

ដានជើងឌីជីថល (Digital Footprint)

នាយុគសម័យឌីជីថល ការធ្វើទំនាក់ទំនង, ការសិក្សា, ការបំពេញកិច្ចការងារ, ការកម្សាន្ត និង ការរស់នៅប្រចាំថ្ងៃ សុទ្ធតែពឹងផ្អែកលើអ៊ីនធឺណិត និងឧបករណ៍ឌីជីថល។ មនុស្សចំណាយពេល កាន់តែច្រើនឡើងនៅលើអនឡាញ ហើយគ្រប់សកម្មភាពនៃការប្រើប្រាស់អ៊ីនធឺណិតប្រចាំថ្ងៃអាចបង្កើត បានជាដានជើងឌីជីថល ដែលអ្នកប្រើប្រាស់ស្ទើរតែគ្រប់រូបមិនបានចាប់អារម្មណ៍ ព្រោះថាស្ទើរតែគ្រប់ សកម្មភាពនៅលើអ៊ីនធឺណិតបានបន្សល់ទុកនូវទិន្នន័យ ឬព័ត៌មាន ដែលអាចប្រើប្រាស់សម្រាប់ការ តាមដាន ការរក្សាទុក និងការវិភាគជាដើម។ ដូច្នេះ ដានជើងឌីជីថល (Digital Footprint) សំដៅលើ ដាននៃទិន្នន័យ ឬព័ត៌មាន ដែលអ្នកប្រើប្រាស់បន្សល់ទុកនៅពេលប្រើប្រាស់អ៊ីនធឺណិត។ អ្នកប្រើប្រាស់ អាចបន្សល់ទុកដាននៃទិន្នន័យដោយមិនបានដឹងខ្លួន តាមរយៈសកម្មភាពមួយចំនួន ដូចជា ការបង្ហោះ តាមបណ្តាញសង្គម, ការទិញទំនិញអនឡាញ, ការបំពេញព័ត៌មានអនឡាញ និងការចូលមើលគេហទំព័រ នានាជាដើម។ សកម្មភាពទាំងនេះអាចនឹងបន្សល់ទុកដានលើអ៊ីនធឺណិតជារៀងរហូត ដែលអាច ប៉ះពាល់ដល់ការបាត់បង់ឯកជនភាពនៃទិន្នន័យ និងការបន្តអត្តសញ្ញាណពីជនខិលខូចមួយចំនួន ជាដើម ប៉ុន្តែជាមួយគ្នានេះ ដានជើងឌីជីថលក៏អាចជួយឱ្យអាជីវកម្ម ឬក្រុមហ៊ុនអាចយល់ពីការប្រមូល ទិន្នន័យដោយភាពត្រឹមត្រូវ ដើម្បីអាចយកមកវិភាគពីអាកប្បកិរិយារបស់អតិថិជន ដែលអនុញ្ញាតឱ្យ អាជីវកម្ម ឬក្រុមហ៊ុនអាចផ្តល់ឱ្យនូវសេវាកម្មកាន់តែប្រសើរ។

I. ប្រភេទនៃ Digital Footprint

ដានជើងឌីជីថលត្រូវបានគេស្គាល់ថាជាដានជើងអនឡាញ ឬការបន្សល់ទុកដានរបស់អ្នក ប្រើប្រាស់នៅលើប្រព័ន្ធអ៊ីនធឺណិត។ មនុស្សមួយចំនួនហៅដានជើងឌីជីថលថាជាផ្លូវអត្តសញ្ញាណ លើអ៊ីនធឺណិត ព្រោះវាអាចបង្ហាញពីកន្លែង និងអាសយដ្ឋានដែលអ្នករស់នៅ និងសកម្មភាពដែល អ្នកបានធ្វើនៅលើប្រព័ន្ធអ៊ីនធឺណិត។ ដានជើងឌីជីថលក៏បង្ហាញអំពីអាកប្បកិរិយាអនឡាញរបស់ ប្រើប្រាស់ ដែលរួមបញ្ចូលពីរបៀប ដែលអ្នកប្រើប្រាស់ធ្វើអន្តរកម្មជាមួយគេហទំព័រ កម្មវិធី និងបណ្តាញ ផ្សព្វផ្សាយសង្គម។ បច្ចុប្បន្ននេះ ដានជើងឌីជីថលត្រូវបានបែងចែកជា ២ ប្រភេទសំខាន់ៗមាន៖

► Passive Digital Footprint

Passive Digital Footprint សំដៅលើទិន្នន័យរបស់អ្នកប្រើប្រាស់ត្រូវបានប្រមូលតាមរយៈ សកម្មភាព ដែលអ្នកប្រើប្រាស់បង្កើតដោយគ្មានចេតនា រួមមាន ការចូលទៅកាន់ Websites និង

ការទទួលយក Cookies, ទិន្នន័យទីតាំងពីទូរសព្ទ ឬកម្មវិធីរបស់អ្នក, ការទិញទំនិញអនឡាញ ឬការប្រើប្រាស់ Search Engine ផ្សេងៗដូចជា Google ឬ Bing ជាដើម។ ការចូលប្រើប្រាស់ Website នឹងបង្កើតដានជើងឌីជីថលរបស់អ្នកប្រើប្រាស់ម្នាក់ៗ តាមរយៈការទទួលយក Cookies, ប្រវត្តិស្វែងរក (Search) និងប្រវត្តិទិញទំនិញ។ ទិន្នន័យរបស់អ្នកប្រើប្រាស់នឹងត្រូវបានប្រមូលព្រោះតាមរយៈការទទួលយកលក្ខខណ្ឌនៃការប្រើប្រាស់គេហទំព័រទាំងនោះ។

► **Active Digital Footprint**

Active Digital Footprint កើតឡើងនៅពេលដែលអ្នកប្រើប្រាស់បន្សល់ទុកដោយចេតនា រួមមាន ការបង្ហោះនៅលើបណ្តាញផ្សព្វផ្សាយសង្គម (រូបថត, វីដេអូ, Tweet និង Status ជាដើម), សរសេរ Review ឬ Comments, បំពេញ Form អនឡាញ (ចុះឈ្មោះ - Sign Up ឬបង្កើតគណនី) ឬការផ្ញើអ៊ីមែល ឬសារ។ អ្នកប្រើប្រាស់បង្កើតដានសកម្មរបស់ពួកគេដោយចេតនា ទោះបីអ្នកប្រើប្រាស់ទាំងអស់មិនអាចយល់បានថាមានមនុស្សប៉ុន្មាននាក់អាចមើលឃើញការបង្ហោះរបស់ពួកគេ ឬរបៀបដែលទិន្នន័យរបស់ពួកគេអាចប្រើប្រាស់បាន។

► **ឧទាហរណ៍នៃដានជើងឌីជីថល**

ទាំងនេះជាសកម្មភាពប្រចាំថ្ងៃមួយចំនួន ដែលបង្កើតដានជើងឌីជីថលរបស់អ្នកប្រើប្រាស់៖

- ការបង្ហោះនៅលើ Facebook ឬ Instagram ឬថ្នាលផ្សេងៗ
- ការបំពេញបែបបទ ដើម្បីទទួលបានសៀវភៅអេឡិចត្រូនិកឥតគិតថ្លៃ
- ការចុចការផ្សព្វផ្សាយពាណិជ្ជកម្ម ដែលលេចឡើងនៅលើអេក្រង់របស់អ្នក
- ការចូលមើលគេហទំព័រ ដែលតាមដានអាសយដ្ឋាន IP របស់អ្នក
- ការប្រើប្រាស់សេវាកម្មផ្នែកលើទីតាំង ដូចជា Google Map
- ការសរសេរការវាយតម្លៃផលិតផលនៅលើគេហទំព័រ E-commerce
- ការចូលប្រើប្រាស់បណ្តាញ Wi-Fi នៅហាងកាហ្វេ ឬផ្សារទំនើប ឬសាធារណៈនានា
- ការរក្សាទុកព័ត៌មានលម្អិតអំពីការទូទាត់នៅលើគេហទំព័រទិញទំនិញ។

