្ទប់
- ចុចលើចំណុចចុចបី ឬគ្រេបីនៅផ្នែកខាងលើនៃទំព័រ
- ជ្រើសរើស "រាំងខ្ទប់" (Block) ។

គ. របៀបរាំងខ្ទប់គណនីនៅលើថ្នាលកម្មវិធី TikTok៖

- បើកកម្មវិធី TikTok
- ចុចលើប្រូហ្វាល (Profile) របស់មនុស្សដែលត្រូវរាំងខ្ទប់
- ចុចលើចំណុចចុចបី ឬគ្រេបីនៅផ្នែកខាងលើនៃទំព័រ (ក្បែរកណ្ដឹង)
- ជ្រើសរើស "រាំងខ្ទប់" (Block) ពីបញ្ជីមុខងារនៅខាងក្រោមអេក្រង់។

ឃ. របៀបរាំងខ្ទប់នៅលើ Telegram មានវិធីសាស្ត្រ ២ យ៉ាង៖

វិធីទី១៖ តាមរយៈការកំណត់ (Settings)

- ចូលទៅកាន់កម្មវិធី Telegram app
- ចុចការកំណត់ (Settings)
- ចូលទៅកាន់ Privacy and Security
- ជ្រើសរើសការរាំងខ្ទប់អ្នកប្រើប្រាស់ (Blocked Users)
- ចុចបន្ថែមអ្នកប្រើប្រាស់ (Add User)
- ជ្រើសរើសឈ្មោះបុគ្គល ដែលអ្នកចង់រាំងខ្ទប់ (block) → ចុច Done

វិធីទី២៖ តាមរយៈប្រូហ្វាល (Profile)

- ចូលទៅកាន់ឈ្មោះ ឬប្រូហ្វាលរបស់អ្នកដែលយើងចង់រាំងខ្ទប់ (block)
- ចុចលើប៊ូតុង ចំណុចចុចបី (⋮) នៅខាងលើ
- ជ្រើសរើសការរាំងខ្ទប់អ្នកប្រើប្រាស់ (Block User) → អ្នកនោះនឹងមិនអាចផ្ញើសារ ឬហៅមកអ្នកបានទៀតទេ។

៤.៦. ការរាយការណ៍នៅលើកម្មវិធី Facebook, Telegram, TikTok និង Instagram

ការរាំងខ្ទប់ (Block) អាចត្រូវបានប្រើ ដើម្បីឆ្លើយតបទៅនឹងការប្រព្រឹត្តមិនល្អ ឬមាតិកាមិនសមរម្យតាមប្រព័ន្ធអនឡាញ។ ស្របគ្នានេះ **ការរាយការណ៍ (Report)** គឺជាជំហានសំខាន់មួយទៀត ដែលត្រូវប្រើនៅពេលដែលមានបទល្មើស មាតិកាមិនសមរម្យ ឬការបង្កឱ្យមានគ្រោះថ្នាក់នៅតាមប្រព័ន្ធអនឡាញ ដោយបង្ហាញពីរបៀបដែលខ្លឹមសារមាតិកានេះត្រូវបានលុបចេញ ឬអ្នកប្រព្រឹត្តអំពើទុច្ចរិតត្រូវបានកំណត់អត្តសញ្ញាណ និងបញ្ឈប់។ ចូរចាំថា ជាទូទៅជំហាននៃការរាយការណ៍ (Report) អំពីខ្លឹមសារមាតិកា និងគណនីមានភាពខុសគ្នាបន្តិចបន្តួច។ **មុខងាររាយការណ៍**អាចស្ថិតនៅកន្លែងស្រដៀងគ្នានឹងមុខងារនៃការរាំងខ្ទប់ (Block) ដែរ។

ក. របៀបរាយការណ៍ (Report) គណនីនៅលើកម្មវិធី Facebook៖

- បើកកម្មវិធី Facebook
- ចុចលើប្រូហ្វាល (Profile) របស់បុគ្គលដែលត្រូវរាយការណ៍
- ចុចលើចំណុចចុចបី ឬត្រៃបីនៅផ្នែកខាងលើនៃទំព័រ
- ជ្រើសរើស "រាយការណ៍" (Report)
- បញ្ជាក់នៅលើអេក្រង់បន្ទាប់ដោយចុច "រាយការណ៍" (Report) ម្តងទៀត ហើយផ្តល់ព័ត៌មានដែលបានស្នើសុំ។

ខ. របៀបរាយការណ៍គណនីនៅលើកម្មវិធី Instagram ៖

- បើកកម្មវិធី Instagram
- ចុចលើប្រូហ្វាល (Profile) របស់បុគ្គលដែលត្រូវរាយការណ៍
- ចុចលើចំណុចចុចបី ឬត្រៃបីនៅផ្នែកខាងលើនៃទំព័រ
- ជ្រើសរើស "រាយការណ៍" (Report)
- ជ្រើសរើសពីបញ្ជីហេតុផលសម្រាប់រាយការណ៍ (ប៉ុន្តែកុំចុចរើសក្នុងបញ្ជី បើមិនដូច្នេះទេ វានឹងផ្ញើរបាយការណ៍)។

គ. របៀបរាយការណ៍នៅលើកម្មវិធី TikTok ៖

- បើកកម្មវិធី TikTok
- ចុចលើប្រូហ្វាល (Profile) របស់បុគ្គលដែលត្រូវរាយការណ៍
- ចុចលើសញ្ញាព្រួញបែរទៅខាងស្តាំ នៅខាងលើ
- ចុចលើប៊ូតុង "រាយការណ៍" (Report) នៅផ្នែកខាងក្រោមនៃអេក្រង់
- ជ្រើសរើស "រាយការណ៍គណនី ឬរាយការណ៍មាតិកា" (Report Account or Report Content)
- ជ្រើសរើសហេតុផលពីបញ្ជី
- ចុចបញ្ជូននៅលើអេក្រង់បន្ទាប់។

ឃ. របៀបរាយការណ៍នៅកម្មវិធី Telegram អាចធ្វើទៅលើគណនីអ្នកប្រើ (User/Channel/Group)

- ចូលទៅកាន់ប្រូហ្វាលរបស់គណនីនៃអ្នកដែលយើងចង់រាយការណ៍
- ចុចលើប៊ូតុងចំណុចចុចបី (⋮) នៅខាងលើ
- ជ្រើសរើសការរាយការណ៍ (Report)
- ជ្រើសរើសមូលហេតុ ដូចជា មេរោគ គណនីក្លែងបន្លំ អំពើហិង្សា ការរំលោភបំពានកុមារ។ល។
- ចុចបញ្ជូន (Submit)។

ជាចុងក្រោយ ត្រូវរំលឹកកុមារឱ្យធ្វើតាមសតិសម្បជញ្ញៈរបស់ពួកគេ។ ប្រសិនបើពួកគេឃើញអ្វីមួយនៅតាមប្រព័ន្ធអនឡាញមិនសមរម្យ គួរឱ្យខ្លាច ហិង្សា ឬអ្វីដែលធ្វើឱ្យពួកគេមានអារម្មណ៍មិនល្អ ពួកគេត្រូវរកមធ្យោបាយដោះស្រាយតាមវិធីខាងលើ។ គេហទំព័រ https://cyberbullying.org/report គឺជាការប្រមូលផ្តុំនូវតំណភ្ជាប់ និងការណែនាំដ៏ល្អសម្រាប់ការរាយការណ៍ (Report) អំពីខ្លឹមសារមាតិកានៅលើថ្នាលកម្មវិធីផ្សេងៗ

គ្នាជាង ១២០ទម្រង់ ដែលកុមារអាចប្រើប្រាស់បាន។ ប៉ុន្តែក្នុងករណីព្រហ្មទណ្ឌ សូមរាយការណ៍ទៅអគ្គស្នងការនគរបាលជាតិតាមរយៈគេហទំព័រ https://hotline.police.gov.kh/ ។

ទន្ទឹមនេះ កុមារក៏អាចប្រើគេហទំព័រ https://takeitdown.ncmec.org/ និង https://report.stopncii.org ដែលផ្តល់សេវាដោយមិនគិតកម្រៃជួយកុមារក្នុងការលុប ឬបញ្ឈប់ការចែករំលែករូបអាក្រាតតាមប្រព័ន្ធអនឡាញ ជាពិសេស រូបភាព ឬវីដេអូផ្លូវភេទ និងអាក្រាតច្បាស់ៗ។

៤.៧. ការកំណត់លើទីតាំងដែលកំពុងស្ថិតនៅ (Live location settings)

ការកំណត់លើទីតាំងដែលកំពុងស្ថិតនៅ គឺជាការអនុញ្ញាតឱ្យអ្នកចែករំលែកទីតាំងក្នុងពេលជាក់ស្តែងរបស់អ្នកជាមួយអ្នកដទៃដោយប្រើកម្មវិធីដូចជា Google Maps, WhatsApp, Telegram, Line, Viber, Facebook, Messenger និង WeChat...។ វាជាមុខងារដ៏មានអានុភាពសម្រាប់ការបន្តទំនាក់ទំនង សម្របសម្រួលការប្រជុំ ឬជានាសុវត្ថិភាព ប៉ុន្តែវាក៏ទាមទារការគ្រប់គ្រងឯកជនភាពយ៉ាងប្រុងប្រយ័ត្នផងដែរ។ ការចែករំលែកទីតាំងដែលយើងកំពុងស្ថិតនៅមានន័យថា ជាការធ្វើបច្ចុប្បន្នភាពទីតាំង GPS បច្ចុប្បន្នរបស់អ្នកជាបន្តបន្ទាប់សម្រាប់រយៈពេលដែលបានកំណត់ វាមិនដូចជាការធ្វើចំណុចដៅទីតាំងនោះទេ វាបង្ហាញចលនារបស់អ្នកក្នុងពេលវេលាជាក់ស្តែង។

ឪពុកម្តាយ និងអ្នកថែទាំគួរតែយល់ផងដែរថា ការចែករំលែកទីតាំងដែលយើងកំពុងស្ថិតនៅ វាហាក់ដូចជាមានប្រយោជន៍សម្រាប់ការរក្សាសុវត្ថិភាពកុមារ ប៉ុន្តែវាក៏អាចកើតឡើងជាមួយនឹងហានិភ័យធ្ងន់ធ្ងរផងដែរ។ ខាងក្រោមនេះ គឺជាការបង្ហាញអំពីគ្រោះថ្នាក់មួយចំនួនសម្រាប់កុមារ នៅពេលប្រើមុខងារទីតាំងដែលយើងកំពុងស្ថិតនៅលើកម្មវិធីដូចជា Facebook, Telegram, Instagram, WhatsApp និងកម្មវិធីផ្សេងទៀត។ ហានិភ័យចម្បងៗនៃការចែករំលែកទីតាំងដែលកំពុងស្ថិតនៅរបស់កុមារ រួមមាន៖

- **ការគំរាមពាក់ព័ន្ធផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ៖** ប្រសិនបើកុមារចែករំលែកទីតាំងរបស់ពួកគេជាមួយនរណាម្នាក់ដែលជាជនទុច្ចរិត បុគ្គលនោះអាចប្រើទីតាំងនេះដើម្បីគំរាមកំហែង ឬប្រព្រឹត្តអ្វីមួយចំពោះកុមារ។ ការផ្តល់ទីតាំងជាក់ស្តែងអាចផ្តល់ឱកាសឱ្យជនទុច្ចរិត ប្រើប្រាស់ដើម្បីបំភិតបំភ័យ ឬបង្ខិតបង្ខំកុមារឱ្យស្ថិតក្នុងស្ថានភាពគ្រោះថ្នាក់។
- **គ្រប់គ្រងទំនាក់ទំនងដោយបង្ខំ៖** កុមារអាចរងសម្ពាធក្នុងការចែករំលែកទីតាំងរបស់ពួកគេជាមួយមិត្តភក្តិ ឬដៃគូស្នេហា។ នេះអាចនាំឱ្យមានការរំលោភបំពានផ្លូវអារម្មណ៍ ដោយសារត្រូវបានគេបង្ខំឱ្យប្រើការតាមដានទីតាំង ដើម្បីតាមដាន គ្រប់គ្រង ឬឱ្យធ្វើតាម។
- **ការតាមដានតាមប្រព័ន្ធអនឡាញ៖** ជនចម្លែក ឬសូម្បីតែអ្នកស្គាល់គ្នាក៏អាចប្រើទិន្នន័យទីតាំងដើម្បីតាមដានចលនារបស់កុមារបានដែរ ដែលអាចនាំទៅរកការជួបផ្ទាល់ ឬការបៀតបៀន។
- **ការរំលោភឯកជនភាព៖** កុមារប្រហែលជាមិនដឹងថាការចែករំលែកទីតាំងរបស់ពួកគេ សូម្បីតែជាមួយមិត្តភក្តិ ដូចជា កន្លែងរស់នៅ សាលារៀន និងទម្លាប់ប្រចាំថ្ងៃ ត្រូវបានមើលឃើញគ្រប់ពេលវេលា។

- **អារម្មណ៍ទុក្ខព្រួយ និងសម្ពាធសង្គម៖** ការឃើញមិត្តភ័ក្តិជួបជុំគ្នាដោយគ្មានវត្តមានពួកគេ អាចនាំឱ្យមានអារម្មណ៍នៃការមិនរាប់បញ្ចូល ឬការអន់ចិត្ត។ កុមារអាចមានអារម្មណ៍ថា មានសម្ពាធក្នុងការបង្ហាញសកម្មភាពសង្គមនានា។
- **ការប្រើទិន្នន័យដោយបំពាន និងភាពងាយរងគ្រោះពីកម្មវិធីឌីជីថល៖** កម្មវិធីជាច្រើនរក្សាទុកទិន្នន័យទីតាំង ដែលអាចត្រូវបានលាតត្រដាងដោយបំពានសុវត្ថិភាព។ សូម្បីតែថ្នាលកម្មវិធីដែលទុកចិត្តបានក៏អាចមានចន្លោះប្រហោងឯកជនភាព ដែលធ្វើឱ្យកុមារប្រឈមនឹងហានិភ័យផងដែរ។

៤.៨. ការប្រមូលវត្ថុតាង

ការប្រមូលវត្ថុតាងក្នុងករណីនៃការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ (OCSEA) គឺជាដំណើរការដ៏សំខាន់ ដែលទាមទារឱ្យមានភាពច្បាស់លាស់ ការយកចិត្តទុកដាក់ខ្ពស់ និងកិច្ចសហការអន្តរវិស័យ។ នេះមិនគ្រាន់តែផ្តោតលើការចាប់ជនទុច្ចរិតប៉ុណ្ណោះទេ តែក៏ជាការការពារ និងធានាយុត្តិធម៌ដល់ជនរងគ្រោះដោយមិនមានបង្កគ្រោះថ្នាក់បន្ថែមទៀតឡើយ។

វត្ថុតាងអាចជា សម្ភារៈឌីជីថល ការធ្វើសក្ខីកម្ម វត្ថុ ឬអាកប្បកិរិយា ដែលក្នុងនោះរួមមាន៖

- **ស្លាកស្នាមឌីជីថល (Digital footprint)** : កំណត់ហេតុការសន្ទនា អ៊ីមែល រូបភាព វីដេអូ មេតាទិន្នន័យ អាសយដ្ឋាន IP និងប្រវត្តិឧបករណ៍។
- **ទិន្នន័យក្នុងថ្នាលកម្មវិធី** : ការប្រើប្រាស់ប្រព័ន្ធផ្សព្វផ្សាយសង្គម ការរក្សាទុកក្នុងក្លោដ (cloud) និងកំណត់ត្រាការប្រើប្រាស់កម្មវិធី។
- **ការលាតត្រដាងរបស់ជនរងគ្រោះ** : ការរាយការណ៍របស់កុមារ ដែលជារឿយៗត្រូវបានចែករំលែកជាមួយមនុស្សពេញវ័យ ឬអ្នកដែលពួកគេទុកចិត្ត។
- **គណនីរបស់សាក្សី** : មិត្តភ័ក្តិ បងប្អូនបង្កើត ឬអ្នកថែទាំ ដែលបានទាក់ទង ឬបានសង្កេត ឬឃើញសកម្មភាពរបស់កុមារ។
- **ឧបករណ៍កោសល្យវិច្ច័យ** : ការទាញយក ឬស្រង់ទិន្នន័យចេញពីទូរសព្ទ ថេបប្លេត ឬកុំព្យូទ័រដោយប្រើឧបករណ៍ឯកទេស។

រឿងមួយដែលត្រូវចងចាំ គឺការប្រមូល និងរក្សាទុកវត្ថុតាង ដែលកុមាររាយការណ៍ទៅក្នុងថ្នាលកម្មវិធី ឬទៅអាជ្ញាធរមានសមត្ថកិច្ច ក្នុងករណីបញ្ហាធ្ងន់ធ្ងរ តាមរយៈវិធីសាស្ត្រនៃកិច្ចការពារកុមារ យើងមិនចាំបាច់ចម្លងរូបភាព ឬវីដេអូផ្ញើទៅថ្នាលកម្មវិធីទៀតទេ ព្រោះថ្នាលកម្មវិធីមានខ្លឹមសារមាតិកា ដែលបានរាយការណ៍រួចជាស្រេចហើយ។ ប៉ុន្តែប្រសិនបើរាយការណ៍ទៅអាជ្ញាធរមានសមត្ថកិច្ច យើងត្រូវតែប្រមូលវត្ថុតាង ដែលរក្សាទុក និងយករូបថតអេក្រង់ (Screenshot) ដែលមាននៅលើទូរសព្ទវៃឆ្លាត ថេបប្លេត កុំព្យូទ័រ និងឧបករណ៍ហ្គេមភ្ជាប់ទៅជាមួយ។ ការថតអេក្រង់ មានសារៈសំខាន់ណាស់ក្នុងការរក្សាកំណត់ត្រានៃការរុកកួនតាមប្រព័ន្ធអនឡាញ (Cyberbully) ការលួងលោម ពាក្យសម្តីស្អប់ខ្ពើម ឬបញ្ហាផ្សេងៗទៀតតាមអ៊ីនធឺណិត។ អ្នកអាចប្រើវត្ថុតាងទាំងនេះ នៅពេល

រាយការណ៍ជាផ្លូវការទៅអាជ្ញាធរមានសមត្ថកិច្ច។ អ្នកក៏អាចប្រើរូបថតអេក្រង់នេះផងដែរ ប្រសិនបើទាក់ទងជាមួយសាលារៀន ក្រុមគ្រួសារ ឬជនទុច្ចរិត។

ចំណាំ៖ នៅពេលឃើញរូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ (CSAM) អ្នកមិនគួរថតអេក្រង់ទេ ព្រោះនេះ គឺជាសកម្មភាពនៃការចម្លងរូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទឱ្យកាន់តែច្រើនឡើងៗ។ អ្នកត្រូវថតចម្លងតំណភ្ជាប់ (Copy link) រាយការណ៍ដោយផ្ទាល់ទៅអាជ្ញាធរមានសមត្ថកិច្ច ដើម្បីដោះស្រាយអំពីគេហទំព័រ ឬមាតិកាដែលមានខ្លឹមសារ CSAM ដែលអ្នកបានឃើញ។

របៀបប្រើទូរសព្ទដៃឆ្លាតថតលើអេក្រង់៖

- ចុចប៊ូតុង "បន្ថយសំឡេង" និងប៊ូតុង "បិទបើក" ក្នុងពេលតែមួយ។ ប្រសិនបើធ្វើបានត្រឹមត្រូវ អេក្រង់នឹងភ្លឺ ហើយរូបភាពនឹងត្រូវបានចម្លង និងរក្សាទុកក្នុងទូរសព្ទដៃឆ្លាត
- គំរូនេះត្រូវបានអនុវត្តដូចគ្នា នៅលើឧបករណ៍ដែលប្រើប្រាស់ប្រតិបត្តិការ Android
- ចំពោះទូរសព្ទដៃឆ្លាត IOS ម៉ូដែលចាស់ៗ អ្នកចុចប៊ូតុង "Home" និងប៊ូតុង "បិទបើក"។ ចំពោះទូរសព្ទដៃឆ្លាត IOS ជំនាន់ថ្មី អ្នកចុចប៊ូតុង "ដំឡើងសំឡេង" និងប៊ូតុង "បិទបើក" ក្នុងពេលតែមួយ។

របៀបប្រើទូរសព្ទដៃឆ្លាតថតវីដេអូលើអេក្រង់ (Screen record)៖

- ចូលទៅកាន់ទំព័រ Notifications នៃអេក្រង់ដើម (អូសពីលើចុះក្រោមនៃអេក្រង់)
- ជ្រើសរើសការថតវីដេអូលើអេក្រង់ "Screen record"

នៅពេលយើងបញ្ចប់ការថត ឯកសារនេះនឹងរក្សាទុកនៅក្នុងកម្រងរូបថតនៃឧបករណ៍របស់យើង។

៥. ការអភិវឌ្ឍជំនាញកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ

គោលដៅស្នូលនៃការការពារកុមារតាមប្រព័ន្ធអនឡាញ គឺជាការប្តេជ្ញាចិត្តដើម្បីធានាថា សិទ្ធិរបស់កុមាររួមមាន សិទ្ធិក្នុងការទទួលបានសុវត្ថិភាព សិទ្ធិឯកជន ការការពារពីអំពើហិង្សា ការរំលោភបំពាន និងការកេងប្រវ័ញ្ច ត្រូវបានគោរពនៅគ្រប់ទីកន្លែងទាំងអស់ រួមទាំងក្នុងពិភពឌីជីថល។ ចំណេះ ជំនាញ និងបំណិនពាក់ព័ន្ធនឹងការការពារកុមារតាមប្រព័ន្ធអនឡាញ គឺជាជំនាញមួយ ដែលកម្លាំងសេវាសង្គមត្រូវបំពេញបន្ថែម ឱ្យស្របទៅតាមបរិបទនៃបរិវត្តិកម្មឌីជីថល ដើម្បីធានាដល់ឧត្តមប្រយោជន៍របស់កុមារ។

៥.១. ប្រភេទហានិភ័យតាមប្រព័ន្ធអនឡាញ

ហានិភ័យតាមប្រព័ន្ធអនឡាញចំពោះកុមារត្រូវបានចែកចេញជា ៤ប្រភេទ (4C)៖ ១.ហានិភ័យមាតិកា (Content Risk) ២.ហានិភ័យនៃទំនាក់ទំនង (Contact Risk) ៣.ហានិភ័យនៃការប្រព្រឹត្ត (Conduct Risk) និង ៤.ហានិភ័យនៃកិច្ចសន្យា (Contract Risk)។ ហានិភ័យទាំងនេះបានផ្សារភ្ជាប់គ្នានៅលើថ្នាលកម្មវិធី ដូចជា Facebook, Telegram, TikTok, Instagram និង Roblox ។ល។

ហានិភ័យមាតិកា (Content Risk)៖ គឺជាខ្លឹមសារមាតិកា ដែលបង្កឱ្យមានគ្រោះថ្នាក់។ ឧទាហរណ៍ កុមារមើលឃើញរូបភាព ឬសម្ភារៈមិនសមរម្យ ជ្រុលនិយម រូបភាពហិង្សា រើសអើង រូបភាព-វីដេអូអាសអាភាស ព័ត៌មានមិនពិតជាដើម។ ហានិភ័យនេះពាក់ព័ន្ធនឹងកុមារដែលបានជួបប្រទះ ឬទទួលបានបទពិសោធមិនមានសុវត្ថិភាព ដែលអាចធ្វើឱ្យគ្រោះថ្នាក់ដល់កុមារ ដូចជា មាតិកាមិនសមរម្យ ឬខុសច្បាប់ដែលជាការបង្ហាញរូបភាពអាសអាភាស ហិង្សា ព័ត៌មានមិនពិត ឬព័ត៌មានក្លែងក្លាយ។

ហានិភ័យទំនាក់ទំនង (Contact Risk)៖ គឺជាការបោកបញ្ឆោត និងព្យាយាមធ្វើបាប។ ឧទាហរណ៍ កុមារទទួលរងការលួងលោម ការកេងប្រវ័ញ្ច ការបៀតបៀន ការរើសអើង ការព្យាយាមធ្វើបាប ការគំរាម ការដាក់សម្ពាធ ការរុកកួន ការទទួលបានសារពីជនចម្លែកតាមប្រព័ន្ធអនឡាញ។ ហានិភ័យនេះ កើតឡើងពីការចូលរួមដោយផ្ទាល់ជាមួយមិត្តភក្តិ ជនចម្លែក ឬជនទុច្ចរិត។ មនុស្សពេញវ័យលួងលោម ឬបង្កើតទំនុកចិត្តក្លែងក្លាយដើម្បីរំលោភបំពានកុមារ។ ការរុកកួន ឬការបៀតបៀនតាមប្រព័ន្ធអនឡាញ គឺជាការវាយប្រហារ ដោយប្រើសារ និងមាតិកាផ្សេងៗតាមប្រព័ន្ធអនឡាញ។

ហានិភ័យនៃការប្រព្រឹត្ត (Conduct Risk)៖ គឺជាអំពើរបស់កុមារដែលនាំឱ្យមានគ្រោះថ្នាក់។ ឧទាហរណ៍ កុមារចូលរួមប្រព្រឹត្តអំពើដែលនាំឱ្យគ្រោះថ្នាក់ ការសម្លុតគំរាមកំហែងបែបផ្លូវភេទ ការបំភិតបំភ័យ ការបង្ខូចកេរ្តិ៍ឈ្មោះ ការផលិតចែកចាយ CSAM ជាដើម។ ហានិភ័យនេះទាក់ទងនឹងសកម្មភាពរបស់កុមារ ដែលនាំឱ្យមានការរីករាយ ឬផលវិបាកដែលពួកគេមិនបានដឹង។ ការផ្ញើរូបភាពអាក្រាត ឬចែករំលែកមាតិកាមិនច្បាស់លាស់ ការផ្ញើរូបភាពផ្ទាល់ខ្លួនក្រោមសម្ពាធផ្សេងៗ។ ការចែករំលែកព័ត៌មានច្រើនពេក ការបង្ហាញទីតាំង ឬព័ត៌មានលម្អិតនៅក្នុងការបង្ហោះ ឬការជជែក។

ហានិភ័យនៃកិច្ចសន្យា (Contract Risk)៖ គឺជាសកម្មភាពទាក់ទងនឹងពាណិជ្ជកម្ម ដែលប្រកបដោយគ្រោះថ្នាក់ ឬផលប្រយោជន៍ពាណិជ្ជកម្ម។ ឧទាហរណ៍ ការផ្តល់ទិន្នន័យផ្ទាល់ខ្លួន រូបថត លេខទូរសព្ទ អ៊ីមែល។ល។

ហានិភ័យនេះ រួមមាន គ្រោះថ្នាក់ផ្នែកហិរញ្ញវត្ថុ ឬទិន្នន័យពីក្រុមហ៊ុន។ ការរំលោភទិន្នន័យឯកជនភាព ដូចជាកម្មវិធីប្រមូល ឬលក់ទិន្នន័យរបស់កុមារ។ ការលួងលោមឱ្យទិញក្នុងកម្មវិធី ដោយការផ្តល់ឱ្យទិញកម្មវិធីតូចៗ ដែលនាំឱ្យកុមារញៀន។

៥.២. ការកេងប្រវ័ញ្ច និងរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ

ដើម្បីយល់អំពីការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ យើងត្រូវយល់នូវគន្លឹះមួយចំនួនដូចខាងក្រោម៖

ការរំលោភបំពានផ្លូវភេទលើកុមារ៖ *"សំដៅទៅលើសកម្មភាពផ្លូវភេទទាំងឡាយណាដែលប្រើកម្លាំង ឬអំណាចពីមនុស្សធំទៅលើកុមារ ឬកុមារធ្វើលើកុមារ (មិនថាភេទដូចគ្នាឬខុសគ្នា) ដើម្បីឱ្យកុមារចូលរួមសកម្មភាពផ្លូវភេទ"* ។ សកម្មភាពផ្លូវភេទ រួមមាន ការរំលោភសេពសន្ថវៈ ការរួមភេទតាមមាត់ រួមភេទតាមរន្ធគូទ ការប្រើម្រាមដៃស៊កបញ្ចូលទៅក្នុងប្រដាប់ភេទ ការប្រើឧបករណ៍ផ្សេងៗស៊កបញ្ចូលទៅក្នុងប្រដាប់ភេទ ការលេងប្រដាប់ភេទកុមារ ការឱ្យកុមារលេងប្រដាប់ភេទរបស់ខ្លួន ការបៀម ឬលិឍប្រដាប់ភេទ។

ការកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារ៖ *"សំដៅទៅលើការប្រើប្រាស់កុមារដើម្បីផលប្រយោជន៍ ដែលមិនអាចទទួលយកបាន ដោយធ្វើឱ្យកុមារបាត់បង់កុមារភាព ការអប់រំ ការអភិវឌ្ឍ ឬសេចក្តីថ្លៃថ្នូរ។ ការកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារ រួមមានការជួញដូរផ្លូវភេទ និងអំពើអាសអាភាសលើកុមារជាដើម"*។ ការកេងប្រវ័ញ្ចផ្លូវភេទ ក៏ជាប្រភេទនៃការរំលោភបំពានផ្លូវភេទផងដែរ។ កុមារដែលស្ថិតក្នុងស្ថានភាព និងទំនាក់ទំនងបែបកេងប្រវ័ញ្ច តែងតែទទួលបាននូវរបស់ផ្សេងៗដូចជា អំណោយ លុយកាក់ ឬក្តីស្រលាញ់ ដើម្បីជាថ្នូរនឹងការអនុវត្តសកម្មភាពផ្លូវភេទ ឬឱ្យអ្នកផ្សេងអនុវត្តសកម្មភាពផ្លូវភេទទៅលើពួកគេ។

ការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ ផ្សារភ្ជាប់ជាមួយទម្រង់ផ្សេងៗនៃអំណាច។ អំណាចទាំងនេះមានភាពខុសគ្នា អាស្រ័យលើអាយុ ភេទ យេនឌ័រ ឬក្រុមដែលគេមិនអើពើដទៃទៀត ដូចជា កុមារមានពិការភាព ក្រុមចម្រុះភេទ (LGBTIQ+)។

អំណាចមានច្រើនទម្រង់ ដែលក្នុងនោះរួមមាន៖

- **អំណាចមើលឃើញ (Visible Power)៖** គឺជាអំណាចដែលអាចមើលឃើញ និងដឹងជាទូទៅ។ ឧទាហរណ៍ មាឌ អាយុ ឋានៈ ធនធាន មេដឹកនាំស្ថាប័ន រដ្ឋាភិបាល និងអាជ្ញាធរ ការដាក់ប្រូហ្វាលស្អាតៗ...។
- **អំណាចលាក់បាំង (Hidden Power)៖** គឺជាអំណាចនៅពីក្រោយ និងមានឥទ្ធិពលលើការសម្រេចចិត្តណាមួយ។ ឧទាហរណ៍ ក្រុមដែលមានឥទ្ធិពល ក្រុមសាសនា ក្រុមជ្រុលនិយម ក្រុមរកលុយតាមប្រព័ន្ធអនឡាញ (MMO)... ។
- **អំណាចមើលមិនឃើញ (Invisible Power)៖** ជាអំណាចដែលមាននៅក្នុងផ្នត់គំនិត ជំនឿ ឬបទដ្ឋានសង្គម ដែលបិទបាំងអំណាចរបស់ខ្លួន។ ឧទាហរណ៍ ស្ត្រីតែងជឿថាប្តីរបស់គាត់ត្រូវតែជាអ្នកសម្រេចចិត្តក្នុងគ្រួសារ ការជឿថាបច្ចេកវិទ្យាមានភាពស្មុគស្មាញ...។

យើងអាចគិតតាមរយៈទម្រង់ផ្សេងៗ នៃអំណាចខាងលើនេះ ដែលមានឥទ្ធិពលដល់ការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ។ ឧទាហរណ៍ តើមានអតុល្យភាពនៃអំណាចដូចម្តេចខ្លះ រវាងស្ត្រី និងកុមារ? រវាងអ្នកថែទាំ និងកុមារដែលមានពិការភាព? រវាងយុវជន និងយុវនារី? តើមានទម្រង់នៃអំណាចមើលឃើញ អំណាចលាក់បាំង ឬអំណាចមើលមិនឃើញដែរឬទេ? តើអតុល្យភាពនៃអំណាចទាំងនេះនាំឱ្យកើតមាននូវការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញដូចម្តេច?

