សន្តិសុខអត្តសញ្ញាណឌីជីថល

នាយុគសម័យឌីជីថល អត្តសញ្ញាណឌីជីថលបានវិវត្តន៍ពីមធ្យោបាយសម្រាប់បញ្ជាក់អត្តសញ្ញាណបុគ្គលដ៏សាមញ្ញ ទៅជាហេដ្ឋារចនាសម្ព័ន្ធឌីជីថលដ៏សំខាន់ ដែលគាំទ្រដល់ដំណើរការរបស់រដ្ឋ, សេដ្ឋកិច្ច និងសង្គម។ បច្ចុប្បន្ន អត្តសញ្ញាណឌីជីថល បានក្លាយជាគ្រឹះមិនអាចខ្វះបានសម្រាប់ការផ្តល់សេវាពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក (E-commerce), សេវាធនាគារឌីជីថល, រដ្ឋាភិបាលឌីជីថល, និងការបំពេញការងារពីចម្ងាយ ព្រមទាំងសេវាឌីជីថលជាច្រើនទៀត។ ផ្អែកតាម **«ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា ២០២១-២០៣៥»** អត្តសញ្ញាណឌីជីថល គឺជាព័ត៌មានដែលបញ្ជាក់ពីអត្តសញ្ញាណរូបវន្តបុគ្គល និងនីតិបុគ្គលនៅក្នុងពិភពឌីជីថល ដែលព័ត៌មាននេះបានភ្ជាប់ទៅនឹងអត្តសញ្ញាណរូបវន្តបុគ្គល និងនីតិបុគ្គលនៅក្នុងពិភពពិត។ អត្តសញ្ញាណឌីជីថលបានដើរតួនាទីជាហេដ្ឋារចនាសម្ព័ន្ធគន្លឹះមិនអាចខ្វះបាន ក្នុងការជំរុញការធ្វើបរិវត្តកម្មឌីជីថល ក្នុងការផ្តល់លទ្ធភាពឱ្យរូបវន្តបុគ្គល និងនីតិបុគ្គល អាចចូលប្រើប្រាស់សេវាសាធារណៈរបស់រដ្ឋ និងសេវាឯកជននានា។ ទោះជាយ៉ាងណាក៏ដោយ ស្របពេលជាមួយនឹងការផ្តល់អត្ថប្រយោជន៍ដ៏ច្រើនលើសលប់នេះ ការធានាសុវត្ថិភាពក្នុងការប្រើប្រាស់ក៏ជាកត្តាចាំបាច់ដែលមិនអាចមើលរំលងបានឡើយ។ ការណ៍នេះ ទាមទារឱ្យសាធារណជនត្រូវស្វែងយល់ផងដែរអំពី **«សន្តិសុខអត្តសញ្ញាណឌីជីថល»** ដែលសំដៅលើការធានាបាននូវសន្តិសុខលើការគ្រប់គ្រងប្រតិបត្តិការ និងការប្រើប្រាស់ប្រព័ន្ធឌីជីថល ដើម្បីកសាងទំនុកចិត្តលើប្រព័ន្ធរដ្ឋាភិបាលឌីជីថល តាមរយៈការកំណត់នីតិវិធីសុវត្ថិភាព និងការបំពាក់សម្ភារបរិក្ខារបច្ចេកទេសសម្រាប់តាមដាន ត្រួតពិនិត្យ និងទប់ស្កាត់ការវាយប្រហារនានា ស្របតាមស្តង់ដាសន្តិសុខឌីជីថល។

I. ការវិវត្តនៃសន្តិសុខអត្តសញ្ញាណឌីជីថល

ការផ្ទៀងផ្ទាត់ និងការបញ្ជាក់អត្តសញ្ញាណមានតាំងពីរាប់ពាន់ឆ្នាំមកហើយ ដោយបានចាប់ផ្តើមពីដំបូងៗក្នុងទម្រង់ ដូចជា ការប្រើប្រាស់គ្រឿងអលង្ការ និងស្នាមសាក់ ដើម្បីបង្ហាញពីឋានៈ, អត្តសញ្ញាណផ្ទាល់ខ្លួន ឬទំនាក់ទំនងជាមួយក្រុមមនុស្សជាក់លាក់មួយ។ ទន្ទឹមនេះ ស្នាមម្រាមដៃត្រូវបានគេយកមកប្រើប្រាស់ជាទម្រង់កំណត់អត្តសញ្ញាណតាំងពីបុរាណកាលនៅក្នុងប្រទេសបាប៊ីឡូន (Babylonians), រ៉ូម, ចិន និងជប៉ុន រហូតឈានដល់ការប្រើប្រាស់ជាផ្លូវការលើកដំបូងក្នុងឆ្នាំ១៨៥៨ ដោយចៅក្រមអាណានិគមអង់គ្លេស។ ចំពោះការប្រើប្រាស់ឯកសារធ្វើដំណើរវិញ លិខិតឆ្លងដែនដំបូងបានលេចឡើងតាំងពីឆ្នាំ៤៥០ មុនគ្រិស្តសករាជនៅពែរ្សបុរាណ (Ancient Persia) ហើយបានវិវត្តន៍ជាបន្តបន្ទាប់រហូតដល់រជ្ជកាលព្រះអង្គ ហេនរី ទី៥ (King Henry V) នៃប្រទេសអង់គ្លេស និងបានប្រែប្រួលមកជាសៀវភៅលិខិតឆ្លងដែន **៣២ទំព័រ** បែបទំនើបនៅឆ្នាំ ១៩២១។ ឈានចូលយុគសម័យបច្ចេកវិទ្យា