II. បញ្ហាប្រឈមនៃ Digital Footprint

ការប្រើប្រាស់អ៊ីនធឺណិតបានធ្វើឱ្យអ្នកប្រើប្រាស់បន្សល់ទុកនូវដានទិន្នន័យជាច្រើន ដែលបង្កជាហានិភ័យមួយចំនួនដូចខាងក្រោម៖

● **ការលួចអត្តសញ្ញាណ៖** ព័ត៌មានលម្អិត ដូចជា ឈ្មោះ ថ្ងៃខែឆ្នាំកំណើត និងអាសយដ្ឋានដែលបានដាក់នៅបណ្តាញផ្សព្វផ្សាយសង្គម និងបំពេញក្នុងទម្រង់អនឡាញនានា អាចត្រូវបានលួចប្រើប្រាស់ដោយជនខិលខូចនៅលើប្រព័ន្ធអ៊ីនធឺណិត។ ព័ត៌មានទាំងនេះអាចត្រូវបានប្រើដើម្បីក្លែងបន្លំធ្វើអត្តសញ្ញាណ ដើម្បីបម្រើដល់ផលប្រយោជន៍ផ្សេងៗ ហើយត្រូវចំណាយពេលវេលាយក្នុងការស្ដារអត្តសញ្ញាណឡើងវិញ។

● **ការបាត់បង់ឱកាសការងារ៖** និយោជកតែងតែពិនិត្យមើលលើបណ្តាញផ្សព្វផ្សាយសង្គមរបស់បេក្ខជនក្នុងអំឡុងពេលបេក្ខជនដាក់ពាក្យការងារ មុននឹងធ្វើការសម្រេចចិត្តជួល។ ការបង្ហោះមិនសមរម្យ មតិចម្រូងចម្រាស ឬកង្វះវិជ្ជាជីវៈលើអ៊ីនធឺណិតអាចជះឥទ្ធិពលអវិជ្ជមានដល់ឱកាសទទួលបានការងារ។

● **សុវត្ថិភាពផ្ទាល់ខ្លួន៖** ការចែករំលែកទីតាំងរបស់អ្នកនៅលើបណ្តាញផ្សព្វផ្សាយសង្គមអាចធ្វើឱ្យសុវត្ថិភាពផ្ទាល់ខ្លួនរបស់អ្នក និងមនុស្សជាទីស្រឡាញ់របស់អ្នកប្រឈមនឹងហានិភ័យ។ Cyberstalkers និងអ្នកគំរាមគំហែងផ្សេងទៀតអាចប្រើប្រាស់ព័ត៌មានទាំងនេះ ដើម្បីធ្វើការតាមដាន និងកំណត់គោលដៅរបស់អ្នក ដែលនឹងបង្កឱ្យមានគ្រោះថ្នាក់។

● **ការបោកប្រាស់តាមអ៊ីនធឺណិត៖** ជានជើងឌីជីថល អាចធ្វើឱ្យអ្នកក្លាយជាគោលដៅសម្រាប់ការបោកប្រាស់តាមអ៊ីនធឺណិត ដូចជា ការក្លែងក្លាយការវិនិយោគ និងការក្លែងបន្លំហាងលក់ទំនិញអនឡាញជាដើម។ ជាក់ស្តែង ប្រសិនបើគំរូឌីជីថលរបស់អ្នកបង្ហាញថាអ្នកចាប់អារម្មណ៍ក្នុងការវិនិយោគ លទ្ធភាពនៃការបោកប្រាស់ផ្នែកហិរញ្ញវត្ថុអាចនឹងកាន់តែខ្ពស់។



► ដំណោះស្រាយ

ដើម្បីកាត់បន្ថយហានិភ័យដែលអាចកើតមានឡើងដោយសារតែដានជើងឌីជីថល អ្នកគួរតែស្វែងយល់ពីចំណុចសំខាន់ៗដូចខាងក្រោម ដើម្បីជួយឱ្យការប្រើប្រាស់អ៊ីនធឺណិត និងបណ្តាញសង្គមមានសុវត្ថិភាព។

● **ពិនិត្យឡើងវិញនូវការកំណត់ឯកជនភាព៖** ការកំណត់ឯកជនភាពនៅលើបណ្តាញផ្សព្វផ្សាយសង្គមអនុញ្ញាតឱ្យអ្នកគ្រប់គ្រង អ្នកដែលអាចឃើញការបង្ហោះផ្សព្វផ្សាយ។ ឧទាហរណ៍ Facebook អនុញ្ញាតឱ្យអ្នកកំណត់ការបង្ហោះទៅកាន់មិត្តភក្តិ ឬកំណត់ឯកជនភាពផ្ទាល់ខ្លួន សម្រាប់អ្នកដែលអាចមើលឃើញការបង្ហោះជាក់លាក់ណាមួយ។

● **ជៀសវាងការចែករំលែកច្រើននៅលើបណ្តាញផ្សព្វផ្សាយសង្គម៖** បណ្តាញផ្សព្វផ្សាយសង្គមធ្វើឱ្យមានភាពងាយស្រួលក្នុងការភ្ជាប់ទំនាក់ទំនងជាមួយអ្នកដទៃ ប៉ុន្តែក៏អាចធ្វើឱ្យការចែករំលែកទិន្នន័យផ្ទាល់ខ្លួនមានភាពងាយស្រួលផងដែរ។ មុននឹងបង្ហាញទីតាំង ឬគម្រោងធ្វើដំណើរ ឬព័ត៌មានផ្ទាល់ខ្លួនត្រូវគិតគូរឱ្យបានល្អិតល្អន់ ជៀសវាងការបង្ហាញលេខទូរសព្ទ ឬអាសយដ្ឋានអ៊ីមែល នៅក្នុងបណ្តាញផ្សព្វផ្សាយសង្គម។

● **ជៀសវាងគេហទំព័រដែលមិនមានសុវត្ថិភាព៖** ត្រូវប្រាកដថាអ្នកកំពុងធ្វើប្រតិបត្តិការជាមួយគេហទំព័រដែលមានសុវត្ថិភាព URL គួរតែចាប់ផ្តើមដោយ https:// ជាជាង http://, “s” តំណាងឱ្យ “secure” ហើយបង្ហាញថាគេហទំព័រមានវិញ្ញាបនបត្រសុវត្ថិភាព។ វាក៏គួរតែមានរូបតំណាងសោនៅខាងឆ្វេងនៃរូបភាពអាសយដ្ឋានផងដែរ។ សូមប្រុងប្រយ័ត្នលើការចុចលើតំណភ្ជាប់ ឬទាញយកឯកសារ ពីប្រភពឬបុគ្គលចែករំលែកព័ត៌មានដែលមិនស្គាល់។

● **លុបគណនីចាស់៖** ដើម្បីកាត់បន្ថយដានជើងឌីជីថលរបស់អ្នក គឺលុបគណនីចាស់។ ការលុបគណនីអសកម្ម បានកាត់បន្ថយការប៉ះពាល់ទៅនឹងការបំពានទិន្នន័យដែលអាចកើតមាន និងកាត់បន្ថយការបែកធ្លាយទិន្នន័យសំខាន់ៗ។