អំណាចអាចប្រើនៅក្នុងវិធីផ្សេងៗជាច្រើន។ វិធីមួយចំនួនដែលអំណាចអាចដំណើរការ រួមមាន៖

- **អំណាចលប់លើ (Power over)៖** ជាអំណាចដែលមនុស្សម្នាក់ ឬក្រុមមួយ ប្រើប្រាស់ដើម្បីត្រួតត្រាមនុស្ស ឬក្រុមដទៃ។ ការត្រួតត្រានេះអាចកើតចេញជាអំពើហិង្សាដោយផ្ទាល់ ឬប្រយោលកើតចេញពីជំនឿរបស់សហគមន៍ ដែលបង្កឱ្យមានការរំលោភបំពាន និងភាពអយុត្តិធម៌។ ឧទាហរណ៍ អំណាចចៅហ្វាយនាយ និងកូនចៅ។
- **អំណាចចំពោះ ឬដើម្បី (Power to)៖** គឺជាជំនឿ ថាមពល សកម្មភាព និងការប្តេជ្ញាចិត្តរបស់បុគ្គល ឬក្រុម ដើម្បីបង្កើតការផ្លាស់ប្តូរវិជ្ជមាន។ ឧទាហរណ៍ មេភូមិធានាថា ប្រជាជនក្នុងភូមិទទួលបានទឹកស្អាតប្រើប្រាស់។
- **អំណាចជាមួយ (Power with)៖** ជាអំណាចនៃការចូលរួម និងសហការដែលមនុស្សពីរនាក់ ឬច្រើននាក់ ធ្វើអ្វីម៉្យាងដែលពួកគេមិនអាចធ្វើតែម្នាក់ឯងបាន។ ឧទាហរណ៍ មេភូមិបានសហការជាមួយស្ថាប័នពាក់ព័ន្ធ អង្គការដៃគូ និងប្រជាជន ដើម្បីកសាងស្ថានីយ៍ទឹកស្អាតនិងបណ្តាញចែកចាយនៅក្នុងភូមិ។
- **អំណាចខាងក្នុង (Power in)៖** ជាភាពរឹងមាំកើតចេញពីក្នុងខ្លួនរបស់យើងតាមរយៈចំណេះដឹង ទស្សនៈ បទពិសោធ គុណតម្លៃ ដែលជះឥទ្ធិពលលើជីវិត និងសហគមន៍របស់យើង។ ឧទាហរណ៍ មេភូមិមានចំណេះដឹង បទពិសោធ និងទំនាក់ទំនងល្អ ដើម្បីកៀរគរអ្នកពាក់ព័ន្ធ...។

ក្រុមមនុស្សខ្លះអាចមានអំណាចច្រើនជាងក្រុមដទៃទៀត ដែលអាចឱ្យពួកគេប្រើអំណាចនេះ ដើម្បីកេងប្រវ័ញ្ច ឬរំលោភបំពានទៅដល់យុវជន និងកុមារ រួមទាំងតាមប្រព័ន្ធអនឡាញផងដែរ។

ការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ **កើតឡើងតាមរយៈការប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យាឌីជីថល អ៊ីនធឺណិត និងបច្ចេកវិទ្យាទូរគមនាគមន៍**។ ទម្រង់នៃការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ[6] មាន៥ទម្រង់ ដូចខាងក្រោម៖

- ការលួងលោមកុមារតាមប្រព័ន្ធអនឡាញ (Child Online Grooming)
- រូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ (Child Sexual Abuse Material-CSAM)
- ការគំរាមពាក់ព័ន្ធសកម្មភាពផ្លូវភេទ (Sextortion)
- ការផ្សាយផ្ទាល់អំពីការរំលោភបំពានផ្លូវភេទលើកុមារ (Live-streaming)
- ការផ្ញើសារបែបផ្លូវភេទ (Sexting)

[6] គោលការណ៍ណែនាំថ្នាក់ជាតិស្តីពីកិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ ឆ្នាំ២០២៣

ការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ មានជាប់ពាក់ព័ន្ធនឹងធាតុផ្សំសំខាន់ៗចំនួន ៣ រួមមាន ការផ្សារភ្ជាប់ អនាមិកភាព និងអចិន្រ្តៃយ៍។

៥.២.១. ការលួងលោមកុមារតាមប្រព័ន្ធអនឡាញ (Child Online Grooming)

ការលួងលោមកុមារតាមប្រព័ន្ធអនឡាញ សំដៅទៅលើសកម្មភាព ឬមធ្យោបាយ ដែលព្យាយាមទាក់ទងកុមារតាមប្រព័ន្ធអនឡាញ **ដើម្បីកសាងទំនុកចិត្ត**ក្នុងគោលបំណងកេងប្រវ័ញ្ចផ្លូវភេទ។ ការលួងលោមទាំងនោះរួមមាន ការបង្ហាញនូវសម្ភារៈអាសអាភាស ដូចជា តាមរយៈការផ្ញើនូវមាតិកា សារ វីដេអូ ឬរូបភាពបែបផ្លូវភេទទៅកាន់កុមារ។ វិធីទាំងនេះ អាចបន្សុំកុមារទៅនឹងរឿងរ៉ាវផ្លូវភេទ ក្នុងគោលបំណងបង្កើនឱកាសឱ្យកុមារបញ្ជូនរូបភាព-សម្ភារៈផ្លូវភេទដោយខ្លួនឯង ។

ជនទុច្ចរិតអាចលួងលោមកុមារតាមដំណាក់កាល ដូចខាងក្រោមនេះ៖

- កំណត់អត្តសញ្ញាណកុមារ និងបង្កើនទំនុកចិត្ត
- បំពេញតម្រូវការដែលកុមារចង់បាន ដូចជា ក្តីស្រឡាញ់ ផ្តល់កិច្ចគាំទ្រជាថវិកា សម្ភារៈ ឬទ្រព្យសម្បត្តិ
- ផ្តាច់ចេញឆ្ងាយពីមិត្តភក្តិ និងគ្រួសារ
- បង្កើតទំនាក់ទំនងផ្លូវភេទ និងកេងប្រវ័ញ្ច
- បន្តការគ្រប់គ្រងលើកុមារ។

ចំពោះកុមារនៅពេលប្រើប្រាស់ប្រព័ន្ធអនឡាញត្រូវគិតពីហានិភ័យទាំងនេះ។ ពួកគេមិនត្រូវជឿភ្លាមៗទេថា អ្នកដែលកំពុងនិយាយជាមួយពួកគេនោះជានរណាឱ្យប្រាកដ។ ការដឹងអំពីអត្តសញ្ញាណពិតរបស់បុគ្គលណាម្នាក់តាមប្រព័ន្ធអនឡាញ គឺជាការពិបាក។ ជនទុច្ចរិតមានភាពស្ទាត់ជំនាញក្នុងការក្លែងបន្លំខ្លួន ជារឿយៗពួកគេបង្ហោះរូបក្លែងបន្លំជាកុមារវ័យជំទង់។

ជនទុច្ចរិតនិយមផ្លាស់ប្តូរការប្រើប្រាស់ពីថ្នាលកម្មវិធីមួយទៅថ្នាលកម្មវិធីមួយទៀត៖ ការលួងលោមបានចាប់ផ្តើមពី**លក្ខណៈជាសាធារណៈ** តាមរយៈបណ្តាញផ្សព្វផ្សាយសង្គម ឬហ្គេម បន្ទាប់មកទំនាក់ទំនងរបស់ពួកគេបានផ្លាស់ប្តូរការសន្ទនាទៅជា**លក្ខណៈឯកជន**។

ជនទុច្ចរិតអាចជាមនុស្សដែលកុមារបានស្គាល់ ឬមិនស្គាល់៖ ផ្អែកលើធាតុផ្សំ **"អនាមិកភាព"** យើងគ្រប់គ្នាមិនអាចស្គាល់ ឬដឹងច្បាស់ថា យើងកំពុងសន្ទនាជាមួយនរណានោះទេ។ ដូច្នេះការប្រុងប្រយ័ត្ននៅពេលបង្កើតទំនាក់ទំនងជាមួយនរណាម្នាក់តាមប្រព័ន្ធអនឡាញ គឺមានសារៈសំខាន់ណាស់ ជាពិសេសនៅពេលដែលពួកគេចង់បង្កើតទំនាក់ទំនង ឬសារសន្ទនាជាលក្ខណៈឯកជន។ ឪពុកម្តាយគួរតាមដាន និងផ្តល់ដំបូន្មានដល់កុមារអំពីការសម្រេចចិត្តទាំងនេះ។ ពួកគាត់គួរតែពិនិត្យមើលទំនាក់ទំនងរបស់កុមារតូចៗជាមួយមនុស្សថ្មី ប៉ុន្តែកិច្ចការនេះ គួរកាត់បន្ថយនៅពេលដែលកុមារកាន់តែធំ។

ជនទុច្ចរិតភាគច្រើនស្គាល់កុមាររួចទៅហើយ៖ តាមការស្រាវជ្រាវបានបង្ហាញថា ខណៈពេលដែលកុមារគឺជាគោលដៅនៃទំនាក់ទំនងរបស់មនុស្សជុំវិញពិភពលោក ជនទុច្ចរិតតាមប្រព័ន្ធអនឡាញភាគច្រើនគឺជាបុគ្គល

ដែលរស់នៅក្នុងសហគមន៍មូលដ្ឋានជាមួយគ្នា ដោយប្រើបច្ចេកវិទ្យាឌីជីថល ដើម្បីទាក់ទងកុមារ ។

ជនទុច្ចរិតមានជំនាញច្បាស់លាស់ក្នុងការប្រើប្រាស់បច្ចេកវិទ្យា៖ ជនទុច្ចរិតប្រើថ្នាលកម្មវិធី និងលេងហ្គេមដូចគ្នានឹងអ្វីដែលកុមារចូលចិត្ត ដើម្បីមានភាពងាយស្រួលក្នុងការទំនាក់ទំនង កសាងទំនុកចិត្ត និងបង្កើតមិត្តភាព។

ជនទុច្ចរិតមានភាពប៉ិនប្រសប់ចំពោះអ្វីដែលពួកគេប្រព្រឹត្ត៖ ជាទូទៅជនទុច្ចរិតព្យាយាមធ្វើជាមិត្តជាមួយកុមារតាមរយៈការបង្ហាញចំណូលចិត្ត និងការកម្សាន្តដូចគ្នា។

ជនទុច្ចរិតចែករំលែកព័ត៌មានទៅវិញទៅមក៖ ដោយប្រើពាក្យពេចន៍ និងឃ្លាប្រយោគ ដែលកុមារនិយមប្រើប្រាស់ ចំណូលចិត្ត និងទំនោររបស់កុមារ ដើម្បីពួកគេមានភាពងាយស្រួលក្នុងការលួងលោមកុមារ។

ជនទុច្ចរិតតែងប្រើគណនី និងរូបភាពក្នុងប្រូហ្វាល (Profile) ក្លែងក្លាយ ដើម្បីឱ្យមើលទៅមានវ័យប្រហាក់ប្រហែលគ្នា។ ដំបូងកុមារវ័យជំទង់រំភើបរីករាយ នៅពេលដែលទទួលបានការយកចិត្តទុកដាក់ពីមិត្តភ័ក្តិថ្មីៗតាមប្រព័ន្ធអនឡាញ ជាពិសេសនៅពេលដែលពួកគេទទួលបានអំណោយ ឬថវិកា។

ពេលខ្លះជនទុច្ចរិតមិនក្លែងបន្លំអត្តសញ្ញាណទេ តែពួកគេសម្តែងជាមនុស្សដែលយកចិត្តទុកដាក់ និងគួរឱ្យទុកចិត្តសម្រាប់កុមារ ដូចជា ធ្វើជាគ្រូបង្វឹក ឬជាអ្នកផ្តល់ប្រឹក្សា។ ចំពោះកុមារដែលងាយរងគ្រោះខ្លាំង គឺជាកុមារដែលមិនមានមនុស្សអាចទុកចិត្តនៅក្នុងជីវិតរបស់ពួកគេ។ កុមារទាំងនោះអាចត្រូវបានគេអូសទាញដោយប្រើវិធីសាស្ត្រនេះ។ យើងអាចបង្រៀនកុមារឱ្យចេះពិនិត្យអង្កេតលើសញ្ញាណនៃការលួងលោមមួយចំនួន ដូចជា៖

- ភាសាដែលគេប្រើប្រាស់ប្លែកៗ ខុសប្រក្រតី
- ជាមនុស្ស ដែលពួកគេមិនស្គាល់
- ពួកគេមិនបានបង្ហាញអត្តសញ្ញាណ ឬព័ត៌មានច្រើនទាក់ទងនឹងខ្លួនគេ
- បុគ្គលនោះធ្វើឱ្យកុមារមានអារម្មណ៍មិនស្រួល ឬដាក់សម្ពាធលើកុមារ
- កុមារគួរជឿជាក់លើអារម្មណ៍ខ្លួនឯងថា អ្វីទាំងនោះមិនត្រឹមត្រូវ។

ជនទុច្ចរិតដែលលួងលោមកុមារ ជារឿយៗតែងធ្វើនូវរឿង ដូចខាងក្រោមនេះ៖

- ចាប់ផ្តើមដោយទាក់ទងជាមួយកុមារក្នុងថ្នាលកម្មវិធីជាសាធារណៈ បន្ទាប់មកពួកគេសុំឱ្យប្តូរទៅជជែកជាឯកជនវិញ
- ពួកគេប្រើគេហទំព័រ ហ្គេម ឬកម្មវិធីដូចកុមារ ដើម្បីធ្វើឱ្យកុមារមានការទុកចិត្ត
- ធ្វើពុតជាមានចំណាង់ចំណូលចិត្ត ឬការកម្សាន្តដូចកុមារដែរ
- ប្រើរូបថត និងប្រូហ្វាលក្លែងក្លាយ ដើម្បីបោកបញ្ឆោតថា មានអាយុប្រហាក់ប្រហែលកុមារ
- ព្យាយាមទាញកុមារចេញពីគ្រួសារ និងមិត្តភ័ក្តិ។

គន្លឹះដែលមានប្រយោជន៍ គឺការលើកទឹកចិត្តកុមារឱ្យធ្វើតាមសតិសម្បជញ្ញៈរបស់ពួកគេ។ មុនពេលកុមារបន្តទំនាក់ទំនងជាមួយនរណាម្នាក់ ប្រសិនបើមានអ្វីមួយធ្វើឱ្យពួកគេមានអារម្មណ៍មិនល្អ ពួកគេគួរតែគិត

ឱ្យបានហ្មត់ចត់ ឬស្វែងរកជំនួយពីមិត្តភក្តិ និងពីមនុស្សពេញវ័យដែលពួកគេទុកចិត្ត។ ការរកឃើញបញ្ហាជាមុន និងទាន់ពេលវេលាជារឿងល្អបំផុតក្នុងការបង្ការ ទប់ស្កាត់ហានិភ័យ។

៤.២.២. រូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ (Child Sexual Abuse Material-CSAM)

ហានិភ័យចម្បងៗចំពោះកុមារតាមប្រព័ន្ធអនឡាញ រួមមានការផលិត ការប្រើប្រាស់ ការកាន់កាប់ និងការចែករំលែករូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ ដែលអាចស្គាល់តាមរយៈអក្សរកាត់ថា "CSAM"។ កន្លងមក គេប្រើពាក្យ "រូបភាពអាសអាភាសកុមារ" តែពាក្យនេះមិនត្រូវបានប្រើប្រាស់ទៀតទេ ដោយសារពាក្យនេះ គ្រាន់តែជាប្រភេទខ្លឹមសារទាក់ទងនឹងផ្លូវភេទប៉ុណ្ណោះ។ បច្ចុប្បន្ននេះ រូបភាព ឬវីដេអូអំពីការរំលោភបំពានផ្លូវភេទលើកុមារ គឺជាបទឧក្រិដ្ឋកម្មធ្ងន់ធ្ងរ ដូច្នេះពាក្យ **"រូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ"** ត្រូវបានយកមកប្រើប្រាស់។ រូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ (CSAM) សំដៅលើសម្ភារៈ ដែលបង្ហាញពីកុមារក្នុងស្ថានភាពអាក្រាត ពិពណ៌នាដោយផ្តោតលើកេរ្តិ៍ភេទរបស់កុមារ ឬសម្ភារៈដែលពិពណ៌នាអំពីកុមារបែបអាសអាភាស។ សម្ភារៈទាំងនោះរួមមាន រូបភាព វីដេអូ អត្ថបទ និងសារសំឡេង ដែលមានលក្ខណៈបែបអាសអាភាសជាដើម។

រាល់ពេលដែលយើងមើល CSAM គឺជាការរំលោភបំពាន ប៉ុន្តែមនុស្សជាច្រើនក្នុងសហគមន៍តែងបដិសេធថា នេះគ្រាន់តែជាការមើលរូបភាពប៉ុណ្ណោះ។ យើងត្រូវតែប្រឆាំងនឹងទង្វើនេះ ដោយប្រាប់ថា ករណី CSAM ជាច្រើនត្រូវបានគេប្តឹង ហើយរបាយការណ៍នៃការប្តឹងនេះ ទទួលបានតែពីក្រុមហ៊ុនដែលមានមូលដ្ឋាននៅសហរដ្ឋអាមេរិកប៉ុណ្ណោះ ក្នុងនោះរួមមានថ្នាលកម្មវិធីធំៗដូចជា Facebook, Instagram ប៉ុន្តែថ្នាលកម្មវិធីផ្សេងទៀតមិនបានធ្វើការរាយការណ៍ទេ ឧទាហរណ៍ ដូចជា Telegram។ ការមើលរូបភាពអាសអាភាសកុមារអាចមានផលប៉ះពាល់ជាច្រើនដល់កុមារ បន្ថែមលើការរំលោភបំពានដែលបានកើតឡើង។

៤.២.៣. ការគំរាមពាក់ព័ន្ធសកម្មភាពផ្លូវភេទ (Sextortion)

ការគំរាមពាក់ព័ន្ធសកម្មភាពផ្លូវភេទ (Sextortion) គឺជាទង្វើដែលជនទុច្ចរិត ប្រើប្រាស់រូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទ (ជាញឹកញាប់) ដែលបានទទួលពីកុមារ តាមរយៈការផ្ញើ ឬការបញ្ជូនរូបភាពអាក្រាត ឬបង្ហាញសកម្មភាពផ្លូវភេទដែលបង្កើតឡើងដោយខ្លួនឯង ដើម្បីគំរាមកុមារឱ្យបញ្ជូនរូបថត ឬវីដេអូផ្លូវភេទបន្ថែមទៀតដល់ពួកគេ ដើម្បីជួបផ្ទាល់ក្នុងគោលបំណងផ្លូវភេទ ឬដើម្បីទទួលបាននូវផលប្រយោជន៍ផ្សេងទៀតដូចជា ថវិកា សម្ភារៈ ឬការគ្រប់គ្រងលើកុមារជាដើម។

ទម្រង់ធ្ងន់ធ្ងរបំផុតនៃការល្បួងលោមគឺ **"ការគំរាមពាក់ព័ន្ធសកម្មភាពផ្លូវភេទ"**។ ជារឿយៗជនទុច្ចរិតតែងប្រព្រឹត្តចំពោះកុមារ តាមវិធីខាងក្រោម៖

- ការទទួលបានរូបភាព ឬវីដេអូផ្លូវភេទជាញឹកញាប់ គឺដោយសារការបោកបញ្ឆោត ឬគំរាមកំហែង
- ជនទុច្ចរិតនឹងប្រើការបោកបញ្ឆោត និងការគំរាមកំហែង ដោយប្រាប់កុមារថា ពួកគេនឹងលាតត្រដាង ឬចែករំលែកព័ត៌មាន ឬខ្លឹមសារដល់ក្រុមគ្រួសារ និងមិត្តភក្តិរបស់ពួកគេ

- ជាទូទៅកុមារមានការភ័យខ្លាចយ៉ាងខ្លាំង នៅពេលដែលជនទុច្ចរិតព្យាយាមណែនាំឱ្យផលិត និងផ្ញើសម្ភារៈបន្ថែម ឬជម្រិតទាមទារជាថវិកាដោយការគំរាមកំហែង
- ការគំរាមកំហែងដើម្បីលាតត្រដាងរឿងរ៉ាវអាចជាការពិត ឬមិនពិត។

ជនទុច្ចរិតអាចប្រើប្រាស់ខ្លឹមសារមាតិកាមានស្រាប់មួយចំនួន ដែលពួកគេទទួលបានពីកុមារផ្សេងទៀត ដើម្បីបោកបញ្ឆោត ឬគំរាមកំហែងកុមារឱ្យបង្កើត និងចែករំលែកខ្លឹមសារមាតិកាបន្ថែម ឬជម្រិតទាមទារថវិកា។ ពេលខ្លះជនទុច្ចរិតមិនមានខ្លឹមសារមាតិកាទាំងនោះទេ ប៉ុន្តែពួកគេធ្វើពុតដូចជាមាន ឬនិយាយថា ពួកគេបានចូលប្រើកុំព្យូទ័រ និងបានទាញយកប្រវត្តិរបស់កុមារទាំងនោះ។

ការប្រើរូបភាព ដែលទទួលបានពីកុមារយកទៅចែករំលែកបន្ត ដើម្បីធ្វើឱ្យកុមារមានភាពអាម៉ាស់ ហើយជំរុញ និងគំរាមកំហែងកុមារនោះ ឱ្យចែករំលែកខ្លឹមសារបន្ថែមទៀត។ នេះជាវិធីសាស្ត្រទូទៅ ដែលធ្វើឱ្យកុមារមានភាពភ័យខ្លាច ហើយជំរុញឱ្យពួកគេបង្កើត និងបញ្ជូនសម្ភារៈបន្ថែមទៀត ដើម្បីជាថ្នូររួចផុតពីភាពអាម៉ាស់ ហើយសកម្មភាពរំលោភបំពាននេះ នៅតែបន្តដដែលៗ។

ចំពោះគ្រួសារដែលមានការពិភាក្សាអំពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ អាចជួយឱ្យរកឃើញនូវបញ្ហាទាំងនេះជាមុន និងទាន់ពេលវេលា ហើយអាចបញ្ឈប់សកម្មភាពរំលោភបំពានដដែលៗនេះបាន។

៥.២.៤. ការផ្សាយផ្ទាល់នៃការរំលោភបំពានផ្លូវភេទលើកុមារ (Live online child sexual exploitation)

ការផ្សាយផ្ទាល់នៃការរំលោភបំពានផ្លូវភេទលើកុមារ សំដៅលើការផ្សាយផ្ទាល់ នៃសកម្មភាពកេងប្រវ័ញ្ចផ្លូវភេទពាក់ព័ន្ធកុមារ ឬការឱ្យកុមារសំដែងសកម្មភាពផ្លូវភេទនៅមុខកាមេរ៉ា (អាចក្នុងស្ថានភាពអាក្រាត ឬក្នុងស្ថានភាពផ្លូវភេទ) ដែលភ្ជាប់ទៅនឹងអ៊ីនធឺណិត និងអាចឱ្យអ្នកដទៃចូលទស្សនាបានពីចម្ងាយ ឬតាមប្រព័ន្ធអនឡាញក្នុងពេលតែមួយ។ ពេលខ្លះជនទុច្ចរិតផ្តល់ជាថវិកា សម្ភារៈមានតម្លៃដល់កុមារផ្ទាល់ ឬតាមរយៈអ្នកសម្របសម្រួល ឬអន្តរការី ដើម្បីដោះដូរជាមួយនឹងសកម្មភាពនេះ។

ជនទុច្ចរិតចំណាយថវិកា ដើម្បីទទួលបានការផ្សាយផ្ទាល់ ឬដឹកនាំកុមារឱ្យធ្វើសកម្មភាពផ្លូវភេទដោយខ្លួនឯងក្នុងការផ្សាយផ្ទាល់។ ប្រភេទនៃការរំលោភបំពាននេះ គឺខុសពីការផលិត ឬការចែករំលែក CSAM ដោយសារមិនបានរក្សាទុកនូវវីដេអូនោះទេ ករណីនេះ ធ្វើឱ្យមន្ត្រីអនុវត្តច្បាប់ពិបាករកវត្តតាងក្នុងការស៊ើបអង្កេត ប៉ុន្តែករណីខ្លះជនទុច្ចរិតមួយចំនួនក៏អាចចម្លង និងរក្សាទុកវីដេអូទាំងនោះផងដែរ។

៥.២.៥. ការផ្ញើសារបែបផ្លូវភេទ (Sexting)

ការផ្ញើសារបែបផ្លូវភេទ គឺជាទម្រង់មួយដែលស្ថិតនៅក្នុងអន្តរកម្មនៃទម្រង់ ៣ ខាងលើ គឺ៖ ១.ការល្បួងលោម ២.រូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ និង៣.ការគំរាមពាក់ព័ន្ធសកម្មភាពផ្លូវភេទ។ ប្រទេសជាច្រើនមិនដាក់បញ្ចូលការផ្ញើសារបែបផ្លូវភេទនេះ នៅក្នុងទម្រង់នៃការកេងប្រវ័ញ្ចនិងការរំលោភបំពានផ្លូវភេទកុមារតាមប្រព័ន្ធអនឡាញទេ។ ប៉ុន្តែដោយឈរលើគោលការណ៍ណែនាំលុចហ្សំបួរ (Luxembourg Guidelines) កម្ពុជានៅតែរក្សាទម្រង់នេះ ជាការរំលោភបំពាន និងកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ។

ការផ្ញើសារបែបផ្លូវភេទ ដំបូងជាសកម្មភាពនៃការផ្ញើសារ គឺមានលក្ខណៈស្ម័គ្រចិត្តទៅវិញទៅមក ក្នុងការបញ្ជូន ការទទួល និងការចែករំលែកបន្តនូវសារ រូបថត វីដេអូផ្លូវភេទ ដែលបង្កើតឡើងដោយខ្លួនឯង ឬទទួលបានពីអ្នកផ្សេងទៀត។ សកម្មភាពនេះ អាចនាំឱ្យកើតមានការរំលោភបំពានផ្លូវភេទនៅពេលភាគីណាមួយឈប់ចង់ទទួលបានសារ ឬរូបភាពផ្លូវភេទ ប៉ុន្តែភាគីម្ខាងទៀតនៅតែបន្តផ្ញើឬបញ្ជូន។

៥.៣. ការរុកកួនតាមប្រព័ន្ធអនឡាញ (Cyberbully)

ការរុកកួនតាមប្រព័ន្ធអនឡាញ គឺជាអាកប្បកិរិយាដដែលៗពាក់ព័ន្ធនឹងបច្ចេកវិទ្យា ដែលប្រព្រឹត្តទៅតាមប្រព័ន្ធអនឡាញ ជួនកាលអាចធ្វើឡើងតាមអហ្វឡាញផងដែរ។ ទង្វើនេះអាចប្រព្រឹត្តទៅតាមរយៈបណ្តាញផ្សព្វផ្សាយសង្គម ថ្នាលកម្មវិធីផ្ញើសារសន្ទនា ហ្គេមកម្សាន្ត និងទូរសព្ទវៃឆ្លាត ឬថេបប្លេតដោយផ្ទាល់(ការផ្ញើសារ)។

គ្រប់កុមារអាចនឹងរងហានិភ័យពីការរុកកួន ឬជនទុច្ចរិតតាមប្រព័ន្ធអនឡាញ ហើយកុមារា កុមារី កុមារដែលមានអត្តសញ្ញាណយេនឌ័រចម្រុះ និងកុមារមានពិការភាពអាចរងនូវការរុកកួនខុសៗគ្នា។ ឧទាហរណ៍ កុមារីអាចត្រូវបានរុកកួនតាមការបន្ទុះបង្អាប់លើរូបរាង ទទួលបាននូវរូបភាពអាសអាភាស ឬរូបថតរបស់កុមារីត្រូវបានគេបង្ហោះដោយគ្មានការអនុញ្ញាត។ កុមារាអាចត្រូវបានរុកកួនថា គ្មានលក្ខណៈជាបុរស។ កុមារមានពិការភាពអាចរងហានិភ័យខ្ពស់ពីការរុកកួនតាមប្រព័ន្ធអនឡាញ ដូចជាកុមារមានភាពខ្សោយផ្នែកបញ្ញា ឬការរៀនសូត្រ។ ចូរពន្យល់ថា "**ការរុកកួនតាមប្រព័ន្ធអនឡាញ**" តែងកើតឡើងដោយមនុស្សស្គាល់គ្នា ដូចជាមិត្តភ័ក្តិនៅសាលា ឬសហគមន៍ ឬតាមប្រព័ន្ធអនឡាញ ឬក្រុមលេងហ្គេមកម្សាន្តជាមួយគ្នា ។

ការរុកកួនតាមប្រព័ន្ធអនឡាញខុសគ្នាពីការរុកកួនអហ្វឡាញ ពីព្រោះការរុកកួនតាមប្រព័ន្ធអនឡាញអាចសាយភាយ និងរីករាលដាលខ្លាំង។ កំណត់ត្រាបង្ហាញពីការរុកកួន ដែលអាចមើលឃើញជាសាធារណៈ ហើយព័ត៌មាននេះនៅបន្តមានរហូត។ ការឈ្លោះគ្នាតាមប្រព័ន្ធអនឡាញរវាងមិត្តភក្តិអាចរីករាលដាលកាន់តែធំនៅក្នុងសហគមន៍អនឡាញ ហើយជនរងគ្រោះអាចត្រូវបានគេព្រួតគ្នារុកកួន។ ដោយសារជាតុផ្សំ "**អនាមិកភាព**" ពួកអ្នករុកកួនមានអារម្មណ៍ថា ដូចជាមិនមានផលវិបាកទេ ហើយក៏មិនមានអ្នកណាអាចមើលឃើញពួកគេកំពុងពាក់ព័ន្ធនោះដែរ ដោយសារមានអ្នកពាក់ព័ន្ធច្រើន។ ដោយសារតែជាតុផ្សំ "**អចិន្ត្រៃយ៍**" នៃអ៊ីនធឺណិត បញ្ហានេះនៅតែអាចបន្តនៅក្នុងជីវិតរស់នៅរបស់ជនរងគ្រោះ។ កុមារអាចមានអារម្មណ៍ថា គ្មានវិធីណាមួយដែលអាចគេចចេញពីការរុកកួននេះបានទេ ដោយសារ ពួកគេធ្លាប់ទទួលរងគ្រោះទាំងនៅសាលា សហគមន៍ និងនៅផ្ទះ។ កុមារគិតថាគ្រប់គ្នាសុទ្ធតែដឹងអំពីរឿងនេះ។

មនុស្សពេញវ័យអាចដឹងអំពីហានិភ័យ ដែលកើតឡើងចំពោះកុមារពីមនុស្សដែលពួកគេមិនស្គាល់ ហើយមានបំណងចង់ធ្វើបាបពួកគេ។ ការរុកកួននេះ មានផលប៉ះពាល់ដល់កុមារជាច្រើន រួមទាំងកុមារផ្សេងទៀតដែលពួកគេស្គាល់ និងរស់នៅក្នុងសហគមន៍ជាមួយគ្នា។ ប៉ុន្តែមនុស្សពេញវ័យហាក់ដូចជាមិនសូវដឹងពីផលប៉ះពាល់ដែលកើតចេញអំពីហានិភ័យ និងគ្រោះថ្នាក់នេះទេ ហើយគិតថាវាមិនសូវសំខាន់។ ការគិតបែបនេះត្រូវតែមានការផ្លាស់ប្តូរ។ កុមារមួយចំនួន ដែលរងការរុកកួនតាមប្រព័ន្ធអនឡាញមានក្តីបារម្ភខ្លាំងណាស់។ កុមារជាច្រើនមានអារម្មណ៍ថា មិនអាចគេចចេញពីស្ថានភាពទាំងនេះ ហើយពួកគេបានបន្តរស់នៅដោយមានអារម្មណ៍បែបនេះពេញមួយជីវិត។