ការប្រែក្លាយទៅជាអត្តសញ្ញាណឌីជីថលបានចាប់ផ្តើមឡើងជាមួយនឹងការណែនាំអំពីលេខសម្ងាត់ (PIN) សម្រាប់ម៉ាស៊ីន ATM ក្នុងទសវត្សរ៍ឆ្នាំ១៩៦០។

ក្នុងពេលជាមួយគ្នានោះ លោក Fernando Corbat នៅវិទ្យាស្ថាន MIT បានបង្កើតប្រព័ន្ធមួយដោយមានឈ្មោះអ្នកប្រើប្រាស់ និងពាក្យសម្ងាត់ (Username & Password) ជាលើកដំបូង ដែលក្រោយមកត្រូវបានក្រុមហ៊ុន Microsoft យកមកផ្សព្វផ្សាយយ៉ាងទូលំទូលាយ។ បន្ទាប់មក ក្រុមហ៊ុនបណ្តាញសង្គមធំៗ ដូចជា Facebook និង Google បានអភិវឌ្ឍន៍ប្រព័ន្ធ Social Login ដើម្បីសម្រួលដល់ការចូលប្រើប្រាស់សេវាកម្មផ្សេងៗបានយ៉ាងងាយស្រួល។ នាពេលបច្ចុប្បន្ន បច្ចេកវិទ្យាជីវមាត្រ (Biometrics) បានផ្លាស់ប្តូរមុខមាត់នៃសន្តិសុខអត្តសញ្ញាណឌីជីថលទាំងស្រុង ដោយទូរសព្ទឆ្លាតវៃបានចាប់ផ្តើមដាក់ឱ្យប្រើប្រាស់ការស្កេនស្នាមម្រាមដៃ និងផ្ទៃមុខ ដូចជា Touch ID ក្នុងឆ្នាំ២០១៣ និង Face ID ក្នុងឆ្នាំ២០១៧ របស់ Apple។ បច្ចេកវិទ្យាជីវមាត្រនេះបានក្លាយជាស្តង់ដាដ៏សំខាន់សម្រាប់ធានាសុវត្ថិភាពក្នុងវិស័យជាច្រើន ដូចជា ធនាគារ ការថែទាំសុខភាព និងសេវារដ្ឋាភិបាល ដោយផ្តល់នូវដំណើរការផ្ទៀងផ្ទាត់ដែលមានភាពងាយស្រួល, រហ័ស និងសុវត្ថិភាពខ្ពស់ ជំនួសឱ្យវិធីសាស្ត្របុរាណ។

យ៉ាងណាមិញ យោងតាមការស្ទង់មតិថ្មីរបស់ក្រុមហ៊ុន Regula ទាក់ទងនឹង «រូបរាងថ្មីនៃទម្រង់គំរាមកំហែងអត្តសញ្ញាណឆ្នាំ២០២៦» បានឱ្យដឹងថា ទំនុកចិត្តលើឧបករណ៍ផ្ទៀងផ្ទាត់អត្តសញ្ញាណបច្ចុប្បន្ននៅតែមានកម្រិតទាបនៅឡើយក្នុងចំណោមអង្គភាព និងក្រុមហ៊ុនភាគច្រើន។ ក្នុងនោះ **៩២%** នៃអង្គភាពទាំងនោះ បានរាយការណ៍ពីផលប៉ះពាល់អវិជ្ជមានដល់អាជីវកម្ម ដោយសារតែការផ្ទៀងផ្ទាត់អត្តសញ្ញាណមិនត្រឹមត្រូវ។ នៅពេលដែលមានកំហុសឆ្គងក្នុងការសម្រេចចិត្តលើអត្តសញ្ញាណ ផលវិបាកទាំងនោះអាចវាយប្រហារទៅលើប្រាក់ចំណូល និងប្រតិបត្តិការអាជីវកម្ម, ការអនុលោមតាមច្បាប់ (Compliance), ទំនុកចិត្តពីអតិថិជន និងកេរ្តិ៍ឈ្មោះម៉ាកយីហោក្នុងពេលតែមួយ។ ចំណុចប្រឈមដ៏ធំបំផុតនាពេលនេះ គឺប្រព័ន្ធសុវត្ថិភាពអត្តសញ្ញាណកំពុងប្រជែងយ៉ាងប្រកៀកប្រកិតជាមួយនឹងការបោកប្រាស់តាមរយៈបច្ចេកវិទ្យា AI ដែលកំពុងរីកចម្រើនយ៉ាងឆាប់រហ័ស។

ទន្ទឹមនេះ ទិន្នន័យថ្មីពីក្រុមហ៊ុន Microblink បានបង្ហាញថា ការក្លែងបន្លំអត្តសញ្ញាណ «មិនមែនគ្រាន់តែជាការវិវត្តសាមញ្ញទៀតនោះទេ» ហើយបច្ចេកវិទ្យា Deepfakes ព្រមទាំង AI បង្កើតថ្មី លែងជាការគំរាមកំហែងដែលទើបតែលេចឡើងទៀតហើយ ប៉ុន្តែបានក្លាយជា «មូលដ្ឋានគ្រឹះថ្មី» សម្រាប់ការក្លែងបន្លំឌីជីថលយ៉ាងប្រុងប្រយ័ត្ន។ លោក Hartley Thompson III នាយកប្រតិបត្តិក្រុមហ៊ុន Microblink បានថ្លែងថា «បច្ចេកវិទ្យា AI បង្កើតថ្មី បានផ្លាស់ប្តូររបៀបនៃការក្លែងបន្លំអត្តសញ្ញាណយ៉ាងស៊ីជម្រៅ។ អ្នកបោកប្រាស់លែងចាំបាច់បង្កើតអត្តសញ្ញាណក្លែងក្លាយពីចំណុចសូន្យទៀតហើយ។ ពួកគេអាចកែប្រែឯកសារស្របច្បាប់បានយ៉ាងរហ័ស, ចំណាយដើមទុនទាប និងធ្វើបានក្នុងទំហំធំ ដែលធ្វើឱ្យវិធីសាស្ត្រផ្ទៀងផ្ទាត់បែបប្រពៃណីលែងសូវមានប្រសិទ្ធភាព»។