● **បង្កើតពាក្យសម្ងាត់ខ្លាំង ហើយប្រើកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់៖** ពាក្យសម្ងាត់ខ្លាំង គឺពាក្យសម្ងាត់វែង យ៉ាងហោចណាស់ ១២ តួអក្សរ មានទាំងអក្សរធំ អក្សរតូច លាយបញ្ចូលគ្នា ឬក្រុមនិមិត្តសញ្ញា និងលេខ។ ពាក្យសម្ងាត់កាន់តែស្មុគស្មាញ វាកាន់តែពិបាកក្នុងការបំបែក ដែលជួយរក្សាសុវត្ថិភាពអ៊ីនធឺណិត។ ការប្រើប្រាស់កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់នឹងជួយបង្កើត រក្សាទុក និងគ្រប់គ្រងពាក្យសម្ងាត់ទាំងអស់នៅក្នុងគណនីអនឡាញដែលមានសុវត្ថិភាព។ ការរក្សាសុវត្ថិភាពទិន្នន័យទាំងនេះ ចាំបាច់ណាស់ក្នុងការរក្សាពាក្យសម្ងាត់ជាឯកជន, ជៀសវាងការចែករំលែកជាមួយអ្នកដទៃ ហើយព្យាយាមជៀសវាងការប្រើពាក្យសម្ងាត់ដូចគ្នាសម្រាប់គណនីទាំងអស់ និងឧស្សាហ៍ផ្លាស់ប្តូរឱ្យបានទៀងទាត់។

● **ធ្វើបច្ចុប្បន្នភាពកម្មវិធីឱ្យបានជាប់ជាប្រចាំ៖** ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតអាចចូលប្រើឧបករណ៍ និង ទិន្នន័យរបស់អ្នកបានយ៉ាងងាយស្រួល ដោយការទាញយកទិន្នន័យសំខាន់ៗនៅពីកម្មវិធីដែលមិនបាន ធ្វើបច្ចុប្បន្នភាព។ ដូច្នេះ អ្នកប្រើប្រាស់គួរធ្វើបច្ចុប្បន្នកម្មវិធីឱ្យបានជាប់ជាប្រចាំ ដើម្បីការពារកម្មវិធី ដែលអ្នកប្រើប្រាស់ពីការវាយប្រហារនានា។

III. អត្ថប្រយោជន៍នៃការយល់ដឹងពីដានជើងឌីជីថល

រាល់សកម្មភាពនៅលើអ៊ីនធឺណិត ទាំងការបង្ហោះ, ការចុច Like Share និង Comment, ការស្វែងរក ឬប្រតិបត្តិការអនឡាញតែងតែបន្សល់ទុកនូវដានជើងឌីជីថលរបស់អ្នកប្រើប្រាស់។ ដានជើងឌីជីថលអាចផ្តល់ឱ្យនូវបទពិសោធនៅលើអ៊ីនធឺណិតកាន់តែប្រសើរ និងងាយស្រួលជាងមុន ប៉ុន្តែក៏នាំមកនូវបញ្ហាប្រឈមមួយចំនួន ដែលអាចប៉ះពាល់ដល់ឯកជនភាព និងសុវត្ថិភាពអ្នកប្រើប្រាស់ ទាំងលើអនឡាញ និងផ្ទាល់ខ្លួនផងដែរ។ ដូច្នេះ ការយល់ដឹងពីដានជើងឌីជីថលពិតជាសំខាន់ និង ចាំបាច់សម្រាប់អ្នកប្រើប្រាស់ ដោយផ្តល់ឱ្យនូវអត្ថប្រយោជន៍ជាច្រើន ដូចខាងក្រោម៖

● **សុវត្ថិភាព និងអាកប្បកិរិយាទទួលខុសត្រូវ**

តាមរយៈការយល់ដឹងពីរបៀបដែលដានជើងឌីជីថលត្រូវបានបង្កើតឡើង អ្នកប្រើប្រាស់អាច កាន់តែមានការប្រុងប្រយ័ត្នចំពោះសកម្មភាពដែលពួកគេធ្វើនៅលើអ៊ីនធឺណិត។ ជាឧទាហរណ៍ ការប្រើពាក្យសម្ងាត់ខ្លាំង ការកែតម្រូវការកំណត់ឯកជនភាពនៅលើបណ្តាញផ្សព្វផ្សាយសង្គម និង ការជៀសវាងតំណភ្ជាប់គួរឱ្យសង្ស័យ អាចជួយការពារអ្នកប្រើប្រាស់ពីការលួចចូល ការគំរាមកំហែង ការក្លែងបន្លំ ឬការលួចអត្តសញ្ញាណជាដើម។ ដូច្នេះ ចំណេះដឹងនេះនឹងកាត់បន្ថយការខូចខាតពី ហានិភ័យនានា ដូចជា ការបំពានឯកជនភាព ប្រាក់កាក់ ពេលវេលា និងកិត្តិយស ជាពិសេសសុវត្ថិភាព ផ្ទាល់ខ្លួន។ បន្ថែមពីនេះ ការយល់ដឹងនេះក៏ជំរុញឱ្យការប្រើប្រាស់បច្ចេកវិទ្យាប្រកបដោយក្រមសីលធម៌ កាត់បន្ថយការផ្សព្វផ្សាយព័ត៌មានមិនពិត លើកទឹកចិត្តដល់ការប្រាស្រ័យទាក់ទងគ្នាប្រកបដោយ ការគោរព និងការបង្រៀនបុគ្គលឱ្យមានតុល្យភាពរវាងភាពងាយស្រួលជាមួយនឹងភាពឯកជនផងដែរ។

● **ការជួយបង្កើនប្រសិទ្ធភាពនៃដំណើរការអាជីវកម្ម**

ការយល់ដឹងបានច្បាស់ពីដានជើងឌីជីថលមិនត្រឹមតែអាចជួយអ្នកប្រើប្រាស់ឱ្យបង្កើនការ ប្រុងប្រយ័ត្ន និងគ្រប់គ្រងបាននូវព័ត៌មានដែលគួរ និងមិនគួរចែករំលែកប៉ុណ្ណោះទេ ប៉ុន្តែក៏ជួយអាជីវកម្ម និងក្រុមហ៊ុន ដែលជាអ្នកមានតម្រូវការទិន្នន័យ អាចយកទិន្នន័យមកប្រើប្រាស់ប្រកបដោយភាព ត្រឹមត្រូវ។ អាជីវកម្ម និងក្រុមហ៊ុន អាចធ្វើការវិភាគពីដានឌីជីថលរបស់អតិថិជនគោលដៅ ដើម្បី យល់ដឹងកាន់តែច្បាស់អំពីតម្រូវការ និងអាកប្បកិរិយារបស់អតិថិជន។ អាជីវកម្មអាចតាមដានលំនាំ ស្វែងរក (Browsing Patterns), Online Reviews ឬប្រវត្តិនៃការទិញដើម្បីណែនាំ ឬផ្តល់ឱ្យនូវ ផលិតផល ឬសេវាកម្មដែលមានលក្ខណៈផ្ទាល់ខ្លួន។ ជាក់ស្តែង គេហទំព័រពាណិជ្ជកម្មអេឡិចត្រូនិក