ការរុកគួនតាមអនឡាញ គឺជាសកម្មភាព ឬអាកប្បកិរិយាអាក្រក់ ដែលធ្វើឡើងដដែលៗ ក្នុងគោលបំណងបំភ័យ ធ្វើឱ្យមានកំហឹង មានភាពអាម៉ាស់ ការរំខាន ការដៀមដាម ការឈ្លោះប្រកែក ដែលកើតមានឡើងតាមប្រព័ន្ធអនឡាញ។ ការរុកគួនអាចមើលឃើញជាសាធារណៈ ហើយព័ត៌មាននៅបន្តមានរហូត។ ការរុកគួនតាមប្រព័ន្ធអនឡាញអាចកើតឡើងនៅលើថ្នាលកម្មវិធី បណ្ដាញសង្គម សារសន្ទនា និងហ្គេម។ ការរុកគួនជាទូទៅប្រព្រឹត្តដោយអ្នកដែលស្គាល់គ្នា ក្នុងគោលដៅបំភ័យ ធ្វើឱ្យខឹង ឬធ្វើឱ្យខ្មាស់គេ វាធ្វើឱ្យប៉ះពាល់ដល់ការរស់នៅរបស់កុមារ ទាំងក្នុងជីវិតអនឡាញ និងអហ្វឡាញ។ ការរុកគួនតាមប្រព័ន្ធអនឡាញមានលក្ខណៈ ដូចជា៖

- ការផ្ញើសារបែបគំរាមកំហែង ឬធ្វើឱ្យឈឺចាប់
- ការរើសអើង ឬមិនរាប់រកនរណាម្នាក់តាមប្រព័ន្ធអនឡាញ
- ការបង្ហោះរឿងមិនពិត ឬរឿងដែលធ្វើឱ្យនរណាម្នាក់អាម៉ាស់
- ការបង្កើតគណនីក្លែងក្លាយប្រើប្រាស់សម្រាប់ចំអកចំអន់នរណាម្នាក់
- ការចែករំលែករូបថតគួរឱ្យអាម៉ាស់របស់នរណាម្នាក់តាមប្រព័ន្ធអនឡាញ។

សញ្ញាណដែលបង្ហាញថា កុមារកំពុងទទួលរងការរុកគួនតាមប្រព័ន្ធអនឡាញ៖

- កុមារកើតទុក្ខ ក្រៀមក្រំ ខឹង ឬឆេវឆាវ
- កុមារផ្លាស់ប្ដូរអាកប្បកិរិយាតាមរយៈការប្រើប្រាស់ប្រព័ន្ធអនឡាញ ឧទាហរណ៍ ពួកគេភ័យខ្លាចនៅពេលប្រើទូរសព្ទវៃឆ្លាត ឬពេលខ្លះចង់ប្រើប្រព័ន្ធអនឡាញគ្រប់ពេល ឬមិនចង់ប្រើ
- កុមារផ្លាស់ប្ដូរលក្ខណៈទំនាក់ទំនងនៅក្នុងក្រុម
- កុមារចង់ចំណាយពេលជាមួយគ្រួសារជាងមិត្តភ័ក្តិ ឬនៅតែឯង។ល។

៥.៤. ការប្រឈមនឹងមាតិកាមិនសមរម្យតាមប្រព័ន្ធអនឡាញ

ជាតុផ្សំសំខាន់នៃអ៊ីនធឺណិត គឺមានលក្ខណៈសាធារណៈ ហើយមនុស្សគ្រប់គ្នាអាចចែករំលែក ឬដាក់បញ្ចូលរាល់ខ្លឹមសារមាតិកាដែលមាន។ រាល់ការចែកចាយតាមអ៊ីនធឺណិតនឹងត្រូវបានមើលឃើញជាសាធារណៈទូទាំងពិភពលោក។ ជាទូទៅ មានការប្រើពាក្យសម្ដីមិនសមរម្យ ហិង្សា ភាពភ័យខ្លាច ដែលគ្មានសុវត្ថិភាពសម្រាប់កុមារក្នុងការមើលតាមប្រព័ន្ធអនឡាញ។

ខាងក្រោមនេះគឺជាសកម្មភាពមិនសមរម្យតាមប្រព័ន្ធអនឡាញ ៖

- អំពើហិង្សា (ទាំងក្នុងជីវិតពិត ឬនៅលើវីដេអូហ្គេម)
- ចោរកម្ម ឬធ្វើអំពើខុសច្បាប់
- រូបភាព ឬវីដេអូបែបផ្លូវភេទ
- កុមារត្រូវបានគេធ្វើឱ្យឈឺចាប់
- ការធ្វើទារុណកម្ម រួមទាំងការធ្វើទារុណកម្មលើសត្វផងដែរ
- សកម្មភាពភេរវកម្ម
- ការប្រកាន់ពូជសាសន៍ ឬភេទ
- ភាសាអសុរោះ

- ជំរុញនានដែលផ្ដល់នូវគ្រោះថ្នាក់ ឧទាហរណ៍ ធ្វើបាបខ្លួនឯង ញុះញង់ ញ៉ាំអាហារមិនត្រឹមត្រូវ។

ខ្លឹមសារមាតិកាបែបនេះអាចកើតឡើងគ្រប់ពេល ខណៈយើងប្រើប្រាស់ប្រព័ន្ធអនឡាញ។ ក្នុងនោះរួមមានបណ្ដាញផ្សព្វផ្សាយសង្គម ការចែកចាយដោយផ្ទាល់ ជាពិសេសតាមរយៈការសន្ទនាជាក្រុម ដើម្បីធ្វើឱ្យអ្នកស្លុតចិត្ត និងស្អប់ខ្ពើមអ្នកដទៃ។ ការសិក្សាស្រាវជ្រាវថ្មីៗ ក៏បានផ្ដោតសំខាន់ទៅលើខ្លឹមសារមាតិកានេះ តាមរយៈការលេងហ្គេមកម្សាន្តផងដែរ ដែលពីមុនមានការស្រាវជ្រាវតិចតួចណាស់ក្នុងផ្នែកនេះ។ ការពិភាក្សាអំពីហានិភ័យនៅក្នុងថ្នាលកម្មវិធីហ្គេមកម្សាន្តពិតជាមានសារៈសំខាន់។ ប៉ុន្តែមិនមានការស្រាវជ្រាវច្បាស់លាស់ណាមួយ ដែលបង្ហាញពីទំនាក់ទំនងរវាងការលេងហ្គេម និងអាកប្បកិរិយាក្នុងជីវិតពិតឡើយ (សូម្បីតែដែលហ្គេមដែលមានលក្ខណៈហិង្សា)។ ហានិភ័យដែលកើតមានឡើងចំពោះកុមារ គឺមិនមែនមកពីការលេងហ្គេមកម្សាន្តផ្ទាល់នោះទេ ប៉ុន្តែហានិភ័យអាចបណ្ដាលមកពីមនុស្ស ដែលពួកគេកំពុងលេងជាមួយ។

ការិយាល័យអង្គការសហប្រជាជាតិប្រឆាំងអំពើភេរវកម្ម និងលទ្ធិជ្រុលនិយមបានចេញផ្សាយរបាយការណ៍មួយនៅចុងឆ្នាំ២០២២[7] ដោយបង្ហាញអំពីទំនាក់ទំនងខ្លឹមសារមាតិកាដែលគួរឱ្យស្អប់ខ្ពើម និងបង្កគ្រោះថ្នាក់ក្នុងបរិបទនៃការលេងហ្គេមជាក្រុម បានបង្ហាញដូចខាងក្រោម ៖

- មានមនុស្សចំនួនបីពាន់លាននាក់ នៅជុំវិញពិភពលោកដែលកំពុងលេងហ្គេមយ៉ាងសកម្ម
- ៨២% នៃប្រជាជនដែលរស់នៅទីប្រជុំជនក្នុងបណ្ដាប្រទេសតំបន់អាស៊ានកំពុងលេងហ្គេម
- ថវិកាចំនួន ៥.៥ពាន់លានដុល្លារអាមេរិកត្រូវបានចំណាយលើការលេងហ្គេមទូទាំងសាកលលោក នៅឆ្នាំ២០២២
- ហ្គេមបានផ្លាស់ប្ដូរ ហើយការយល់ឃើញរបស់យើងអាចរងឥទ្ធិពល ដោយសារកង្វះការយល់ដឹង
- ខណៈអ្នកលេងហ្គេមតាមកុំព្យូទ័រជាច្រើន បានផ្លាស់ប្ដូរទៅលេងតាមទូរសព្ទវៃឆ្លាតបានកើនឡើង។ ក្នុងរយៈពេលប៉ុន្មានឆ្នាំថ្មីៗនេះ ទិន្នន័យបង្ហាញថា មានអ្នកលេងជាងពាក់កណ្ដាលបានលេងហ្គេមតាមទូរសព្ទវៃឆ្លាត។
- កុមារ និងយុវជនដែលមានអាយុចន្លោះពី ១០-២០ឆ្នាំ (ស្មើនឹង ៣០% នៃអ្នកលេងហ្គេម) ចូលចិត្តលេងហ្គេម Minecraft, Fortnite និង Roblox (ថ្នាលកម្មវិធីហ្គេមទាំងបីនេះកំពុងពេញនិយមខ្លាំង)។
- ការលេងហ្គេមជាញឹកញាប់ប្រើប្រាស់ថ្នាលកម្មវិធីច្រើន ក្នុងពេលតែមួយ ដោយគេអាចប្រើទាំងថ្នាលកម្មវិធីលេងហ្គេម ថ្នាលកម្មវិធីសារសន្ទនា និងថ្នាលកម្មវិធីផ្សាយផ្ទាល់។

ការលេងហ្គេម គឺជាបទពិសោធវិជ្ជមាន ប្រសិនបើការលេងក្នុងលក្ខណៈ ជាប្រកួតប្រជែងគ្នា ហើយមានអត្ថប្រយោជន៍ស្រដៀងគ្នាសម្រាប់ជាក្រុម អភិវឌ្ឍជំនាញសង្គម មិត្តភាព និងសហគមន៍ ព្រមទាំងអភិវឌ្ឍជំនាញវិជ្ជមាន មានដូចជា ការផ្ដោតអារម្មណ៍ ការដោះស្រាយបញ្ហា ជំនាញនៃការធ្វើចលនា និងការយល់ចិត្ត។

៨០%នៃអ្នកលេងហ្គេម បានរាយការណ៍ថាមានការប្រឈមនឹងខ្លឹមសារមាតិកាគួរឱ្យស្អប់ខ្ពើម ឬហិង្សា។ ៣០% បានរាយការណ៍ថា មានការប្រឈមជាញឹកញាប់ទៅនឹងការស្អប់ និងរើសអើងចំពោះស្ត្រី ការរើសអើង

[7] https://www.un.org/counterterrorism/cct/publications-reports

ជាតិសាសន៍ ឬការស្រឡាញ់ភេទដូចគ្នា។ សូមបញ្ជាក់ថា ហានិភ័យទាំងនេះកើតចេញពីអ្នកដែលកុមារមានទំនាក់ទំនងជាមួយ នៅពេលពួកគេលេងជាមួយគ្នា។

ដូចដែលបានជជែករួចហើយក្នុងផ្នែកនេះ វិធីល្អបំផុតដើម្បីធានាថាកុមារមិនរងឥទ្ធិពលពីខ្លឹមសារមាតិកាដែលគួរឱ្យស្អប់ខ្ពើម និងមានគ្រោះថ្នាក់ គឺការជជែកបើកចំហរវាងឪពុកម្តាយ និងកុមារវ័យជំទង់។ ដើម្បីធ្វើកិច្ចការនេះ មនុស្សពេញវ័យត្រូវស្វែងយល់អំពីការលេងហ្គេម និងការវិវឌ្ឍរបស់ហ្គេម។ ជាថ្មីម្តងទៀត ពួកគេអាចស្នើឱ្យកុមារបង្រៀនពួកគេអំពីរបៀបនៃការលេងហ្គេមទាំងនេះ។ ការជជែកពិភាក្សាជាមួយកុមារនៅក្នុងគ្រួសារគឺជាការចាំបាច់បំផុត ព្រោះថា ប្រសិនបើកុមារមានអារម្មណ៍មិនល្អ ឬមានបញ្ហាពាក់ព័ន្ធនឹងការប្រើប្រាស់អ៊ីនធឺណិត ពួកគេអាចចូលរួមពិគ្រោះគ្នា ដើម្បីរកវិធីដោះស្រាយ។ ពួកគេអាចរាំងខ្ទប់ (Block) រាយការណ៍ (Report) ឬប្រឹក្សាយោបល់ជាមួយមនុស្សពេញវ័យដែលពួកគេទុកចិត្ត។ ប៉ុន្តែប្រការសំខាន់ គឺមនុស្សពេញវ័យត្រូវយល់ដឹងអំពីហានិភ័យតាមប្រព័ន្ធអនឡាញ ដើម្បីជួយឱ្យមានការពិភាក្សាគ្នាកាន់តែប្រសើរ។ វាមានសារៈសំខាន់ណាស់ដែលមនុស្សពេញវ័យឈ្វេងយល់អំពីការលេងហ្គេម និងបញ្ហាដែលកុមារកំពុងជួបប្រទះ ហើយមិនគួរផ្តោតលើតែហ្គេមប៉ុណ្ណោះទេ ប៉ុន្តែត្រូវយកចិត្តទុកដាក់ផងដែរទៅលើទំនាក់ទំនងបណ្តាញសង្គម ដូចជា ទំនាក់ទំនងដែលកុមារមានជាមួយមនុស្សផ្សេងទៀត ពេលពួកគេកំពុងលេងហ្គេម។

៥.៥. បាតដៃសុវត្ថិភាព

បាតដៃសុវត្ថិភាព គឺជាវិធីសាស្ត្រសាមញ្ញងាយស្រួល ដែលកម្លាំងសេវាសង្គម ឪពុកម្តាយ អាណាព្យាបាល និងអ្នកថែទាំអាចប្រើប្រាស់ ដើម្បីបង្រៀនកុមារអំពីការការពារខ្លួន នៅពេលមានហានិភ័យ ឬពេលត្រូវការជំនួយ។ វិធីសាស្ត្រនេះមានគោលបំណងបង្កើនការយល់ដឹងរបស់កុមារអំពីសិទ្ធិ និងសុវត្ថិភាព ដោយផ្តល់នូវវិធីសាស្ត្រសាមញ្ញសម្រាប់កុមារក្នុងការស្វែងរកជំនួយ ដោយបង្កើតបណ្តាញការពារ ដែលមានគ្រួសារ មិត្តភក្តិ និងសហគមន៍។ ការប្រើរូបភាពបាតដៃគឺដើម្បីឱ្យកុមារងាយយល់ ហើយឱ្យកុមារសរសេរឈ្មោះមនុស្ស ដែលគេជឿទុកចិត្តលើម្រាមដៃនីមួយៗ។ បាតដៃសុវត្ថិភាពជាវិធីសាស្ត្រសិក្សា ឬល្បែង ដើម្បីឱ្យកុមារចងចាំបានល្អ។ កម្លាំងសេវាសង្គមត្រូវឱ្យកុមារគូររូបបាតដៃ និងម្រាមដៃទាំង ៥ សម្រាប់ជាជំហានសុវត្ថិភាព ដូចខាងក្រោម៖

- ម្រាមមេដៃសម្រាប់កុមារខ្លួនឯង
  - កុមារត្រូវរៀនស្គាល់អារម្មណ៍របស់ខ្លួន (សប្បាយ ភ័យ ខឹង ឬអាម៉ាស់)
  - បង្រៀនឱ្យកុមារជឿជាក់លើអារម្មណ៍របស់ខ្លួន។
- ម្រាមចង្អុលដៃសម្រាប់មនុស្សជិតស្និទ្ធនឹងកុមារ
  - ជ្រើសរើសមនុស្សដែលកុមារជឿទុកចិត្ត (ឪពុក ម្តាយ គ្រូ ឬអ្នកថែទាំ)
  - បង្រៀនឱ្យកុមារប្រាប់ពួកគេពេលមានបញ្ហា។
- ម្រាមដៃកណ្តាលសម្រាប់មិត្តភក្តិ
  - កុមារអាចស្វែងរកជំនួយពីមិត្តភក្តិដែលគេជឿទុកចិត្ត
  - លើកទឹកចិត្តកុមារមិននៅតែឯងពេលមានហានិភ័យ។
- ម្រាមនាងដៃសម្រាប់មនុស្សដែលអាចផ្តល់ជំនួយនៅក្នុងសហគមន៍
  - អ្នកជិតខាង គ្រូពេទ្យ ឬអ្នកផ្តល់សេវាសង្គមកិច្ច

- ○ បង្រៀនឱ្យកុមារស្គាល់ថា មានមនុស្សជាច្រើនអាចជួយបាន។
- ម្រាមកូនដៃសម្រាប់សេវាជំនួយបន្ទាន់
    - ○ លេខទូរស័ព្ទបន្ទាន់
    - ○ បង្រៀនឱ្យកុមារចេះរកជំនួយពេលមានស្ថានភាពគ្រោះថ្នាក់។

៥.៦. ការជួយឪពុកម្តាយក្នុងការពិភាក្សាអំពីសុវត្ថិភាពតាមប្រព័ន្ធអនឡាញ

៥.៦.១. កិច្ចព្រមព្រៀងស្តីពីការប្រើប្រាស់អនឡាញនៅផ្ទះ

កិច្ចព្រមព្រៀងស្តីពីការប្រើប្រាស់អនឡាញនៅក្នុងផ្ទះ គឺជាការសម្រេចចិត្តរួមរបស់សមាជិកគ្រួសារ ដើម្បីធានាថាការប្រើប្រាស់អ៊ីនធឺណិតមានសុវត្ថិភាព សមរម្យ និងមានសុចរិត។ វាជាឧបករណ៍សំខាន់ក្នុងការបង្រៀនកុមារអំពីការទទួលខុសត្រូវ និងការការពារខ្លួនឯង ព្រមទាំងជួយឲ្យឪពុកម្តាយអាចតាមដាន និងគ្រប់គ្រងការប្រើប្រាស់ឌីជីថលរបស់កុមារបានប្រសើរឡើង។ ការបង្កើតកិច្ចព្រមព្រៀងនេះឡើង ក្នុងគោលបំណងធ្វើជាវិន័យច្បាស់លាស់មួយសម្រាប់គ្រួសារក្នុងការប្រើប្រាស់អ៊ីនធឺណិត។ កិច្ចព្រមព្រៀងនេះ នឹងការពារកុមារពីមាតិកាមិនសមរម្យ និងហានិភ័យតាមប្រព័ន្ធអនឡាញ ដោយបង្កើនការយល់ដឹង និងការទទួលខុសត្រូវក្នុងការប្រើប្រាស់ឧបករណ៍ឌីជីថល ព្រមទាំងជំរុញការប្រាស្រ័យទាក់ទង និងការជួយគាំទ្ររវាងសមាជិកគ្រួសារ។

កិច្ចព្រមព្រៀងស្តីពីការប្រើប្រាស់អនឡាញនៅក្នុងផ្ទះ គឺជាវិធីសាស្ត្រដ៏មានប្រសិទ្ធភាពក្នុងការការពារកុមារ និងផ្តល់ផលប្រយោជន៍ ដូចជា៖

- ស្វែងយល់អំពីការប្រើប្រាស់ និងសារៈសំខាន់នៃប្រព័ន្ធអនឡាញ
- រៀនពីគ្នាទៅវិញទៅមក
- ជួយបង្កើតវិន័យក្នុងគ្រួសារ
- កុមារមានសុវត្ថិភាព ពេលប្រើអ៊ីនធឺណិត
- ជួយឱ្យឪពុកម្តាយមានភាពជឿជាក់ និងអាចតាមដានបានងាយ
- បង្កើតវប្បធម៌ឌីជីថលវិជ្ជមានក្នុងគ្រួសារ
- ជួយឱ្យកុមាររៀនជំនាញឌីជីថល ដោយមានការណែនាំត្រឹមត្រូវ
- មានសារៈសំខាន់តាំងពីពេលចាប់ផ្តើមដំណើរការរហូតទទួលបានលទ្ធផល។

ដើម្បីរៀបចំកិច្ចព្រមព្រៀងបានល្អ យើងត្រូវដឹងនូវគន្លឹះមួយចំនួន ដូចខាងក្រោម៖

- ត្រូវឆ្លើយតបទៅនឹងតម្រូវការផ្សេងៗគ្នា ទៅតាមកម្រិតអាយុរបស់កុមារនៅក្នុងផ្ទះ
- **ពេលវេលា៖** កំណត់ម៉ោងប្រើប្រាស់អ៊ីនធឺណិតឧទាហរណ៍ មិនលើសពី ២ម៉ោងក្នុងមួយថ្ងៃ
- **មាតិកា៖** កំណត់ប្រភេទគេហទំព័រ ឬកម្មវិធីដែលអាចប្រើបាន និងមិនអាចប្រើបាន
- **សុវត្ថិភាព៖** កុមារត្រូវរាយការណ៍បញ្ហា ឬការរំខាននានាទៅឪពុកម្តាយ
- **ការគោរព៖** មិនប្រើអ៊ីនធឺណិតដើម្បីរំលោភសិទ្ធិអ្នកដទៃ ឬបង្កការរំខាន
- **ការទទួលខុសត្រូវ៖** ប្រើប្រាស់ឧបករណ៍ឌីជីថលដោយមានការយល់ដឹង និងគោរពច្បាប់
- កិច្ចព្រមព្រៀងត្រូវមានការចូលរួមពីកុមារ ដើម្បីឱ្យកុមារមានអារម្មណ៍ថា ខ្លួនជាផ្នែកមួយនៃការសម្រេចចិត្ត
- ប្រើភាសាសាមញ្ញ និងរូបភាព ដើម្បីកុមារងាយយល់
- កិច្ចព្រមព្រៀងគួរតែជាឯកសារដែលមានសុពលភាពអចិន្ត្រៃយ៍
- ត្រួតពិនិត្យឡើងវិញពេលកុមារចម្រើនវ័យ និងនៅពេលមានការវិវឌ្ឍផ្លាស់ប្តូរនៃបច្ចេកវិទ្យា។ ការពិនិត្យកែតម្រូវឡើងវិញនេះ ជារឿងល្អទៅតាមស្ថានភាពជាក់ស្តែង
- ដំណោះស្រាយដែលល្អ គួរតែមានយុត្តិធម៌សម្រាប់ទាំងអស់គ្នា។

៥.៦.២. ការពិភាក្សាអំពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ

ឪពុកម្តាយ អាណាព្យាបាល និងអ្នកថែទាំ គួរពិភាក្សាអំពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ ដោយផ្តោតលើចំណុចមួយចំនួនដូចខាងក្រោម៖

- បច្ចេកវិទ្យាទូទៅ
  - តើថ្នាលកម្មវិធីណាខ្លះ ដែលមិត្តភក្តិរបស់កុមារតែងតែប្រើ?
  - តើកុមារធ្លាប់ត្រូវបានអ្នកមិនស្គាល់ទាក់ទងមកដែរឬទេ?
  - តើកុមារធ្លាប់សន្ទនាជាមួយនរណាម្នាក់ ដែលមិនរៀននៅសាលាជាមួយកុមារដែរឬទេ?

- ការរុកកួនតាមប្រព័ន្ធអនឡាញ
  - តើកុមារធ្លាប់បានឃើញមនុស្សព្រួតគ្នាវាយប្រហារតាមប្រព័ន្ធអនឡាញដែរឬទេ?
  - តើគណនីរបស់កុមារធ្លាប់ត្រូវបានគេភ្ជាប់(tag) ជាមួយរូបភាព ដែលធ្វើឱ្យកុមារមិនសប្បាយចិត្តដែរឬទេ?
- ប្រព័ន្ធផ្សព្វផ្សាយសង្គម/ហ្គេម
  - តើកុមារចង់ឱ្យកម្មវិធី Facebook, TikTok, Instagram បង្ហាញថាតើកុមារជានរណាដែរឬទេ?
  - តើកុមារសម្រេចចិត្តដូចម្តេចនៅពេលមានការស្នើសុំធ្វើជាមិត្តភក្តិ?
  - តើកុមារធ្លាប់ឃើញមិត្តភក្តិរបស់ខ្លួនមិនសប្បាយចិត្តនឹងអ្វីដែលពួកគេបានបង្ហោះដែរឬទេ? ហេតុអ្វី?
- ជំនាញដោះស្រាយ
  - តើកុមារធ្លាប់ទទួលបានសារ ដែលធ្វើឱ្យកុមារមិនសប្បាយចិត្តដែរឬទេ? តើកុមារធ្វើដូចម្តេច?
  - តើកុមារដឹងពីរបៀបដកការភ្ជាប់(un-tag) គណនីរបស់កុមារពីខ្លឹមសារមាតិការបស់នរណាម្នាក់ដែរឬទេ?

៥.៧. គន្លឹះឆ្លើយតបទៅនឹងបញ្ហាធ្ងន់ធ្ងរតាមប្រព័ន្ធអនឡាញ

មានវិធីសាស្ត្រជាច្រើនដែលមនុស្សពេញវ័យអាចធ្វើ ដើម្បីជួយកុមារឆ្លើយតបទៅនឹងបញ្ហាធ្ងន់ធ្ងរតាមប្រព័ន្ធអនឡាញ ដែលមានដូចជា ការរំលោភបំពានផ្លូវភេទ និងការរុកកួនតាមប្រព័ន្ធអនឡាញជាដើម។ កិច្ចការពារកុមារតាមប្រព័ន្ធអនឡាញ គឺដូចគ្នានឹងកិច្ចការពារកុមារតាមអហ្វឡាញដែរ ដោយយើងត្រូវពិចារណាបញ្ចូលបន្ថែមនូវការប្រើប្រាស់ប្រព័ន្ធអនឡាញប្រចាំថ្ងៃរបស់យើង។

វិធីសាស្ត្រទាំងនេះ គឺជាមូលដ្ឋានដែលយើងត្រូវធ្វើរួមគ្នា និងត្រូវមានការចូលរួមពីឳពុកម្តាយ អាណាព្យាបាល និងអ្នកថែទាំ ដើម្បីណែនាំចំពោះការឆ្លើយតបនីមួយៗ។ វិធីទាំងនេះក៏មានលម្អិតអំពីសកម្មភាពអនុវត្តនៅក្នុងមេរៀនការផ្តល់ប្រឹក្សា និងការងារគ្រប់គ្រងករណីផងដែរ។ ដើម្បីជួយកុមារឱ្យមានសុវត្ថិភាពតាមប្រព័ន្ធអនឡាញ មានគន្លឹះមួយចំនួនសម្រាប់កម្លាំងសេវាសង្គម៖

- **គិត៖** គាំទ្រកុមារឱ្យចេះពិចារណាអំពីផលវិបាកនៃអ្វីដែលពួកគេនិយាយ និងធ្វើនៅតាមប្រព័ន្ធអនឡាញ។ លើកទឹកចិត្តពួកគេឱ្យពិចារណាអំពីកេរ្តិ៍ឈ្មោះនិងកិត្តិយស មុនពេលបញ្ចេញមតិ (comment) ចែករំលែក (share) និងចូលចិត្ត(like) អ្វីៗនៅតាមប្រព័ន្ធអនឡាញ។
- **រៀន៖** ឈ្វេងយល់អំពីអ្វីដែលកុមារធ្វើតាមប្រព័ន្ធអនឡាញដោយការសួរនាំពួកគេ។ ឳពុកម្តាយត្រូវដឹងពីថ្នាលកម្មវិធីដែលពួកគេកំពុងប្រើ និងចំណាយពេលវេលាផ្ទាល់ខ្លួន ដើម្បីឈ្វេងយល់អំពីថ្នាលកម្មវិធីទាំងនោះ។ យើងអាចកំណត់ព្រំដែន និងគ្រប់គ្រងថ្នាលកម្មវិធីដែលកុមារអាចប្រើតែម្នាក់ឯងបាន ឬដាក់កំរិតហួតដល់ពួកគេមានវ័យកាន់តែច្រើន។ ដូចគ្នានេះដែរ គួរព្យាយាមឈ្វេងយល់ពីពាក្យពេចន៍ ដែលកុមារកំពុងប្រើ ដើម្បីឱ្យអ្នកអាចធ្វើការពិភាក្សាគ្នាបាន។
- **ស្តាប់៖** សុំឱ្យកុមារនិយាយអំពីបទពិសោធន៍នៃការប្រើប្រាស់ប្រព័ន្ធអនឡាញរបស់ពួកគេ ដោយមិនមានការស្តីបន្ទោស ឬវិនិច្ឆ័យ។ បញ្ហាដែលរារាំងកុមារក្នុងការសុំជំនួយ ឬជំនួយពីមនុស្ស

ពេញវ័យដែលគេទុកចិត្តនោះ គឺការភ័យខ្លាចថា ពួកគេនឹងត្រូវស្ដីបន្ទោសចំពោះទង្វើរបស់ពួកគេ។ សូមចាំថា ជនទុច្ចរិតជាអ្នកទទួលខុសត្រូវចំពោះទង្វើនេះ។