II. ផលវិបាកនៃអសន្តិសុខអត្តសញ្ញាណឌីជីថល

ក្នុងបរិបទដែលបច្ចេកវិទ្យាឌីជីថលកំពុងរីកចម្រើនយ៉ាងឆាប់រហ័ស អត្តសញ្ញាណឌីជីថលបានក្លាយជាទ្រព្យសម្បត្តិដ៏មានតម្លៃ ក្នុងនោះមានដូចជា ព័ត៌មានផ្ទាល់ខ្លួន, ព័ត៌មានបញ្ជាក់អត្តសញ្ញាណ (Credentials), កំណត់ត្រា, ការប្រើប្រាស់ប្រព័ន្ធឌីជីថល, កេរ្តិ៍ឈ្មោះនៅលើប្រព័ន្ធអ៊ីនធឺណិត និងព័ត៌មានដែលអ្នកដទៃអាចសន្និដ្ឋានបានពីឥរិយាបថនៅលើថ្នាលឌីជីថលរបស់អ្នកប្រើប្រាស់តាមរយៈការស្វែងរក ឬទំនាក់ទំនងជាមួយអ្នកដទៃ។ ទោះជាយ៉ាងណា នៅពេលអត្តសញ្ញាណឌីជីថលមិនត្រូវបានការពារប្រកបដោយប្រសិទ្ធភាព នឹងបង្កឱ្យកើតមានការលួចអត្តសញ្ញាណ (Identity Theft) ដែលជាទម្រង់មួយនៃបទល្មើសសាយប័រដ៏គ្រោះថ្នាក់។ ការលួចអត្តសញ្ញាណដែលបណ្តាលមកពីអសន្តិសុខអត្តសញ្ញាណឌីជីថល ប៉ះពាល់ដល់បុគ្គល, ស្ថាប័ន, សេដ្ឋកិច្ច និងសង្គមជាតិទាំងមូល។ ក្នុងន័យនេះ ផលវិបាកចម្បងៗ រួមមាន៖

- **ការលួចអត្តសញ្ញាណផ្នែកហិរញ្ញវត្ថុ (Financial Identity Theft)**

នេះជាប្រភេទនៃការលួចអត្តសញ្ញាណដែលរីករាលដាល និងងាយចំណាំបំផុត។ ជនល្មើសនឹងកេងប្រវ័ញ្ចលើទិន្នន័យផ្ទាល់ខ្លួន ឬទិន្នន័យធនាគារដែលលួចបាន ដើម្បីចូលប្រើប្រាស់គណនី, ស្នើសុំកាតឥណទាន, ខ្ចីប្រាក់ ឬធ្វើប្រតិបត្តិការហិរញ្ញវត្ថុដោយគ្មានការអនុញ្ញាត។ ជនរងគ្រោះភាគច្រើនដឹងខ្លួន លុះត្រាតែប្រវត្តិឥណទានរបស់ពួកគេត្រូវបានគេរាយការណ៍ ឬនៅពេលដែលបំណុលនានាចាប់ផ្តើមលេចឡើង។ ផ្អែកលើបទពិសោធក្នុងការដាក់ឱ្យប្រើប្រាស់ប្រព័ន្ធប្រឆាំងការសម្អាតប្រាក់ (AML) និងប្រព័ន្ធសម្គាល់អត្តសញ្ញាណអតិថិជន (KYC) នៅតាមគ្រឹះស្ថានហិរញ្ញវត្ថុបង្ហាញថា ការលួចអត្តសញ្ញាណផ្នែកហិរញ្ញវត្ថុជាញឹកញាប់មានប្រភពចេញពីយុទ្ធនាការបោកប្រាស់តាមអ៊ីនធឺណិត (Phishing Campaigns) ឬការលេចធ្លាយទិន្នន័យក្នុងទ្រង់ទ្រាយធំ។

- **ការលួចអត្តសញ្ញាណផ្នែកព្រហ្មទណ្ឌ (Criminal Identity Theft)**

នៅក្នុងករណីនៃការលួចអត្តសញ្ញាណផ្នែកព្រហ្មទណ្ឌ ជនល្មើសបានយកព័ត៌មានលម្អិតរបស់បុគ្គលម្នាក់ទៀតទៅប្រើប្រាស់ នៅពេលដែលពួកគេត្រូវបានឃាត់ខ្លួន ឬសាកសួរដោយមន្ត្រីអនុវត្តច្បាប់។ ផលវិបាកដែលកើតឡើងអាចមានសភាពធ្ងន់ធ្ងរខ្លាំង ចាប់តាំងពីការជាប់ឈ្មោះក្នុងប្រវត្តិរូបព្រហ្មទណ្ឌទាំងអយុត្តិធម៌ រហូតដល់ការចេញដីកាចាប់ខ្លួនខុសមនុស្ស ដែលបង្កឱ្យមានការខូចកេរ្តិ៍ឈ្មោះ និងជាប់ពាក់ព័ន្ធក្នុងផ្លូវច្បាប់រយៈពេលវែង។