ប្រើប្រាស់ទិន្នន័យដែលទទួលបានពីដានជើងឌីជីថល ដើម្បីណែនាំផលិតផលឱ្យចំគោលដៅ ដែលនេះមិនត្រឹមតែបង្កើនការលក់ប៉ុណ្ណោះទេ ថែមទាំងបង្កើនការពេញចិត្តរបស់អតិថិជនផងដែរ។

● **ការជួយពង្រឹងការអនុវត្តច្បាប់ និងការដាក់ចេញគោលនយោបាយ**

រដ្ឋាភិបាលអាចពឹងផ្អែកលើដានជើងឌីជីថល ដើម្បីពង្រឹងការអនុវត្តច្បាប់ប្រយុទ្ធប្រឆាំងនឹងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត និងធានាសុវត្ថិភាព និងសន្តិសុខជាតិ។ ជាឧទាហរណ៍ ការវិភាគទិន្នន័យឌីជីថលជួយតាមដានសកម្មភាពខុសច្បាប់ ដូចជា ការក្លែងបន្លំតាមអ៊ីនធឺណិត ការជួញដូរ ឬព័ត៌មានមិនពិត។ លើសពីនេះ រដ្ឋាភិបាលអាចប្រើប្រាស់ទិន្នន័យនេះសម្រាប់ជាមូលដ្ឋានក្នុងការរៀបចំគោលនយោបាយនានាទាក់ទងនឹងបច្ចេកវិទ្យាឌីជីថល, ការកែលម្អអភិបាលកិច្ចតាមប្រព័ន្ធអេឡិចត្រូនិក និងការផ្តល់សេវាសាធារណៈឱ្យបានកាន់តែប្រសើរឡើង។

IV. ករណីសិក្សា៖

➤ **ការគ្រប់គ្រងដានជើងឌីជីថលរបស់ប្រទេសសិង្ហបុរី**

ប្រទេសសិង្ហបុរីត្រូវបានចាត់ទុកថាជាប្រទេស ដែលមានការគ្រប់គ្រងដានជើងឌីជីថលល្អបំផុតមួយ តាមរយៈការរួមបញ្ចូលគ្នានៃច្បាប់ដ៏តឹងរ៉ឹង គំនិតផ្តួចផ្តើមរបស់រដ្ឋាភិបាលដ៏រឹងមាំ និងការអប់រំសាធារណៈយ៉ាងទូលំទូលាយ។ ក្នុងនោះ យើងសង្កេតឃើញមានការជំរុញពីរដ្ឋាភិបាលដោយបានដាក់ចេញនូវច្បាប់សំខាន់ៗ ដូចជា ច្បាប់ការពារទិន្នន័យផ្ទាល់ខ្លួន (Personal Data Protection Act) គ្រប់គ្រងពីរបៀប ដែលស្ថាប័នឯកជនគ្រប់គ្រងទិន្នន័យផ្ទាល់ខ្លួន ខណៈដែលមានច្បាប់ផ្សេងទៀតគ្រប់គ្រងសុវត្ថិភាពតាមអ៊ីនធឺណិត និងឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។ បន្ថែមពីនេះ ប្រជាពលរដ្ឋក៏ជាតួអង្គមួយដែលចូលរួមយ៉ាងសកម្មផងដែរ ព្រមទាំងត្រូវបានជំរុញឱ្យកម្រិតអក្ខរកម្មឌីជីថលខ្ពស់តាមរយៈការផ្តល់នូវការបណ្តុះបណ្តាលអក្ខរកម្មឌីជីថលដោយរដ្ឋាភិបាល ដើម្បីការពារខ្លួនលើប្រព័ន្ធអ៊ីនធឺណិត។

➤ **បទប្បញ្ញត្តិរបស់រដ្ឋាភិបាល**

● **ច្បាប់ការពារទិន្នន័យផ្ទាល់ខ្លួន ២០១២ (Personal Data Protection Act)៖** គឺជាក្របខ័ណ្ឌច្បាប់ដែលគ្រប់គ្រងការការពារទិន្នន័យនៅក្នុងប្រទេសសិង្ហបុរី។ ច្បាប់នេះត្រួតពិនិត្យជាពិសេសលើការគ្រប់គ្រងទិន្នន័យផ្ទាល់ខ្លួននៅក្នុងវិស័យឯកជន និងកំណត់ថាក្រុមហ៊ុនត្រូវទទួលបានការយល់ព្រមច្បាស់លាស់ និងប្រើប្រាស់ទិន្នន័យក្នុងគោលបំណងសមហេតុផល ដើម្បីការពារទិន្នន័យផ្ទាល់ខ្លួនរបស់បុគ្គល។

● **Cybersecurity Act៖** បានអនុម័តក្នុងឆ្នាំ២០១៨ និងបានធ្វើបច្ចុប្បន្នភាពនៅឆ្នាំ២០២៤ គឺជាក្របខ័ណ្ឌច្បាប់សម្រាប់ការត្រួតពិនិត្យ និងថែរក្សាសន្តិសុខតាមអ៊ីនធឺណិតជាតិក្នុងប្រទេសសិង្ហបុរីដោយតម្រូវឱ្យប្រតិបត្តិករនៃ **Critical Information Infrastructure (CII)** ធ្វើការវាយតម្លៃហានិភ័យជាប្រចាំ និងរាយការណ៍អំពីឧប្បត្តិហេតុសុវត្ថិភាពអ៊ីនធឺណិត។

● **Computer Misuse Act:** ច្បាប់នេះដោះស្រាយឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត ដោយផ្ដោតសំខាន់លើការបោកប្រាស់ និងការប្រើប្រាស់មិនត្រឹមត្រូវនៃលិខិតសម្គាល់ផ្ទាល់ខ្លួន ដូចជា Singpass ជាដើម។

● **Digital Trust Centre:** បានចាប់ផ្ដើមនៅឆ្នាំ២០២២ គំនិតផ្ដួចផ្ដើមនេះផ្ដោតលើការអភិវឌ្ឍនិងផ្សព្វផ្សាយ AI និងបច្ចេកវិទ្យាជឿទុកចិត្តផ្សេងទៀត ដើម្បីជំរុញការប្រើប្រាស់ឱ្យបានកាន់តែច្រើននិងកាន់តែមានសុវត្ថិភាព។

➤ **ទំនួលខុសត្រូវរបស់បុគ្គល**

● **ការចែករំលែកដោយការយកចិត្តទុកដាក់:** ប្រជាពលរដ្ឋរបស់ប្រទេសសិង្ហបុរីត្រូវបានលើកទឹកចិត្តឱ្យគិតគូរយ៉ាងហ្មត់ចត់នូវអ្វីដែលពួកគេចែករំលែកនៅលើប្រព័ន្ធអ៊ីនធឺណិត ជៀសវាងការចែករំលែកព័ត៌មានផ្ទាល់ខ្លួនហួសហេតុ និងត្រូវដឹងពីហានិភ័យនៃការបង្ហោះនានាតាមអ៊ីនធឺណិត។ ទន្ទឹមនេះដោយសារប្រទេសនេះមានប្រជាជនតិច និងមានប្រជាជនមានចំណេះដឹងច្រើនទើបងាយស្រួលក្នុងគ្រប់គ្រងជាងប្រទេសដែលមានប្រជាជនច្រើន។

● **អក្ខរកម្មឌីជីថល:** តាមរយៈគំនិតផ្ដួចផ្ដើម ដូចជា Digital For Life បុគ្គលម្នាក់ៗត្រូវរៀនពីការសម្រេចចិត្តនៅលើអ៊ីនធឺណិតឱ្យបានកាន់តែប្រសើរ ការកំណត់ឯកជនភាព និងធានាវត្តមានឌីជីថលផ្ទាល់ខ្លួនរបស់ពួកគេ។