- **ពិនិត្យ៖** គាំទ្រកុមារក្នុងការពិនិត្យ និងវាយតម្លៃភាពជឿជាក់ នៃព័ត៌មានតាមប្រព័ន្ធអនឡាញ។ បង្ហាញឧទាហរណ៍នៃព័ត៌មានពិតឬមិនពិត និងបង្រៀនពួកគេពីរបៀបស្វែងរកប្រភពព័ត៌មានត្រឹមត្រូវ ឬមិនត្រឹមត្រូវ។ បង្រៀនពួកគេឱ្យចេះវិភាគ ពិចារណា មុននឹងចែករំលែក(share)។
- **ចាកចេញ៖** ណែនាំកុមារឱ្យចេះរាំងខ្ទប់(Block) ឬផ្ដាច់ចេញពីខ្លឹមសារមាតិកា ការសន្ទនា ឬគណនីដែលធ្វើឱ្យពួកគេមិនសប្បាយចិត្ត។ បង្រៀនកុមារឱ្យជឿជាក់លើសតិសម្បជញ្ញៈរបស់ពួកគេ ដោយរំលឹកថា ពួកគេអាចជ្រើសរើសអ្វីមួយ ឬនរណាម្នាក់ដែលពួកគេចង់ទាក់ទងជាមួយដែលមិនមានសម្ពាធអារម្មណ៍។
- **ប្រាប់៖** ស្នើឱ្យកុមារប្រាប់មនុស្សពេញវ័យដែលពួកគេទុកចិត្ត ប្រសិនបើនរណាម្នាក់ ឬមានអ្វីមួយកើតឡើងនៅតាមប្រព័ន្ធអនឡាញ ដែលធ្វើឱ្យពួកគេមិនសប្បាយចិត្ត។ រំលឹកកុមារថា ពួកគេនឹងមិនមានបញ្ហាអ្វីនោះទេ ចំពោះការប្រាប់អំពីបញ្ហាតាមអនឡាញទាំងនោះ។
- **បង្រៀន៖** បង្រៀនកុមារអំពីជំនាញមួយចំនួន ដើម្បីជៀសវាងហានិភ័យដែលអាចបង្កគ្រោះថ្នាក់ ដូចជាការរក្សាព័ត៌មានផ្ទាល់ខ្លួនជាឯកជនភាព និងត្រូវយកចិត្តទុកដាក់ស្វែងយល់ ចំពោះទំនាក់ទំនងថ្មីជាមួយមនុស្ស ដែលពួកគេមិនធ្លាប់ស្គាល់នៅក្នុងជីវិតពិត។
- **លើកទឹកចិត្ត៖** គាំទ្រកុមារឱ្យធ្វើរឿងត្រឹមត្រូវតាមប្រព័ន្ធអនឡាញ និងធ្វើតាមសតិសម្បជញ្ញៈរបស់ពួកគេ។ ណែនាំកុមារលើសកម្មភាពដែលពួកគេពាក់ព័ន្ធតាមប្រព័ន្ធអនឡាញ។
- **ប្រមូល៖** បង្ហាញកុមារពីរបៀបប្រមូល និងរក្សាទុកភស្តុតាង។ ក្នុងករណីវត្ថុតាងជាសារអត្ថបទ សូមថតអេក្រង់ទុកជាភស្តុតាង។ ក្នុងករណីរូបភាព-សម្ភារៈដែលបង្ហាញពីស្ថានភាពអក្រាត សូមកុំថតអេក្រង់ តែត្រូវថតចម្លងតំណភ្ជាប់ (Copy link) ដើម្បីធ្វើជូននគរបាល។
- **រាយការណ៍៖** ជូនដំណឹងដល់ថ្នាលកម្មវិធី ឬនគរបាលដោយផ្ទាល់អំពីបញ្ហា។ ត្រូវប្រាជកថាយើងបានត្រៀមទុកជាមុនសម្រាប់អ្វីមួយដែលនឹងអាចក្លាយជាបញ្ហា។
- **តាមដាន៖** ពិនិត្យមើលថាតើកុមារកំពុងធ្វើអ្វីតាមប្រព័ន្ធអនឡាញ ហើយនរណាដែលពួកគេកំពុងប្រាស្រ័យទាក់ទង។ វិធីដ៏ល្អត្រូវមានការព្រមព្រៀងចំពោះការតាមដាន និងចូលរួមនៅក្នុងបណ្ដាញទំនាក់ទំនងរបស់ពួកគេដោយបើកចំហ និងមិនមានការលាក់លៀម។ តាមដានគណនីរបស់ពួកគេហើយពិភាក្សាអំពីអ្វីដែលអ្នកឃើញ ដូចជា ការចូលចិត្ត (like) ការផ្ដល់យោបល់ (comment) និងចែករំលែក (share) របស់ពួកគេ។
- **បញ្ជូន៖** ជួយកុមារឱ្យទទួលសេវាគាំទ្រដែលអាចផ្ដល់ការណែនាំពីអ្នកជំនាញ ប្រសិនបើមានបញ្ហាធ្ងន់ធ្ងរកើតឡើង។

៥.៨. ការគាំទ្រចំពោះការលាតត្រដាងបញ្ហារបស់កុមារ

វិធីដែលយើងឆ្លើយតបចំពោះការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញមានផលប៉ះពាល់ខ្លាំងណាស់។ ទី១ គឺផលប៉ះពាល់ចំពោះកុមារដែលពាក់ព័ន្ធនឹងបញ្ហា និងកុមារដែលបានឃើញ

ហេតុការណ៍ និងរបៀបឆ្លើយតបរបស់គ្រួសារ សហគមន៍ និងកម្លាំងសេវាសង្គម។ ទី២ យើងនឹងមិនអាចដឹងថា នៅថ្ងៃខាងមុខ កុមារនឹងប្រាប់យើងដែរឬទេ បើពួកគេជួបបញ្ហាបែបហ្នឹង។ ការឆ្លើយតបរបស់យើង អាចបន្ទច់បង្អាក់កុមារក្នុងការនិយាយអំពីបញ្ហា ដោយសារពួកគេភ័យខ្លាចការបញ្ឈប់មិនឱ្យប្រើប្រាស់អ៊ីនធឺណិត។ ប្រសិនបើយើងប្រើវិធីការស្តីបន្ទោស នោះអាចជះឥទ្ធិពលកាន់តែខ្លាំង នឹងនាំឱ្យកុមារមិនប្រាប់យើងអំពីរឿងរ៉ាវរបស់គេ។ មានគន្លឹះសំខាន់ៗចំនួន ៣ សម្រាប់ការឆ្លើយតបទៅនឹងការព្រួយបារម្ភរបស់កុមារអំពីការកេងប្រវ័ញ្ច និងការរំលោភបំពានតាមប្រពន្ធ័អនឡាញ៖

១. **បង្ហាញការជឿជាក់** ចំពោះការលាតត្រដាងរបស់កុមារ។
២. ត្រូវបញ្ជាក់ថាការលួងលោម និងរំលោភបំពានតាមប្រព័ន្ធអនឡាញ**មិនមែនជាកំហុសរបស់កុមារ**ទេ កុមារមិនមានការទទួលខុសត្រូវ និងមិនគួរមានអារម្មណ៍អាម៉ាស់ឡើយ។
៣. **ជនទុច្ចរិតទើបជាអ្នកដែលត្រូវស្តីបន្ទោស** កុមារមិនបានធ្វើអ្វីដែលនាំឱ្យមានបញ្ហានោះទេ។

មានការណែនាំមួយចំនួន ដែលកម្លាំងសេវាសង្គម ឪពុកម្តាយ អាណាព្យាបាល និងអ្នកថែទាំត្រូវអនុវត្តនៅពេលដែលកុមារលាតត្រដាងប្រាប់អំពីការរំលោភបំពាន ឬបង្ហាញឱ្យឃើញថា ពួកគេកំពុងប្រឈមនឹងគ្រោះថ្នាក់។ ដើម្បីឱ្យការអនុវត្តបានល្អ យើងគួរបែងចែកការណែនាំនេះជាជំហានតូចៗដូចខាងក្រោម ប៉ុន្តែនៅពេលយើងសម្ភាសន៍ជាមួយកុមារជំហានទាំងនេះ អាចនឹងត្រូវបត់បែន៖

ក. ការជួយឱ្យកុមារមានអារម្មណ៍សុវត្ថិភាព

- ត្រូវប្រាកដថា កុមារមានសុវត្ថិភាពដោយគិតទាំងទីកន្លែងជួប គម្លាតនៃការអង្គុយ អ្នកណាខ្លះដែលអាចចូលរួមបាន និងត្រូវគិតថា តើយើងនឹងត្រូវឆ្លើយតបដូចម្តេច បើកុមារកំពុងមានអារម្មណ៍ភ័យខ្លាចខ្លាំង។ល។
- ត្រូវធានាថា អ្វីដែលយើងធ្វើនឹងបង្កើនការគាំពារ មិនមែនជាការធ្វើឱ្យកុមារកាន់តែរងគ្រោះនោះទេ
- ត្រូវរក្សាការសម្ងាត់ មានតែមនុស្សសំខាន់ទេដែលអាចចូលរួមសម្ភាសន៍បាន ហើយនេះមិនមែនជាការនិយាយដើម ឬពិភាក្សាបែបរសើបនោះទេ សូមចែករំលែកព័ត៌មានដែលចាំបាច់តែប៉ុណ្ណោះ
- ត្រូវសួរកុមារថា តើគេចង់ឱ្យមនុស្សពេញវ័យ ឬមិត្តភក្តិដែលគេទុកចិត្តណាមួយនៅជាមួយគេក្នុងពេលនេះដែរឬទេ ?
- ត្រូវបញ្ជាក់ប្រាប់កុមារឱ្យច្បាស់ថា រឿងរ៉ាវទាំងអស់នេះមិនមែនជាកំហុសរបស់កុមារទេ ហើយកុមារគឺជាជនរងគ្រោះ
- ត្រូវស្មោះត្រង់ និងបង្ហាញឱ្យកុមារដឹងថា អ្នកជឿជាក់លើគេ
- សូមកុំសន្យានូវអ្វី ដែលយើងមិនអាចធ្វើបាន។

ខ. ស្តាប់ដោយយកចិត្តទុកដាក់

- ត្រូវប្រាកដថា យើងបានត្រៀមខ្លួនរួចរាល់ ដើម្បីស្តាប់អ្វីដែលកុមារនិយាយ
- ត្រូវស្តាប់ដោយយកចិត្តទុកដាក់នូវអ្វីដែលកុមារប្រាប់ និងមិនត្រូវបង្ខិតបង្ខំឱ្យពួកគេនិយាយ ឬស្តីបន្ទោសដាក់កំហុសលើកុមារឡើយ

- ត្រូវប្រាកដថា យើងមិនបង្ខាប់ឱ្យកុមារនិយាយ ឬមិនត្រូវធ្វើការបកស្រាយ ឬវិនិច្ឆ័យឡើយ សូមទទួលយកនូវអ្វីដែលកុមារនិយាយ
- ត្រូវអនុញ្ញាតឱ្យកុមារនិយាយ ដោយមិនត្រូវកាត់ ឬបញ្ឈប់ការនិយាយរបស់កុមារឡើយ ហើយមិនត្រូវដាក់សម្ពាធឱ្យពួកគេត្រូវតែនិយាយនោះទេ
- ត្រូវអនុវត្តការស្តាប់សកម្ម ដោយព្យាយាមប្រើពាក្យរបស់គេឱ្យបានច្រើនតាមដែលអាចធ្វើបាន
- ត្រូវស្មោះត្រង់ និងបង្ហាញឱ្យកុមារដឹងថា យើងជឿជាក់លើពួកគេ
- ត្រូវឱ្យកុមារដឹងថា គេពិតជាមានសេចក្តីក្លាហាន និងគួរឱ្យស្ងើចសរសើរ ដែលហ៊ាននិយាយអំពីបទពិសោធរបស់គេ
- បើអាចធ្វើបាន ត្រូវសុំការអនុញ្ញាតកត់ត្រានូវអ្វីដែលកុមារបាននិយាយ។

គ. បង្ហាញឱ្យកុមារដឹងថាយើងនឹងជួយពួកគេ

- ត្រូវធានាបាននូវការឆ្លើយតបទាន់ពេលវេលា មានប្រសិទ្ធភាព រក្សាការសម្ងាត់ និងសមស្រប ដោយធ្វើឡើងក្នុងរយៈពេល ២៤ម៉ោង
- សូមកុំសន្យានូវអ្វី ដែលយើងមិនអាចធ្វើបាន
- ប្រសិនបើអាច សូមឱ្យកុមារចូលរួមក្នុងការសម្រេចចិត្តណាដែលពាក់ព័ន្ធនឹងខ្លួនគេ
- ត្រូវពន្យល់ថា ការងាររបស់យើងផ្នែកខ្លះ គឺត្រូវធ្វើឱ្យប្រាកដថា កុមារពិតជាមានសុវត្ថិភាព និងពិតជាទទួលបានជំនួយដែលគេត្រូវការ ហេតុនេះហើយទើបយើងមិនអាចរក្សារឿងនេះជារឿងសម្ងាត់ទាំងស្រុងបានទេ ព្រោះយើងប្រហែលជាត្រូវការប្រាប់បន្តទៅនរណាម្នាក់ ដែលអាចជួយពួកគេបានប្រសើរជាងយើង
- ត្រូវសុំយោបល់ពីអ្នកដែលមានបទពិសោធន៍ច្រើនជាងយើង ប្រសិនបើអ្នកគិតថា កុមារចង់ប្រាប់យើងពីអ្វីមួយ និងប្រសិនបើយើងមិនប្រាកដអំពីរបៀបដែលត្រូវដោះស្រាយជាមួយនឹងស្ថានភាពបែបនោះទេ។

ឃ. កំណាត់សំណួរដែលត្រូវសួរ

- ជៀសវាងប្រើសំណួរផ្សេងក្រៅពី តើប្អូនអាចប្រាប់ខ្ញុំបន្តិចទៀតបានទេ? (តែម្តងបានហើយ) ឬតើមានអ្វីកើតឡើងបន្ទាប់មក?
- ត្រូវសួរសំណួរដែលសាមញ្ញពាក់ព័ន្ធករណី ឧទាហរណ៍ តើប្អូនចូលចិត្តប្រើកម្មវិធីអ្វីជាងគេ? តើប្អូនប្រើដើម្បីអ្វី? តើប្អូននឹងធ្វើអ្វីនៅពេលឃើញនរណាម្នាក់ត្រូវបានគេរុកកួន? តើប្អូនធ្លាប់ស្គាល់ពួកគេនៅក្រៅប្រព័ន្ធអនឡាញច្បាស់កម្រិតណា?

៦. គន្លឹះសុវត្ថិភាពសម្រាប់កុមារតាមប្រព័ន្ធអនឡាញ

ពិភពឌីជីថលបានផ្តល់ឱ្យកុមារ និងយុវជននូវឱកាស ដែលមិនធ្លាប់មានជាច្រើនពាក់ព័ន្ធនឹងការរៀនសូត្រ ការទំនាក់ទំនង និងការបញ្ចេញគំនិតច្នៃប្រឌិត។ ប៉ុន្តែបរិយាកាសនេះក៏មានហានិភ័យ និងគ្រោះថ្នាក់ ដែលពោរពេញដោយភាពស្មុគស្មាញ និងការវិវត្តឥតឈប់ឈរផងដែរ។ ការបញ្ឈប់ ឬមិនឱ្យកុមារប្រើប្រាស់អ៊ីនធឺណិត មិនមែនជាដំណោះស្រាយទេ។ ប៉ុន្តែការណែនាំពួកគេឱ្យប្រើប្រាស់អ៊ីនធឺណិតដោយភាពឈ្លាសវៃ ទើបជាគន្លឹះសំខាន់។ សុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញផ្តើមចេញពីការណែនាំ ការយល់ដឹង និងការការពារទុកជាមុន។ មានវិធីសាស្ត្រមួយចំនួន ដែលអាចជួយកុមារឱ្យគេចចេញពីហានិភ័យតាមប្រព័ន្ធអនឡាញ តាមរយៈការផ្តល់អំណាចដល់កុមារក្នុងការចូលរួមលើថ្នាលកម្មវិធីដោយសមភាព ដើម្បីសិក្សាស្វែងយល់ និងគិតដោយល្អិតល្អន់ (Critical thinking) ជាមួយនឹងសកម្មភាព និងការអនុវត្តជាក់ស្តែង ដើម្បីបង្កើតភាពធន់នឹងការគំរាមកំហែងតាមប្រព័ន្ធអនឡាញ។

៦.១. គន្លឹះគេចចេញពីជនទុច្ចរិតតាមប្រព័ន្ធអនឡាញ

មានគន្លឹះមួយចំនួន ដែលអាចជួយឱ្យកុមារគេចចេញពីជនទុច្ចរិត ដែលកេងចំណេញផលប្រយោជន៍លើពួកគេ។ កុមារត្រូវដឹងពីទង្វើ ឬសកម្មភាពដែលពួកគេគួរ ឬមិនគួរធ្វើតាមប្រព័ន្ធអនឡាញ។

តើអ្វីដែលកុមារគួរធ្វើ និងមិនគួរធ្វើតាមប្រព័ន្ធអនឡាញ ?

ក. អ្វីដែលគួរធ្វើ៖

- កំណត់ឯកជនភាពទៅជា "Friends only" ឬ "Private" ដូច្នេះការចែករំលែករបស់យើង មិនអាចមើលឃើញជាសាធារណៈទៀតទេ
- គិតមុនពេលចែករំលែកព័ត៌មានផ្ទាល់ខ្លួនរបស់យើង
- ស្រាវជ្រាវ ឬពិនិត្យព័ត៌មានលម្អិតអំពីអ្នកដែលយើងមានទំនាក់ទំនងថ្មីៗ ដោយរុករកពួកគេតាម Google ឬពិនិត្យមើលមិត្តជិតស្និទ្ធរបស់ពួកគេ
- យើងអាចប្រើឈ្មោះហៅក្រៅជំនួសឱ្យឈ្មោះពិត នៅលើគណនីរបស់យើង
- គោរពសិទ្ធិឯកជនភាពរបស់អ្នកដទៃដោយសួរពួកគេ មុនពេលយើងផុស (Post) និងភ្ជាប់ (Tag) ក្នុងប្រូហ្វាល (Profile) ឬចែករំលែកខ្លឹមសារមាតិកា រូបភាព ឬព័ត៌មានទាក់ទងនឹងពួកគេ។

ខ. អ្វីដែលមិនគួរធ្វើ៖

- កុំប្រើឈ្មោះពេញ
- កុំបង្ហាញលេខទូរសព្ទជាសាធារណៈតាមប្រព័ន្ធអនឡាញ
- កុំបង្ហាញអាសយដ្ឋានអ៊ីមែលជាសាធារណៈតាមប្រព័ន្ធអនឡាញ
- កុំដាក់បញ្ចូលថ្ងៃខែឆ្នាំកំណើតពិតក្នុងប្រូហ្វាល (Profile)
- កុំប្រើមុខងារ "check-in" ភ្ជាប់ទីតាំងក្នុងរូបភាពរបស់យើង

- ពិនិត្យមើលថា រូបភាពរបស់យើងមិនមានបង្ហាញទីតាំង ឬព័ត៌មានលម្អិតដែលងាយស្រួលរក (ឧទាហរណ៍ ឈ្មោះសាលារៀននៅលើឯកសណ្ឋានយើង)
- កុំប្រើឈ្មោះ ឬថ្ងៃខែឆ្នាំកំណើត ជាឈ្មោះគណនី (username)
- កុំចែករំលែកអាសយដ្ឋានផ្ទះរបស់យើង
- កុំចែកចាយរូបភាព ឬវីដេអូផ្ទាល់ខ្លួន ដែលមានលក្ខណៈរសើប ជាមួយនរណាម្នាក់ទោះបីយើងស្គាល់ពួកគេក៏ដោយ។

ខាងក្រោមនេះ គឺជាមធ្យោបាយ និងជាដំបូន្មានមានប្រយោជន៍សម្រាប់កុមារ។ ប្រសិនបើពួកគេសង្ស័យលើនរណាម្នាក់ សូមឱ្យពួកគេរាយការណ៍ ឬស្វែងរកជំនួយពីមនុស្សពេញវ័យដែលពួកគេទុកចិត្ត។

ប្រាប់៖ មនុស្សពេញវ័យដែលពួកគេទុកចិត្តក្នុងការសុំជំនួយ ឬដំបូន្មាន។

ប្រមូល៖ រក្សាទុក ថតអេក្រង់សារ និងព័ត៌មានលម្អិតរបស់មនុស្ស ដែលធ្វើឱ្យយើងមិនមានអារម្មណ៍សុវត្ថិភាព។

រាយការណ៍៖ ទៅថ្នាលកម្មវិធី ឬនគរបាលដោយផ្ទាល់ អំពីបញ្ហាទាំងនោះ។

៦.២. ផែនការសុវត្ថិភាពសម្រាប់កុមារ

នៅពេលអ្នកកំពុងអនឡាញ នរណាក៏អាចឃើញព័ត៌មានរបស់អ្នកដែរ។ ដូច្នេះ ពិភពអនឡាញគឺពោរពេញដោយឱកាស និងគ្រោះថ្នាក់ ប្រការសំខាន់បំផុត គឺត្រូវចងចាំអំពីធាតុផ្សំសំខាន់ៗនៃអ៊ីនធឺណិត ដើម្បីជាមូលដ្ឋាននៃការពិចារណាមុននឹងសម្រេចចិត្ត ឬធ្វើសកម្មភាពអ្វីមួយតាមប្រព័ន្ធអនឡាញ។ ការបង្កើតផែនការសុវត្ថិភាព គឺជាសកម្មភាពដែលត្រូវតែមានជានិច្ចសម្រាប់កុមារ នៅពេលដែលពួកគេចាប់ផ្តើមមានវត្តមានតាមប្រព័ន្ធអនឡាញ។ ការធ្វើបែបនេះនឹងជួយដល់កុមារឱ្យដឹងថា តើត្រូវធ្វើអ្វីនៅពេលដែលកុមារមានអារម្មណ៍ថាគ្មានសុវត្ថិភាពតាមប្រព័ន្ធអនឡាញ។ ពួកគេគួរកត់ត្រាទុកលើបាតដៃសុវត្ថិភាព នៅពេលដែលពួកគេមានអារម្មណ៍ថា គ្មានសុវត្ថិភាពតាមប្រព័ន្ធអនឡាញ ដោយសួរថា តើកុមារនឹងប្រាប់អ្នកណាខ្លះ? តើត្រូវទៅកន្លែងណា? តើត្រូវទូរសព្ទទៅនរណា?

បាតដៃសុវត្ថិភាព គឺជាផែនទីសម្រាប់ការស្វែងរកជំនួយរបស់កុមារ នៅពេលដែលពួកគេជួបបញ្ហាតាមប្រព័ន្ធអនឡាញ។ កុមារត្រូវកត់ត្រា និងរក្សាទុកបាតដៃសុវត្ថិភាពតាមខ្លួន សម្រាប់ជួយការពារដល់ពួកគេនៅពេលមានបញ្ហាតាមប្រព័ន្ធអនឡាញជាយថាហេតុណាមួយ។

៦.៣. កេរ្តិ៍ឈ្មោះតាមប្រព័ន្ធអនឡាញ

អ៊ីនធឺណិតមានលក្ខណៈជាសាធារណៈ និងអចិន្ត្រៃយ៍គឺមានន័យថា រាល់អ្វីៗដែលយើងផុស ចែករំលែកចូលចិត្ត នរណាក៏អាចមើលឃើញបានដែរ។ ទោះបីយើងផុសជាអនាមិកក៏ដោយ ក៏នៅតែគេអាចរកឃើញថាយើងជាអ្នកផុសដែរ។ ចូរចាំថា អ្វីៗដែលយើងបញ្ចេញមតិ និងផុសតាមប្រព័ន្ធអនឡាញអាចប៉ះពាល់ដល់កេរ្តិ៍ឈ្មោះរបស់យើង។ រឿងសំខាន់បំផុត មុននឹងយើងផុស បញ្ចេញមតិ ឬចែករំលែកអ្វីមួយត្រូវគិតអំពីអ្នកដទៃ។

ដើម្បីការពារកេរ្តិ៍ឈ្មោះរបស់អ្នក យើងត្រូវប្រព្រឹត្តល្អតាមប្រព័ន្ធអនឡាញ។ យើងត្រូវគោរពចំពោះខ្លួនយើង និងមនុស្សគ្រប់គ្នាតាមប្រព័ន្ធអនឡាញ។ ខាងក្រោមនេះ គឺជាទង្វើប្រកបដោយការទទួលខុសត្រូវ និងការគោរពគ្នាតាមប្រព័ន្ធអនឡាញចំនួន ៥ ចំណុចៈ

- ត្រូវគិតពីផលប៉ះពាល់មុននឹងធ្វើអ្វីមួយ
- ត្រូវសួរខ្លួនឯង ថាតើការផុសរបស់យើងធ្វើឱ្យប៉ះពាល់ដល់អ្នកដទៃ ឬធ្វើឱ្យនរណាម្នាក់ឈឺចាប់ដែរឬទេ?
- ត្រូវប្រព្រឹត្តចំពោះមនុស្សគ្រប់គ្នាតាមប្រព័ន្ធអនឡាញឱ្យដូចអ្វី ដែលអ្នកចង់ឱ្យពួកគេធ្វើត្រឡប់មកវិញ
- ប្រើសញ្ញាអារម្មណ៍ ឬអេម៉ូជី ដើម្បីជួយឱ្យគេយល់
- ត្រូវឆ្លុះបញ្ចាំង ថាតើយើងប្រព្រឹត្តដូចនៅអហ្វឡាញដែរឬទេ?

មុននឹងយើងចែករំលែកមាតិកាអ្វីមួយយើងត្រូវគិតថា តើវាចាំបាច់ដាច់ខាតត្រូវតែចែករំលែកដែរឬទេ? តើមានវិធីសមរម្យផ្សេងទៀតក្នុងការចែករំលែកដែរឬទេ? តើត្រូវបន្ថែមសារជាស់តឿន មុនពេលចុចមើលដែរឬទេ? ហេតុអ្វីយើងត្រូវចែករំលែក? ប៉ុន្តែបើមាតិកាជាកង្វល់របស់សហគមន៍ ដូចជាការរំលោភសិទ្ធិមនុស្សជាដើម យើងគួរតែចែករំលែក។

ប្រសិនបើមាននរណាម្នាក់មានអាកប្បកិរិយាឈ្លើយចំពោះយើងតាមប្រព័ន្ធអនឡាញ យើងត្រូវប្រកាន់គោលជំហរប្រើប្រាស់ភាសាសមរម្យ។ រាំងខ្ទប់ ឬស្នើរាំងខ្ទប់ចំពោះអ្នកដែលឈ្លើយនោះ ហើយរាយការណ៍ពីបុគ្គលនោះ និងលុបមតិយោបល់របស់គេចេញ។ យើងមិនគួរចែករំលែកនូវព័ត៌មានរអេចរអូច ឬការខ្សឹបខ្សៀវនិយាយដើមគ្នាតាមប្រព័ន្ធអនឡាញ ដែលនាំឱ្យនរណារម្នាក់មានការឈឺចាប់នោះទេ។ ត្រូវប្រាប់អ្នកដែលផុសព័ត៌មានរអេចរអូច ឬការខ្សឹបខ្សៀវនិយាយដើមគ្នាតាមប្រព័ន្ធអនឡាញ ឱ្យចេះគោរពគ្នាតាមប្រព័ន្ធអនឡាញផងដែរ។ ត្រូវផ្តល់ការគាំទ្រចំពោះអ្នករងគ្រោះ។

មុននឹងផុសមាតិកាដែលមានភាពស្រើបស្រាលតាមប្រព័ន្ធអនឡាញ យើងត្រូវគិត និងសួរខ្លួនឯងថា តើវាជាការផ្សព្វផ្សាយនូវឥរិយាបទមិនល្អដែរឬទេ? តើវាជះឥទ្ធិពលដល់ជីវិតរស់នៅរបស់យើងដែរឬទេ? តើជះឥទ្ធិពលមិនល្អដល់អ្នកដទៃដែរឬទេ? តើយើងគួរធ្វើបែបណាចំពោះមាតិកាមានភាពស្រើបស្រាលតាមប្រព័ន្ធអនឡាញ?

៦.៤. ការទទួលខុសត្រូវតាមប្រព័ន្ធអនឡាញ

ពលរដ្ឋឌីជីថលដែលមានការទទួលខុសត្រូវ គឺត្រូវចូលរួមក្នុងសហគមន៍អនឡាញប្រកបដោយសីលធម៌ និងការគោរព ទោះបីកំពុងប្រើប្រាស់ថ្នាលកម្មវិធីដែលមានគណនីអនាមិកក៏ដោយ។ មានចំណុចមួយចំនួនដែលយើងត្រូវចងចាំ នៅពេលប្រើប្រាស់អ៊ីនធឺណិត ឬអនឡាញ ដែលក្នុងនោះរួមមានៈ

- ត្រូវប្រព្រឹត្តដោយគោរពច្បាប់មិនត្រូវលួចបន្លំ ឬធ្វើឱ្យខូចខាតដល់នរណាម្នាក់នោះទេ
- ការពារឯកជនភាពរបស់យើង និងអ្នកដទៃ
- គោរពសិទ្ធិរបស់អ្នកដទៃ និងត្រូវមានការទទួលខុសត្រូវតាមប្រព័ន្ធអនឡាញ

- ត្រូវគិតពីផលប៉ះពាល់នៃសកម្មភាពតាមប្រព័ន្ធអនឡាញមកលើខ្លួនយើង និងអ្នកដទៃ។

យើងមិនគួរផុសនូវសកម្មភាពខុសច្បាប់តាមប្រព័ន្ធអនឡាញទេ។ ការប្រព្រឹត្តខុសច្បាប់ ទោះបីមើលទៅដូចជាមិនអី តែវានាំឱ្យយើងមានបញ្ហា។ ការពិនិត្យឡើងវិញលើការចែករំលែកគឺជាវិធីដ៏ល្អមួយ តែត្រូវប្រាកដថា អ្វីដែលយើងផុសគឺជាការពិត និងគួរឱ្យគោរព។ យើងត្រូវគិតឱ្យបានទ្វេដង មុននឹងចែករំលែករូបភាពអាក្រាតស្រើបស្រាលរបស់ខ្លួនយើង ឬនរណាម្នាក់។ យើងត្រូវដឹងថា រូបដែលយើងផុសអាចទៅដល់ទីណា ឬត្រូវបាននរណាយកទៅប្រើប្រាស់ធ្វើអ្វីនោះទេ។ សូមប្រុងប្រយ័ត្ន ចំពោះការចែករំលែកព័ត៌មានមិនពិត ឬព័ត៌មានមិនសមរម្យ។

ទង្វើខាងលើនេះ អាចធ្វើឱ្យមនុស្សគ្រប់គ្នាមានការភ័ន្តច្រឡំចំពោះយើង ឬអាចធ្វើឱ្យប៉ះពាល់ដល់កេរ្តិ៍ឈ្មោះរបស់យើង។ ការផុសបែបនេះអាចធ្វើឱ្យខាតបង់ មិនត្រឹមតែបុគ្គលដែលយើងផុសពីគេនោះទេ ប៉ុន្តែខ្លួនរបស់យើង និងអ្នកចែករំលែកបន្ត ក៏រងការប៉ះពាល់ផងដែរ។

៦.៥. ព័ត៌មានតាមប្រព័ន្ធអនឡាញ

ទន្ទឹមនឹងការគិតពីអ្វីៗដែលយើងផុសតាមប្រព័ន្ធអនឡាញ យើងក៏ត្រូវគិតផងដែរចំពោះអ្វីៗ ដែលយើងឃើញតាមអ៊ីនធឺណិត ថាតើវាមានប្រភពមកពីណា? មុននឹងទាញយកព័ត៌មានណាមួយមកប្រើប្រាស់ ឬចែករំលែក យើងត្រូវពិនិត្យពីភាពជាក់លាក់ និងទុកចិត្តបានជាមុនសិន។ បើមិនអញ្ចឹងទេ យើងនឹងក្លាយជាចំណែកមួយនៃបញ្ហា ដោយសារការចែករំលែកព័ត៌មានមិនពិត។

មិនមែនអ្វីៗនៅលើអ៊ីនធឺណិតសុទ្ធតែមានសុវត្ថិភាព និងគួរឱ្យទុកចិត្តនោះទេ។ បើយើងមិនចង់ឱ្យមានផលប៉ះពាល់ដល់កេរ្តិ៍ឈ្មោះរបស់យើង ឬធ្វើឱ្យនរណាម្នាក់មានការភ័ន្តច្រឡំ យើងត្រូវប្រុងប្រយ័ត្នមុនចែករំលែក។ នៅពេលយើងស្វែងរកព័ត៌មានតាមអ៊ីនធឺណិត ឬអនឡាញ យើងត្រូវគិតពិចារណាថា តើព័ត៌មាននោះមានប្រភពមកពីណា?