- **ការលួចអត្តសញ្ញាណផ្នែកវេជ្ជសាស្ត្រ (Medical Identity Theft)**

ការលួចអត្តសញ្ញាណផ្នែកវេជ្ជសាស្ត្រ កើតឡើងនៅពេលដែលព័ត៌មានសម្គាល់ខ្លួនផ្នែកសុខាភិបាលដែលលួចបាន ត្រូវបានយកទៅប្រើប្រាស់ដើម្បីទទួលបានការព្យាបាល, ការទិញឧបករណ៍វេជ្ជសាស្ត្រ ឬការទិញឱសថតាមវេជ្ជបញ្ជា។ ក្រៅពីផលប៉ះពាល់ផ្នែកហិរញ្ញវត្ថុ ការលួច

អត្តសញ្ញាណប្រភេទនេះអាចធ្វើឱ្យខូចខាតដល់ប្រវត្តិនៃការព្យាបាលរបស់បុគ្គលម្នាក់ ដែលបង្កឱ្យមានភាពមិនត្រឹមត្រូវ និងគ្រោះថ្នាក់យ៉ាងខ្លាំងដល់ដំណើរការថែទាំសុខភាពនៅថ្ងៃអនាគត។

- **ការបង្កើតអត្តសញ្ញាណសិប្បនិម្មិតដើម្បីបោកប្រាស់ (Synthetic Identity Theft)**

ការបង្កើតអត្តសញ្ញាណសិប្បនិម្មិត គឺជាទម្រង់នៃការបោកប្រាស់ដ៏ពេញនិយមមួយ ហើយក៏ជាប្រភេទនៃការលួចអត្តសញ្ញាណដែលមានលក្ខណៈស្មុគស្មាញ និងរីកដុះដាលលឿនបំផុតមួយផងដែរ។ ជនល្មើសនឹងយកទិន្នន័យសម្គាល់ខ្លួនពិតប្រាកដមកបញ្ចូលគ្នាជាមួយទិន្នន័យដែលប្រឌិតឡើង ដើម្បីបង្កើតជាអត្តសញ្ញាណថ្មីស្រឡាងមួយ ដែលមើលទៅហាក់បីដូចជាស្របច្បាប់។ ប្រវត្តិរូបសិប្បនិម្មិតទាំងនេះអាចលាក់ខ្លួនក្នុងប្រព័ន្ធដោយមិនមានការសង្ស័យ រហូតដល់ឱកាសល្អមកដល់ ទើបពួកគេប្រើប្រាស់វា ដើម្បីបោកប្រាស់ក្នុងទម្រង់ណាមួយជាដើម។

- **ការលួចអត្តសញ្ញាណផ្នែកឌីជីថល និងអនឡាញ (Digital and Online Identity Theft)**

ការរីកចម្រើននៃបណ្ដាញសង្គមបានបើកផ្លូវថ្មីៗ សម្រាប់ការយកអត្តសញ្ញាណទៅប្រើប្រាស់ក្នុងផ្លូវខុស។ ជនបោកប្រាស់តែងតែលួចចម្លងប្រវត្តិរូប (Clone Profiles) ក្លែងបន្លំជាបុគ្គលសាធារណៈ ឬសូម្បីតែប្រើប្រាស់បច្ចេកវិទ្យា Deepfake ដើម្បីបោកប្រាស់អ្នកដទៃ។ ការក្លែងបន្លំអត្តសញ្ញាណឌីជីថលទាំងនេះ អាចបំផ្លាញកេរ្តិ៍ឈ្មោះ, បង្កលក្ខណៈងាយស្រួលដល់ការបំភ័ន្ត ឬបោកប្រាស់ទំនុកចិត្តនៅលើប្រព័ន្ធអ៊ីនធឺណិត។

- **ការលួចគ្រប់គ្រងគណនី (Account Takeover - ATO)**

ការលួចគ្រប់គ្រងគណនី កើតឡើងនៅពេលដែលគណនីស្របច្បាប់មួយត្រូវបានគេលួចបន្លំចូលប្រើប្រាស់ តាមរយៈការបោកប្រាស់តាមអ៊ីនធឺណិត (Phishing), ការវាយប្រហារដោយសាកល្បងលេខសម្ងាត់ដោយស្វ័យប្រវត្តិ (Credential Stuffing) ឬការលួចប្ដូរប្រព័ន្ធស៊ីមកាត (SIM-swapping)។ នៅពេលដែលចូលទៅក្នុងប្រព័ន្ធបានសម្រេច ជនល្មើសអាចផ្លាស់ប្ដូរលេខសម្ងាត់ លួចដកយកថវិកា ឬក្លែងបន្លំធ្វើជាជនរងគ្រោះ ដើម្បីបន្តសកម្មភាពបោកប្រាស់ដទៃទៀត។