● **ការប្រុងប្រយ័ត្ននឹងការគំរាមកំហែង:** ក្រុមឆ្លើយតបបន្ទាន់តាមអ៊ីនធឺណិតរបស់សិង្ហបុរី (SingCERT) ផ្តល់ការប្រឹក្សាអំពីការគំរាមកំហែងតាមអ៊ីនធឺណិតជាប្រចាំ ហើយបុគ្គលម្នាក់ៗក៏ត្រូវបានណែនាំនិងជូនដំណឹងជាប្រចាំអំពីហានិភ័យនានានៅលើប្រព័ន្ធអ៊ីនធឺណិត ដើម្បីការពារប្រឆាំងនឹងការបោកប្រាស់និងការវាយប្រហារ។

➤ **ប្រទេសកម្ពុជា**

កម្ពុជាក៏មិនខុសគ្នាពីប្រទេសដទៃលើសកលលោក បាននិងកំពុងយកចិត្តទុកដាក់ខ្លាំងលើការផ្សព្វផ្សាយដើម្បីជំរុញការយល់ដឹង និងគ្រប់គ្រងដានជើងឌីជីថល ដើម្បីប្រើប្រាស់វាឱ្យមានប្រយោជន៍ដើម្បីអភិវឌ្ឍន៍សេដ្ឋកិច្ច សង្គមឌីជីថល និងការពារឱ្យបាននូវហានិភ័យដល់ឯកជនភាព និងសុវត្ថិភាពសន្តិសុខជាតិ។ ដូច្នេះ ដើម្បីគ្រប់គ្រងដានជើងឌីជីថល, អត្តសញ្ញាណឌីជីថល, សន្តិសុខសាយប័រ និងការគ្រប់គ្រងឯកជនភាព រាជរដ្ឋាភិបាល និងភាគីពាក់ព័ន្ធបានដាក់ចេញនូវវិធានការមួយចំនួនដូចខាងក្រោម៖

● **សេចក្តីព្រាងច្បាប់សន្តិសុខសាយប័រ**

រាជរដ្ឋាភិបាលបាននិងកំពុងជំរុញការរៀបចំនូវសេចក្តីព្រាងច្បាប់សន្តិសុខសាយប័រ ដើម្បីការពារលំហសាយប័រនៅកម្ពុជា កសាងទំនុកចិត្ត និងភាពជឿជាក់លើប្រព័ន្ធបច្ចេកវិទ្យាឌីជីថលដែលគាំទ្រដល់ការអភិវឌ្ឍសេដ្ឋកិច្ច និងសង្គមឌីជីថល។ ច្បាប់សន្តិសុខសាយប័រ ពិតជាមានសារៈសំខាន់ណាស់

សម្រាប់ស្ថាប័ន និងប្រព័ន្ធរបស់រាជរដ្ឋាភិបាលដើម្បីការពារព័ត៌មានរសើប រក្សាការជឿទុកចិត្តសាធារណៈ ធានាប្រតិបត្តិការរបស់រាជរដ្ឋាភិបាល ការពារការក្លែងបន្លំ និងការគំរាមកំហែងតាមអ៊ីនធឺណិត។

● **អនុក្រឹត្យ ស្តីពីការគ្រប់គ្រង ការប្រើប្រាស់ និងការការពារសុវត្ថិភាពទិន្នន័យអត្តសញ្ញាណបុគ្គល**

អនុក្រឹត្យ លេខ២៥២ អនក្រ.បក ចុះថ្ងៃទី២២ ខែធ្នូ ឆ្នាំ២០២១ ស្តីពីការគ្រប់គ្រង ការប្រើប្រាស់ និងការការពារសុវត្ថិភាពទិន្នន័យអត្តសញ្ញាណបុគ្គល បានកំណត់អំពីការគ្រប់គ្រង ការប្រើប្រាស់ និងការការពារសុវត្ថិភាពទិន្នន័យអត្តសញ្ញាណបុគ្គល ក្នុងគោលបំណងធានាការពារសន្តិសុខ សណ្តាប់ធ្នាប់ ផលប្រយោជន៍សាធារណៈ លើកកម្ពស់គុណភាពនៃការផ្តល់សេវានានា និងអភិវឌ្ឍជាតិ ប្រកបដោយប្រសិទ្ធភាព និងសុវត្ថិភាពខ្ពស់។

● **គោលនយោបាយរដ្ឋាភិបាលឌីជីថលកម្ពុជា ២០២២-២០៣៥**

រាជរដ្ឋាភិបាលបានចេញនូវគោលនយោបាយនេះ ក្នុងគោលបំណងកសាងរដ្ឋាភិបាលឆ្លាតដោយឈរលើមូលដ្ឋាននៃការប្រើប្រាស់ហេដ្ឋារចនាសម្ព័ន្ធ និងបច្ចេកវិទ្យាឌីជីថលជាប្រព័ន្ធអេកូឡូស៊ីសម្រាប់ការធ្វើទំនើបកម្មប្រព័ន្ធអភិបាលកិច្ច និងការកែទម្រង់លើគ្រប់វិស័យ ប្រកបដោយតម្លាភាព និងភាពជឿទុកចិត្ត សំដៅបង្កើតបរិយាកាសអំណោយផលដល់ការអភិវឌ្ឍសេដ្ឋកិច្ច និងសង្គមឌីជីថលប្រកបដោយបរិយាបន្ន។ ដើម្បីសម្រេចនូវគោលបំណងនេះ រាជរដ្ឋាភិបាលបានដាក់ចេញគោលដៅជាយុទ្ធសាស្ត្រចំនួន ៤ និងយុទ្ធសាស្ត្រចំនួន ១០ ដោយក្នុងនោះ គឺផ្ដោតលើការរៀបចំ និងការពង្រឹងហេដ្ឋារចនាសម្ព័ន្ធសន្តិសុខឌីជីថល ដើម្បីការពារហេដ្ឋារចនាសម្ព័ន្ធឌីជីថលឱ្យបានគ្រប់ជ្រុងជ្រោយ និងធានាសុវត្ថិភាពនិងសន្តិសុខខ្ពស់លើការគ្រប់គ្រង ប្រតិបត្តិការ និងការប្រើប្រាស់ប្រព័ន្ធឌីជីថលសំដៅកសាងជំនឿទុកចិត្តលើប្រព័ន្ធរដ្ឋាភិបាលឌីជីថល។