មានគន្លឹះមួយចំនួន ដែលអាចជួយអ្នកក្នុងការពិនិត្យលើភាពជឿជាក់នៃព័ត៌មាន៖

- ផ្ទៀងផ្ទាត់ប្រភពព័ត៌មាន (ពិនិត្យលើគេហទំព័រ)
- ស្វែងរកព័ត៌មានអ្នកនិពន្ធ និងកម្មសិទ្ធិបញ្ញា
- ពិនិត្យរកភស្តុតាង និងអំណះអំណាង
- សុំមតិយោបល់ពីមនុស្សដែលអ្នកទុកចិត្ត។

៦.៦. ការចែករំលែកព័ត៌មានតាមប្រព័ន្ធអនឡាញ

ថ្នាលកម្មវិធីបណ្តាញសង្គម គឺជាមធ្យោបាយដ៏អស្ចារ្យមួយ ដើម្បីទំនាក់ទំនងជាមួយមិត្តភក្តិ និងក្រុមគ្រួសារ។ ប៉ុន្តែការចែករំលែកអំពីរឿងរ៉ាវផ្ទាល់ខ្លួនតាមប្រព័ន្ធអនឡាញច្រើនពេក អាចមានហានិភ័យផងដែរ។ វាអាចធ្វើឱ្យខូចកេរ្តិ៍ឈ្មោះរបស់យើង ឬអ្នកដែលយើងមិនស្គាល់ទាក់ទងមកយើង។ ត្រូវចាំថា អ៊ីនធឺណិតគឺអនាមិក ដូច្នេះយើងមិនគួរជឿជាក់ចំពោះបុគ្គលដែលយើងស្គាល់តាមប្រព័ន្ធអនឡាញទាំងស្រុងនោះទេ។

រឿងសំខាន់បំផុត គឺយើងត្រូវដឹងថា យើងមិនអាចគ្រប់គ្រងរូបថត វីដេអូ ឬសារដែលយើងបង្ហោះតាមប្រព័ន្ធអនឡាញបានទេ ព្រោះអ្វីៗដែលយើងបង្ហោះតាមប្រព័ន្ធអនឡាញអាចត្រូវបានអ្នកដទៃយកទៅប្រើប្រាស់តាមចិត្តរបស់គេ។ ដើម្បីប្រាកដថា យើងមិនចែករំលែកព័ត៌មានតាមប្រព័ន្ធអនឡាញច្រើនពេក មានគន្លឹះមួយចំនួនដែលអាចជួយដល់យើង ដូចខាងក្រោម៖

- ត្រូវគិតមុនពេលផុស ឬចែករំលែកព័ត៌មានផ្ទាល់ខ្លួន
- ត្រូវពិនិត្យមើលការកំណត់ឯកជនភាពនៅលើទូរសព្ទដៃ កម្មវិធី និងគេហទំព័រ
- មិនភ្ជាប់ ឬដកខ្លួនចេញពីការផុសដែលមានលក្ខណៈឈ្លើយ ឬគួរឱ្យអៀនខ្មាស់
- ប្រើ Google ដើម្បីរុករកព័ត៌មានផ្ទាល់ខ្លួនរបស់យើង
- ត្រូវសួរថា តើយើងបានដកចេញនូវអ្វីដែលមានលក្ខណៈផ្ទាល់ខ្លួន ឬគួរឱ្យអាម៉ាស់ហើយឬនៅ?
- មិនត្រូវចែករំលែកឈ្មោះពេញ អាសយដ្ឋាន លេខទូរសព្ទ ថ្ងៃខែឆ្នាំកំណើត និងពាក្យសម្ងាត់។

ការចែករំលែកព័ត៌មានផ្ទាល់ខ្លួនតាមប្រព័ន្ធអនឡាញ ដោយប្រុងប្រយ័ត្ននឹងធ្វើឱ្យអ្នកដទៃពិបាកទាក់ទង ឬធ្វើបាបយើងបាន។ វាក៏ជាការជួយការពារខ្លួនយើងពីអ្នកបោកប្រាស់ (Scammer) និងអ្នកលួចចូលគណនី (Hacker) ផងដែរ។ យើងអាចកម្រិតការមើលឃើញព័ត៌មានរបស់យើង ឬស្គាល់យើងថាជានរណាតាមប្រព័ន្ធអនឡាញ ដោយការកំណត់ឯកជនភាព និងទីតាំង ដែលក្នុងនោះរួមមាន៖

- ការកំណត់ទីតាំងឧបករណ៍
- ការកំណត់ទីតាំងនៅក្នុងបណ្តាញសង្គម
- ការកំណត់ឯកជនភាពនៅក្នុងបណ្តាញសង្គម
- ការកំណត់សារជាឯកជនភាព។

ការការពារឯកជនភាពរបស់យើងតាមប្រព័ន្ធអនឡាញនឹងជួយឱ្យយើងមានសុវត្ថិភាព នៅពេលរុករកអ្វីៗនៅលើអ៊ីនធឺណិត។ យើងក៏ត្រូវចងចាំដែរថា ការភ្ជាប់ទំនាក់ទំនងជាមួយមិត្តភក្តិថ្មីៗគឺជារឿងល្អ ប៉ុន្តែត្រូវយល់ថា បើយើងមិនប្រយ័ត្នប្រយែងចំពោះអ្វីដែលយើងចែករំលែកតាមប្រព័ន្ធអនឡាញទេ វាក៏អាចនាំទៅរកទំនាក់ទំនងបែបអវិជ្ជមានផងដែរ។

៦.៧. ការរុកគួនតាមប្រព័ន្ធអនឡាញ

ការរុកគួនតាមប្រព័ន្ធអនឡាញខុសពីការរុកគួនផ្សេងៗ ព្រោះអ្នកដែលបានឃើញតាមប្រព័ន្ធអនឡាញអាចនឹងចូលរួមរុកគួនផងដែរ។ ដោយសារតែការចែករំលែកអ្វីៗតាមប្រព័ន្ធអនឡាញមានលក្ខណៈសាធារណៈ និងអចិន្ត្រៃយ៍ ការរុកគួនតាមប្រព័ន្ធអនឡាញមានបន្សល់ទុកនូវក្នុងកំណត់ត្រាឌីជីថល ដែលយើងអាចរកឃើញ និងអាចប្រើជាភស្តុតាងដើម្បីបញ្ឈប់ការរំលោភបំពាននានាបាន។ យើងគិតថា ការរុកគួនតាមប្រព័ន្ធអនឡាញជារឿងរ៉ាវធម្មតា ប៉ុន្តែវាជាបញ្ហា។ វិធីល្អដើម្បីបញ្ឈប់ការរុកគួនតាមប្រព័ន្ធអនឡាញ គឺការប្រព្រឹត្តដោយគោរព និងមានសុជីវធម៌តាមប្រព័ន្ធអនឡាញ ដែលយើងត្រូវលើកទឹកចិត្តធ្វើឱ្យបានគ្រប់គ្នា។ ខាងក្រោមនេះ គឺជាគន្លឹះមួយចំនួន ដើម្បីឆ្លើយតបនឹងការរុកគួនតាមប្រព័ន្ធអនឡាញ៖

- មិនអើពើ និងមានប្រតិកម្មចំពោះការរុកគួន

- កុំជឿរឿងអាក្រក់ដែលនិយាយរុកកួនតាមប្រព័ន្ធអនឡាញ
- រាំងខ្ទប់ការរុកកួនដើម្បីបញ្ឈប់ការរំខានរបស់ពួកគេ
- ការពារអ្នកដែលជួបការរុកកួនដោយស្តាប់ និងគាំទ្រ
- ប្រមូលវត្ថុតាង ដើម្បីបង្ហាញពីអ្វីដែលកើតឡើង
- ប្រាប់មនុស្សពេញវ័យដែលយើងទុកចិត្តឱ្យបានលឿនតាមតែអាចធ្វើទៅបាន។

ការឆ្លើយតប និងដំណោះស្រាយចំពោះការរុកកួនតាមប្រព័ន្ធអនឡាញ យើងអាចធ្វើបានភ្លាមៗតាមរយៈការលុបមាតិកា ឬគណនីចេញពីថ្នាលកម្មវិធី។ កុមារក៏ចង់ដឹងពីដំណោះស្រាយ និងអន្តរាគមន៍ល្អៗពីមនុស្សពេញវ័យផងដែរ។

៦.៨. ការលួងលោមតាមប្រព័ន្ធអនឡាញ

ការលួងលោមតាមប្រព័ន្ធអនឡាញ កើតឡើងនៅពេលដែលនរណាម្នាក់ព្យាយាមចងមិត្តជាមួយកុមារតាមប្រព័ន្ធអនឡាញ ហើយកសាងភាពជឿទុកចិត្ត ក្នុងគោលបំណងដើម្បីធ្វើបាបពួកគេ។ កុមារតែងត្រូវបានលួងលោម មុនពេលពួកគេត្រូវបានរំលោភបំពាន ឬកេងប្រវ័ញ្ចផ្លូវភេទ។ ដំបូងកុមារអាចត្រូវបានបោកបញ្ឆោតឱ្យគិតថា ទំនាក់ទំនងនោះធម្មតា និងមានសុវត្ថិភាព។ ពួកគេមិនដឹងថា មានរឿងមិនល្អកើតឡើងនោះទេ ហើយមានអារម្មណ៍ថា គ្មានជម្រើសនិងត្រូវតែរងការរំលោភបំពាន។ អ្នកដែលលួងលោមមានជំនាញខ្ពស់ ពួកគេកេងចំណេញលើកុមារដោយផ្តល់ការគាំទ្រ ការយល់ចិត្ត និងស្វែងយល់ពីតម្រូវការផ្សេងៗ។ កុមារងាយនឹងចាញ់កលល្បិច ឬការបញ្ឆោររបស់អ្នកលួងលោមណាស់។

មានគន្លឹះមួយចំនួន ដែលកុមារអាចការពារខ្លួនពីការលួងលោមតាមប្រព័ន្ធអនឡាញ៖

- កុំទុកចិត្តលើរឿងល្អៗដែលមនុស្សយើងមិនធ្លាប់ស្គាល់បានប្រាប់យើង
- រាំងខ្ទប់មនុស្ស ដែលយើងមិនដែលស្គាល់ បើពួកគេសួរពីព័ត៌មានផ្ទាល់ខ្លួនរបស់យើង
- ប្រមូលភស្តុតាង និងបង្ហាញទៅកាន់មនុស្សពេញវ័យ
- ប្រាប់នរណាម្នាក់ ដែលយើងទុកចិត្តឱ្យបានលឿនតាមដែលអាចធ្វើទៅបាន។

យើងត្រូវដឹង និងយល់ពីសញ្ញាគ្រោះថ្នាក់ ដែលអាចបង្ហាញថា មាននរណាម្នាក់ដែលយើងស្គាល់តាមប្រព័ន្ធអនឡាញព្យាយាមធ្វើបាបយើង។ ការលួងលោមតាមប្រព័ន្ធអនឡាញគឺពិតជាគួរឱ្យខ្លាច តែយើងមានមធ្យោបាយដែលអាចការពារខ្លួនរបស់យើងឱ្យមានសុវត្ថិភាពបាន។ បុគ្គលដែលព្យាយាមទាក់ទងកុមារតាមថ្នាលកម្មវិធីច្រើនលើកច្រើនសារ ហើយជាបុគ្គលដែលកុមារមិនស្គាល់អាចជាសញ្ញាគ្រោះថ្នាក់។

បើចង់ប្តូរថ្នាលកម្មវិធី លុះត្រាតែអ្នកស្គាល់មនុស្សម្នាក់នោះច្បាស់ ប៉ុន្តែល្អបំផុតគឺការទាក់ទងនៅលើថ្នាលកម្មវិធីសាធារណៈ។ ការបើកចំហរ និងស្មោះត្រង់តាមប្រព័ន្ធអនឡាញមានសារៈសំខាន់ណាស់សម្រាប់អ្នក។ ត្រូវពិចារណាឱ្យបានហ្មត់ចត់ ចំពោះអ្នកដែលសុំឱ្យកុមាររក្សាការសម្ងាត់ពីអ្នកដទៃ។ ការចែករំលែកព័ត៌មានផ្ទាល់ខ្លួនតាមប្រព័ន្ធអនឡាញអាចគ្រោះថ្នាក់ ត្រូវចាំថា អាចមានគេយកព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នកទៅប្រើប្រាស់ដើម្បីធ្វើបាបអ្នក។ បើនរណាម្នាក់សុំអ្នកនូវព័ត៌មានប្រភេទខាងលើនេះ អ្នកគួរតែចាកចេញពីកិច្ចសន្ទនា រាំងខ្ទប់ពួកគេ ហើយប្រាប់ទៅមនុស្សដែលអ្នកទុកចិត្តឱ្យបានឆាប់តាមដែលអាចធ្វើទៅបាន។ ប្រសិនបើនរណាម្នាក់ ដែលអ្នក

ស្គាល់តាមប្រព័ន្ធអនឡាញសុំរូបអាក្រាត នេះគឺជាសញ្ញាយ៉ាងច្បាស់នៃការលួងលោម។ ត្រូវរាយការណ៍ និងរាំងខ្ទប់ពួកគេភ្លាម។

៦.៩. តើខ្ញុំនិយាយជាមួយនរណាតាមប្រព័ន្ធអនឡាញ?

ដោយសារអ៊ីនធឺណិតមានលក្ខណៈជាអនាមិក វាអាចជាមធ្យោបាយសម្រាប់ជនទុច្ចរិតបន្លំខ្លួនធ្វើជានរណាផ្សេងទៀតតាមប្រព័ន្ធអនឡាញផងដែរ។ យើងត្រូវប្រុងប្រយ័ត្ន នៅពេលមាននរណាម្នាក់ដែលយើងមិនស្គាល់ ទទួលយើងជាមិត្ត ឬជជែកជាមួយយើងតាមប្រព័ន្ធអនឡាញ។ មុននឹងជឿលើមិត្តថ្មីណាម្នាក់ អ្នកត្រូវស្វែងយល់ពីគេឱ្យបានច្រើនតាមដែលអាចធ្វើបាន។ បើយើងមិនទុកចិត្តពីទំនាក់ទំនងតាមប្រព័ន្ធអនឡាញ យើងត្រូវមានការប្រុងប្រយ័ត្ន។ សំខាន់បំផុតត្រូវគិតពិចារណា និងមិនត្រូវជឿជាក់ភ្លាមៗនោះទេ។ នេះជារឿងមិនល្អ បើមាននរណាម្នាក់ធ្វើឱ្យអ្នកភ័យខ្លាច ឈឺចាប់ ឬមានអារម្មណ៍មិនមានសុវត្ថិភាព ទាំងក្នុងជីវិតពិត និងតាមប្រព័ន្ធអនឡាញ។ ប្រសិនបើវាកើតមានត្រូវប្រាប់ទៅមនុស្សដែលអ្នកទុកចិត្តឱ្យបានឆាប់តាមដែលអាចធ្វើបាន។

មានវិធីមួយចំនួនដែលអាចជួយឱ្យយើងមានសុវត្ថិភាព នៅពេលនិយាយជាមួយនរណាម្នាក់តាមប្រព័ន្ធអនឡាញ។ ជាក់ស្តែងយើងអាចប្រើអ៊ីនធឺណិត ដើម្បីការពារខ្លួនយើងតាមរយៈការកំណត់ឯកជនភាព និងសកម្មភាព មួយចំនួនដូចខាងក្រោម៖

- ចាកចេញពីក្រុមសន្ទនានៅលើបណ្តាញសង្គម
- ចាកចេញពីក្រុមសន្ទនានៅលើកម្មវិធីសារសន្ទនា
- រាំងខ្ទប់នរណាម្នាក់នៅលើបណ្តាញសង្គម
- រាំងខ្ទប់នរណាម្នាក់នៅលើកម្មវិធីសារសន្ទនា
- បដិសេធនរណាម្នាក់នៅលើបណ្តាញសង្គម
- រាយការណ៍នរណាម្នាក់នៅលើបណ្តាញសង្គម។

៦.១០. អ្នកបោកប្រាស់ និងអ្នកលួចគណនីតាមប្រព័ន្ធអនឡាញ

យើងត្រូវប្រុងប្រយ័ត្នចំពោះអ្នកដែលយើងជឿជាក់តាមអ៊ីនធឺណិត ព្រោះមានជនមួយចំនួន ដូចជា៖ អ្នកបោកប្រាស់ (Scammer) និងអ្នកលួចចូលគណនី (Hacker) អាចព្យាយាមធ្វើបាបយើង និងអ្នកដទៃ។ អ្នកបោកប្រាស់ ជាជនដែលព្យាយាមបោកបញ្ឆោតអ្នកឱ្យផ្តល់សិទ្ធិដល់គេ ដើម្បីចូលគណនីរបស់យើង។ ជនបោកប្រាស់មានជំនាញ និងតែងតែប្រព្រឹត្តនូវទង្វើ ដូចជា៖

- អះអាងថាមកពីក្រុមហ៊ុនល្បីៗ
- ធ្វើពុតដូចជានរណាម្នាក់ដែលអ្នកស្គាល់
- បង្កើតរឿងបែបបន្ទាន់ៗ ដែលធ្វើឱ្យការសម្រេចចិត្តរបស់យើងមិនបានគិតដិតដល់
- ណែនាំឱ្យផ្ទៀងផ្ទាត់ព័ត៌មានផ្ទាល់ខ្លួនតាមវិធីរបស់ពួកគេ ដូចជា៖ ចូលទៅកាន់គេហទំព័ររបស់ពួកគេ ឬទូរសព្ទទៅលេខដែលពួកគេផ្តល់ឱ្យ។

អ្នកលួចចូលគណនី ជាមនុស្សដែលអាចបង្កើត និងកែប្រែសូហ្វវែរ (Software) ដើម្បីអាចចូលទៅប្រើព័ត៌មាន និងពាក្យសម្ងាត់របស់យើងដោយគ្មាននរណាដឹង។ នៅពេលអ្នកលួចចូលគណនីចូលប្រើគណនីរបស់

យើងពួកគេអាចផ្ញើសារក្លែងក្លាយ មេរោគកុំព្យូទ័រ សម្ភារៈបំពានច្បាប់ ឬសារដែលមានខ្លឹមសារមិនល្អទៅកាន់មនុស្សដែលយើងស្គាល់។

ដើម្បីការពារខ្លួនពីអ្នកបោកប្រាស់ (Scammer) និងអ្នកលួចចូលគណនី (Hacker) យើងត្រូវចេះគិតពិចារណាចំពោះមនុស្ស និងគេហទំព័រដែលគួរទុកចិត្តនៅតាមប្រព័ន្ធអនឡាញ។ យើងត្រូវគិតឱ្យបានច្បាស់លាស់មុនធ្វើអ្វីមួយ ដើម្បីជាការការពារខ្លួនរបស់យើងពីការបោកបញ្ឆោត និងលួចគណនី។

មានគន្លឹះជាច្រើន ដែលយើងអាចធ្វើ ដើម្បីការពារកុំឱ្យគេចូលប្រើគណនីរបស់យើង ដូចខាងក្រោម៖

- កំណត់ឯកជនភាពកម្រិតខ្ពស់ ហើយត្រូវពិនិត្យលើការកំណត់ឱ្យបានទៀងទាត់
- ចាកចេញពីគណនីបណ្ដាញសង្គម និងការផ្ញើសារ
- កុំចែករំលែកពាក្យសម្ងាត់ ឬព័ត៌មានផ្ទាល់ខ្លួនដូចជាឈ្មោះពេញ ថ្ងៃខែឆ្នាំកំណើត លេខទូរសព្ទ ឬអាសយដ្ឋាន
- បង្កើតពាក្យសម្ងាត់ដែលពិបាកទាយ និងធ្វើការផ្លាស់ប្ដូរជាទៀងទាត់
- កំណត់ការធ្វើបច្ចុប្បន្នភាពសូហ្វវែរ(Software)ទូរសព្ទ និងកុំព្យូទ័រដោយស្វ័យប្រវត្តិ
- ធ្វើការផ្ទៀងផ្ទាត់ដោយហ្មត់ចត់ (Authentication) នៅលើថ្នាលកម្មវិធី ដែលអនុញ្ញាត។

បើយើងបារម្ភថា យើងជាគោលដៅនៃការបោកបញ្ឆោត ឬលួចគណនី យើងត្រូវប្រាប់ទៅមនុស្សដែលយើងទុកចិត្តឱ្យបានលឿនតាមដែលអាចធ្វើទៅបាន យើងគួរតែ៖

- ចាកចេញពីគ្រប់កម្មវិធី និងគេហទំព័រទាំងអស់ជាបន្ទាន់
- ផ្លាស់ប្ដូរពាក្យសម្ងាត់របស់យើងទាំងអស់
- រាយការណ៍បញ្ហាទៅកាន់គេហទំព័រ ឬថ្នាលកម្មវិធី ធនាគារ ឬនគរបាល
- ប្រាប់មនុស្សពេញវ័យ និងសុំជំនួយ។

ត្រូវប្រុងប្រយ័ត្នចំពោះអ៊ីមែល ដែលយើងមិនស្គាល់ ហើយស្នើសុំឱ្យយើងចូលតាមតំណភ្ជាប់របស់គេ។ បើយើងទទួលបានអ៊ីមែលបែបនេះ យើងត្រូវ៖

- រាំងខ្ទប់អ្នកផ្ញើ
- លុបអ៊ីមែល
- ហាមមិត្តភក្តិ និងគ្រួសារ។

បើយើងត្រូវបានគេបោកប្រាស់តាមប្រព័ន្ធអនឡាញ យើងគួរតែ៖

- ចាកចេញពីកម្មវិធី ដើម្បីការពារព័ត៌មានផ្ទាល់ខ្លួនរបស់យើង
- ផ្លាស់ប្ដូរពាក្យសម្ងាត់ ដើម្បីកុំឱ្យគេអាចចូលបាន រាំងខ្ទប់អ្នកផ្ញើ ដើម្បីការពារការផ្ញើអ៊ីមែលនាពេលខាងមុខ។

៦.១០. មាតិកាមានលក្ខណៈប្រមាថ និងបង្កគ្រោះថ្នាក់

អ៊ីនធឺណិតគឺជាសាធារណៈ ដែលមនុស្សគ្រប់គ្នាអាចផុស ឬផ្ទុកលើវាបាន។ ហេតុនេះហើយទើបមានរឿងគួរឱ្យខ្លាច ហិង្សា ឬឃោឃៅតាមប្រព័ន្ធអនឡាញ ដែលមិនមានសុវត្ថិភាពសម្រាប់កុមារមើល។ ប្រសិនបើយើងបានឃើញអ្វីមួយ ដែលឃោឃៅ ហិង្សា ឬគួរឱ្យខ្លាចនៅលើអ៊ីនធឺណិត យើងត្រូវជឿជាក់លើសតិសម្បជញ្ញៈរបស់យើង ថាយើងអាចដោះស្រាយបាន។

មាតិកាមានលក្ខណៈប្រមាថតាមប្រព័ន្ធអនឡាញ មានដូចជា៖

- រូបភាពអវិជ្ជមាន ឬរូបភាពមិនពិតនៃពិភពលោក
- ធ្វើឱ្យយើងគិតថា ភាសាអសុរោះ អំពើហិង្សា ឬសកម្មភាពខុសច្បាប់ មិនមែនជាបញ្ហា
- ធ្វើឱ្យយើងមានបញ្ហា ដោយការមើលមាតិកាខុសច្បាប់។

មានវិធីជាច្រើនដែលយើងអាចធ្វើបាន ដើម្បីដោះស្រាយនៅពេលយើងឃើញអ្វីមួយដែលធ្វើឱ្យយើងមានអារម្មណ៍មិនល្អ។ បើយើងបានឃើញអ្វីដែលឃោឃៅ ហិង្សា ឬគួរឱ្យខ្លាចនៅលើអ៊ីនធឺណិត ជំហានដំបូងយើងត្រូវប្រាប់រឿងហ្នឹងដល់មនុស្សដែលយើងទុកចិត្ត។ នៅលើអ៊ីនធឺណិតក៏មានឧបករណ៍ ដែលត្រូវបានបង្កើតឡើង ដើម្បីជួយបញ្ឈប់មាតិកា ដែលបង្កគ្រោះថ្នាក់ និងប្រមាថផងដែរ។ យើងអាចច្រោះមាតិកា ដែលមានលក្ខណៈមិនសមរម្យ ឬសើប ដោយការដំឡើងកម្មវិធីរុករកដោយសុវត្ថិភាព។ គេហទំព័រ និងកម្មវិធីភាគច្រើនតែងតែមានវិធីរាយការណ៍ចំពោះមាតិកាមិនសមរម្យ ហិង្សា និងគួរឱ្យខ្លាច។

៦.១១. ការចំណាយពេលច្រើនពេកតាមប្រព័ន្ធអនឡាញ

អ៊ីនធឺណិតជាទីកន្លែងដ៏អស្ចារ្យ ដោយយើងអាចប្រើដើម្បីលេងហ្គេម ឆាតសន្ទនាជាមួយមិត្តភក្តិ មើលបណ្តាញសង្គម ទិញនិងលក់របស់របរ ឬតាមដានព័ត៌មាន។ ប៉ុន្តែមិនគួរឱ្យសកម្មភាពទាំងនេះ គ្របដណ្តប់លើជីវិតយើងពេកទេ។ ការចំណាយពេលច្រើនពេកតាមប្រព័ន្ធអនឡាញអាចទាញយើងចេញពីអ្វីដែលយើងចង់ធ្វើនៅក្នុងជីវិតពិត ដូចជា ការជួបជុំមិត្តភក្តិ និងគ្រួសារ ការងារ កិច្ចការផ្ទះ ឬការហាត់ប្រាណ។ វាអាចជះឥទ្ធិពលអាក្រក់ដល់សុខភាពរាងកាយ និងផ្លូវចិត្តរបស់យើង។

ការយល់ដឹងអំពីសញ្ញាណនៃការចំណាយពេលច្រើនតាមប្រព័ន្ធអនឡាញ គឺជារឿងសំខាន់ ដែលបង្ហាញពីការចំណាយពេលច្រើនតាមប្រព័ន្ធអនឡាញ ដូចជា៖

- មានភាពតានតឹងខ្លាំងក្នុងអារម្មណ៍
- តែងតែប៉ះ ឬមើលទូរសព្ទជានិច្ច
- មានអារម្មណ៍តប់ប្រមល់ នៅពេលមិនបានស្វែងរក ឬមើលអ្វីមួយក្នុងទូរសព្ទ
- ឈឺក្បាល និងមើលអ្វីៗមិនសូវច្បាស់
- អស់កម្លាំង និងពិបាកដេក
- កម្រិតនៃការរៀនសូត្រធ្លាក់ចុះ
- មិនសូវមានពេលជាមួយគ្រួសារ និងមិត្តភក្តិ
- រាងកាយមិនសូវសកម្ម

- ពិបាកឈប់លេងហ្គេមអនឡាញ។

ប្រសិនបើយើងរកឃើញសញ្ញាណទាំងនេះនៅក្នុងជីវិតប្រចាំថ្ងៃរបស់យើង ឬមិត្តយើង នោះយើងគួរតែឈប់ ហើយរៀបចំពេលវេលាអនឡាញរបស់យើងឡើងវិញ។ ទាំងនេះ គឺជាគំនិតមួយចំនួនដែលជួយដល់ការរៀបចំពេលវេលាអនឡាញរបស់យើងរួមមាន៖

- បិទទូរសព្ទនៅពេលយប់
- បិទការជូនដំណឹង សំឡេង ឬរំញ័រ ជាពិសេសនៅពេលធ្វើកិច្ចការផ្សេងៗ
- ចៀសវាងការលេងទូរសព្ទពេលកំពុងធ្វើកិច្ចការផ្ទះ ឬពេលនៅជាមួយគ្រួសារ ឬមិត្តភក្តិ
- ដំឡើងការកំណត់ពេលវេលានៅលើទូរសព្ទ

ត្រូវដឹងថាយុទ្ធសាស្ត្ររបស់ថ្នាលកម្មវិធី គឺគេចង់ឱ្យយើងនៅលើអនឡាញឱ្យបានយូរ។

៦.១២. ហ្គេមអនឡាញ

ការលេងហ្គេមអនឡាញធ្វើឱ្យយើងសប្បាយ តែយកល្អយើងគួរចំណាយពេលជាមួយមិត្តភក្តិយើងវិញ។ មានរឿងរ៉ាវជាច្រើន ដែលយើងត្រូវចងចាំនៅពេលយើងលេងហ្គេម។ បើមិនប្រុងប្រយ័ត្នទេ នៅពេលយើងលេងហ្គេមតាមប្រព័ន្ធអនឡាញ យើងនឹងអាច៖

- ចំណាយពេលច្រើនលើការលេងហ្គេម តាមប្រព័ន្ធអនឡាញ
- មើលឃើញអំពើហិង្សា និងរឿងរ៉ាវដែលធ្វើឱ្យយើងមានអារម្មណ៍មិនល្អ
- មានការសាកសួរពីព័ត៌មានផ្ទាល់ខ្លួនរបស់យើង និងអ្នកដទៃ
- ត្រូវរងការរុកកួន ឬធ្វើឱ្យមានអារម្មណ៍មិនល្អ
- ត្រូវសុំឱ្យបង់លុយដើម្បីដំឡើងកម្រិត ឬមុខងារ
- ញៀននឹងការលេងហ្គេមអនឡាញ។

ការលេងហ្គេមអនឡាញផ្តល់នូវការសប្បាយរីករាយ តែវាក៏អាចគ្រោះថ្នាក់ផងដែរ ប៉ុន្តែយើងក៏មានវិធីច្រើន ដែលអាចជួយរក្សាសុវត្ថិភាពយើងពេលលេងហ្គេមផងដែរ។ មានវិធីសាស្ត្រមួយចំនួន ដើម្បីរក្សាសុវត្ថិភាពពេលលេងហ្គេមអនឡាញ រួមមាន៖

- រាំងខ្ទប់ ឬរាយការណ៍ពីនរណាម្នាក់ដែលធ្វើឱ្យយើងមានអារម្មណ៍មិនល្អ
- ការពារខ្លួនរបស់យើង ដោយការមិនចែករំលែកព័ត៌មានផ្ទាល់ខ្លួន ឬឈ្មោះពិត
- ប្រាប់មនុស្សពេញវ័យដែលយើងទុកចិត្ត នៅពេលមានអ្នកលេងហ្គេមណាមួយធ្វើឱ្យយើងមានអារម្មណ៍មិនល្អ
- គិតមុនពេលចំណាយលុយ ឬផ្តល់ព័ត៌មានផ្ទាល់ខ្លួន
- ឈប់លេង បើយើងបានឃើញអ្វីមួយដែលធ្វើឱ្យយើងមានអារម្មណ៍មិនល្អ ឬមិនសប្បាយចិត្ត
- កម្រិតដែនកំណត់សម្រាប់រយៈពេលដែលយើងត្រូវលេងហ្គេម និងត្រូវធ្វើឱ្យបានខ្ជាប់ខ្ជួន ដើម្បីចៀសវាងការចំណាយពេលច្រើនពេកតាមប្រព័ន្ធអនឡាញ។

អ្នកលេងហ្គេមដែលយើងជួបតាមហ្គេមអនឡាញ អាចមិនមែនជារូបមនុស្សដែលយើងមើលឃើញនោះទេ។ ប្រសិនបើនរណាម្នាក់ធ្វើឱ្យយើងមានអារម្មណ៍មិនល្អ យើងអាចគ្រប់គ្រងការលេងហ្គេមតាមរយៈ៖

- រាំងខ្ទប់អ្នកលេងហ្គេមជាមួយយើង
- ចាកចេញ ឬឈប់លេងហ្គេម
- ប្រាប់មនុស្សដែលយើងទុកចិត្ត។

ចូរចាំថា ត្រូវការពារឯកជនភាពរបស់យើងជានិច្ចពេលលេងហ្គេមអនឡាញ និងមិនត្រូវចែករំលែកព័ត៌មានផ្ទាល់ខ្លួនទេ។ នេះមានន័យថា ត្រូវជ្រើសរើសរូបប្រូហ្វាល និងឈ្មោះលើអេក្រង់ ដែលការពារអត្តសញ្ញាណរបស់យើង។ ប្រសិនបើយើងគិតថា ត្រូវបានគេបោកប្រាស់ ឬលួចគណនីតាមប្រព័ន្ធអនឡាញ យើងអាចមានជំហានជាច្រើនទៀត ដែលជួយការពារខ្លួនរបស់យើង និងអ្នកដទៃ ក្នុងនោះរួមមាន៖

- ចាកចេញពីគ្រប់គណនីទាំងអស់
- ប្តូររាល់ពាក្យសម្ងាត់របស់យើង
- បង្ហាញពីសញ្ញាអាសន្នដល់គ្រួសារ និងមិត្តភក្តិ
- រាយការណ៍អំពីការបោកប្រាស់ ឬលួចគណនី។

ការផុសពីផ្លូវភេទ ការប្រកាន់ពូជសាសន៍ ពិការភាព ឬការស្អប់ការស្រឡាញ់ភេទដូចគ្នា មិនល្អទេ។ ទាំងនេះជាការរំលោភបំពានតាមប្រព័ន្ធអនឡាញ ដូច្នេះយើងត្រូវឆ្លើយតប ដូចខាងក្រោម៖

