# សន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិតក្នុងបរិបទកម្ពុជា

បច្ចុប្បន្ននេះ ស្ទើរគ្រប់សកម្មភាពប្រចាំថ្ងៃរបស់យើង ដូចជា ការបំពេញការងារ ការរៀនសូត្រ ការទំនាក់ទំនង និងការកំសាន្តជាដើម ត្រូវពឹងផ្អែកលើអ៊ីនធឺណិត។ ក្នុងន័យនេះ គ្រប់សកម្មភាព និងប្រតិបត្តិការនៅតាមអ៊ីនធឺណិត តួយ៉ាង ការស្វែងរក (Browsing) ព័ត៌មាន, ការបញ្ជាទិញទំនិញតាមអនឡាញ, ការប្រើប្រាស់អ៊ីម៉ែល និងការទាញយកនៅតាមបណ្តាញអ៊ីនធឺណិត អាចប្រឈមនឹងការគំរាមកំហែងមួយចំនួន ដូចជា ការបន្លំ (Phishing), ការឆ្លងមេរោគចូលក្នុងប្រព័ន្ធកុំព្យូទ័រ, ការលួចចូល (Hack) និងការលួចទិន្នន័យជាដើម។ ដូច្នេះ ការយល់ដឹងពីសន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិតពិតជាមានសារៈសំខាន់ណាស់សម្រាប់បុគ្គលគ្រប់រូប ក៏ដូចជាស្ថាប័នរដ្ឋ និងឯកជន ដើម្បីបង្ការការខូចខាតដោយសារតែហានិភ័យតាមប្រព័ន្ធអ៊ីនធឺណិតនេះ។ យោងតាមគេហទំព័រ McAfee **«សន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិត»** (Internet Security) ជាផ្នែកសំខាន់មួយ**នៃសន្តិសុខសាយប័រ** (Cybersecurity) ដែលផ្តោតលើការការពារពីការគំរាមកំហែងនានាតាមប្រព័ន្ធអ៊ីនធឺណិត ដែលរួមបញ្ចូលទាំងការលួចចូលប្រព័ន្ធកុំព្យូទ័រ អាសយដ្ឋានអ៊ីម៉ែល និងគេហទំព័រ, មេរោគ (Malware) ដែលអាចឆ្លង និងបំផ្លាញប្រព័ន្ធនានា និងការលួចទិន្នន័យផ្ទាល់ខ្លួនទាក់ទងនឹងព័ត៌មានគណនីធនាគារ និងលេខកាតឥណទានជាដើម។

ខណៈដែលបច្ចេកវិទ្យាកាន់តែរីកចម្រើនជាលំដាប់ អ្នកវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតក៏កាន់តែស្វែងរកគន្លឹះ និងវិធីសាស្ត្រថ្មីៗក្នុងការប្រព្រឹត្តល្មើស ដើម្បីចំណេញប្រាក់បានកាន់តែច្រើន។ យោងតាមគេហទំព័រ Techopedia កាលពីឆ្នាំ ១៩៧១ មេរោគកុំព្យូទ័រដំបូងគេត្រូវបានបង្កើតឡើងដោយលោក Bob Thomas ដែលមានឈ្មោះថា **Creeper**។ បន្ទាប់មក នៅក្នុងទសវត្សរ៍ឆ្នាំ ៨០ **ការលួចចូល** (Hack) ក៏ចាប់ផ្តើមកើតមានឡើង ហើយមេរោគកុំព្យូទ័រប្រភេទ Worm ត្រូវបានបង្កើតឡើងជាបន្តបន្ទាប់ ដោយក្នុងនោះមេរោគ **Brain** ត្រូវបានគេស្គាល់ថាជាមេរោគ **Worm** ដំបូងគេ។ ក្រោយមកទៀត នៅក្នុងទសវត្សរ៍ឆ្នាំ ៩០ យើងបានឃើញពីវត្តមាននៃមេរោគប្រភេទ **Malware** ដែលជាមេរោគប្រើសម្រាប់**ការបន្លំ** (Phishing)។ អ្នកបន្លំ (Phisher) បានធ្វើការបោកបញ្ឆោតតាមរយៈអ៊ីម៉ែល និងគេហទំព័រនានាដោយទាក់ទាញឱ្យយើងផ្តល់នូវព័ត៌មានផ្ទាល់ខ្លួនដល់ពួកគេ។ បច្ចុប្បន្ន ចំនួនព័ត៌មានដែលបានបង្កើតនិងរក្សាទុកនៅលើអ៊ីនធឺណិតកំពុងកើនឡើងជាលំដាប់ ដែលអាចប្រឈមនឹងហានិភ័យខ្ពស់នៃការបំពានដោយពួក Hacker និងឧក្រិដ្ឋជនតាមប្រព័ន្ធអ៊ីនធឺណិត។ ការលួចអត្តសញ្ញាណបុគ្គលជាបញ្ហាចម្បងមួយដែលត្រូវយកចិត្តទុកដាក់ ហើយបើយោងតាមគេហទំព័រ Define Financial នៅឆ្នាំ២០២០ ការលួចអត្តសញ្ញាណនៅសហរដ្ឋអាមេរិកមានចំនួនរហូតដល់ប្រមាណ **១,៣លាន**ករណី។ ដូច្នេះ ជាមួយនឹងការវិវត្តន៍ឥតឈប់ឈរនៃការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិត យើងគួរយកចិត្តទុកដាក់ឱ្យ

បានហ្មត់ចត់លើសន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិត ព្រោះថាវាអាចជួយការពារឯកជនភាព និងអត្តសញ្ញាណរបស់យើង ព្រមទាំងអាចការពារកុំព្យូទ័ររបស់យើងពីការលួចចូល និងការឆ្លងមេរោគផងដែរ។ ចំពោះក្រុមហ៊ុនវិញ សន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិតអាចជួយរក្សាទំនុកចិត្តរបស់អតិថិជន ដោយហេតុថាព័ត៌មានរបស់ពួកគេត្រូវបានរក្សាទុកយ៉ាងមានសុវត្ថិភាព។