III. វិធីសាស្ត្រក្នុងការការពារអត្តសញ្ញាណឌីជីថល

ការការពារអត្តសញ្ញាណឌីជីថលមិនមែនជាកាតព្វកិច្ចដាច់ដោយឡែកសម្រាប់តែបុគ្គលម្នាក់ៗឡើយ ប៉ុន្តែជាតម្រូវការយុទ្ធសាស្ត្រចាំបាច់មិនអាចខ្វះបាន សម្រាប់អាជីវកម្ម, ស្ថាប័នក្នុងវិស័យឯកជន និងវិស័យរដ្ឋផងដែរ។ ការធ្វេសប្រហែសអាចបង្កជាផលប៉ះពាល់ដល់សាធារណជន, ការខូចខាតកេរ្តិ៍ឈ្មោះស្ថាប័ន, ការបាត់បង់ទំនុកចិត្តពីអតិថិជន និងការខាតបង់ថវិកាយ៉ាងធ្ងន់ធ្ងរ។ ទាំងបុគ្គល និងស្ថាប័ននីមួយៗចាំបាច់ត្រូវតែមានយន្តការផ្ទៀងផ្ទាត់ដ៏រឹងមាំ ដើម្បីធានាឱ្យបានថា បុគ្គលដែលកំពុងចូលប្រើប្រាស់ប្រព័ន្ធ និងទិន្នន័យទាំងនោះ គឺជាម្ចាស់អត្តសញ្ញាណពិតប្រាកដ មិនមែនជាការលួចបន្លំ។ ហេតុនេះ មានវិធានការសំខាន់ៗមួយចំនួនដែលត្រូវបានណែនាំសម្រាប់ការគ្រប់គ្រងអត្តសញ្ញាណឌីជីថលប្រកបដោយសុវត្ថិភាព ដូចជា៖

ការយល់ដឹង និងការបណ្តុះបណ្តាល

អ្នកប្រើប្រាស់ បុគ្គលិក និងដៃគូសហការ ត្រូវតែយល់ដឹងឱ្យបានច្បាស់អំពីហានិភ័យ, វិធីសាស្ត្រល្អៗ និងការអនុវត្តប្រកបដោយសុវត្ថិភាព ដូចជា របៀបសម្គាល់ការលួចបន្លំតាមប្រព័ន្ធអ៊ីនធឺណិត (Phishing), ការមិនចែករំលែកទិន្នន័យដែល Sensitive និងការគ្រប់គ្រងដានឌីជីថល (Digital Footprints) របស់ខ្លួនដោយប្រុងប្រយ័ត្ន។

ការផ្ទៀងផ្ទាត់ពហុកត្តា (MFA / 2FA)

ការប្រើប្រាស់ត្រឹមតែពាក្យសម្ងាត់ គឺមិនទាន់គ្រប់គ្រាន់ឡើយ។ ការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវរួមមាន លេខកូដដែលផ្ញើទៅកាន់ទូរសព្ទដៃ (Tokens) ឬជីវមាត្រ (Biometrics - ដូចជាការស្កេនក្រយៅដៃ ឬទម្រង់មុខ) នឹងជួយពង្រឹងសុវត្ថិភាពបន្ថែមទៀត ដែលអាចជួយកាត់បន្ថយហានិភ័យនៃការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាតបានយ៉ាងមានប្រសិទ្ធភាព។

ការគ្រប់គ្រងពាក្យសម្ងាត់ប្រកបដោយការទទួលខុសត្រូវ

ត្រូវប្រើប្រាស់ពាក្យសម្ងាត់ដែលខ្លាំង និងប្លែកៗគ្នាសម្រាប់សេវាកម្មនីមួយៗ ហើយជៀសវាងដាច់ខាតនូវការប្រើប្រាស់ពាក្យសម្ងាត់ជាន់គ្នា។ អ្នកអាចប្រើប្រាស់កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager) ដើម្បីជាជំនួយនៃការចងចាំ។

គោលការណ៍ផ្តល់សិទ្ធិអប្បបរមា

នៅក្នុងបរិបទនៃអាជីវកម្ម ឬស្ថាប័ន ត្រូវកម្រិតសិទ្ធិចូលប្រើប្រាស់ទៅកាន់បុគ្គលណាដែលចាំបាច់បំផុតប៉ុណ្ណោះ, គ្រប់គ្រងការអនុញ្ញាតដោយប្រុងប្រយ័ត្ន និងត្រួតពិនិត្យជាប្រចាំនូវអ្នកដែលមានសិទ្ធិលើទិន្នន័យដែល Sensitive។

ការត្រួតពិនិត្យ និងការកាត់បន្ថយដានជើងឌីជីថល ដែលមិនចាំបាច់

ត្រូវតាមដានរាល់ការចូលប្រើប្រាស់ដែលគួរឱ្យសង្ស័យ, សកម្មភាពខុសប្លែកពីធម្មតា ឬការប៉ុនប៉ងមិនប្រក្រតីណាមួយ។ គួរធ្វើការជាមួយប្រព័ន្ធណា ដែលអាចបង្កើតកំណត់ហេតុនៃព្រឹត្តិការណ៍ចូលប្រើប្រាស់ (Access Logs) និងអនុញ្ញាតឱ្យមានការធ្វើសវនកម្មបាន។ ជាមួយគ្នានេះ ត្រូវពិនិត្យឡើងវិញនូវទិន្នន័យផ្ទាល់ខ្លួនដែលបានបង្ហាញជាសាធារណៈ ដូចជា ប្រវត្តិរូបសាធារណៈ (Public Profiles), ការអនុញ្ញាតសិទ្ធិ (Permissions) និងទិន្នន័យដែលបានចែករំលែក ព្រមទាំងលុបគណនីដែលឈប់ប្រើប្រាស់ និងកំណត់ការបង្ហាញខ្លួននៅលើបណ្តាញផ្សព្វផ្សាយសង្គម ឬទីសាធារណៈផ្សេងៗ។

តាមដានរបាយការណ៍ឥណទាន និងបិទការប្រើប្រាស់បណ្តោះអាសន្ន ប្រសិនបើមិនមានការស្នើសុំកម្ចី

អ្នកប្រើប្រាស់ត្រូវពិនិត្យមើលរបាយការណ៍ឥណទានឥតគិតថ្លៃប្រចាំឆ្នាំ, ការបង្កើតគណនីថ្មី