- គិតមុនប្រតិកម្មតប
- កុំជឿនូវអ្វីដែលគេនិយាយ
- ដើម្បីមានអារម្មណ៍សុវត្ថិភាព យើងមិនគួរផុស ឬបញ្ចេញមតិមិនល្អទេ
- ត្រូវគាំទ្រអ្នកដែលរងការរំលោភបំពានតាមប្រព័ន្ធអនឡាញ
- បើយើងមានអារម្មណ៍ថា រងការគំរាមកំហែង ត្រូវប្រាប់មនុស្សពេញវ័យដែលយើងទុកចិត្ត
- ពិនិត្យមើលឯកជនភាព កំណត់ទីតាំង រាយការណ៍ និងរាំងខ្ទប់បុគ្គលនោះ។

បើយើងរងការរុកកួនតាមការលេងហ្គេមអនឡាញ យើងត្រូវប្រាប់មនុស្សដែលយើងទុកចិត្តឱ្យបានឆាប់បំផុត ហើយរាំងខ្ទប់ ឬរាយការណ៍ការរុកកួននេះទៅថ្នាលកម្មវិធីផ្ទាល់។ គួរលេងហ្គេមជាមួយមនុស្សដែលយើងស្គាល់នៅក្នុងជីវិតពិត។ យើងអាចប្រើនូវជំនាញដែលយើងបានរៀននេះ ដើម្បីគ្រប់គ្រងការលេងហ្គេមអនឡាញរបស់យើង។ ការតាមដានលើពេលវេលា ឬរយៈពេលនៃការលេងហ្គេមអនឡាញរបស់យើង គឺសំខាន់ណាស់។ ចូរចាំថា ការចំណាយពេលច្រើនពេកតាមប្រព័ន្ធអនឡាញ អាចប៉ះពាល់ដល់សុខភាពរាងកាយ និងផ្លូវចិត្ត។

៦.១៣. ការរាយការណ៍

ផលប្រយោជន៍នៃការរាយការណ៍៖

- ការរាយការណ៍គឺជាការបង្កើនលទ្ធភាពនៃការលុបបំបាត់មាតិកាបែបរំលោភបំពានពីគេហទំព័រ និងជួយបញ្ឈប់ការរំលោភបំពាន

- ជួយឱ្យកុមារទទួលបានការគាំទ្រ និងជំនួយ
- ពង្រឹងឱកាសក្នុងការស្វែងរកជនល្មើស និងនាំពួកគេទៅកាន់តុលាការ
- នៅពេលមានការរាយការណ៍កាន់តែច្រើន ជនទុច្ចរិតដែលធ្វើសកម្មភាពនេះនឹងកាន់តែតិច ដោយសារភ័យខ្លាចចំពោះការចាប់ខ្លួន។

ភាពងាយស្រួលក្នុងការរាយការណ៍ជួយដល់កុមារ ដែលរងផលប៉ះពាល់ពីការកេងប្រវ័ញ្ចផ្លូវភេទ ឱ្យមានជំនឿចិត្តក្នុងការនិយាយនៅពេលមានបញ្ហាកើតឡើង និងដឹងថាពួកគេនឹងទទួលបានជំនួយគាំទ្រសមស្រប។

ក្នុងករណីព្រហ្មទណ្ឌ អ្នកអាចទាក់ទងដោយផ្ទាល់ទៅបណ្ដាញទូរសព្ទទាន់ហេតុការណ៍របស់នគរបាលតាមរយៈលេខ **១២៨៨** ឬគេហទំព័ររបស់អគ្គស្នងការនគរបាល http://hotline.police.gov.kh។

យើងក៏អាចធ្វើការបញ្ជូនទៅកាន់សេវាគាំទ្រផ្សេងទៀត ដូចខាងក្រោម៖

- អង្គភាពការពារកុមារ (CPU) : (០៧៨) ៩៥៩ ០៩០ ឬ (០៧៧) ២៤៧ ២៤៧
- អង្គការសកម្មភាពដើម្បីកុមារ (APLE) : (០៩២) ៣១១ ៥១១
- អង្គការសេរីភាពកម្ពុជាអូស្ត្រាលី (AusCam) : (០១១) ៤៤៤ ០៨០
- អង្គការហាការ (Hagar) : (០៧១) ៥៧១ ៣៣៣៣ ឬ (០៨៦) ៩៩៩ ៧២២
- អង្គការសម្ពន្ធចាប់ដៃ : (០១២) ៥៣២ ៥៥៤
- អង្គការមិត្តសំឡាញ់ : (០១២) ៣១១ ១១២

-

៧. សង្ខេប

កម្ពុជាបានអភិវឌ្ឍសង្គម និងសេដ្ឋកិច្ចយ៉ាងឆាប់រហ័សក្នុងពីរទសវត្សរ៍ចុងក្រោយ ដែលបានបង្កើតឱកាសល្អសម្រាប់សុខុមាលភាព និងការអប់រំរបស់កុមារ។ ការរីកចម្រើនបច្ចេកវិទ្យាឌីជីថលបាននាំឱ្យកុមារទទួលបានឱកាសអភិវឌ្ឍ និងប្រឈមនឹងហានិភ័យតាមប្រព័ន្ធអនឡាញ ដូចជា ការកេងប្រវ័ញ្ចផ្លូវភេទ ការលួងលោម ការរុកកួន ព័ត៌មានមិនពិត និងការរំលោភឯកជនភាព។ ដោយសារហានិភ័យទាំងនេះ ការការពារកុមារតាមប្រព័ន្ធអនឡាញ ក្លាយជាកិច្ចការសំខាន់ដែលត្រូវការសហការពីគ្រួសារ សាលារៀន សហគមន៍ អង្គការសង្គមស៊ីវិល និងអាជ្ញាធរ។

សៀវភៅមេរៀន សុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញនេះ ជាលទ្ធផលនៃកិច្ចសហការរវាងវិទ្យាស្ថានជាតិសង្គមកិច្ច និងអង្គការឆាលហ្វាន កម្ពុជា ដែលបានរួមចំណែកយ៉ាងសកម្មក្នុងការបង្កើតឡើង។ សៀវភៅនេះនឹងក្លាយជាឧបករណ៍សំខាន់សម្រាប់និស្សិត និងកម្លាំងសេវាសង្គមក្នុងការគាំទ្រកុមារ និងយុវជនឱ្យប្រើប្រាស់អ៊ីនធឺណិតដោយសុវត្ថិភាព និងទទួលបានអត្ថប្រយោជន៍ពីបច្ចេកវិទ្យាឌីជីថលដោយគ្មានហានិភ័យ។

ដើម្បីជួយកុមារឱ្យយល់អំពីហានិភ័យ និងវិធីសាស្ត្រការពារខ្លួន សៀវភៅមេរៀននេះ បានណែនាំគោលគំនិត "ធាតុផ្សំទាំងប្រាំមួយ" ដែលជាគន្លឹះសម្រាប់យល់ពីការប្រើប្រាស់ប្រព័ន្ធអនឡាញ៖

១- ធាតុផ្សំ "សាធារណៈ"	បង្ហាញថាអ្វីដែលបង្ហោះ អាចត្រូវឃើញដោយមនុស្សជាច្រើនក្នុងពិភពលោក
២- ធាតុផ្សំ "អចិន្ត្រៃយ៍"	បង្ហាញថាមាតិកាដែលយើងផុសលើប្រព័ន្ធអនឡាញអាចនៅតែមាន សូម្បីតែយើងលុបវាចោលក៏ដោយ
៣- ធាតុផ្សំ "ការផ្សារភ្ជាប់"	បង្ហាញពីការតភ្ជាប់មនុស្សគ្រប់ទីកន្លែង ដែលអាចនាំឱ្យមានទាំងឱកាស និងហានិភ័យផងដែរ
៤- ធាតុផ្សំ "អនាមិកភាព"	បង្ហាញពីការលាក់អត្តសញ្ញាណរបស់អ្នកប្រើប្រាស់ ដែលជាហានិភ័យសម្រាប់ការលួងលោម និងការកេងប្រវ័ញ្ច
៥- ធាតុផ្សំ "ប្រភពព័ត៌មាន"	បង្ហាញថាព័ត៌មានតាមប្រព័ន្ធអនឡាញ មិនមែនសុទ្ធតែត្រឹមត្រូវនោះទេ ហើយកុមារងាយជឿព័ត៌មានមិនពិត
៦- ធាតុផ្សំ "ការគោរព"	បង្ហាញថាការប្រាស្រ័យទាក់ទងតាមប្រព័ន្ធអនឡាយមិនប្រាកដថា តែងតែមានការគោរពនោះទេ ដោយសារលក្ខណៈអនឡាញមានធាតុផ្សំ ដូចជាសារធារណៈ អនាមិក ជាដើម។

សៀវភៅមេរៀនក៏ផ្តោតលើការប្រើប្រាស់ មុខងារសុវត្ថិភាពលើថ្នាលកម្មវិធី ដូចជា Facebook, TikTok, Telegram, Instagram និង YouTube ដែលមានដូចជា៖

- ការកំណត់ឯកជនភាព (Privacy) ជួយកំណត់ថានរណាអាចឃើញព័ត៌មានរបស់កុមារ។

- ការរុករកដោយសុវត្ថិភាព (SafeSearch) ជួយច្រោះមាតិកាអាសអាភាស និងអំពើហិង្សា ដើម្បីធានាឱ្យកុមារធ្វើការរុករកតាមអ៊ីនធឺណិតក្នុងបរិយាកាសសុវត្ថិភាព។ វាអាចបើកតាមកម្មវិធី Google ហើយអាចចាក់សោរតាម Family Link ដើម្បីកុំឱ្យកុមារអាចបិទវាបាន។
- ការរឹតបន្តឹង (Restrict) ជួយលាក់វីដេអូមិនសមរម្យ ដូចជា មាតិកាផ្លូវភេទ និងអំពើហិង្សា ដើម្បីធ្វើឱ្យ YouTube មានសុវត្ថិភាពសម្រាប់កុមារ។
- ការរាំងខ្ទប់ (Block) ជួយទប់ស្កាត់គណនី ឬមាតិកាដែលរំខានកុមារ ដោយធ្វើឱ្យគេមិនអាចទាក់ទង ឬមើលឃើញខ្លឹមសាររបស់កុមារបាន។
- ការរាយការណ៍ (Report) ជួយឱ្យកុមារប្រាប់ថ្នាលកម្មវិធីអំពីមាតិកា ឬគណនីគួរឱ្យសង្ស័យ។
- ការកំណត់ទីតាំងមិនឲ្យគេដឹង (Restrict Location) ជួយការពារកុមារពីការចែករំលែកព័ត៌មានអំពីទីតាំងពិតប្រាកដ។

មុខងារទាំងនេះជាឧបករណ៍សំខាន់សម្រាប់ការការពារកុមារ និងត្រូវបានណែនាំឱ្យប្រើប្រាស់ជាប្រចាំ។

ក្នុងផ្នែកអភិវឌ្ឍជំនាញ កុមារត្រូវបានណែនាំអំពីប្រភេទហានិភ័យតាមប្រព័ន្ធអនឡាញ ដែលពួកគេអាចជួបប្រទះ មានដូចជា ហានិភ័យមាតិកា ហានិភ័យទំនាក់ទំនង ហានិភ័យការប្រព្រឹត្ត និងហានិភ័យកិច្ចសន្យា ដែលអាចកើតឡើងលើថ្នាលកម្មវិធីផ្សេងៗ។ កុមារត្រូវការការណែនាំ និងការការពារ ដើម្បីទប់ស្កាត់ហានិភ័យទាំងនេះពេលប្រើប្រាស់អនឡាញ។

ដូចគ្នានេះដែរ កុមារត្រូវបានណែនាំអំពីការកេងប្រវ័ញ្ច និងការរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ រួមមាន៖

- ការលួងលោមកុមារតាមប្រព័ន្ធអនឡាញ (Child Online Grooming)
- រូបភាព-សម្ភារៈរំលោភបំពានផ្លូវភេទលើកុមារ (Child Sexual Abuse Material-CSAM)
- ការគំរាមកំហែងពាក់ព័ន្ធសកម្មភាពផ្លូវភេទ (Sextortion)
- ការផ្សាយផ្ទាល់អំពីការរំលោភបំពានផ្លូវភេទលើកុមារ (Live-streaming)
- ការផ្ញើសារបែបផ្លូវភេទ (Sexting)

ការរុកគួនតាមប្រព័ន្ធអនឡាញ (cyberbullying) ក៏ជាបញ្ហាធ្ងន់ធ្ងរ ដែលអាចប៉ះពាល់ដល់សុខភាពផ្លូវចិត្ត និងកេរ្តិ៍ឈ្មោះរបស់កុមារ។ កុមារអាចត្រូវបានបង្ខូចកេរ្តិ៍ឈ្មោះ ត្រូវបានគំរាម ឬត្រូវបានបង្ខំឱ្យធ្វើអ្វីដែលកុមារមិនចង់ធ្វើ។ ដូច្នេះ ការបណ្តុះបណ្តាលកុមារឱ្យស្គាល់ បាតដៃសុវត្ថិភាព កិច្ចព្រមព្រៀងប្រើអនឡាញនៅផ្ទះ និង គន្លឹះឆ្លើយតបបញ្ហាធ្ងន់ធ្ងរ គឺមានសារៈសំខាន់ណាស់។ កុមារត្រូវបានលើកទឹកចិត្តឱ្យរក្សាវត្តតាង កុំឆ្លើយតបអ្នកបង្កបញ្ហា និងត្រូវស្វែងរកជំនួយពីមនុស្សពេញវ័យដែលទុកចិត្តបាន។

នៅផ្នែកចុងបញ្ចប់នៃសៀវភៅមេរៀននេះ បានផ្តល់នូវគន្លឹះសុវត្ថិភាពសម្រាប់កុមារ ដូចជា ការការពារកេរ្តិ៍ឈ្មោះតាមប្រព័ន្ធអនឡាញ ការចែករំលែកព័ត៌មានដោយមានការទទួលខុសត្រូវ ការទប់ស្កាត់អ្នកបោកប្រាស់ ការគ្រប់គ្រងពេលវេលាអនឡាញ ហ្គេមអនឡាញ និងការរាយការណ៍ពេលមានបញ្ហា។ កុមារត្រូវបានណែនាំឱ្យគិតមុនបង្ហោះ មិនចែករំលែកព័ត៌មានផ្ទាល់ខ្លួន និងប្រើប្រាស់ប្រព័ន្ធអនឡាញដោយគោរពអ្នកដទៃ។

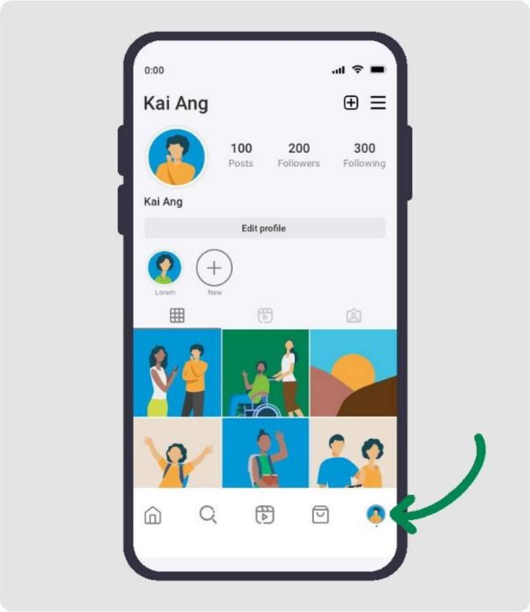
សំណួរ

១. ការប្រើអ៊ីនធឺណិតបានផ្តល់អត្ថប្រយោជន៍ដល់មនុស្សជាតិ ទោះជាយ៉ាងណាក៏ដោយ ក៏មានហានិភ័យផងដែរ សូមរៀបរាប់ពីប្រភេទហានិភ័យមានអ្វីខ្លះ ?
២. តើកង្វល់អ្វីខ្លះដែរកុមារត្រូវរាយការណ៍ ?
៣. តើឪពុកម្តាយត្រូវធ្វើអ្វីខ្លះក្នុងការការពារកូន ?
៤. តើអ្នកគិតថា អ្នកណាខ្លះគួរចូលរួមក្នុងការការពារកុមារតាមប្រព័ន្ធអនឡាញ ?
៥. តើអ៊ីនធឺណិតមានជាតុផ្សំប៉ុន្មាន ? ចូរពន្យល់ជាតុផ្សំនីមួយៗ ?
៦. តើអ្នកធ្លាប់ប្រើការកំណត់ឯកជនភាពលើ Facebook ឬ Telegram ដែរឬទេ ? តើធ្វើដូច្នេះមានផលប្រយោជន៍អ្វីខ្លះ ?
៧. សូមពន្យល់អំពីរបៀបនៃការរាំងខ្ទប់ (Block) នៅលើថ្នាលកម្មវិធីណាមួយ ដែលអាចជួយការពារកុមារលើប្រព័ន្ធអនឡាញ។
៨. តើអ្នកគិតថា ការរាយការណ៍ (Report) ដល់អាជ្ញាធរមានសមត្ថកិច្ច មានសារៈសំខាន់យ៉ាងដូចម្តេច ?
៩. តើអ្នកគិតថា ការរាយការណ៍ (Report) នៅលើថ្នាលកម្មវិធី (platform) មានសារៈសំខាន់យ៉ាងដូចម្តេច ?
១០. ចូរពិពណ៌នាអំពីទម្រង់នៃការកេងប្រវ័ញ្ច និងរំលោភបំពានផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញ ?
១១. សូមពន្យល់អំពីវិធីសាស្ត្រប្រើ "បាតដៃសុវត្ថិភាព" ?
១២. តើឪពុកម្តាយត្រូវធ្វើអ្វីខ្លះ ដើម្បីការពារកូនឱ្យមានសុវត្ថិភាព ?
១៣. សូមរៀបរាប់គន្លឹះឆ្លើយតបចំពោះបញ្ហាកុមារតាមប្រព័ន្ធអនឡាញ។

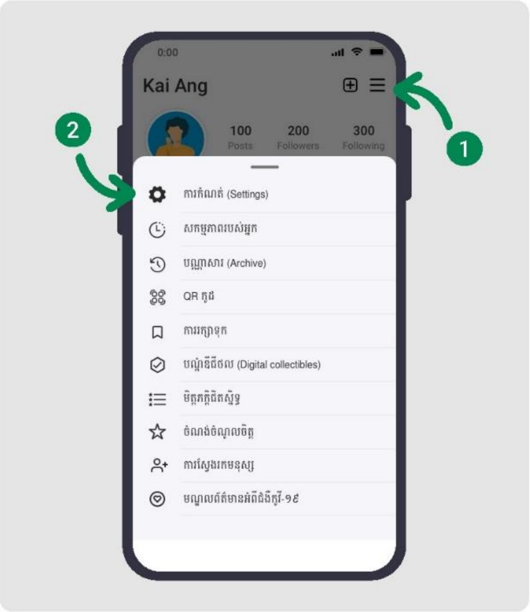
ឧបសម្ព័ន្ធ១ ៖ ការណែនាំអនុវត្តមុខងារសុវត្ថិភាពលើថ្នាលកម្មវិធី

១. ការកម្រិតការមើលឃើញជាសាធារណៈ

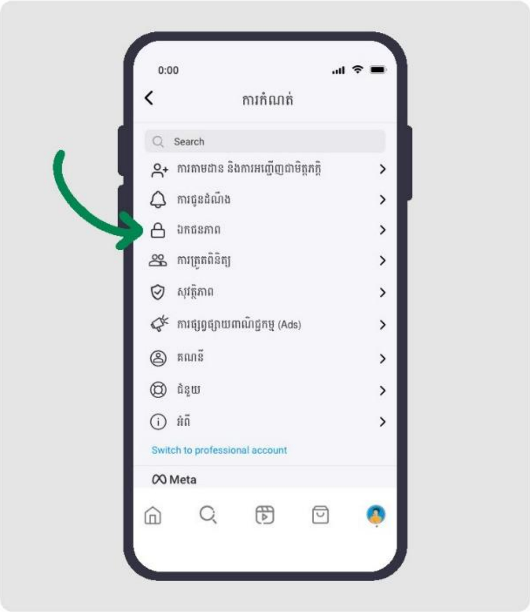
ក. ថ្នាលកម្មវិធី INSTAGRAM



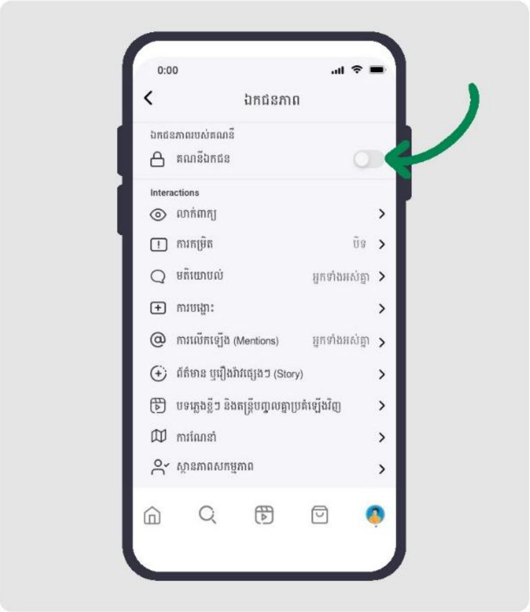
១. បើកកម្មវិធី Instagram ហើយជ្រើសរើសប្រូហ្វាល (Profile) របស់អ្នក។



២. ជ្រើសរើស "more" ដែលមានលក្ខណៈជា បន្ទាត់ត្រេបី បន្ទាប់មកជ្រើសរើសការកំណត់ "setting" ដែលនឹងលេចឡើងនៅលើអេក្រង់

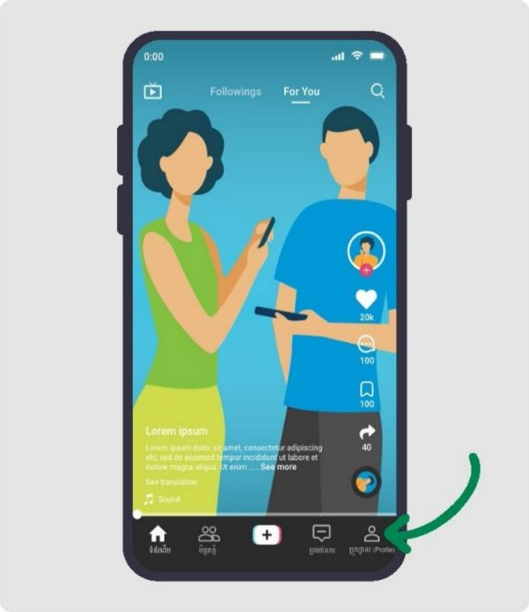


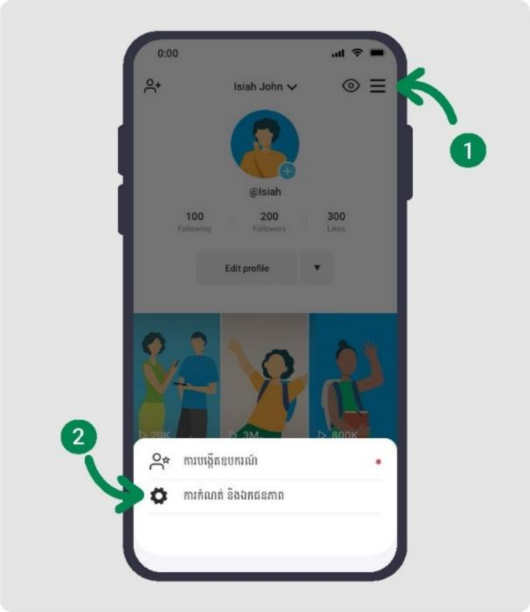
៣. ជ្រើសរើស "ឯកជនភាព(Privacy)" ដែលមានរូប សោ ជាតំណាង



៤. ចុកពាក្យ "On (បើក)" សម្រាប់ដាក់គណនីឯកជនភាព

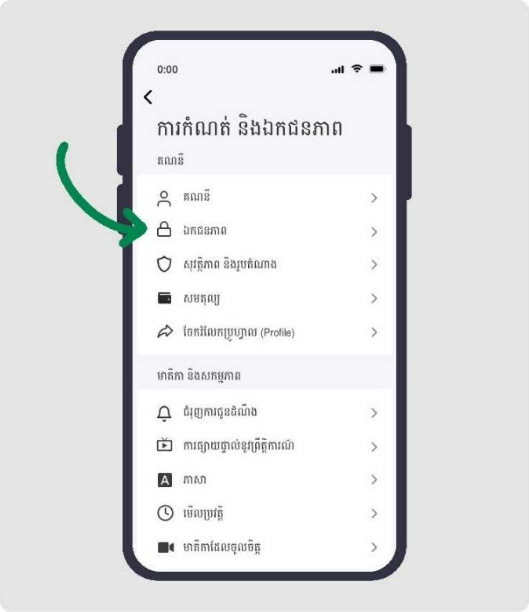
ខ. ផ្ទាំលកម្មវិធី INSTAGRAM

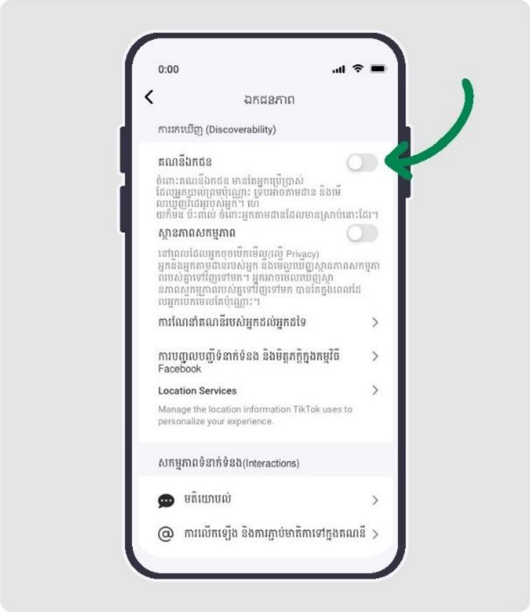




១. បើកកម្មវិធី TikTok រួចជ្រើសរើសប្រូហ្វាល(Profile) របស់អ្នក

២. ជ្រើសរើស "more" ដែលមានលក្ខណៈជា បន្ទាត់ត្រេបី បន្ទាប់មកជ្រើសរើសការកំណត់ "setting" ដែលនឹងលេចឡើងនៅលើអេក្រង់



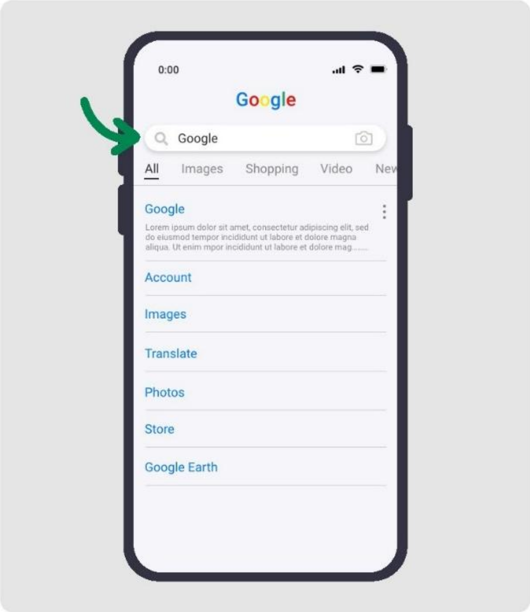


៣. ជ្រើសរើស "privacy" ដែលមានរូបសោ ជាតំណាង

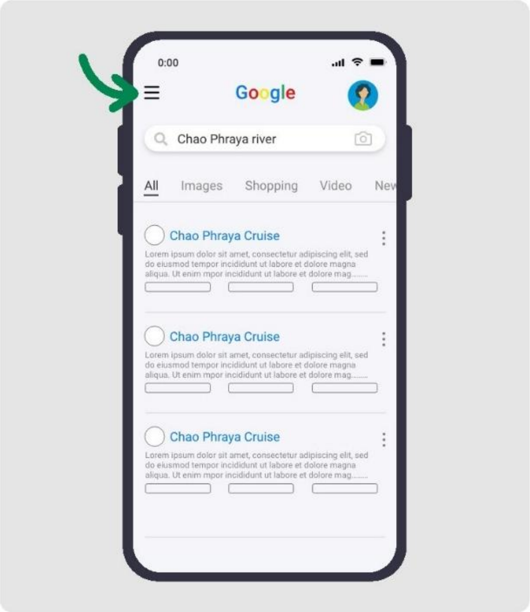
៤. ចុកពាក្យ 'On (បើក)' ដើម្បីបើកគណនីជាឯកជនភាព

២. ការលាក់លទ្ធផលច្បាស់ៗ (Hide Explicit Results) និងការរុករកដោយសុវត្ថិភាព

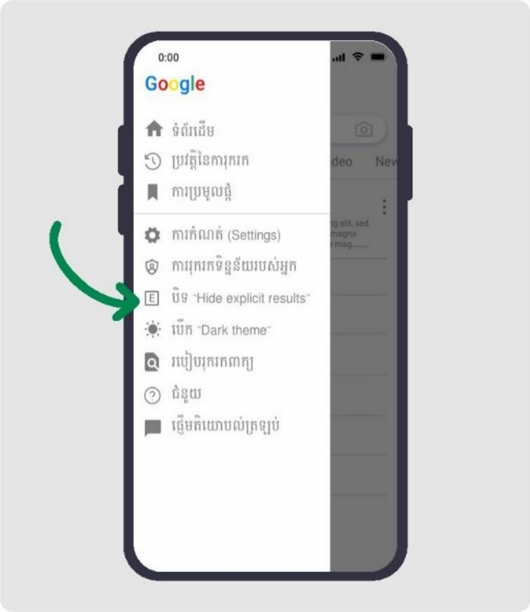
ក. ការលាក់លទ្ធផលច្បាស់នៅលើថ្នាលកម្មវិធី Google



១. បើកកម្មវិធី Google ហើយបំពេញពាក្យដែលចង់រុករក (ជម្រើសមិនផ្តល់ឱ្យទេ លុះត្រាតែធ្វើដំណើរការរុករក)។



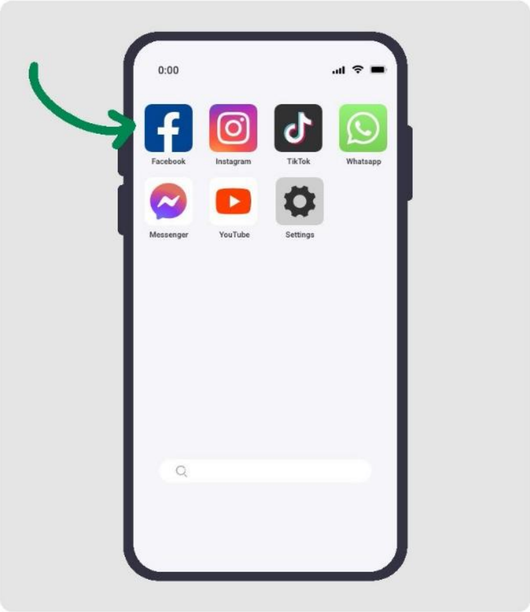
២. ជ្រើសរើស "More" ដែលមានលក្ខណៈជា បន្ទាត់ត្រេបី