● **ថ្នាលសម្គាល់អត្តសញ្ញាណអតិថិជនឌីជីថលកម្ពុជា (CamDigiKey)**

ក្រោមអាណាព្យាបាលរបស់ក្រសួងសេដ្ឋកិច្ច និង ហិរញ្ញវត្ថុ មជ្ឈមណ្ឌលបណ្តុះធុរកិច្ចថ្មី “តេជោ” បានចាប់ផ្តើមបង្កើតថ្នាល CamDigiKey នៅឆ្នាំ២០១៩ ក្នុងគោលបំណងផ្តល់ជូននូវសេវាកម្មជាច្រើនរួមមាន កម្មវិធីទូរសព្ទដៃ, សេវាកម្មធ្វើយថាភូតកម្មតែមួយដង/យថាភូតកម្មរួម (Single Sign-On Service), ការធ្វើយថាភូតកម្មជាមួយពាក្យ/លេខសម្ងាត់តិច (Password-less authentication), ការផ្តល់ Open APIs សម្រាប់ការផ្ទៀងផ្ទាត់អត្តសញ្ញាណអតិថិជន (Open KYC Verification APIs)។ ដំបូងថ្នាលនេះជាប្រព័ន្ធផ្ទៀងផ្ទាត់អត្តសញ្ញាណសម្រាប់ការចូលទៅកាន់ប្រព័ន្ធចុះបញ្ជីអាជីវកម្មតាមថ្នាលបច្ចេកវិទ្យាព័ត៌មាន។ ក្រោយមក ថ្នាលនេះត្រូវបានប្រើប្រាស់នៅក្នុងថ្នាលធុរកិច្ចថ្មីកម្ពុជាប្រព័ន្ធ “ទេពកោសល្យសម្រាប់សេដ្ឋកិច្ចឌីជីថល” និងប្រព័ន្ធដាក់ពាក្យស្នើសុំចូលបម្រើការងារនៃអគ្គលេខាធិការដ្ឋាននៃគណៈកម្មាធិការសេដ្ឋកិច្ច និងធុរកិច្ចឌីជីថល ហើយឥឡូវនេះ ថ្នាល CamDigiKey ក៏កំពុងពង្រីកខ្លួនបន្តិចម្តងៗ។ ឥឡូវនេះ, ថ្នាល CamDigiKey ត្រូវបានដាក់ឱ្យប្រើប្រាស់ដល់សាធារណជនទូទៅ ទាំងរូបវន្តបុគ្គល, នីតិបុគ្គល, ស្ថាប័នសាធារណៈ និង ស្ថាប័នឯកជន។

● **ថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា (CamDX)**

ថ្នាលត្រូវបានអភិវឌ្ឍ និងដាក់ឱ្យប្រើប្រាស់ដោយ **មជ្ឈមណ្ឌលបណ្តុះបណ្តាលធុរកិច្ចថ្មី “តេជោ” នៃក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ** ក្នុងគោលបំណងសម្រាប់ផ្លាស់ប្តូរទិន្នន័យដោយប្រើប្រាស់សន្លានកម្មនៃកម្មវិធីកុំព្យូទ័រ (Application Programming Interface-API) រវាងប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានមួយនិងប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានមួយទៀតក្នុងវិស័យសាធារណៈ និងជាមួយវិស័យឯកជន ដែលជាសមាជិក ថ.ជ.ទ. ប្រកបដោយសុវត្ថិភាពតាមរយៈប្រព័ន្ធអ៊ីនធឺណិត ឬបណ្តាញតភ្ជាប់ឌីជីថលផ្សេងៗ។ រាល់ទិន្នន័យនឹងត្រូវបានប្រមូលពីប្រជាពលរដ្ឋ អាជីវកម្ម និងរដ្ឋាភិបាលដោយប្រកាន់ខ្ជាប់នូវច្បាប់/បទប្បញ្ញត្តិការពារទិន្នន័យដោយមានការយល់ព្រមពីអ្នកប្រើប្រាស់។ ទិន្នន័យដែលប្រមូលបាននឹងត្រូវបានចែករំលែកក្នុងចំណោមស្ថាប័នដែលបាន Authorized។

● **គម្រោង «ខែនៃការយល់ដឹងអំពីសន្តិសុខសាយប័រ»**

ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ បានផ្តួចផ្តើមធ្វើនូវគម្រោង «ខែនៃការយល់ដឹង អំពីសន្តិសុខសាយប័រ - Cyber Security Awareness Month» ដែលជាយុទ្ធនាការចូលរួមលើកកម្ពស់និងបញ្ញាបច្ចេកវិទ្យាដឹង អំពីទិន្នន័យឯកជនភាព និងសុវត្ថិភាពសន្តិសុខសាយប័រ។ គម្រោងនេះបានដាក់ចេញនូវផែនការសកម្មភាពជាច្រើន ដូចជា ការផ្សព្វផ្សាយតាមបណ្តាញឌីជីថល, ការរៀបចំសិក្ខាសាលានៅតាមគ្រឹះស្ថានសិក្សា, យុទ្ធនាការផ្សព្វផ្សាយ តាមរយៈវេទិកា ស្តីពីសន្តិសុខសាយប័រសម្រាប់យុវជន (Cybersecurity Youth Forum) រួមទាំងការរៀបចំកិច្ចពិភាក្សាស្តីពី សន្តិសុខសាយប័រនៅក្នុងយុគសម័យសង្គមអេឡិចត្រូនិក និងការបណ្តុះបណ្តាលក្នុងការរក្សាសុវត្ថិភាពតាមអនឡាញ។ គម្រោង «ខែនៃការយល់ដឹងអំពីសន្តិសុខសាយប័រ» មានរយៈពេល ១ខែ ដែលចាប់ផ្តើមពីថ្ងៃទី១ ខែធ្នូ ឆ្នាំ២០២៤ និងបញ្ចប់នៅថ្ងៃទី៣១ ខែធ្នូ ឆ្នាំ២០២៤។

● **ការបញ្ចូលការយល់ដឹងពីដានជើងឌីជីថល**

ក្រៅពីលិខិតបទដ្ឋានគតិយុត្ត, គោលនយោបាយ និងកម្មវិធីនានា រាជរដ្ឋាភិបាល និងភាគីពាក់ព័ន្ធក៏ព្យាយាមជំរុញការបញ្ចូលការយល់ដឹងទៅដល់សាធារណជនពីដានជើងឌីជីថល ដើម្បីអាចគ្រប់គ្រងហានិភ័យនៃដានជើងឌីជីថល ជៀសវាងបង្កការខាតបង់ណាមួយ។ ជាក់ស្តែង ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ តាមរយៈ កម្មវិធីកម្ពុជាឆ្ពោះទៅឌីជីថល - Go Digital Cambodia បានផ្សព្វផ្សាយពីមាតិកាជាច្រើនទាក់ទងនឹងដានជើងឌីជីថល និងរបៀបការពារខ្លួនពីហានិភ័យនានាដែលអាចកើតមានឡើងដោយសារបទល្មើសបច្ចេកវិទ្យា។ ជាមួយគ្នានេះ ក្រសួងមហាផ្ទៃតាមរយៈនាយកដ្ឋានប្រឆាំងបទល្មើសបច្ចេកវិទ្យាក៏តែងតែផ្សព្វផ្សាយ និងរៀបចំការបណ្តុះបណ្តាលនានាទាក់ទងនឹងបញ្ហាសន្តិសុខសាយប័រផងដែរ។ ក្រៅពីនេះ ក៏មាន មជ្ឈមណ្ឌលកម្ពុជា ៤.០ ផ្ទាល់ដោយបានបង្កើតជា Poster អត្ថបទសិក្សាស្រាវជ្រាវ និងវីដេអូអប់រំជាច្រើន ទាក់ទងនឹងប្រធានបទដានជើងឌីជីថល និងសន្តិសុខសាយប័រជាមួយ។

V. អនាគតនៃ Digital Footprint

នៅក្នុងយុគសម័យនៃអន្តរកម្មឌីជីថលដែលកំពុងកើនឡើងយ៉ាងរហ័សនេះ ការគ្រប់គ្រងដានជើងឌីជីថលបានក្លាយជាកិច្ចការសំខាន់មួយដែលប្រជាពលរដ្ឋគ្រប់រូបមិនអាចមើលរំលងបាន ជាពិសេសសម្រាប់អាជីវកម្ម អង្គការ ស្ថាប័នរដ្ឋ និងឯកជន។ នៅពេលយើងមើលទៅមុខ វាជារឿងសំខាន់ក្នុងការយល់ដឹងអំពីនិន្នាការ និងការព្យាករណ៍ពេលអនាគតសម្រាប់ការរីកចម្រើន និងការគ្រប់គ្រងលើដានជើងឌីជីថល។