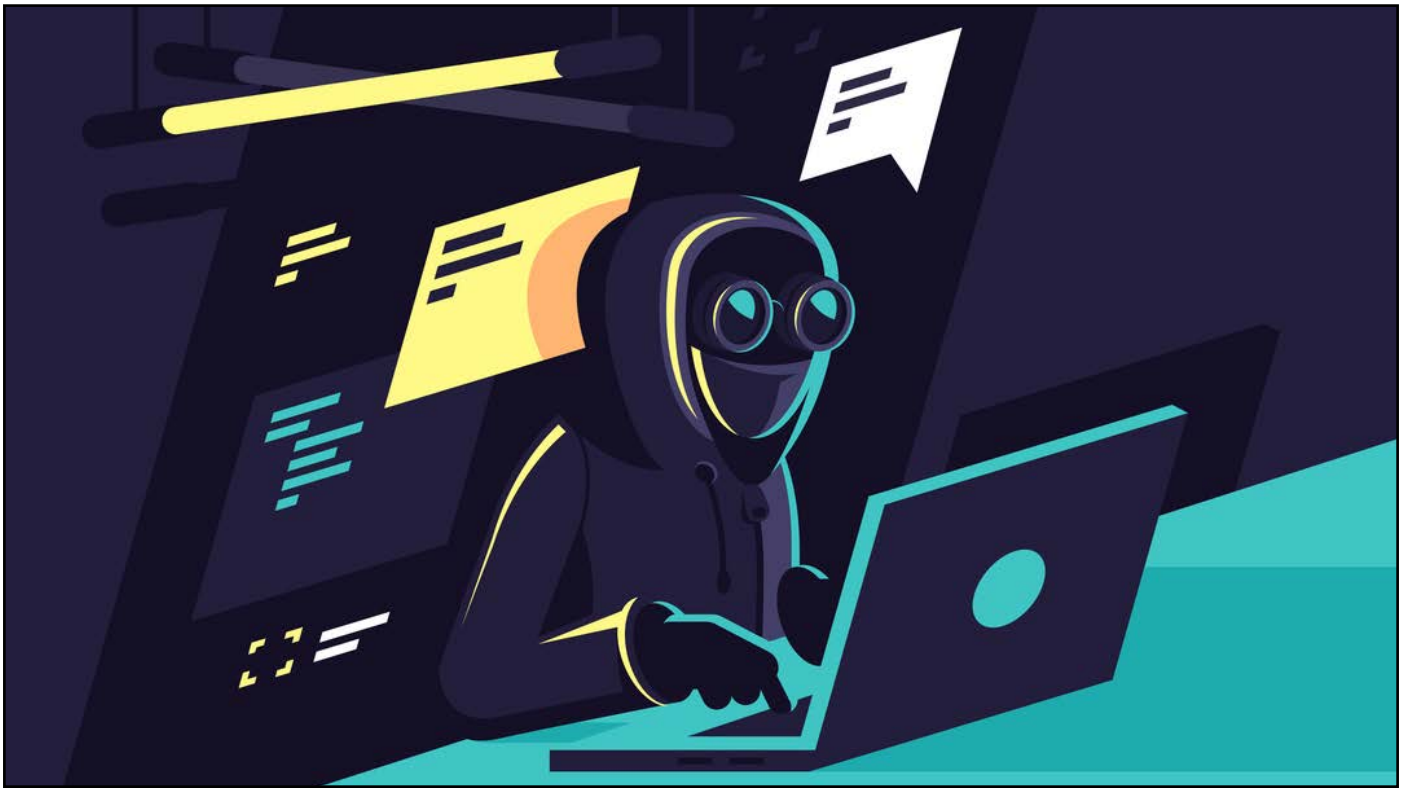
យោងតាមគេហទំព័រ Datareportal នៅដើមឆ្នាំ ២០២១ ប្រជាជនកម្ពុជាចំនួន **៨,៨៦ លាននាក់** ជាអ្នកប្រើប្រាស់អ៊ីនធឺណិត និង **១២ លាននាក់**ជាអ្នកប្រើប្រាស់បណ្តាញសង្គម។ មិនតែប៉ុណ្ណោះ ប្រព័ន្ធទូទាត់ប្រាក់នៅកម្ពុជាក៏មានការរីកចម្រើនគួរឱ្យកត់សម្គាល់ ហើយបើយោងតាមគេហទំព័រ Fresh News នៅឆ្នាំ ២០២១ ប្រតិបត្តិការទូទាត់តាមអេឡិចត្រូនិកនៅកម្ពុជាមានចំនួនប្រមាណ **៦៩៨,៨ លានប្រតិបត្តិការ** គិតជាទឹកប្រាក់ **១៩៩,៧៦ ប៊ីលានដុល្លារអាមេរិក** ស្មើនឹង **៧៨៧% នៃផលិតផលសរុប**។ ទិន្នន័យទាំងនេះបានបង្ហាញពីសញ្ញាណវិជ្ជមាននៃការចាប់យកបច្ចេកវិទ្យាក្នុងប្រទេសកម្ពុជា ប៉ុន្តែកម្ពុជាក៏អាចប្រឈមនឹងការកើនឡើងនៃហានិភ័យតាមប្រព័ន្ធអ៊ីនធឺណិតផងដែរ។ យោងតាម**នាយកដ្ឋានព័ត៌មានវិទ្យា នៃក្រសួងមហាផ្ទៃ** ប្រទេសកម្ពុជាកំពុងជួបប្រទះនូវការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតមួយចំនួន ដូចជា ការលួចកាន់កាប់គណនីបណ្តាញទំនាក់ទំនងសង្គម, ការបន្លំលួចប្រាក់ពីគណនីធនាគារ, ការឆ្លងមេរោគនៅលើកុំព្យូទ័រ និងទូរស័ព្ទដៃ និងការជ្រៀតចូលប្រព័ន្ធព័ត៌មានជាដើម។ ដូច្នេះការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតជាបញ្ហាប្រឈមមួយដែលយើងត្រូវយកចិត្តទុកដាក់ ដើម្បីប្រយុទ្ធប្រឆាំងនឹងការគំរាមកំហែងនានា និងទាញយកផលប្រយោជន៍ពេញលេញពីបច្ចេកវិទ្យាឌីជីថល។

## I. ការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិតក្នុងបរិបទកម្ពុជា

វត្តមាននៃជំងឺកូវីដ-១៩ ក៏ដូចជាបដិវត្តន៍ឧស្សាហកម្ម ៤.០ បានផ្លាស់ប្តូររបៀបរបបដែលប្រជាពលរដ្ឋបំពេញការងារ, ទំនាក់ទំនង, រៀនសូត្រ និងកំសាន្តជាដើម ដែលតម្រូវឱ្យពួកគាត់ត្រូវចេះសម្របខ្លួននឹងការប្រើប្រាស់បច្ចេកវិទ្យាក្នុងជីវភាពប្រចាំថ្ងៃ។ ហេតុនេះហើយ យើងបានឃើញពីកំណើននៃចំនួនអ្នកប្រើប្រាស់អ៊ីនធឺណិត, បណ្តាញសង្គម និងការទូទាត់តាមបែបឌីជីថលនៅកម្ពុជា។ ប៉ុន្តែទន្ទឹមនឹងកំណើននៃការប្រើប្រាស់បច្ចេកវិទ្យាក្នុងប្រទេស យើងក៏បានឃើញពីការកើនឡើងនៃឧក្រិដ្ឋកម្មតាមប្រព័ន្ធអ៊ីនធឺណិត ដែលបង្កជាហានិភ័យដល់ស្ថាប័នរដ្ឋ និងឯកជន និងប្រជាជនទូទៅផងដែរ។ ខាងក្រោមនេះជាការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិតសំខាន់ៗមួយចំនួននៅកម្ពុជា រួមមាន៖