និងមានសកម្មភាពណាមួយគួរឱ្យសង្ស័យ។ បន្ថែមលើនេះ ត្រូវយកចិត្តទុកដាក់តាមដានរបាយការណ៍គណនីធនាគារផងដែរ ព្រោះឧក្រិដ្ឋជនបច្ចេកវិទ្យាភាគច្រើន តែងតែលាក់បាំងប្រតិបត្តិការបន្លំរបស់ពួកគេជាមួយប្រតិបត្តិការស្របច្បាប់ប្រចាំថ្ងៃរបស់អ្នកប្រើប្រាស់ពិតប្រាកដ។ លើសពីនេះ ការដាក់កម្រិតបិទឥណទានបណ្ដោះអាសន្ន (Credit Freeze) គឺជាវិធីសាស្ត្រទប់ស្កាត់ជនលួចបន្លំអត្តសញ្ញាណមិនឱ្យយកឈ្មោះរបស់អ្នកប្រើប្រាស់ទៅស្នើសុំកម្ចី ឬសុំឥណទានផ្សេងៗដោយមិនដឹងខ្លួន។

- **ប្រើប្រាស់សេវាកម្មការពារការលួចបន្លំអត្តសញ្ញាណ**

ប្រើប្រាស់កម្មវិធីការពារការលួចបន្លំអត្តសញ្ញាណ ដូចជា Acronis True Image ដែលធ្វើការស្កេនជាប្រចាំនៅលើបណ្ដាញ Dark web ដើម្បីស្វែងរកព័ត៌មានងាយរងគ្រោះរបស់អ្នក។ កម្មវិធីនេះនឹងជូនដំណឹងដល់អ្នកភ្លាមៗប្រសិនបើទិន្នន័យត្រូវបានវាយប្រហារ និងណែនាំជាជំហានៗក្នុងដំណើរការស្ដារទិន្នន័យឡើងវិញ។ គួរស្វែងរកឧបករណ៍ណាដែលមានផ្ដល់មុខងារតាមដានឥណទាន, ការព្រមានអំពីការធ្លាយទិន្នន័យ, ការចម្លងទុកទិន្នន័យដោយសុវត្ថិភាព (Secure Backup), ធានារ៉ាប់រង និងការគាំទ្រពីអ្នកជំនាញ។

- **ការពារឧបករណ៍របស់អ្នកដោយប្រើកម្មវិធីកម្ចាត់មេរោគ និង Encryption**

ទូរសព្ទ និងកុំព្យូទ័រ ត្រូវទទួលបានការការពារគ្រប់គ្រាន់ ដោយបំពាក់កម្មវិធីកម្ចាត់មេរោគ (Antivirus) ដែលគួរឱ្យទុកចិត្ត ដើម្បីរារាំងមេរោគបំផ្លិចបំផ្លាញ (Malware) និងកម្មវិធីលួចមើលការសម្ងាត់ (Spyware)។ ត្រូវបើកមុខងារ Full-disk Encryption ដើម្បីធានាថា ទោះបីជាឧបករណ៍ត្រូវជនខិលខូចលួចក៏ដោយ ក៏ព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នកនៅតែមានសុវត្ថិភាព។ លើសពីនេះ ត្រូវធ្វើបច្ចុប្បន្នភាពប្រព័ន្ធប្រតិបត្តិការ និងកម្មវិធីទូរសព្ទដៃឱ្យបានជាប់ជានិច្ច ព្រោះកំណែទម្រង់ទាំងនេះនឹងជួយពង្រឹងសុវត្ថិភាពបន្ថែមបាន។

- **ជៀសវាងការប្រើប្រាស់ប្រព័ន្ធ Wi-Fi សាធារណៈសម្រាប់សកម្មភាពងាយរងគ្រោះ**

ត្រូវជៀសវាងដាច់ខាតនូវការប្រើប្រាស់បណ្ដាញ Wi-Fi សាធារណៈ សម្រាប់រាល់សកម្មភាពទាំងឡាយណាដែលតម្រូវឱ្យបញ្ចូលព័ត៌មានផ្ទាល់ខ្លួន ឬព័ត៌មានហិរញ្ញវត្ថុ។ បណ្ដាញភ្ជាប់ទាំងនេះអាចនឹងងាយមានហានិភ័យណាស់ ដែលវាងាយស្រួលបំផុតសម្រាប់ Hackers ក្នុងការលួចយកពាក្យសម្ងាត់ ព័ត៌មានទូទាត់ប្រាក់ និងទិន្នន័យសំខាន់ៗផ្សេងទៀត។

IV. អត្ថប្រយោជន៍នៃការការពារអត្តសញ្ញាណឌីជីថល

ការផ្ទុះឡើងនៃវិបត្តិជំងឺកូវីដ-១៩ បានជំរុញឱ្យការប្រើប្រាស់សេវាកម្មឌីជីថលមានការកើនឡើងយ៉ាងឆាប់រហ័ស ដែលកត្តានេះបានបង្កើតជាតម្រូវការចាំបាច់សម្រាប់ដំណោះស្រាយអត្តសញ្ញាណឌីជីថល ដើម្បីធានាបាននូវការចូលប្រើប្រាស់សេវាកម្មពីចម្ងាយប្រកបដោយសុវត្ថិភាព។ និន្នាការនេះនៅតែបន្តកើនឡើងជាលំដាប់ ដែលជាលទ្ធផលចាប់តាំងពីឆ្នាំ២០២០ មក យើងបានសង្កេតឃើញ