► តួនាទីរបស់បញ្ហាសិប្បនិម្មិត និងម៉ាស៊ីនសិក្សា

ការវិវត្តដ៏សំខាន់បំផុតមួយនៅក្នុងការគ្រប់គ្រងដានជើងឌីជីថល គឺកើនឡើងនៃការប្រើប្រាស់ Artificial Intelligence (AI) និង Machine Learning (ML)។ បច្ចេកវិទ្យាទាំងនេះផ្តល់នូវដំណោះស្រាយដ៏ល្អចំពោះបញ្ហាប្រឈមនៃការគ្រប់គ្រងទិន្នន័យ និងព័ត៌មានដ៏ច្រើនសន្លឹកសន្លាប់។ AI និង ML អាចធ្វើស្វ័យប្រវត្តិកម្មដំណើរការនៃការតាមដាន វិភាគ និងគ្រប់គ្រងដានជើងឌីជីថល។ បច្ចេកវិទ្យាទាំងនេះអាចកំណត់អត្តសញ្ញាណគំរូ និន្នាការ និងភាពមិនប្រក្រតីនៃទិន្នន័យ ដោយផ្តល់នូវការយល់ដឹងសម្រាប់ប្រជាពលរដ្ឋ ម្ចាស់អាជីវកម្ម ស្ថាប័នរដ្ឋ និងឯកជន។ ជាក់ស្តែង ឧបករណ៍ឌីជីថលដែលដំណើរការដោយ AI អាចតាមដានសកម្មភាពលើប្រព័ន្ធអ៊ីនធឺណិត ស្វែងរកការគំរាមកំហែងផ្នែកសុវត្ថិភាព និងផ្តល់ការជូនដំណឹងតាមពេលវេលាជាក់ស្តែង ដែលអនុញ្ញាតឱ្យមានការគ្រប់គ្រងយ៉ាងសកម្មនៃដានជើងឌីជីថល។ លើសពីនេះ AI និង ML ក៏អាចត្រូវបានប្រើប្រាស់ ដើម្បីព្យាករណ៍ពីនិន្នាការថ្មី និងអាកប្បកិរិយានាពេលអនាគត ដោយផ្អែកលើទិន្នន័យប្រវត្តិសាស្ត្រផងដែរ។ សមត្ថភាពព្យាករណ៍នេះអាចជួយអ្នកប្រើប្រាស់ក្នុងការប្រមើលមើលបញ្ហាដែលអាចកើតមាន និងចាត់វិធានការបានទាន់ពេលវេលា ដើម្បីកាត់បន្ថយហានិភ័យ។

► ច្បាប់ និងច្បាប់ឯកជនភាពទិន្នន័យ

ការបោះជំហានទៅមុខនៃឌីជីថលបន្តកើនឡើងក្នុងទំហំធំ និងមានភាពស្មុគស្មាញ បានបង្កជា ការព្រួយបារម្ភចំពោះឯកជនភាព និងសុវត្ថិភាពទិន្នន័យ ហើយដើម្បីឆ្លើយតបនឹងបញ្ហានេះ រដ្ឋាភិបាល ជុំវិញសកលលោកបាននិងកំពុងអនុវត្តច្បាប់ពាក់ព័ន្ធនានា ជាពិសេសច្បាប់ឯកជនភាពទិន្នន័យឱ្យបានកាន់តែតឹងរ៉ឹង ដើម្បីការពារដានជើងឌីជីថលរបស់បុគ្គលម្នាក់ៗ។ ច្បាប់ទាំងនេះគឺពិតជាមានសារៈសំខាន់ណាស់សម្រាប់ប្រជាពលរដ្ឋទាំងអស់នៅលើសកលលោក។ ការអនុលោមតាមបទប្បញ្ញត្តិទាំងនេះមិនត្រឹមតែជាកាតព្វកិច្ចផ្លូវច្បាប់ប៉ុណ្ណោះទេ ប៉ុន្តែក៏ជាផ្នែកសំខាន់មួយក្នុងការរក្សានូវទំនុកចិត្ត និងភាពជឿជាក់ជាមួយអតិថិជន និងអ្នកពាក់ព័ន្ធផងដែរ។ អាជីវកម្ម និងស្ថាប័នរដ្ឋនិងឯកជនទាំងអស់ត្រូវបន្តធ្វើបច្ចុប្បន្នភាពលើច្បាប់ចុងក្រោយបំផុត និងច្បាប់ឯកជនភាពទិន្នន័យទាក់ទងនឹងការវិវត្តយ៉ាងឆាប់រហ័សនៃបច្ចេកវិទ្យាឌីជីថល។ ពួកគេត្រូវធានាថាការអនុវត្តការគ្រប់គ្រងដានជើងឌីជីថលរបស់ពួកគេគឺស្របតាមបទប្បញ្ញត្តិទាំងនេះ ដែលនេះរួមបញ្ចូលទាំងការអនុវត្តវិធានការសុវត្ថិភាព

ទិន្នន័យដ៏រឹងមាំ រក្សាតម្លាភាពក្នុងការប្រមូលនិងប្រើប្រាស់ទិន្នន័យ និងការគោរពសិទ្ធិឯកជនភាព របស់បុគ្គលម្នាក់ៗ។

ជាមួយគ្នានេះ ដើម្បីឱ្យការគ្រប់គ្រងដានជើងឌីជីថលមានភាពរឹងមាំ និងមានសុវត្ថិភាពនាពេល អនាគត មនុស្សគ្រប់រូបត្រូវទទួលយកការប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថលទំនើប ដូចជា AI និង ML បន្ត ធ្វើបច្ចុប្បន្នភាពលើច្បាប់ចុងក្រោយបំផុត និងច្បាប់ឯកជនភាពទិន្នន័យ និងអនុវត្តវិធីសាស្ត្រសកម្មក្នុង ការគ្រប់គ្រងដានជើងឌីជីថល។ តាមរយៈការធ្វើដូច្នេះ យើងទាំងអស់គ្នានឹងអាចកាត់បន្ថយហានិភ័យ នានាលើប្រព័ន្ធអ៊ីនធឺណិត និងធានាបាននូវបរិយាកាសឌីជីថលដែលមានសុវត្ថិភាព និងគួរឱ្យទុកចិត្ត សម្រាប់សង្គមជាតិ។