**≫ *ការវាយប្រហារ DDoS (Distributed Denial-of-Service Attack)*៖** ក្នុងរយៈពេលប៉ុន្មានឆ្នាំចុងក្រោយនេះ ក្រុមហ៊ុននៅប្រទេសកម្ពុជា ពិសេសក្រុមហ៊ុនផ្តល់សេវាកម្មអ៊ីនធឺណិត បាននិងកំពុងជួបប្រទះការវាយប្រហារ DDoS។ ការវាយប្រហារនេះជាការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតដែលឧក្រិដ្ឋជនប្រើប្រាស់ចរាចរណ៍អ៊ីនធឺណិត (Internet Traffic) ដើម្បីធ្វើឱ្យស្ទះម៉ាស៊ីនមេ (Server) ដែលធ្វើឱ្យអតិថិជនមិនអាចប្រើប្រាស់សេវាកម្មរបស់ក្រុមហ៊ុនណាមួយបាន។ តួយ៉ាង នៅឆ្នាំ ២០១៨ ក្រុមហ៊ុនផ្តល់សេវាកម្មអ៊ីនធឺណិតមួយចំនួន ដូចជា EZECOM, SINET, Telcotech និងDigi បានរង

ការវាយប្រហារ DDoS នេះ ដែលធ្វើឱ្យសេវាកម្មអ៊ីនធឺណិតត្រូវផ្អាកវយៈពេលកន្លះថ្ងៃទូទាំងប្រទេស និងដើរយឺតវយៈពេលមួយសប្តាហ៍ពេញ។ ការវាយប្រហារនេះត្រូវបានគេសង្ស័យថាអាចមកពីក្រុមហ៊ុនមួយចង់បិទប្រតិបត្តិការអាជីវកម្មរបស់ក្រុមហ៊ុនដែលជាជនរងគ្រោះក្នុងការវាយប្រហារនេះ។



**មេរោគ Ransomware៖** យោងតាមក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ ករណីការវាយប្រហារដោយមេរោគ Ransomware នៅប្រទេសកម្ពុជាកំពុងមានការកើនឡើងជាលំដាប់ ហើយបាននិងកំពុងបង្កគ្រោះថ្នាក់យ៉ាងខ្លាំងដល់ប្រជាពលរដ្ឋ។ ជាក់ស្តែង យោងតាមគេហទំព័រ Kaspersky គិតត្រឹមដើមខែមករា ឆ្នាំ ២០២២នេះ ចំនួនការវាយប្រហារដោយមេរោគ Ransomware លើអតិថិជននៅកម្ពុជា មានចំនួនប្រមាណ **២៥ករណី**។ មេរោគនេះត្រូវបានឧក្រិដ្ឋជនប្រើប្រាស់ដើម្បីរារាំងការចូលដំណើរការឯកសារ ឬទិន្នន័យរបស់អ្នកប្រើប្រាស់ ដោយតម្រូវឱ្យអ្នកប្រើប្រាស់ធ្វើការបង់ប្រាក់តាមចំនួនកំណត់ ក្នុងរយៈពេលកំណត់ណាមួយ ដើម្បីអាចចូលដំណើរការឯកសារ ឬទិន្នន័យទាំងនោះឡើងវិញបាន។ បើពុំនោះទេ ឯកសារ ឬទិន្នន័យទាំងនោះអាចប្រឈមការបាត់បង់ជារៀងរហូត ឬក៏តម្លៃលោះអាចនឹងឡើងថ្លៃជាងមុន។ មេរោគនេះអាចឆ្លងចូលកុំព្យូទ័រតាមរយៈការទាញយកឯកសារ ឬកម្មវិធីដែលមិនមានប្រភពច្បាស់លាស់នៅតាមអ៊ីនធឺណិត។

**ការបន្លំ (Phishing)៖** យោងតាម**លោក អ៊ូ ជាន់ណារិទ្ធ** ប្រធាននាយកដ្ឋានសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មានវិទ្យា នៃក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ បានលើកឡើងថាអំឡុងពេលនៃការរីករាលដាលនៃជំងឺកូវីដ-១៩ ប្រទេសកម្ពុជាបានរងការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិតជាខ្លាំង ពិសេសគឺការបន្លំ។ ការបន្លំជាឧក្រិដ្ឋកម្មតាមប្រព័ន្ធអ៊ីនធឺណិតដែលប្រើប្រាស់យុទ្ធសាស្ត្រមួយចំនួន ដូចជា អ៊ីម៉ែល, គេហទំព័រក្លែងក្លាយ និងសារជាអក្សរ ដើម្បីបោកបញ្ឆោតជនរងគ្រោះឱ្យផ្តល់នូវព័ត៌មានផ្ទាល់ខ្លួន ដូចជា អាសយដ្ឋានរស់នៅ ថ្ងៃខែឆ្នាំកំណើត ឈ្មោះ លេខសម្ងាត់ធនាគារ និងលេខកាតឥណទានជាដើម។ បន្ទាប់មក ឧក្រិដ្ឋជនក្លែងបន្លំជាជនរងគ្រោះ ហើយប្រើប្រាស់ព័ត៌មានទាំងនេះដើម្បីធ្វើការស្នើសុំប័ណ្ណឥណទាន, ប្រើប្រាស់លុយនៅក្នុងគណនីធនាគារ ឬអាចស្នើសុំប្រាក់កម្ចីជាដើម។ នៅប្រទេសកម្ពុជា ការបោកបញ្ឆោតតាមរយៈអ៊ីម៉ែល ដែលមានផ្ទុកមេរោគ Malware ជាករណីដែលពេញនិយមជាងគេ ហើយបើយោងតាមគេហទំព័រ Kaspersky គិតត្រឹមដើមខែមករា ឆ្នាំ ២០២២នេះ ការផ្ញើអ៊ីម៉ែលដែលមានមេរោគ Malware មកអតិថិជននៅកម្ពុជា មានចំនួនប្រមាណ **១០ ៨៨៩ករណី**។