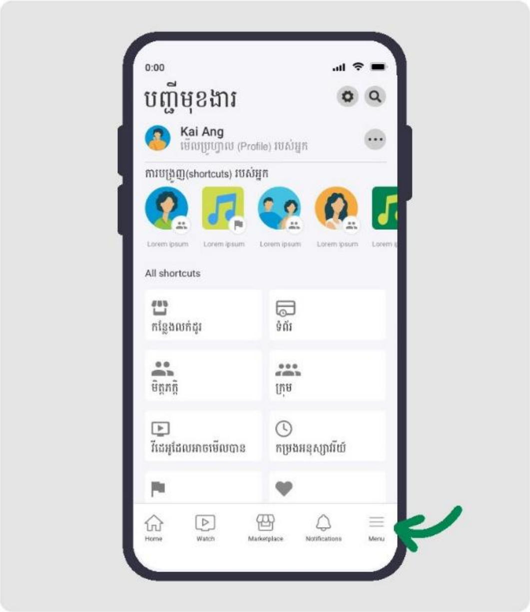
៣. ជ្រើសរើសការលាក់បាំងលទ្ធផល "Hide explicit results" បញ្ជីមុខងារ

៤. ចុចពាក្យ "On" ដើម្បីឱ្យលទ្ធផលជាក់លាក់ត្រូវបានលាក់

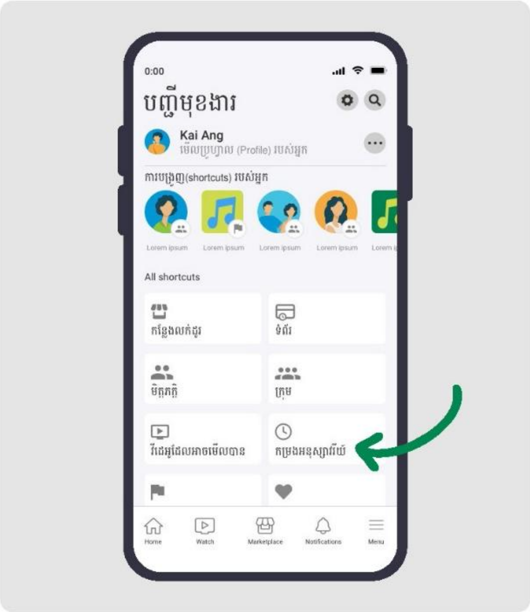
៣. កម្រងអនុស្សាវរីយ៍ (Memories) នៅលើថ្នាលកម្មវិធី Facebook



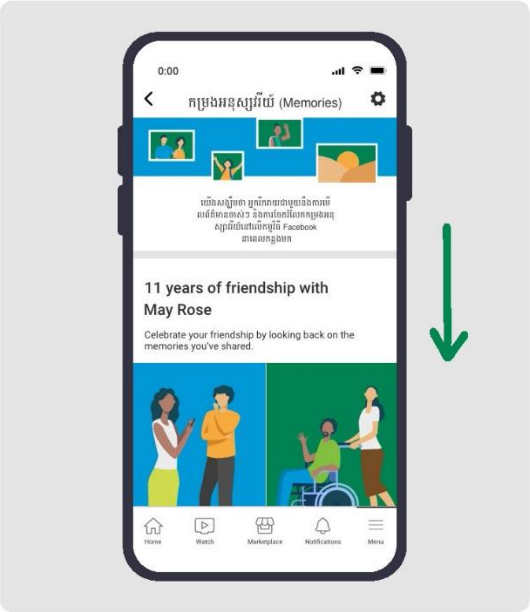
១. បើកកម្មវិធី Facebook



២. ជ្រើសរើស "more" ដែលមានលក្ខណៈជាបន្ទាត់ត្រេបី



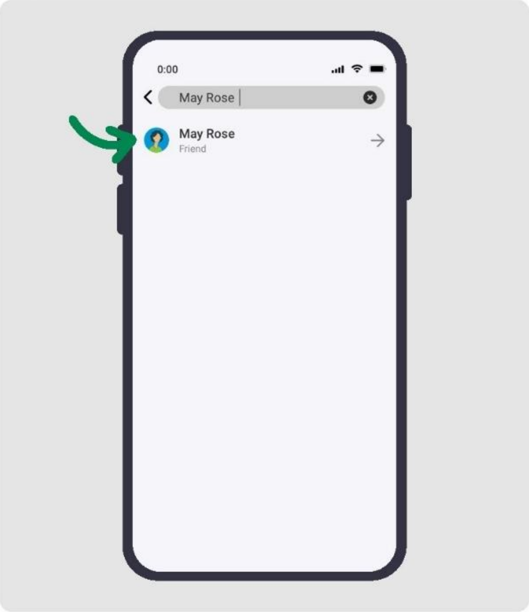
៣. ជ្រើសរើស "កម្រងអនុស្សាវរីយ៍ Memories"



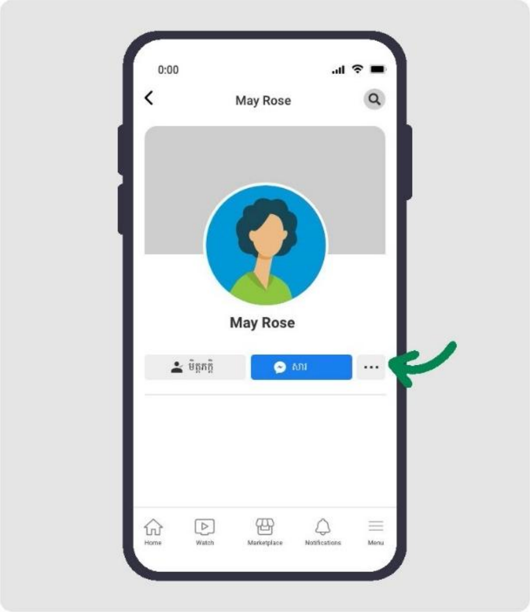
៤. អូសលើអេក្រង់ក្នុងកម្មវិធី Facebook ដើម្បីមើលព័ត៌មានថ្មី និងចាស់

៤. ការរាំងខ្ទប់ (Block)

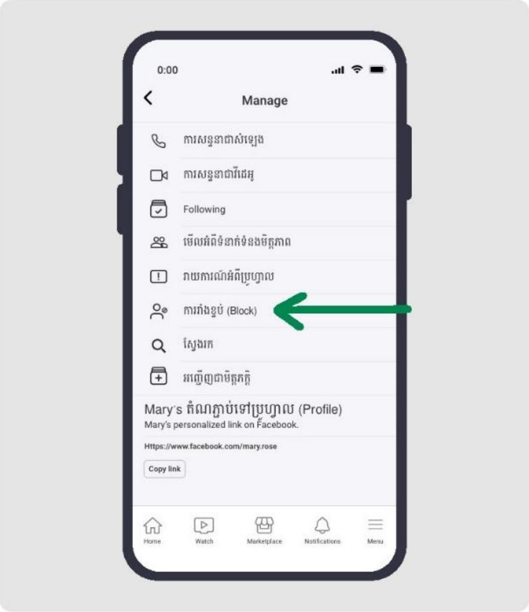
ក. ការរាំងខ្ទប់នៅលើផ្ទាលកម្មវិធី Facebook



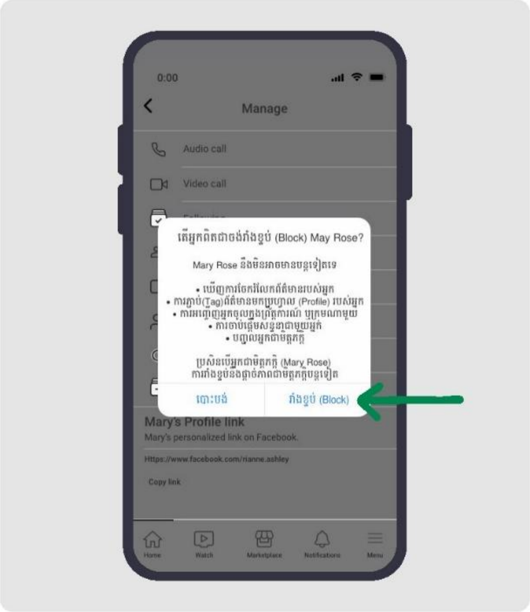
១. បើកកម្មវិធី Facebook បន្ទាប់មកចុចលើឈ្មោះគណនី Facebook ដែលអ្នកចង់រាំងខ្ទប់ (Block)



២. ចូលក្នុងប្រូហ្វាលរបស់ពួកគេ ចុចលើបន្ទាត់ត្រេបី

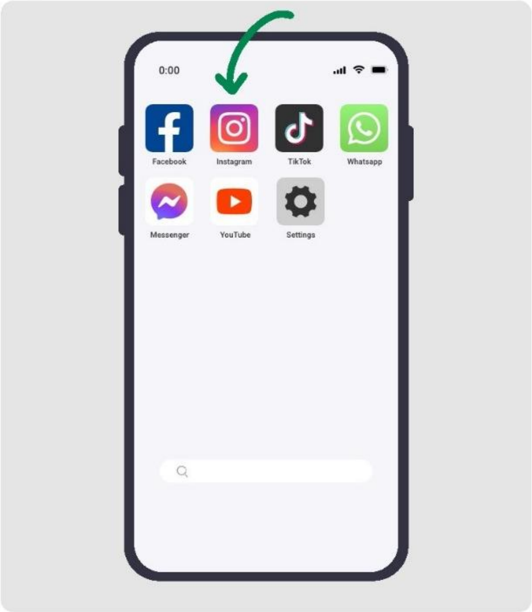


៣. ចុចលើពាក្យ "Block"

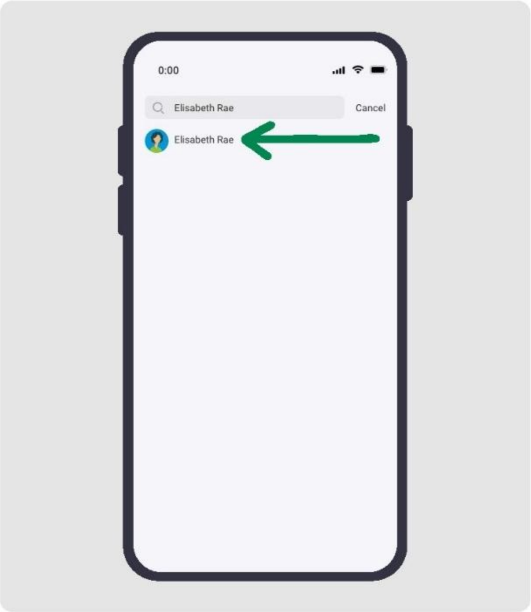


៤. ទំព័រមួយនឹងលេចឡើង រួចសួរបញ្ជាក់។ សូមធ្វើការចុច លើពាក្យ "Block" ម្តងទៀត

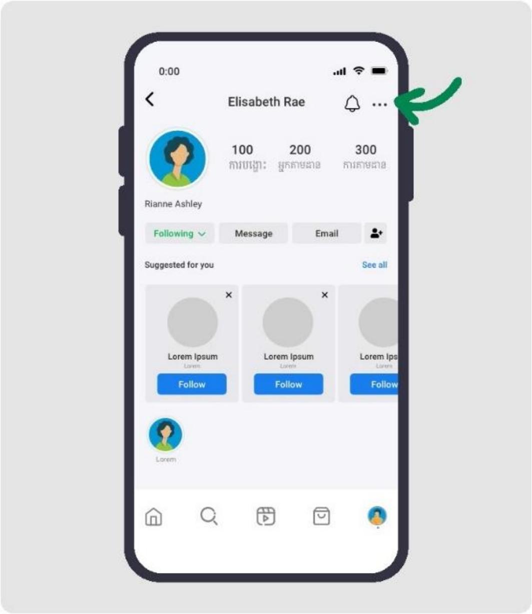
ខ. ការរាំងខ្ទប់នៅលើថ្នាលកម្មវិធី Instagram



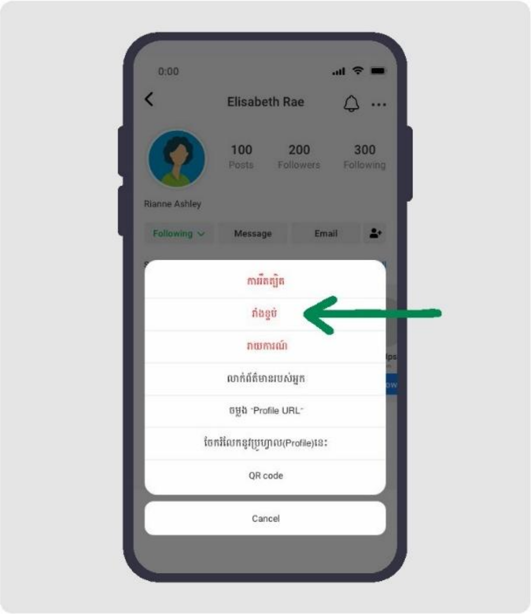
១. បើកកម្មវិធី Instagram



២. ចុចលើប្រូហ្វាល (Profile) ណាដែលអ្នកចង់រាំងខ្ទប់



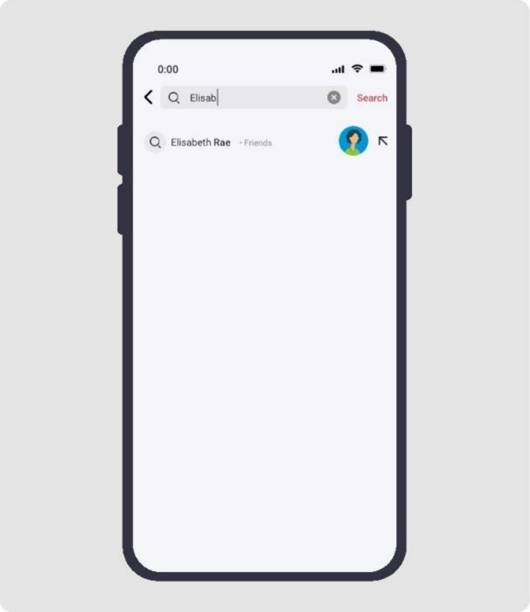
៣. ចុចលើបន្ទាត់ត្រេបី



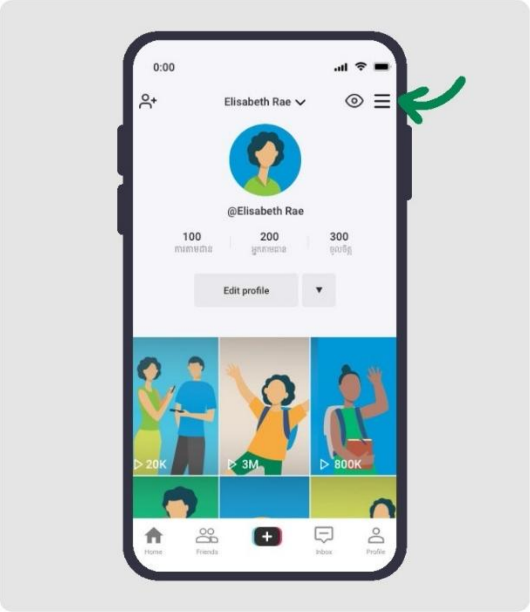
៤. ជ្រើសរើសពាក្យ "Block" បន្ទាប់មកធ្វើការបញ្ជាក់

គ. ការរាំងខ្ទប់នៅលើផ្ទាលកម្មវិធី TikTok

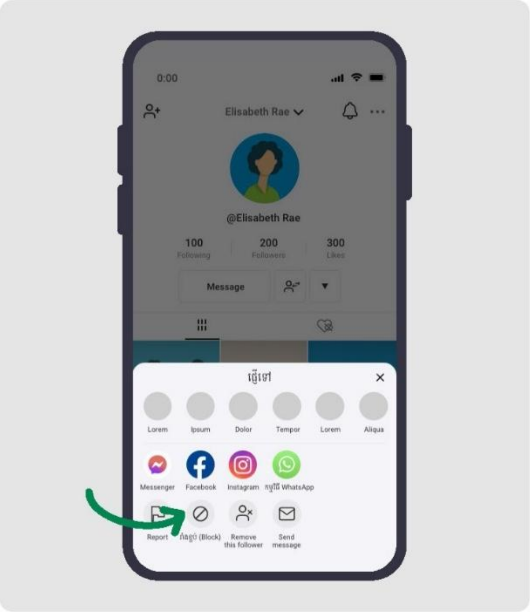
១. បើកកម្មវិធី Tiktok



២. ចុចលើពាក្យ Profile ដែលអ្នកចង់រាំងខ្ទប់ Block

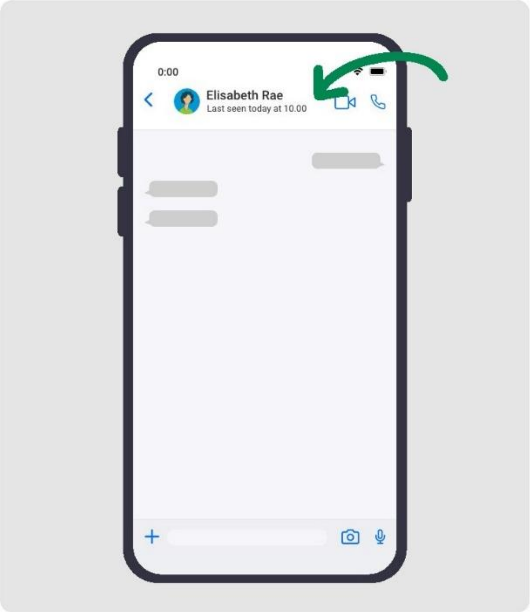


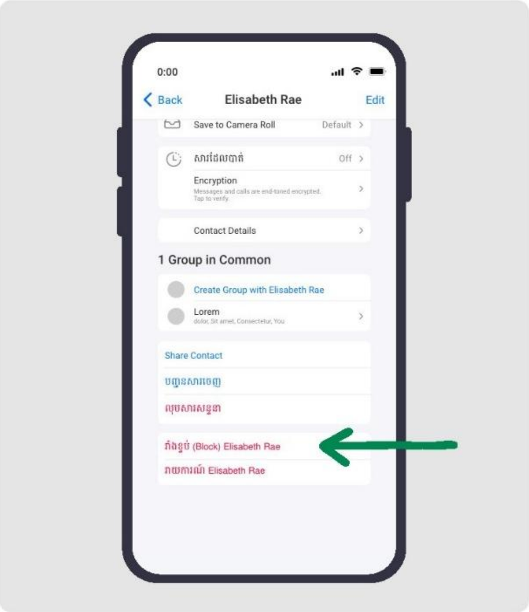
៣. ចុចលើបន្ទាត់ត្រេបី



៤. ជ្រើសរើស "Block" នៅលើផ្ទាំងបញ្ជីដែលលេចឡើង បន្ទាប់មកចុច "Confirm"

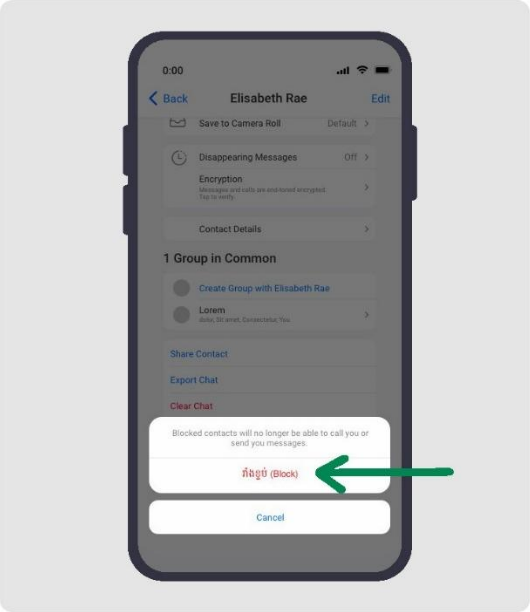
ឃ. ការរាំងខ្ទប់នៅលើថ្នាលកម្មវិធី WhatsApp





១. នៅក្នុងសារ ចុចលើបន្ទាត់ត្រៃបី

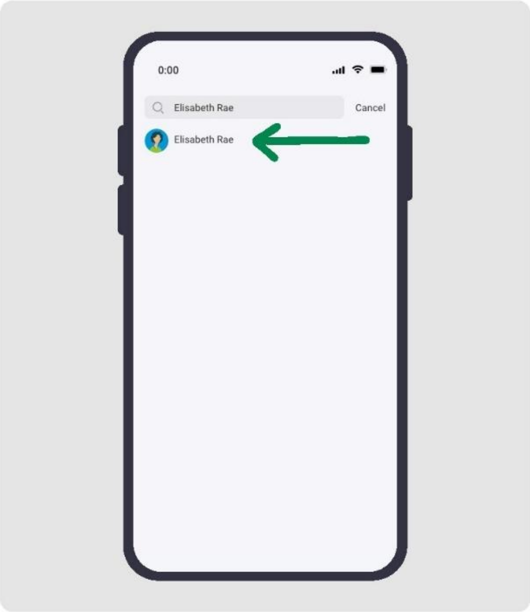
២. ចុចលើពាក្យ "more" បន្ទាប់មកចុចលើពាក្យ "Block"



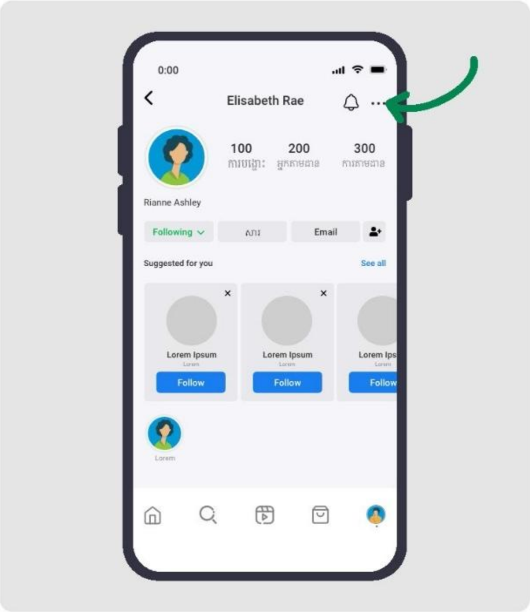
៣. អ្នកអាចត្រូវផ្តល់នូវហេតុផល ឬចុចលើពាក្យ "Block"

៥. ការរាយការណ៍ (Report)

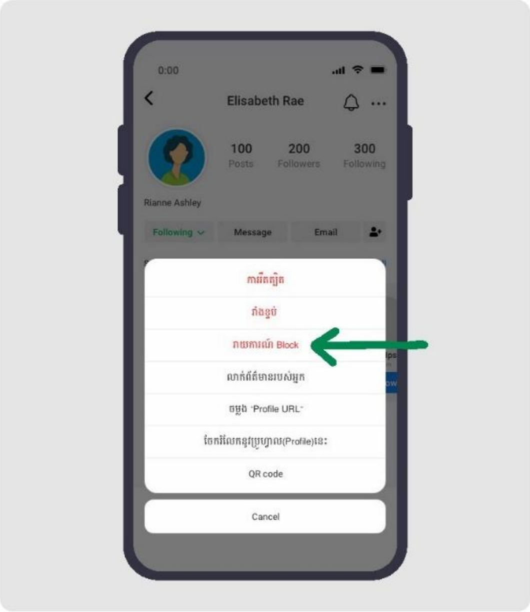
ក. ការរាយការណ៍នៅលើផ្ទាំងកម្មវិធី Instagram



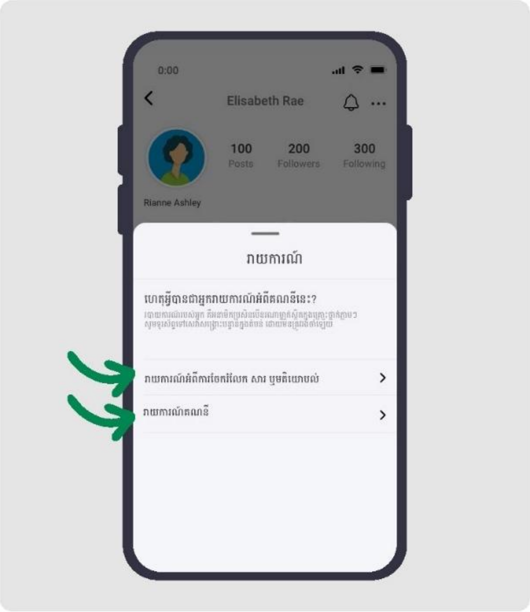
១.បើកកម្មវិធី Instagram រួចចុចលើប្រូហ្វាល (Profile) របស់ បុគ្គល ដែលអ្នកចង់រាយការណ៍



២.ចុចលើបន្ទាត់ត្រេបី

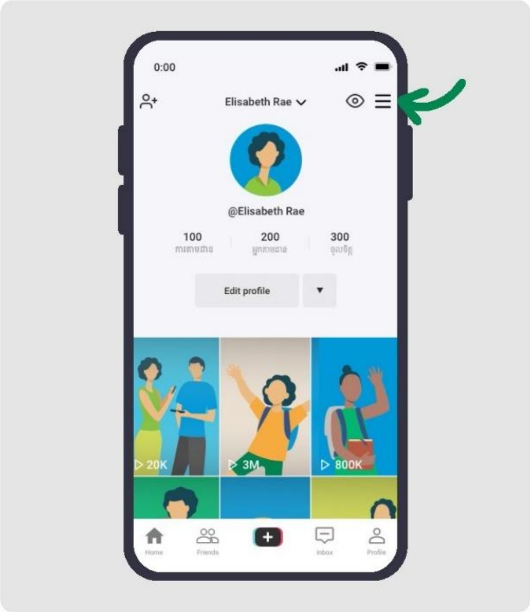


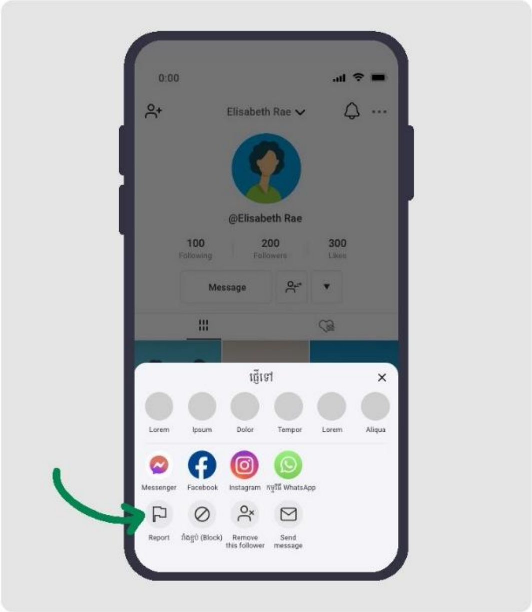
៣.ជ្រើសពាក្យ “Report”



៤.បន្ទាប់មកអ្នកមានជម្រើសចំនួន ២ ។ អ្នកអាចរាយការណ៍ អំពីការបង្ហោះមតិយោបល់ ឬគណនីទាំងមូល។

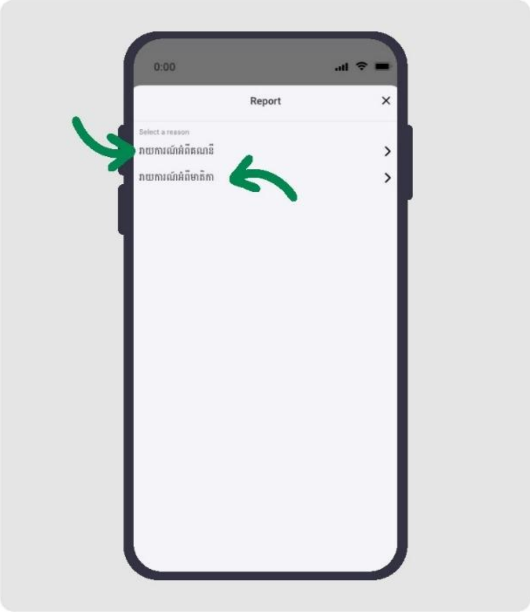
ខ. ការរាយការណ៍នៅលើថ្នាលកម្មវិធី TikTok

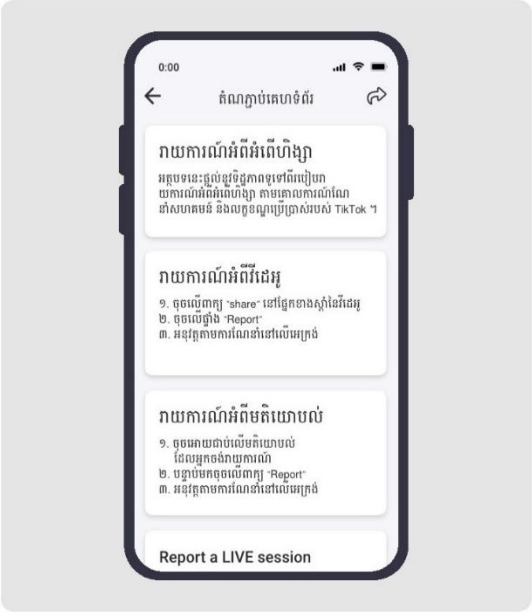




១. ចូលទៅប្រូហ្វាលដែលអ្នកចង់រាយការណ៍ បន្ទាប់មកចុចលើបន្ទាត់ត្រេបី

២. ចុចលើពាក្យ "Report"

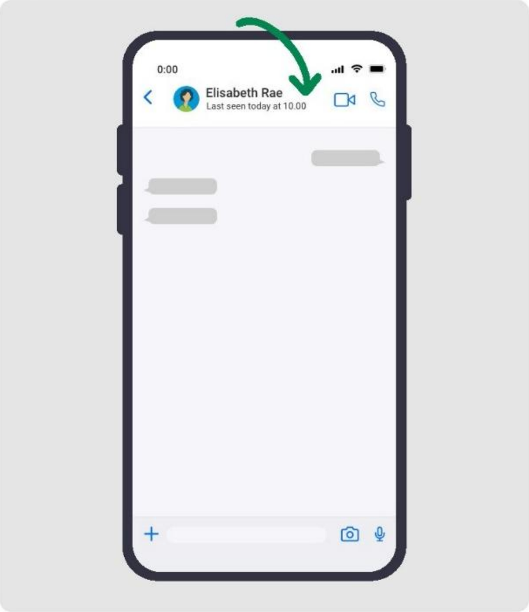




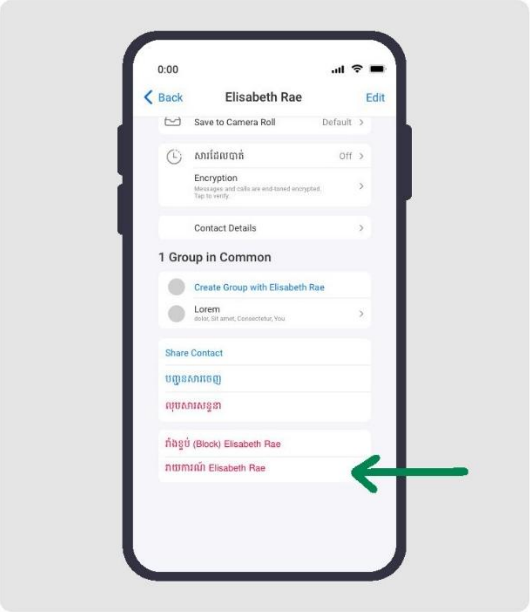
៣. បន្ទាប់មក អ្នកអាចជ្រើសរើសការរាយការណ៍អំពីគណនី ឬមាតិកា

៤. ប្រសិនបើអ្នកជ្រើសរើសមាតិកា (content) នឹងមានជម្រើសផ្សេងៗទៀតដើម្បីចុចបន្តទៀត

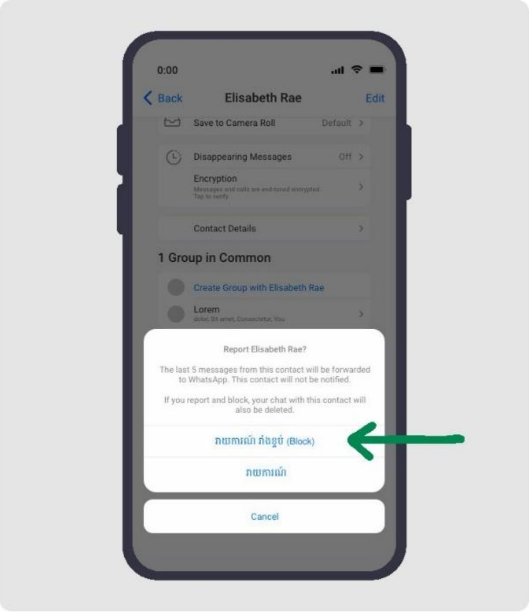
គ. ការរាយការណ៍នៅលើថ្នាលកម្មវិធី WhatsApp