VI. សេចក្តីសន្និដ្ឋាន

នៅក្នុងបរិបទនៃសង្គមឌីជីថលបច្ចុប្បន្ន ដានជើងឌីជីថលបានក្លាយជាផ្នែកមួយយ៉ាងសំខាន់ ដែលនឹងជះឥទ្ធិពលដល់ការរស់នៅប្រចាំថ្ងៃរបស់យើងទាំងអស់គ្នាទាំងការធ្វើទំនាក់ទំនង, ការសិក្សា, ការបំពេញកិច្ចការងារ, ការកម្សាន្ត។ បច្ចុប្បន្ននេះ ដានជើងឌីជីថល ត្រូវបានកំណត់ថាជាដាននៃទិន្នន័យ ឬព័ត៌មាន ដែលអ្នកប្រើប្រាស់បន្សល់ទុកនៅពេលប្រើប្រាស់អ៊ីនធឺណិត។ អ្នកប្រើប្រាស់អាចបន្សល់ទុក ដាននៃទិន្នន័យដោយមិនបានដឹងខ្លួន តាមរយៈសកម្មភាពមួយចំនួន ដូចជា ការបង្ហោះតាមបណ្តាញ សង្គម, ការទិញទំនិញអនឡាញ, ការបំពេញព័ត៌មានអនឡាញ និងការចូលមើលគេហទំព័រនានាជាដើម។ ដានជើងឌីជីថល ប្រៀបបាននឹងអាវុធមុខ ២ ប្រសិនបើយើងប្រើប្រាស់ដោយមិនយកចិត្តទុកដាក់ និង មិនមានការប្រុងប្រយ័ត្នខ្ពស់នោះទេ វានឹងបង្កជាបញ្ហាប្រឈមជាច្រើន ដូចជា ការលួចអត្តសញ្ញាណ, បាត់បង់ឱកាសការងារ, ប៉ះពាល់សុវត្ថិភាពផ្ទាល់ខ្លួន និងការឆបោក តាមអ៊ីនធឺណិតជាដើម។ យ៉ាងណាមិញ ប្រសិនបើយើងម្នាក់ៗប្រើប្រាស់វាប្រកបដោយភាពត្រឹមត្រូវ មានការប្រុងប្រយ័ត្ន នោះដានជើងឌីជីថល នឹងផ្តល់ប្រយោជន៍ជាច្រើន រួមមាន ពង្រឹងសុវត្ថិភាព និងអាកប្បកិរិយាទទួលខុសត្រូវ, បង្កើនប្រសិទ្ធភាព នៃដំណើរការអាជីវកម្ម និងជួយពង្រឹងការអនុវត្តច្បាប់ និងការដាក់ចេញគោលនយោបាយ។ ដោយ មើលឃើញពីគុណសម្បត្តិ និងគុណវិបត្តិទាំងនេះហើយ ទើបប្រទេសជាច្រើននៅលើសកលលោក រួមទាំងកម្ពុជា មានការចិត្តទុកដាក់ខ្ពស់ចំពោះការគ្រប់គ្រងដានជើងឌីជីថល ដើម្បីធានាឱ្យបាននូវ ការពង្រឹងសុវត្ថិភាព និងសន្តិសុខសង្គមទាំងពេលបច្ចុប្បន្ន និងអនាគត។



ឯកសារយោង

- What is a Digital Footprint?: Types, Examples & Risks, ចេញផ្សាយថ្ងៃទី៦ ខែមិថុនា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៦ ខែកញ្ញា ឆ្នាំ២០២៥, <https://razorpay.com/learn/digital-footprint/>
- What Is a Digital Footprint?, ចេញផ្សាយថ្ងៃទី១៣ ខែកក្កដា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៦ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.keepersecurity.com/blog/2023/06/06/what-is-a-digital-footprint/>
- How your digital footprint can impact your life, ចេញផ្សាយថ្ងៃទី១៣ ខែមីនា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, https://www.expressvpn.com/blog/how-your-digital-footprint-can-impact-your-life/?srsltid=AfmBOoqyU8M5AvYgp4v4eUq5KtJUq6SyRLWmkDoF2-WTlJsRX-JBoF_
- What is a digital footprint? And how to protect it from hackers, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>
- Cybersecurity Act, ចេញផ្សាយថ្ងៃទី២ ខែមេសា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៦ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.csa.gov.sg/legislation/cybersecurity-act>
- Singapore's Personal Data Protection Act (PDPA), ចេញផ្សាយថ្ងៃទី២ ខែមិថុនា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៣ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.cookieyes.com/blog/singapore-pdpa/>
- What is a digital footprint? And how to protect it from hackers, ចូលអានថ្ងៃទី៥ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>
- What Is a Digital Footprint and Why Is It Important?, ចេញផ្សាយថ្ងៃទី១៨ ខែកុម្ភៈ ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី៥ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.dashlane.com/blog/what-is-a-digital-footprint>
- What Is a Digital Footprint and Why Is It Important?, ចូលអានថ្ងៃទី៥ ខែកញ្ញា ឆ្នាំ២០២៥, <https://thebclog.com/en/what-is-a-digital-footprint-and-why-is-it-important>
- Digital Footprint: What It Is and Why It Matters, ចេញផ្សាយថ្ងៃទី៩ ខែធ្នូ ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.aratek.co/news/digital-footprint-what-it-is-and-why-it-matters>
- The digital you in 2023: Modern digital footprints and their impact on privacy and security, ចេញផ្សាយថ្ងៃទី១៥ ខែមីនា ឆ្នាំ២០២៣, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.bitdefender.com/en-us/blog/hotforsecurity/the-digital-you-in-2023-modern-digital-footprints-and-their-impact-on-privacy-and-security>
- What is a Digital Footprint and Why is It Important?, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.relateddigital.com/blog/what-is-a-digital-footprint-and-why-is-it-important/>
- The Digital Footprint: Understanding and controlling your online presence, ចេញផ្សាយថ្ងៃទី២០ ខែមិថុនា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://keeex.me/blog/2024/06/20/the-digital-footprint-understanding-and-controlling-your-online-presence/>

- CamDigiKey, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://camdigikey.gov.kh/#aboutus>
- Cambodia Data Exchange Platform, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://camdx.gov.kh/>
- ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ ផ្ដើមធ្វើគម្រោង «ខែនៃការយល់ដឹងអំពីសន្តិសុខសាយប៉ារ» ដែលជាយុទ្ធនាការលើកកម្ពស់ និងបញ្ជ្រាបចំណេះដឹង, ចេញផ្សាយថ្ងៃទី២៣ ខែធ្នូ ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://m.freshnewsasia.com/localnews/369945-2024-12-23-01-16-37.html>
- សម្តេចធិបតី ជំរុញឱ្យពន្លឿនការរៀបចំនូវច្បាប់សន្តិសុខសាយប៉ារ, ចេញផ្សាយថ្ងៃទី៦ ខែកុម្ភៈ ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.kampuchearthmey.com/local-news/850881>
- គោលនយោបាយរដ្ឋាភិបាលឌីជីថលកម្ពុជា ២០២២-២០៣៥, ចេញផ្សាយខែមករា ឆ្នាំ២០២២, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥
- អនុក្រឹត្យលេខ២៥២ អនក្រ.បក ចុះថ្ងៃទី២២ ខែធ្នូ ឆ្នាំ២០២១ ស្តីពីការគ្រប់គ្រង ការប្រើប្រាស់ និងការការពារសុវត្ថិភាពទិន្នន័យអត្តសញ្ញាណបុគ្គល, ចូលអានថ្ងៃទី២៩ ខែកញ្ញា ឆ្នាំ២០២៥
- Computer Misuse Act 1993
- Digital For Life Singapore
- The Future of Digital Footprint Management: Trends and Predictions, ចេញផ្សាយថ្ងៃទី១១ ខែកញ្ញា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៨ ខែកញ្ញា ឆ្នាំ២០២៥, <https://www.webguardiantech.com/digital-footprint-management/future-digital-footprint-management-trends/>



កម្ពុជា ៤.០ - Cambodia 4.0



www.cambodia4point0.org



កម្ពុជា ៤.០ Cambodia 4.0



[cambodia_4.0](https://www.instagram.com/cambodia_4.0)



កម្ពុជា ៤.០ - Cambodia 4.0



កម្ពុជា ៤.០ - Cambodia 4.0



កម្ពុជា ៤.០ - Cambodia 4.0



Cambodia 4.0 Center