**ការបោកបញ្ឆោតតាមរយៈការស្នង់មតិលើប្រព័ន្ធអ៊ីនធឺណិត៖** បច្ចុប្បន្ននេះ នៅប្រទេសកម្ពុជា ការបោកបញ្ឆោតតាមប្រព័ន្ធអនឡាញមានការកើនឡើងជាលំដាប់ ពិសេសនៅតាមបណ្តាញសង្គមនានា។ ជាក់ស្តែង ជនបោកប្រាស់មួយចំនួនបានប្រើប្រាស់ឈ្មោះរបស់ក្រុមហ៊ុន H&M ដើម្បីបោកបញ្ឆោតឱ្យអ្នកលេងបណ្តាញសង្គមធ្វើការឆ្លើយសំណួរស្នង់មតិ តាមរយៈតំណ Link ដែលភ្ជាប់ទៅកាន់គេហទំព័រក្លែងក្លាយរបស់ក្រុមហ៊ុន H&M ព្រមទាំងឱ្យពួកគេធ្វើការចែករំលែកតំណ Link នេះទៅកាន់មិត្តភក្តិ នោះពួកគេនឹងទទួលបានកាតទូរស័ព្ទ ៥0 000រៀលពីក្រុមហ៊ុន។ ប៉ុន្តែ នៅពេលយើងធ្វើការចុចចូលតំណ Link នេះ ជនបោកប្រាស់ទាំងនោះនឹងធ្វើការប្រមូលទិន្នន័យផ្ទាល់ខ្លួន ដើម្បីធ្វើការលួចចូល (Hack) គណនីរបស់យើង ឬធ្វើការបញ្ជូលមេរោគចូលទៅក្នុងកុំព្យូទ័រ ឬទូរស័ព្ទរបស់យើងជាដើម។ មិនតែប៉ុណ្ណោះ ជនបោកប្រាស់មួយចំនួនក៏បានប្រើប្រាស់ឈ្មោះរបស់ក្រុមហ៊ុន Coca-Cola ដើម្បីធ្វើការចែកចាយតំណ Link ស្នង់មតិទាក់ទងនឹងមូលនិធិសុខុមាលភាព Coca-Cola នៅតាមបណ្តាញសង្គម Facebook និងTelegram ដោយបោកបញ្ឆោតថានៅពេលយើងបំពេញការស្នង់មតិរួច យើងអាចមានឱកាសឈ្នះទឹកប្រាក់ចំនួន ២00 000រៀល។ ប៉ុន្តែនៅពេលយើងបំពេញការស្នង់មតិនេះរួច ជនបោកប្រាស់ទាំងនោះនឹងធ្វើការលួចទិន្នន័យផ្ទាល់ខ្លួនរបស់យើង តួយ៉ាង អាសយដ្ឋានបច្ចុប្បន្ន និងលេខកាតឥណទានជាដើម។

## II. កិច្ចខិតខំប្រឹងប្រែងរបស់រដ្ឋាភិបាលក្នុងការការពារពីការគំរាមកំហែងនានាតាមប្រព័ន្ធអ៊ីនធឺណិត

បច្ចុប្បន្ននេះ សេដ្ឋកិច្ចនៃបណ្តាប្រទេសជុំវិញពិភពលោករួមទាំងកម្ពុជាបានពឹងផ្អែកកាន់តែខ្លាំងលើបច្ចេកវិទ្យា តួយ៉ាងពាណិជ្ជកម្មអេឡិចត្រូនិក ដូច្នេះ វិធានការសុវត្ថិភាពសម្រាប់ប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមប្រព័ន្ធអ៊ីនធឺណិតមានភាពចាំបាច់បំផុត ដើម្បីផ្តល់នូវបរិយាកាសសុវត្ថិភាពសម្រាប់អាជីវករ ក៏ដូចជាអ្នកទិញ។ ហេតុនេះហើយ រាជរដ្ឋាភិបាលកម្ពុជាបានដាក់ចេញនូវវិធានការសំខាន់ៗមួយចំនួន ដើម្បីឆ្លើយតបនឹងកំណើននៃឧក្រិដ្ឋកម្មតាមប្រព័ន្ធអ៊ីនធឺណិត និងផ្តល់នូវសុវត្ថិភាពដល់ប្រជាពលរដ្ឋគ្រប់រូប, ក្រុមហ៊ុន ក៏ដូចជាស្ថាប័នរដ្ឋាភិបាលផ្ទាល់ រួមមាន៖

**≫ សេចក្តីព្រាងច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យា៖** ក្នុងឆ្នាំ២០១២ រាជរដ្ឋាភិបាលកម្ពុជាបានប្រកាសពីដំណើរការនៃការតាក់តែងច្បាប់ស្តីពីបទល្មើសតាមអ៊ីនធឺណិត ហើយកាលពីឆ្នាំ២០២០ ក្រសួងមហាផ្ទៃបានរៀបចំកិច្ចប្រជុំ ដើម្បីពិគ្រោះយោបល់ជាមួយអ្នកជំនាញមកពីសហរដ្ឋអាមេរិកក្នុងគោលបំណងធ្វើឱ្យប្រសើរឡើងនូវសេចក្តីព្រាងច្បាប់បទល្មើសបច្ចេកវិទ្យានេះ។ វត្តមាននៃបណ្តាញសង្គមមួយចំនួនដូចជា Facebook និងInstagram, គេហទំព័រ និងកម្មវិធីទូរស័ព្ទនានា បានធ្វើឱ្យប្រជាជនកម្ពុជាចាប់ផ្តើមចេះប្រើប្រាស់ថ្នាលទាំងនេះដើម្បីប្រកបអាជីវកម្ម និងទិញទំនិញបានយ៉ាងលឿន និងងាយស្រួល។ ប៉ុន្តែវាក៏ជាឱកាសដែលអ្នកវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតអាចឆ្លៀតឱកាសក្នុងការបោកបញ្ឆោត, លួចចូល (Hack) ដើម្បីលួចព័ត៌មានឯកជន និងដាក់ចេញនូវកម្មវិធីមេរោគជាដើម ដែលអាចឱ្យប្រជាពលរដ្ឋរងគ្រោះផ្នែកហិរញ្ញវត្ថុ និងអាជីវកម្មបាត់បង់កេរ្តិ៍ឈ្មោះ។ ហេតុនេះហើយ រាជរដ្ឋាភិបាលបានបង្កើតសេចក្តីព្រាងច្បាប់នេះឡើងក្នុងគោលបំណងធ្វើឱ្យការប្រើប្រាស់បច្ចេកវិទ្យានៅកម្ពុជាមានសុវត្ថិភាព ហើយជាមួយនឹងការបង្កើតច្បាប់ដែលគោរពតាមស្តង់ដាអន្តរជាតិនេះ កម្ពុជាក៏អាចទាក់ទាញក្រុមហ៊ុន និងវិនិយោគិនក្នុងវិស័យបច្ចេកវិទ្យាបន្ថែមទៀតផងដែរ។ មិនតែប៉ុណ្ណោះ យោងតាម**លោក អ៊ូ ជាន់ណាវិទ្ធ** ប្រធាននាយកដ្ឋានសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មានវិទ្យា នៃក្រសួងប្រៃសណីយ៍និងទូរគមនាគមន៍ បានលើកឡើងថាច្បាប់ស្តីពីបទល្មើសបច្ចេកវិទ្យានេះអាចនឹងត្រូវបានអនុម័តដាក់ឱ្យប្រើប្រាស់នៅក្នុងឆ្នាំ២០២២នេះ។