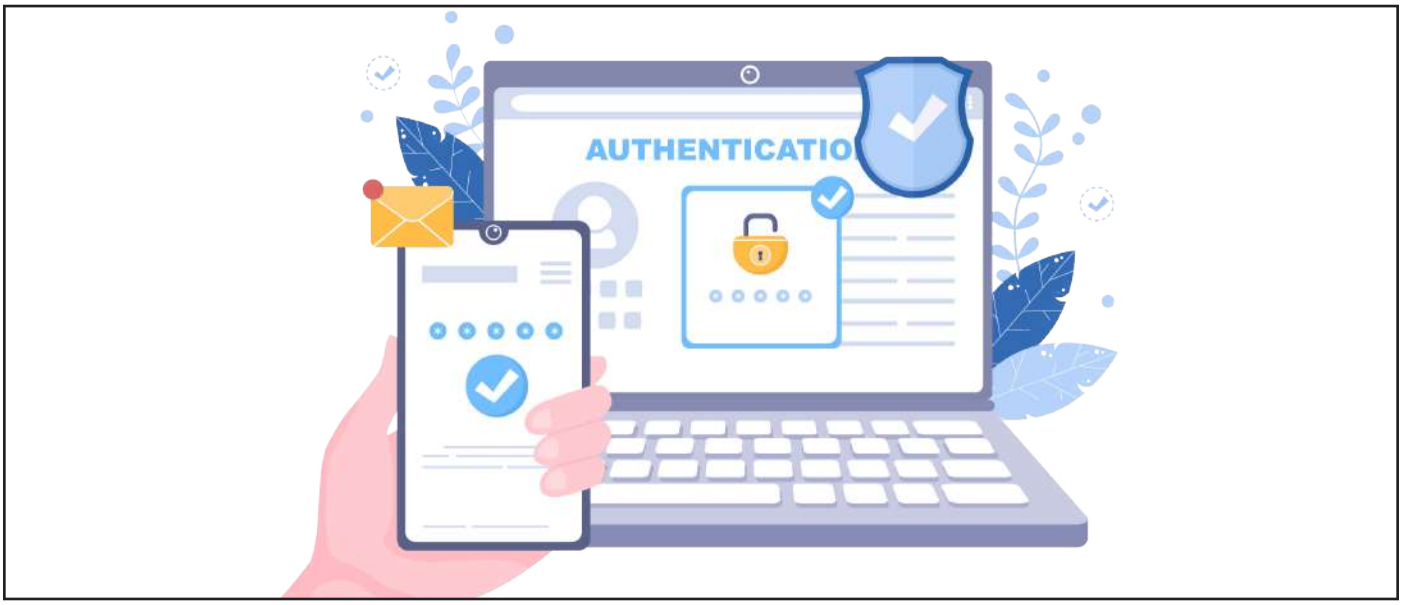
ការធ្វើបរិវត្តកម្មឌីជីថលលើសេវាកម្មយ៉ាងទូលំទូលាយនៅគ្រប់វិស័យ រួមមាន ធនាគារ, សុខាភិបាល និងការអប់រំជាដើម។ ទន្ទឹមនឹងនេះ ការកើនឡើងនៃសេវាកម្មឌីជីថល ដូចជា ការធ្វើពាណិជ្ជកម្មតាមប្រព័ន្ធអេឡិចត្រូនិក (E-commerce) ក៏បានជំរុញឱ្យមានការអភិវឌ្ឍប្រព័ន្ធអត្តសញ្ញាណឌីជីថលដែលអាចផ្ទៀងផ្ទាត់អត្តសញ្ញាណអ្នកប្រើប្រាស់បានលឿន និងមានសុវត្ថិភាពខ្ពស់ សំដៅសម្រួលដល់ប្រតិបត្តិការអនឡាញឱ្យកាន់តែរលូន។ ទោះជាយ៉ាងណា ការរីកចម្រើននេះ ក៏បាននាំមកនូវការកើនឡើងនូវហានិភ័យ និងការគំរាមកំហែងលើសុវត្ថិភាពតាមប្រព័ន្ធអ៊ីនធឺណិតផងដែរ។

ក្នុងន័យនេះ ការការពារអត្តសញ្ញាណឌីជីថល បានក្លាយជាការការពារដ៏មានសារៈសំខាន់បំផុតសម្រាប់បុគ្គល និងស្ថាប័ន នៅក្នុងយុគសម័យដែលការរស់នៅ និងប្រតិបត្តិការការងារត្រូវពឹងផ្អែកលើប្រព័ន្ធអ៊ីនធឺណិត និងបច្ចេកវិទ្យា។ ការយល់ដឹង និងការយកចិត្តទុកដាក់លើកិច្ចការពារនេះ ផ្តល់នូវអត្ថប្រយោជន៍ជាច្រើន ដូចជា៖

● ការការពារទ្រព្យសម្បត្តិ និងសុវត្ថិភាពហិរញ្ញវត្ថុ

អត្ថប្រយោជន៍ចម្បងមួយនៃការការពារអត្តសញ្ញាណឌីជីថល គឺការទប់ស្កាត់អំពើឆបោកផ្នែកហិរញ្ញវត្ថុ និងការលួចបន្លំក្នុងការធ្វើប្រតិបត្តិការនានាលើគណនីធនាគារ។ នៅពេលដែលទិន្នន័យផ្ទាល់ខ្លួន ដូចជា លេខសម្ងាត់, លេខកូដ PIN, ឬព័ត៌មានកាតធនាគារ ត្រូវបានការពារយ៉ាងរឹងមាំ ជនខិលខូចមិនអាចចូលទៅធ្វើប្រតិបត្តិការហិរញ្ញវត្ថុ, បង្កើតបំណុលក្លែងក្លាយ ឬយកអត្តសញ្ញាណ