១.ចុចលើបន្ទាត់ត្រៃបី

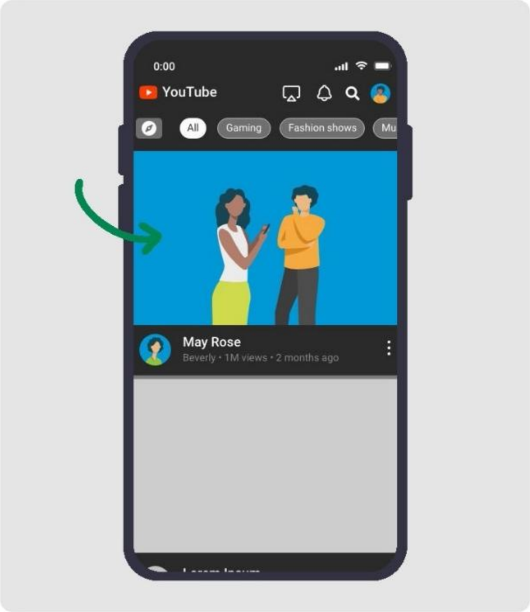


២.ចុចលើពាក្យ "Report"

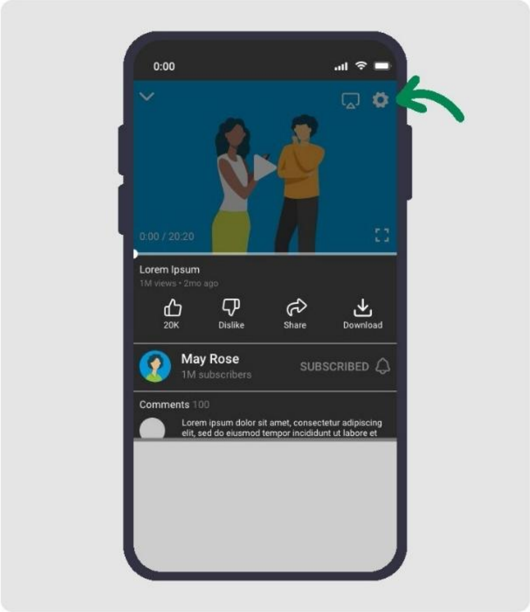


៣.នៅពេលដែលអ្នករាយការណ៍ អ្នកក៏មានជម្រើសសម្រាប់រាំងខ្ទប់ទំនាក់ទំនង និងលុបនូវសារចាស់ៗផងដែរ

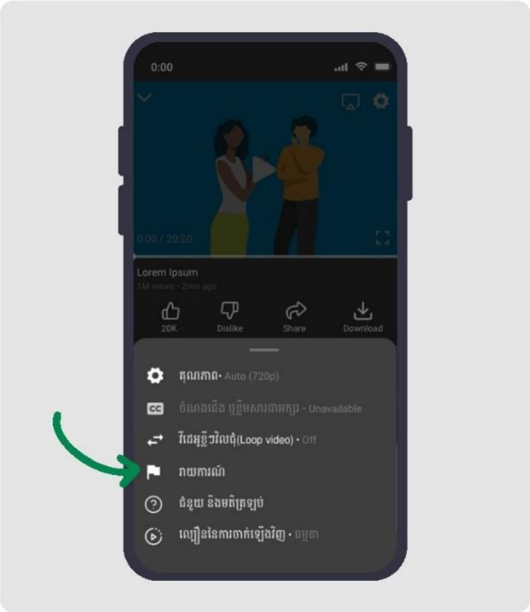
ឃ. ការរាយការណ៍នៅលើថ្នាលកម្មវិធី YouTube



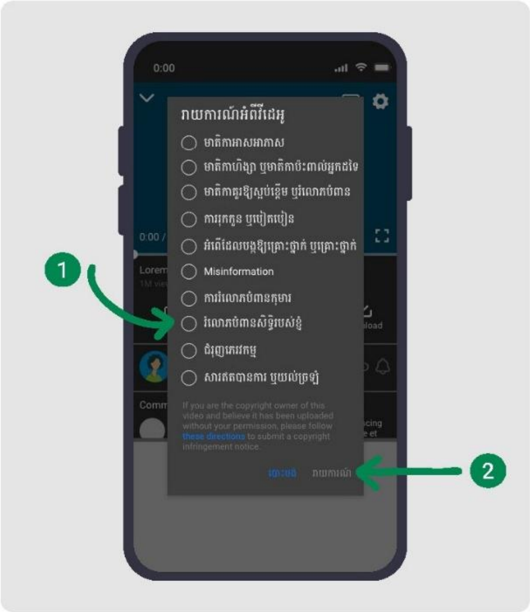
១.ជ្រើសរើសវីដេអូ



២.ចុចលើរូប “Settings”



៣.ចុចលើពាក្យ “Report”



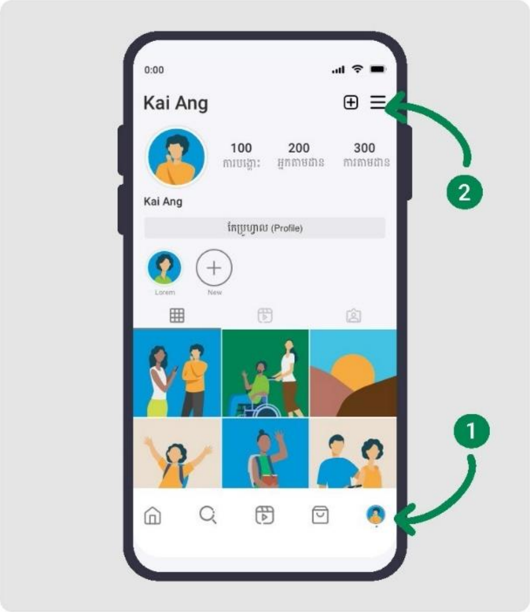
៤.ជ្រើសរើសមូលហេតុក្នុងបញ្ជី បន្ទាប់មកចុច លើពាក្យ “report”

៦. ការកំណត់ទីតាំង នៅលើថ្នាលកម្មវិធី WhatsApp

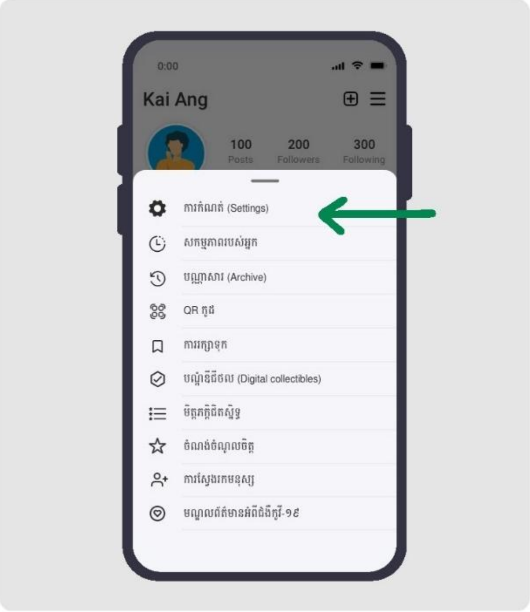
- ចុចបើកលើ "Settings" នៅក្នុងឧបករណ៍របស់អ្នក។ ចូរចងចាំថា វាមិនស្ថិតនៅក្នុងកម្មវិធី WhatsApp ដោយស្វ័យប្រវត្តិទេ។ "Settings" ជាទូទៅ មានរាងដូចកងចក្រ ឬស្ពឺ
- ស្វែងរកការអនុញ្ញាតកម្មវិធី ដែលមាននៅក្នុងបញ្ជី
- អូសលើអេក្រង់ហើយរកពាក្យ "WhatsApp"
- ស្វែងរក "Location" នៅក្នុង "Settings"
- ជ្រើសរើសការកម្រិត ដូចជា "Never" "Don't allow" ឬ "Ask every time"

៧. ការច្រោះ និងកម្រិត

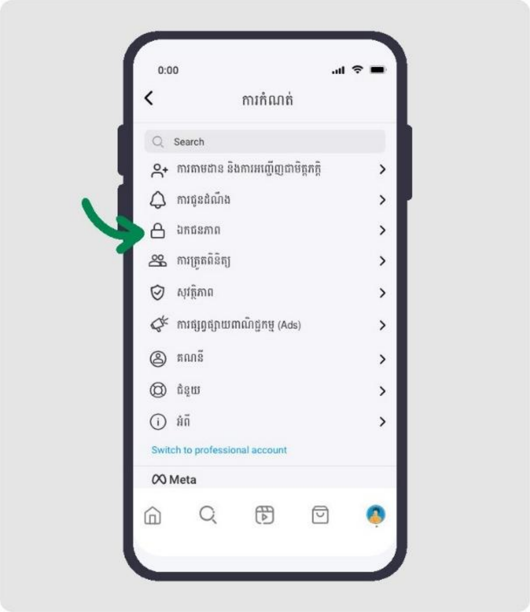
ក. ការច្រោះ និងកម្រិតនៅលើផ្ទាលកម្មវិធី Instagram



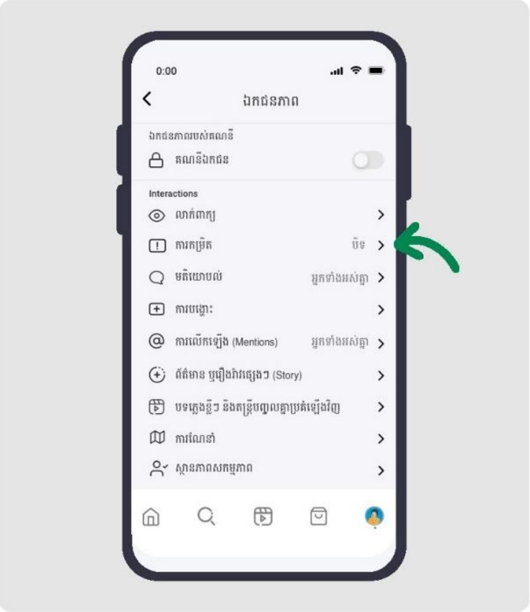
១. បើកកម្មវិធី Instagram រួចជ្រើសរើសប្រូហ្វាល(Profile) របស់អ្នក



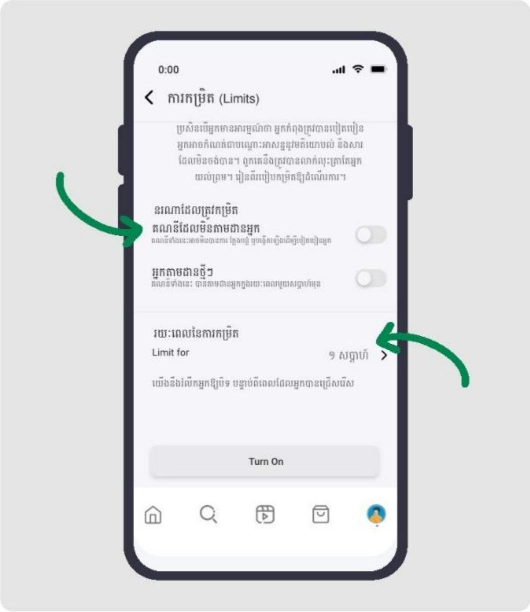
២. ជ្រើសរើស “Settings” ពីបញ្ជីផ្ទាំងដែលលេចឡើង

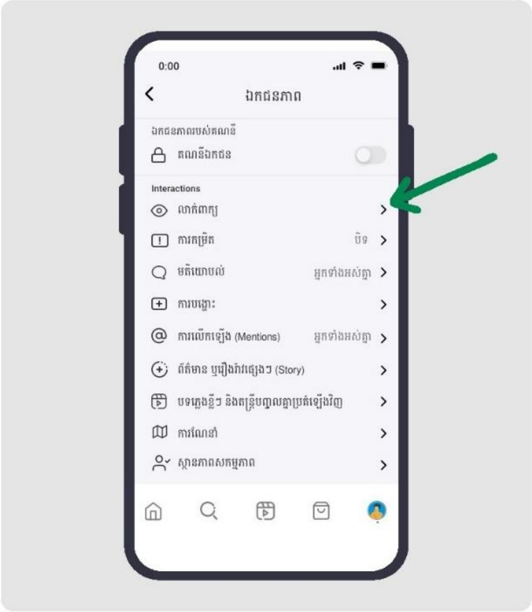


៣. ជ្រើសរើស “privacy” ដែលមានរូបសោ ជាតំណាង



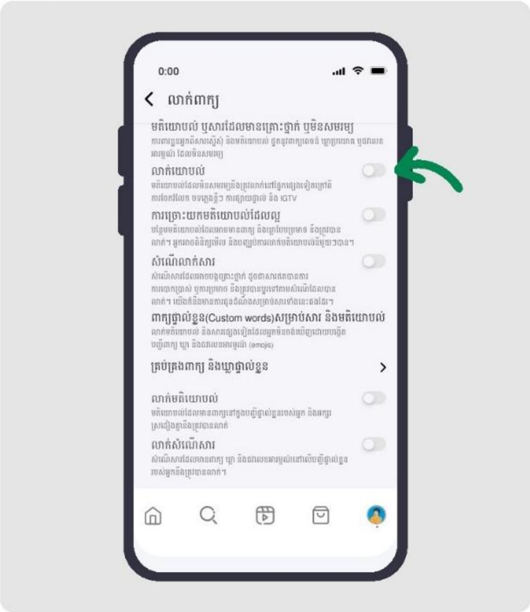
៤. បន្ទាប់មក ជ្រើសរើសពាក្យ “limit”

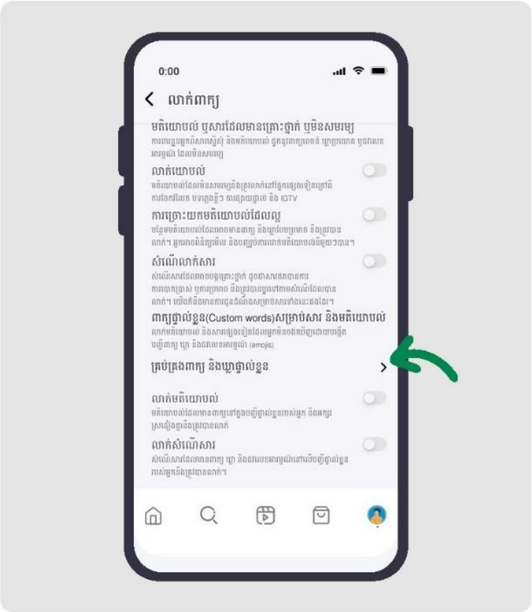




៥. នៅទីនេះ អ្នកអាចកម្រិតមនុស្សដែលអាចសរសេរ មតិយោបល់នៅលើគណនីរបស់អ្នក បានរហូតដល់ ៤ សប្ដាហ៍។

៦. ជ្រើសរើស "hidden word" បញ្ជីឯកជនភាពក៏អាចឱ្យ អ្នកធ្វើការកំណត់អំពីមាតិកាមិនសមរម្យ

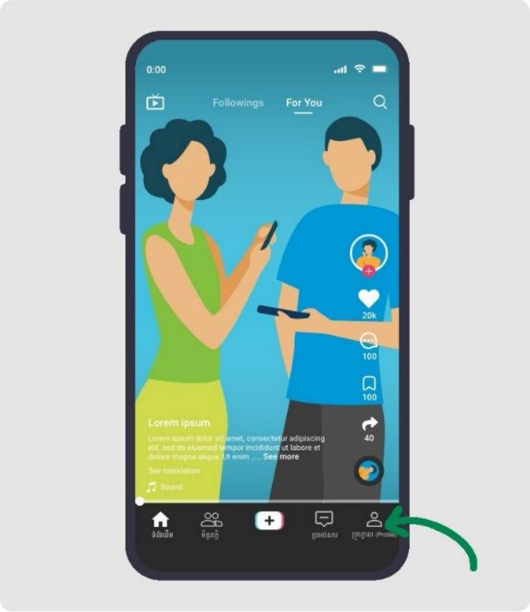


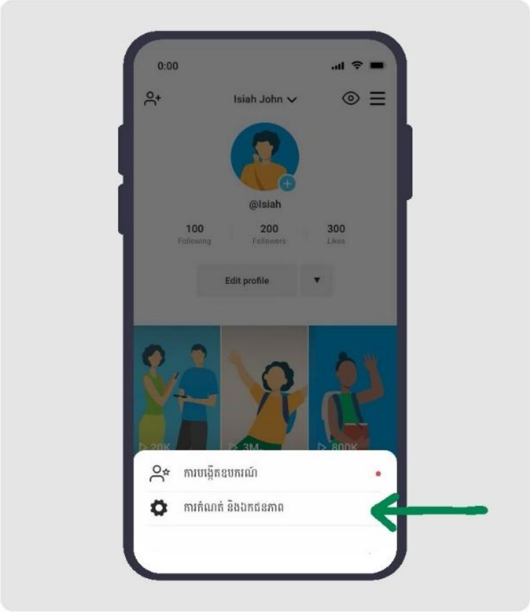


៧. ចុច "hidden comments" និង "hide message request" ដើម្បីឱ្យកម្មវិធី Instagram ធ្វើការច្រោះលើ មតិយោបល់ និងការស្នើសុំដែលមានលក្ខណៈមិនសមរម្យ ជាស្វ័យប្រវត្តិ

៨. មុខងារ "manage custom words and phrases" អា ត្រូវបានបង្កើតឡើងជាមួយនឹងពាក្យ ឃ្លា ឬជវលេខ អារម្មណ៍។ ជ្រើសរើសព្រួញដែលបង្ហាញខាងក្រោម ដើម្បី បន្ថែមឃ្លាទាំងនេះ។

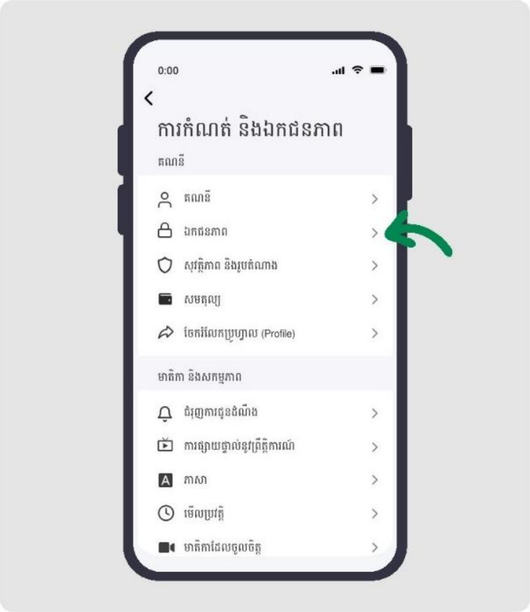
ខ. ការច្រោះ និងកម្រិតនៅលើថ្នាលកម្មវិធី TikTok

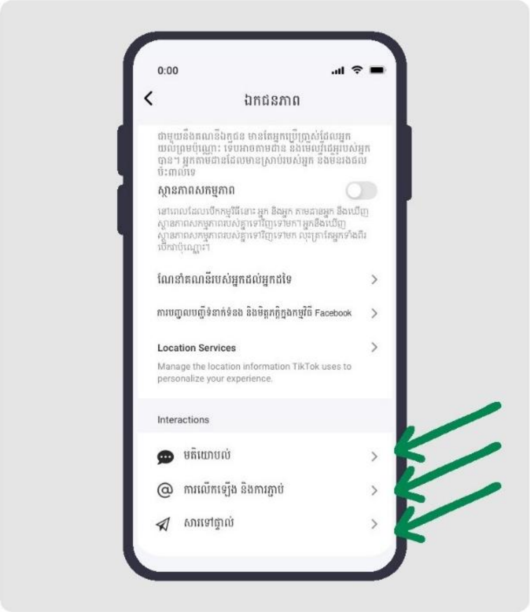




១.បើកកម្មវិធី TikTok នឹងជ្រើសរើសប្រូហ្វាល (Profile) របស់អ្នក

២. ជ្រើសរើស “setting និង privacy” ពីផ្ទាំងបញ្ជីដែលលេចឡើង



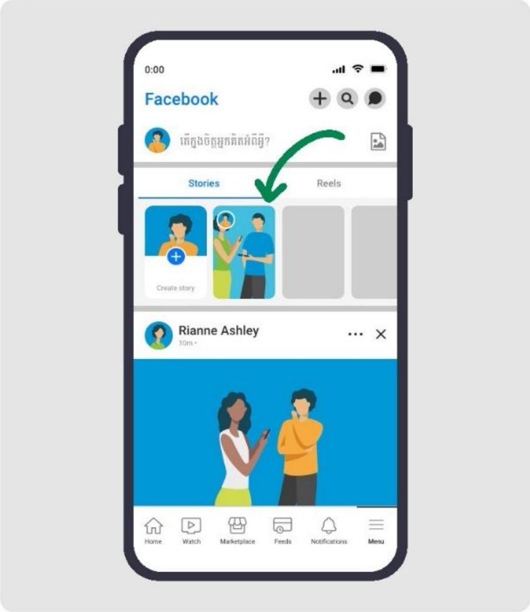


៣. ជ្រើសរើស “privacy” ដែលមានរូបសោ ជាតំណាង

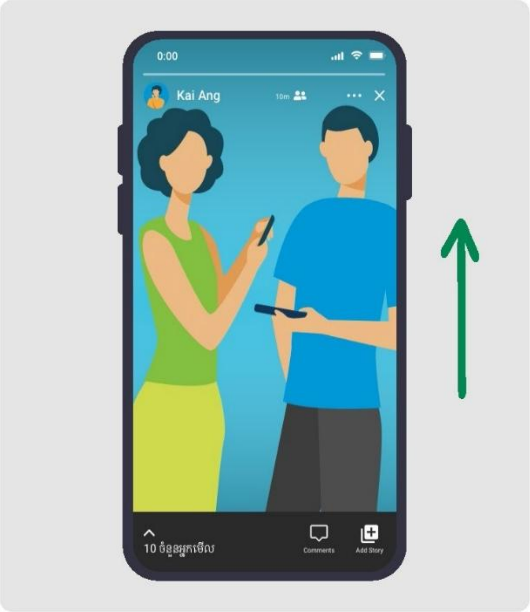
៤. បន្ទាប់មកជ្រើសរើសមួយក្នុងចំណោម comment, mentions, tag ឬ direct messages ដើម្បីកំណត់អ្នកផ្ញើ

៨. ការលាក់

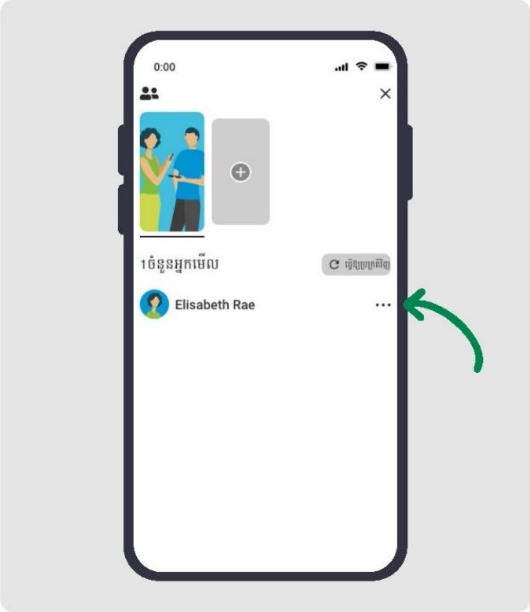
ក. ការលាក់នៅលើថ្នាលកម្មវិធី Facebook



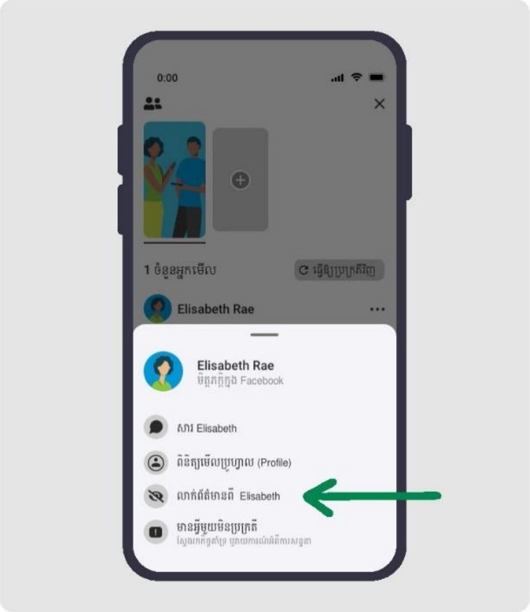
១ .បើកកម្មវិធី Facebook បន្ទាប់មកចុចលើព័ត៌មានរបស់អ្នក



២. អូសលើអេក្រង់របស់អ្នក

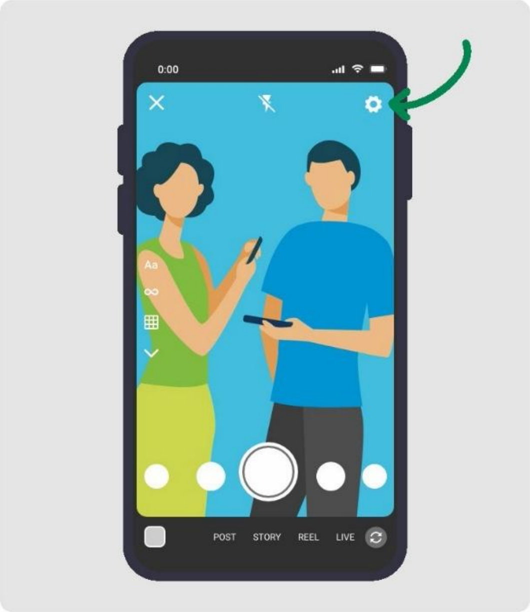


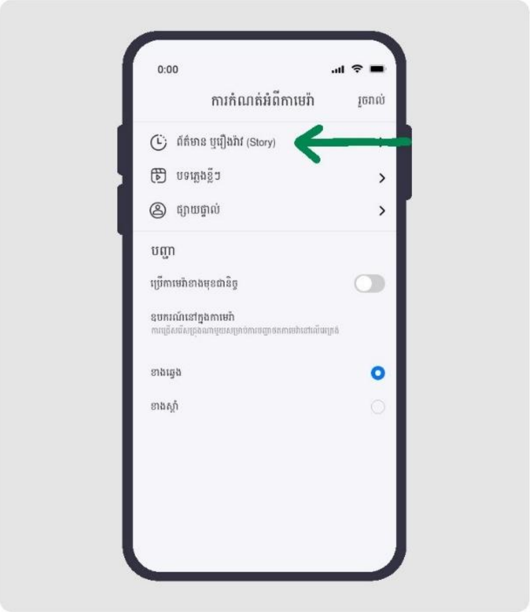
៣. ជ្រើសរើសចំណុច ចុចបី លើគណនីរបស់មនុស្សដែលអ្នកចង់លាក់ព័ត៌មាន



៤. ជ្រើសរើស "hide story" បន្ទាប់មកព័ត៌មានរបស់អ្នកនឹងលាក់ពីពួកគេ

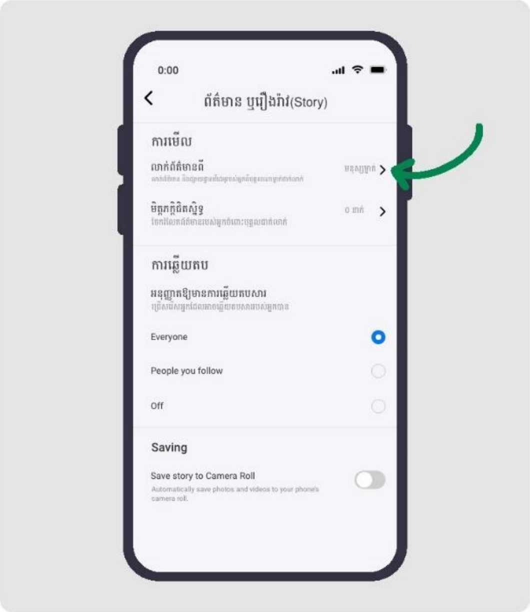
ខ. ការលាក់នៅលើថ្នាលកម្មវិធី Instagram

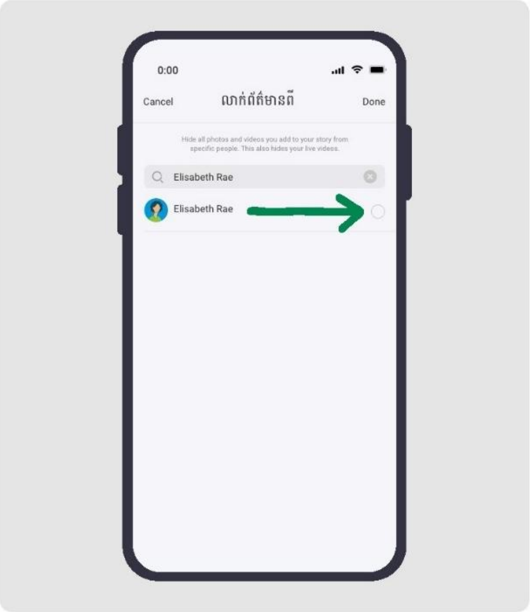




១. បើកកម្មវិធី Instagram រួចអូសទៅស្តាំដើម្បីបង្ហាញមុខងារ កាមេរ៉ា ហើយជ្រើសរើសការកំណត់មុខងារ

២. ជ្រើសរើស "story"





៣. ជ្រើសរើសពាក្យ 'hide story from"។ នៅក្នុងឧទាហរណ៍នេះ ព័ត៌មាន ឬរឿងរ៉ាវត្រូវបានលាក់ពីបុគ្គលណាម្នាក់រួចហើយ

៤. ជ្រើសរើស "Circle" សម្រាប់គណនីដែលអ្នកចង់លាក់ព័ត៌មានពីពួកគេ

ឧបសម្ព័ន្ធ២ ៖ កម្មវិធីអេបអប់រំស្តីពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ

សូមចូលទៅកាន់គេហទំព័រ https://app.swipesafe.org

ឬស្កេន QRcode ក្នុងរូបខាងក្រោមដើម្បីចូលប្រើកម្មវិធីអេប

កម្មវិធីអេបអប់រំអំពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញ (Swipe Safe App) ត្រូវបានបង្កើតឡើងក្នុងគោលបំណងផ្តល់នូវការសិក្សា អំពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញពេញលេញមួយ ដែលត្រូវបានរចនាឡើងសម្រាប់ស្វ័យសិក្សា ឬការសិក្សាដោយមានជំនួយពីអ្នកសម្របសម្រួល។ កម្មវិធីនេះផ្តល់អត្ថប្រយោជន៍យ៉ាងច្រើនដល់កុមារ និងយុវជន ដែលកំពុងស្ថិតនៅទីតាំងមិនមានអ្នកបណ្តុះបណ្តាលស្តីពីសុវត្ថិភាពកុមារតាមប្រព័ន្ធអនឡាញទៅដល់ ឬមិនអាចបណ្តុះបណ្តាលដោយផ្ទាល់បាន។ កម្មវិធីនេះ ផ្តល់ការគាំទ្រជាមូលដ្ឋានដល់ការសិក្សា អក្ខរកម្ម និងការអភិវឌ្ឍបំណិនជីវិត ដោយជួយបណ្តុះសមត្ថភាពលើបច្ចេកវិទ្យា និងអក្ខរកម្មឌីជីថល ការផ្ទង់អារម្មណ៍ ចិត្តសង្គម និងការត្រិះរិះពិចារណា។

សម្របសម្រួល និងសហការដឹកនាំរៀបចំដោយ៖

CAMBODIA NATIONAL COUNCIL FOR CHILDREN

ឧបត្ថម្ភគាំទ្រដោយ៖

ChildFund Cambodia

Swipe Safe developed by ChildFund