**≫ វគ្គបណ្តុះបណ្តាលតាមប្រព័ន្ធអ៊ីនធឺណិតសម្រាប់គ្រូបង្រៀន ស្តីពី សន្តិសុខសាយប័រ៖** ក្រសួងអប់រំបានរៀបចំវគ្គបណ្តុះបណ្តាលតាមប្រព័ន្ធអ៊ីនធឺណិតសម្រាប់គ្រូបង្រៀននៅកម្រិតវិទ្យាល័យ ស្តីពីសន្តិសុខសាយប័រ ក្នុងបរិបទនៃការរៀនពីចម្ងាយនៅអំឡុងពេលនៃការរីករាលដាលនៃជំងឺកូវីដ-១៩។ វគ្គបណ្តុះបណ្តាលនេះបានផ្តោតលើអក្ខរកម្មប្រព័ន្ធផ្សព្វផ្សាយ (Media Literacy), ការកំណត់អត្តសញ្ញាណព័ត៌មានក្លែងក្លាយ, វិធានការសុវត្ថិភាពតាមប្រព័ន្ធអ៊ីនធឺណិត និងការការពារឯកជនភាពលើបណ្តាញសង្គម។ វគ្គបណ្តុះបណ្តាលនេះបង្កើតឡើងក្នុងគោលបំណងលើកទឹកចិត្តឱ្យលោកគ្រូ អ្នកគ្រូចែករំលែកចំណេះដឹងទាំងនេះបន្តទៅកាន់សិស្សានុសិស្ស។

**≫ សន្និសីទអន្តរជាតិ ស្តីពី សន្តិសុខសាយប័រ៖** កាលពីខែវិច្ឆិកា ឆ្នាំ២០១៩ កម្ពុជាបានរៀបចំសន្និសិទ

អន្តរជាតិ ស្តីពីសន្តិសុខសាយប័រ ដែលមានការចូលរួមពីសំណាក់បណ្តាប្រទេសក្នុងតំបន់អាស៊ីប៉ាស៊ីហ្វិច។ សន្និសីទនេះរៀបចំឡើងក្នុងគោលបំណងផ្តល់នូវការយល់ដឹងអំពីនិន្នាការក្នុងប្រទេស និងក្នុងតំបន់ទាក់ទងនឹងឧក្រិដ្ឋកម្ម និងសន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិត ដោយហេតុថា គិតត្រឹមឆ្នាំ ២០១៩ ក្រុមហ៊ុនជាង ៩០% នៅតំបន់អាស៊ីប៉ាស៊ីហ្វិចបានរងគ្រោះដោយសារការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិត ដែលតម្រូវឱ្យមានការយកចិត្តទុកដាក់ពីគ្រប់ភាគីពាក់ព័ន្ធ។

- **ការិយាល័យ "ASEAN Cyber Capability Desk"៖** ក្រៅពីវិធានការការពារពីការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិតនៅក្នុងប្រទេស រាជរដ្ឋាភិបាលកម្ពុជាក៏បានបង្ហាញពីការប្តេជ្ញាចិត្តក្នុងការសហការជាមួយប្រទេសជាសមាជិកផ្សេងទៀតនៅក្នុងតំបន់អាស៊ានផងដែរ។ ការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតនេះអាចរារាំងបណ្តាប្រទេសជាសមាជិកអាស៊ានរួមទាំងកម្ពុជាក្នុងការទាញយកនូវសក្តានុពលពេញលេញពីសេដ្ឋកិច្ចឌីជីថល។ ដូច្នេះ កម្ពុជាបានចូលរួមសហការជាមួយសមាជិកដទៃទៀតក្នុងការបង្កើត **ការិយាល័យ** «ASEAN Cyber Capability Desk» កាលពីឆ្នាំ ២០១៨ ដើម្បីរួមគ្នាដោះស្រាយបញ្ហាប្រឈមទាក់ទងនឹងឧក្រិដ្ឋកម្មតាមប្រព័ន្ធអ៊ីនធឺណិតក្នុងតំបន់ប្រកបដោយប្រសិទ្ធភាព។

- **សេចក្តីថ្លែងការណ៍អាស៊ាន-សហភាពអឺរ៉ុប ស្តីពី កិច្ចសហប្រតិបត្តិការសន្តិសុខសាយប័រ (ASEAN-EU Statement on Cybersecurity Cooperation)៖** លើសពីនេះទៀត កម្ពុជាក៏បានប្តេជ្ញាចិត្តក្នុងការប្រយុទ្ធប្រឆាំងនឹងការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិតជាមួយដៃគូក្រៅតំបន់ តួយ៉ាង សហភាពអឺរ៉ុប។ ជាក់ស្តែង កាលពីឆ្នាំ ២០១៩ កម្ពុជា និងបណ្តាប្រទេសជាសមាជិកអាស៊ានដទៃទៀតបានដាក់ចេញសេចក្តីថ្លែងការណ៍រួមជាមួយសហភាពអឺរ៉ុបក្នុងការបង្ហាញពីការប្តេជ្ញាចិត្តពង្រឹងកិច្ចសហប្រតិបត្តិ និងចែករំលែកគ្នានូវឧត្តមានុវត្ត ដើម្បីឆ្លើយតបនឹងបញ្ហាឧក្រិដ្ឋកម្មតាមប្រព័ន្ធអ៊ីនធឺណិតក្នុងតំបន់ទាំងពីរ។

- **ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា៖** នៅក្នុងក្របខណ្ឌនេះ រាជរដ្ឋាភិបាលកម្ពុជាបានបង្ហាញពីការប្តេជ្ញាចិត្តយ៉ាងម៉ឺតមាំក្នុងការប្រយុទ្ធប្រឆាំងនឹងការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតតាមរយៈការបង្កើតនូវ **«គណៈកម្មាធិការសន្តិសុខឌីជីថល»** ដែលជាស្ថាប័នថ្នាក់ជាតិទទួលបន្ទុកលើបញ្ហាសន្តិសុខសាយប័រនេះ។

## III. គន្លឹះក្នុងការការពារពីការគំរាមកំហែងនានាតាមប្រព័ន្ធអ៊ីនធឺណិត

ការការពារពីការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិតមិនមែនត្រឹមតែជាតួនាទីរបស់រដ្ឋាភិបាលប៉ុណ្ណោះទេ តែប្រជាពលរដ្ឋគ្រប់រូបក៏ត្រូវយល់ដឹងពីវិធានការសុវត្ថិភាពសំខាន់ៗ ដែលអាចជួយឱ្យយើងជៀសផុតពីការវាយប្រហារនានាតាមប្រព័ន្ធអ៊ីនធឺណិតផងដែរ។ ខាងក្រោមនេះជាគន្លឹះសំខាន់ៗក្នុងការការពារខ្លួនពីការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិត ដូចជា៖

- **ជ្រើសរើសពាក្យសម្ងាត់ដែលរឹងមាំ៖** បញ្ហាចម្បងនៃការប្រើប្រាស់ពាក្យសម្ងាត់គឺមនុស្សមួយចំនួនតែងប្រើប្រាស់នូវពាក្យសម្ងាត់ដែលងាយស្រួលចាំ ដូចជា ១២៣៤៥៦ និងឈ្មោះរបស់យើងជាដើម

ដែលធ្វើឱ្យជនខិលខូច និងឧក្រិដ្ឋជនងាយស្រួលក្នុងការទាយ។ ដូច្នេះ យើងគួរប្រើប្រាស់នូវពាក្យសម្ងាត់ដែលមានភាពរឹងមាំ ហើយបើយោងតាមគេហទំព័រ Lafayette ពាក្យសម្ងាត់ដែលរឹងមាំមានលក្ខណៈ ដូចជា មានយ៉ាងតិច៨តួ, លាយឡំដោយអក្សរតូច និងអក្សរធំ, លេខ និងតួអក្សរ រួមជាមួយអក្សរពិសេសយ៉ាងតិចមួយ ដូចជា ! @ # ? ], មិនប្រើពាក្យក្នុងវចនានុក្រម, បង្កើតជាឃ្លាសម្ងាត់ផ្ទាល់ខ្លួន ដូចជា <my$tr0ng_Pa$$word> និងប្រើពាក្យសម្ងាត់ខុសពីឈ្មោះគណនី ព្រមទាំងមិនប្រើពាក្យសម្ងាត់ដដែលក្នុងគណនីផ្សេងគ្នា។ មិនតែប៉ុណ្ណោះ ដើម្បីជាជំនួយក្នុងការរក្សាទុកនូវពាក្យសម្ងាត់ច្រើន និងពិបាកចាំ យើងក៏អាចប្រើនូវកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Management Program) ផងដែរ។

**ប្រុងប្រយ័ត្ននូវអ្វីដែលយើងទាញយក (Download)៖** គោលដៅចម្បងរបស់ឧក្រិដ្ឋជនតាមប្រព័ន្ធអ៊ីនធឺណិតគឺបញ្ឆោតយើងឱ្យទាញយកកម្មវិធីដែលផ្ទុកមេរោគ Malware និងលួចព័ត៌មានផ្ទាល់ខ្លួនរបស់យើង។ ប្រសិនបើយើងទាញយកដោយមិនបានប្រុងប្រយ័ត្ន យើងអាចនឹងបំផ្លាញកុំព្យូទ័ររបស់យើង។ ដូច្នេះ យើងគួរជ្រើសរើសធ្វើការទាញយកពីគេហទំព័រណាដែលគួរឱ្យទុកចិត្តប៉ុណ្ណោះ ហើយធ្វើការស្កេនរកមេរោគមុនពេលធ្វើការទាញយក។ ជាក់ស្តែង កម្មវិធីមួយចំនួន ដូចជា Firefox, Google Chrome និង Safari ជាដើម អាចការពារយើងពីគេហទំព័រដែលផ្ទុកមេរោគ ដោយផ្តល់នូវការដាស់តឿនមុនពេលយើងធ្វើការបើកគេហទំព័រទាំងនោះ។

**ប្រុងប្រយ័ត្ននូវការបន្លំ (Phishing)៖** អ្នកវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតប្រើប្រាស់អ៊ីម៉ែល និងគេហទំព័រក្លែងក្លាយ ដើម្បីបញ្ឆោតឱ្យជនរងគ្រោះផ្តល់នូវព័ត៌មានផ្ទាល់ខ្លួន ហើយព័ត៌មានទាំងនេះត្រូវបានប្រើប្រាស់ ដើម្បីធ្វើការស្នើសុំប័ណ្ណឥណទាន, ប្រើប្រាស់លុយនៅក្នុងគណនីធនាគារ ឬអាចស្នើសុំប្រាក់កម្ចីជាដើម។ ដូច្នេះ យើងត្រូវប្រុងប្រយ័ត្ន និងជៀសវាងការចុចចូលតំណ Link, ឯកសារភ្ជាប់ និងអេក្រង់លេចឡើង (Pop-up screen) ណា ដែលមិនមានប្រភពច្បាស់លាស់។

**ធ្វើបច្ចុប្បន្នភាពកម្មវិធីកម្ចាត់មេរោគជាប្រចាំ៖** យោងតាម The Fact Site ជារៀងរាល់ខែ មានមេរោគកុំព្យូទ័រថ្មីៗ ប្រមាណជាង ៦ 000 ត្រូវបានបង្កើត។ មិនតែប៉ុណ្ណោះ ប្រសិនបើកុំព្យូទ័ររបស់យើងឆ្លងមេរោគ វាក៏អាចរីករាលដាលទៅឧបករណ៍ផ្សេងទៀតនៅក្នុងបណ្តាញតែមួយ។ ដូច្នេះការធ្វើបច្ចុប្បន្នភាពកម្មវិធីកម្ចាត់មេរោគជាប្រចាំពិតជាមានសារៈសំខាន់ណាស់ក្នុងការការពារកុំព្យូទ័ររបស់យើងពីការគំរាមកំហែងនានា។

**រក្សាព័ត៌មានផ្ទាល់ខ្លួន៖** ការចែករំលែកព័ត៌មានផ្ទាល់ខ្លួននៅលើអ៊ីនធឺណិតអាចធ្វើឱ្យឧក្រិដ្ឋជនតាមប្រព័ន្ធអ៊ីនធឺណិតងាយស្រួលក្នុងការលួចអត្តសញ្ញាណ ឬព័ត៌មានហិរញ្ញវត្ថុរបស់យើង។ ដូច្នេះយើងគួរប្រុងប្រយ័ត្ននូវរាល់ព័ត៌មានដែលយើងធ្វើការបង្ហោះ និងចែករំលែកនៅលើអ៊ីនធឺណិត ដែលព័ត៌មានទាំងនោះមានដូចជា ពាក្យសម្ងាត់, អាសយដ្ឋានរស់នៅ, លេខទូរស័ព្ទ, លេខកាតឥណទាន, ព័ត៌មានលិខិតឆ្លងដែន និងលេខប័ណ្ណបើកបរជាដើម។ ដោយឡែក បណ្តាញសង្គមមួយចំនួន ដូចជា

Facebook, Instagram, Twitter និងSnapchat មាននូវការកំណត់ឯកជនភាព (Privacy Setting) ដែលអនុញ្ញាតឱ្យយើងធ្វើការកំណត់នូវព័ត៌មានដែលអាចមើលឃើញដោយអ្នកដទៃ។

**≫ អនុវត្តការស្វែងរកដោយសុវត្ថិភាព៖** គ្រប់គេហទំព័រទាំងអស់មិនមែនសុទ្ធតែមានសុវត្ថិភាពនោះទេ ដូច្នេះយើងត្រូវប្រុងប្រយ័ត្ននូវគេហទំព័រណាដែលមានបង្ហាញសារ «ការភ្ជាប់របស់អ្នកមិនមានភាពឯកជន» (Your connection is not private) នៅលើ browser ព្រោះថាគេហទំព័រនេះមិនអាចទុកចិត្តបាន និងអាចបង្កបញ្ហាសុវត្ថិភាព ដូចជាការលួចទិន្នន័យជាដើម។ ម៉្យាងទៀត យើងក៏ត្រូវប្រុងប្រយ័ត្ននូវតំណ(Link) និងការផ្សាយពាណិជ្ជកម្ម (Ads) មួយចំនួនដែលអាចនាំយើងទៅកាន់គេហទំព័របន្លំ (Phishing Site) ផងដែរ។

**≫ រក្សាសុវត្ថិភាពនៃការតភ្ជាប់អ៊ីនធឺណិតជាមួយ VPN៖** នៅពេលយើងប្រើប្រាស់អ៊ីនធឺណិត ពិសេសប្រើប្រាស់ Wi-Fi សាធារណៈ អ្នកវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតអាចឆ្លៀតឱកាសលួចទិន្នន័យរបស់យើងបានយ៉ាងងាយស្រួល។ ដូច្នេះ យើងគួរប្រើប្រាស់ **«បណ្តាញឯកជននិម្មិត»** (Virtual Private Network-VPN) ព្រោះថាបណ្តាញនេះអាចជួយកែប្រែការតភ្ជាប់អ៊ីនធឺណិតរបស់យើងទៅជាឯកជន និងលាក់ទីតាំងរបស់យើង។ ការណ៍នេះ យើងអាចធ្វើការស្វែងរក (Browsing) និងទិញទំនិញអនឡាញបានយ៉ាងមានសុវត្ថិភាព ដោយមិនចាំបាច់បារម្ភថាមានពួក Hacker លួចព័ត៌មានគណនីធនាគាររបស់យើងឡើយ។

## IV. សន្និដ្ឋាន

ជារួម ជាមួយនឹងការរីកចម្រើនឥតឈប់ឈរនៃបច្ចេកវិទ្យា អ្នកវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតក៏កាន់តែស្វែងរកគន្លឹះ និងវិធីសាស្ត្រថ្មីៗក្នុងការប្រព្រឹត្តល្មើស ដើម្បីអាចទាញយកផលប្រយោជន៍កាន់តែច្រើនពីជនរងគ្រោះ ដែលបង្កជាហានិភ័យយ៉ាងខ្លាំងដល់ស្ថាប័នរដ្ឋ និងឯកជន ព្រមទាំងប្រជាពលរដ្ឋគ្រប់រូបដែលជាអ្នកប្រើប្រាស់អ៊ីនធឺណិត។ ការណ៍នេះ បានធ្វើឱ្យការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតក្លាយជាកង្វល់មួយសម្រាប់ប្រទេសជុំវិញពិភពលោករួមទាំងប្រទេសកម្ពុជាផងដែរ។ ដូច្នេះ ដើម្បីឆ្លើយតបទៅនឹងកំណើននៃការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិត ទាមទារឱ្យប្រទេសក្នុងសកលលោក រួមទាំងកម្ពុជា បន្តរឹតបន្តឹងនូវវិធានការសុវត្ថិភាពក្នុងស្រុក និងពង្រឹងកិច្ចសហប្រតិបត្តិការជាមួយប្រទេសក្នុងតំបន់ និងក្រៅតំបន់ ដើម្បីផ្លាស់ប្តូរ និងចែករំលែកនូវបទពិសោធន៍ និងឧត្តមានុវត្ត សំដៅលើកកម្ពស់សន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណិតទាំងនៅក្នុងស្រុក កម្រិតតំបន់ និងសកលលោក។ មិនតែប៉ុណ្ណោះ ការការពារពីការគំរាមកំហែងតាមប្រព័ន្ធអ៊ីនធឺណិតមិនមែនជាទំនួលខុសត្រូវទាំងស្រុងរបស់រដ្ឋាភិបាលនោះទេ ពោលគឺប្រជាពលរដ្ឋគ្រប់រូបត្រូវចេះស្វែងយល់បន្ថែមពីគន្លឹះក្នុងការការពារខ្លួនពីការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតនេះ ដើម្បីសុវត្ថិភាពផ្ទាល់ខ្លួន និងសុវត្ថិភាពរបស់ស្ថាប័នផងដែរ៕

## ឯកសារយោង


- *What Is Internet Security?, ចូលអានថ្ងៃទី១៧ ខែមករា ឆ្នាំ២០២២, https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-internet-security.html*
- *The Evolution of Internet Security, ចូលអានថ្ងៃទី ១៨ ខែមករា ឆ្នាំ២០២២, https://www.preferreditgroup.com/2018/05/11/the-evolution-of-internet-security/*
- *IDENTITY THEFT AND CREDIT CARD FRAUD STATISTICS 2022, ចូលអានថ្ងៃទី ១៨ ខែមករា ឆ្នាំ២០២២, https://www.definefinancial.com/blog/identity-theft-credit-card-fraud-statistics/*
- *DIGITAL 2021: CAMBODIA, ចូលអានថ្ងៃទី ១៨ ខែមករា ឆ្នាំ២០២២, https://datareportal.com/reports/digital-2021-cambodia*
- *ឆ្នាំ២០២១ ការទូទាត់ប្រាក់តាមប្រព័ន្ធអេឡិចត្រូនិកកើនឡើងខ្ពស់ គិតជាទឹកប្រាក់ជិត ២០០ប៊ីលានដុល្លារ, ចូលអានថ្ងៃទី ១៧ ខែមករា ឆ្នាំ២០២២, http://freshnewsasia.com/index.php/en/business/228262-2022-01-17-10-34-46.html*
- *Kaspersky SECURELIST: Kingdom of Cambodia, ចូលអានថ្ងៃទី ១៧ ខែមករា ឆ្នាំ២០២២, https://statistics.securelist.com/country/cambodia/mail-anti-virus/month*
- *Cybercrime Law Drafted Following the Rise of Cyber Attacks, ចូលអានថ្ងៃទី ១៩ ខែមករា ឆ្នាំ២០២២, https://zico.group/blog/legal-alert-cambodia-cybercrime-law-drafted-following-rise-cyber-attacks/*
- *Ministry holds consultations on draft tech crime law with US experts, ចូលអានថ្ងៃទី ២២ ខែមករា ឆ្នាំ២០២២, https://www.khmertimeskh.com/50734633/ministry-holds-consultations-on-draft-tech-crime-law-with-us-experts/*
- *Teachers learn about online security risks, ចូលអានថ្ងៃទី ២២ ខែមករា ឆ្នាំ២០២២, https://www.khmertimeskh.com/50854625/teachers-learn-about-online-security-risks/*
- *Cybergovernance in Cambodia: A Risk-Based Approach to Cybersecurity, ចូលអានថ្ងៃទី ២៣ ខែមករា ឆ្នាំ២០២២, https://www.ccc-cambodia.org/kh/download?file_id=3474&action=view&view_file_id=16014526135f743a45bb25a6.77181850*
- *Cambodia to host international cybersecurity conference, ចូលអានថ្ងៃទី ២៣ ខែមករា ឆ្នាំ២០២២, https://www.khmertimeskh.com/636876/cambodia-to-host-international-cybersecurity-conference/*
- *ASEAN Cybercrime Operations Desk, ចូលអានថ្ងៃទី ២៤ ខែមករា ឆ្នាំ២០២២,https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk*
- *ASEAN-EU Statement on Cybersecurity Cooperation, ចូលអានថ្ងៃទី ២៤ ខែមករា ឆ្នាំ២០២២,https://asean.org/wp-content/uploads/2021/09/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf*
- *Top 10 Internet Safety Rules & What Not to Do Online, ចូលអានថ្ងៃទី ២៤ ខែមករា ឆ្នាំ២០២២, https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online*

- *7 Ways to Stay Safe Online*, ចូលអានថ្ងៃទី ២៤ ខែមករា ឆ្នាំ២០២២, *https://www.chelseagroton.com/Home/Why-Chelsea-Groton/News-You-Can-Use/View-Article/ArticleId/56/7-Ways-to-Stay-Safe-Online*
- *Top 15 Internet Safety Rules for Everyone*, ចូលអានថ្ងៃទី ២៤ ខែមករា ឆ្នាំ២០២២, *https://clario.co/blog/top-internet-safety-rules/*
- *Cambodia´s ISPs hit by some of the biggest DDoS attacks in the country´s history*, ចូលអានថ្ងៃទី ២៥ ខែមករា ឆ្នាំ២០២២, *https://www.zdnet.com/article/cambodias-isps-hit-by-some-of-the-biggest-ddos-attacks-in-the-countrys-history/*
- បទល្មើសបច្ចេកវិទ្យាព័ត៌មាន កំពុងកើតមានក្នុងព្រះរាជាណាចក្រកម្ពុជា, នាយកដ្ឋានព័ត៌មានវិទ្យា ក្រសួងមហាផ្ទៃ *Department of IT, Ministry of Interior*, ចូលអានថ្ងៃទី ២៥ ខែមករា ឆ្នាំ២០២២, *https://www.facebook.com/IT.Department.MOI/photos/a.1175078316000142/1517138101794160*
- *Organized criminals bring new ransoming pandemic*, ចូលអានថ្ងៃទី ២៥ ខែមករា ឆ្នាំ២០២២, *https://www.phnompenhpost.com/national/organised-criminals-bring-new-ransoming-pandemic*
- *Pandemic sees email scams increase by more than 600 percent in 2020*, ចូលអានថ្ងៃទី ២៥ ខែមករា ឆ្នាំ២០២២, *https://www.khmertimeskh.com/50810860/pandemic-sees-email-scams-increase-by-more-than-600-percent-in-2020/*
- *AVI PERSPECTIVE ISSUE: 2020, No. 01 Cyberwarfare and Its Implications for Cambodia*, ចូលអានថ្ងៃទី ២៥ ខែមករា ឆ្នាំ២០២២, *https://www.asianvision.org/archives/publications/avi-perspective-issue-2020-no-01*
- *Ministry warns of online survey scam Cambodia*, ចូលអានថ្ងៃទី ២៦ ខែមករា ឆ្នាំ២០២២, *https://www.phnompenhpost.com/national/ministry-warns-online-survey-scam*
- *Phone card survey latest online scam*, ចូលអានថ្ងៃទី ២៦ ខែមករា ឆ្នាំ២០២២, *https://www.phnompenhpost.com/national/phone-card-survey-latest-online-scam*
- *សន្តិសុខសាយប័រ, កម្មវិធី ជជែកពីកម្ពុជា ៤.0, វាគ្មិនកិត្តិយស លោក អ៊ូ ផាន់ណារិទ្ធ ប្រធាននាយកដ្ឋានសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មានវិទ្យា នៃក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍, ផ្សាយផ្ទាល់កាលពីថ្ងៃទី ២៨ ខែមករា ឆ្នាំ២០២២*
- *ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា*, ចូលអានថ្ងៃទី ២៨ ខែមករា ឆ្នាំ២០២២, *https://www.ocm.gov.kh/wp-content/uploads/2021/06/ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច_និងសង្គមឌីជីថលកម្ពុជា_ឆ្នាំ២០២១_២០៣៥.pdf*

www.cambodia4point0.org

កម្ពុជា ៤.0 - Cambodia 4.0

cambodia_4.0

កម្ពុជា ៤.0 Cambodia 4.0

កម្ពុជា ៤.0 - Cambodia 4.0

កម្ពុជា ៤.0 - Cambodia 4.0

Cambodia 4.0 Center

Cambodia 4.0