របស់យើងទៅស្នើសុំប្រាក់កម្ចីខុសច្បាប់បានឡើយ។ ការប្រុងប្រយ័ត្ននេះជួយការពារទ្រព្យសម្បត្តិរបស់សាធារណជន និងជៀសផុតពីវិបត្តិហិរញ្ញវត្ថុដែលកើតចេញពីការឆបោកអនឡាញ។

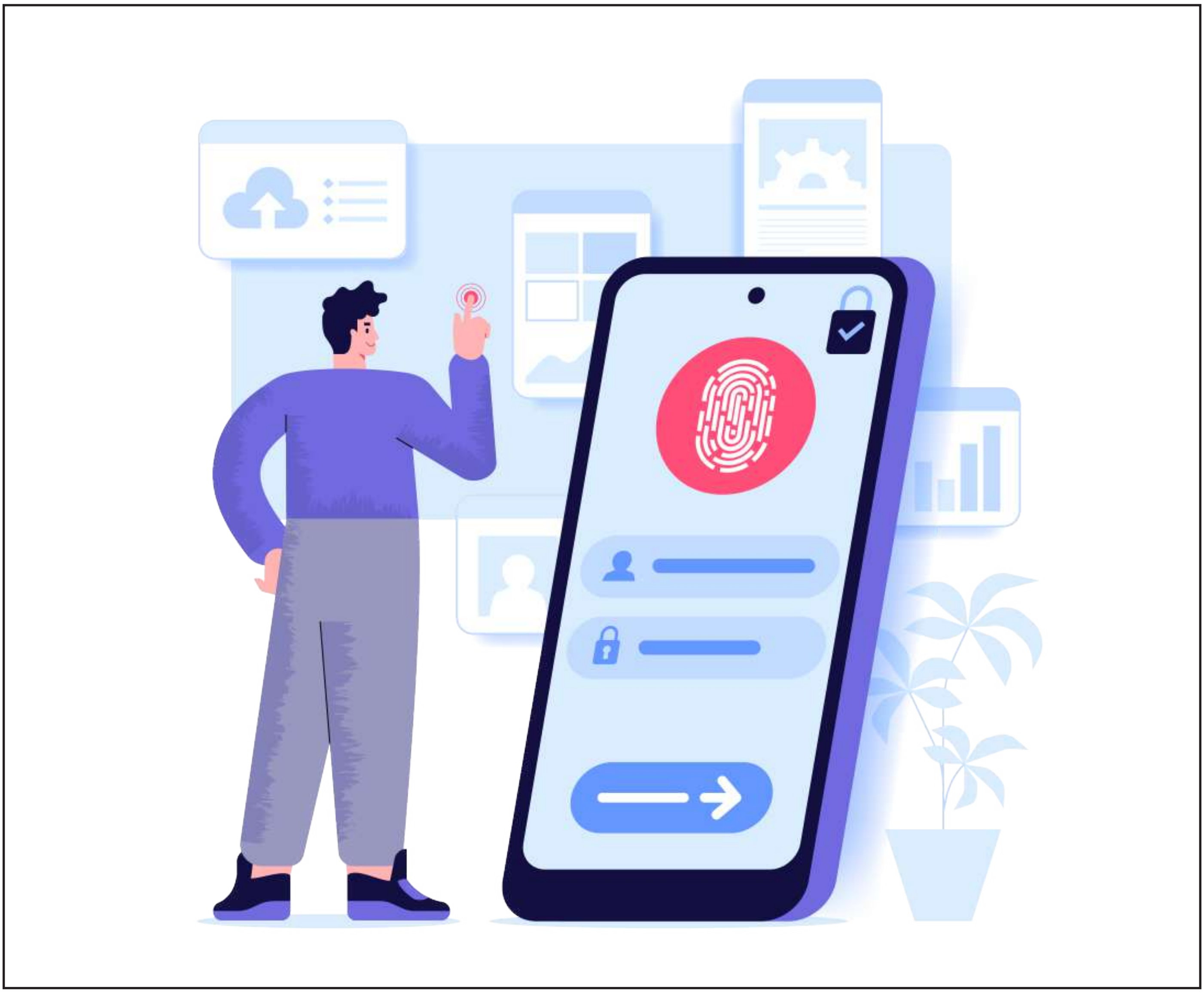


ការរក្សាឯកជនភាព និងសុវត្ថិភាពព័ត៌មានផ្ទាល់ខ្លួន

ការអនុវត្តការការពារអត្តសញ្ញាណឌីជីថលបានយ៉ាងត្រឹមត្រូវ ជួយឱ្យបុគ្គលម្នាក់ៗរក្សាបាននូវភាពម្ចាស់ការលើទិន្នន័យផ្ទាល់ខ្លួន (Data Privacy) ដោយជៀសផុតពីការលួចយកទិន្នន័យ (Data Breach) ទៅលក់បន្ត ឬយកទៅប្រើប្រាស់ក្នុងន័យមិនត្រឹមត្រូវ។ លើសពីនេះ សាធារណជនក៏អាចប្រើប្រាស់សេវាកម្មការពារអត្តសញ្ញាណឌីជីថល ដើម្បីបង្កើនការឃ្លាំមើល និងកម្រិតការចែករំលែកទិន្នន័យរបស់ខ្លួន កុំឱ្យលើសពីតម្រូវការចាំបាច់។ ជាក់ស្តែង ការគ្រប់គ្រង និងពិនិត្យមើលគណនីបណ្តាញសង្គមឱ្យបានហ្មត់ចត់ គឺជាកត្តាសំខាន់បំផុត ដោយហេតុថា បណ្តាញសង្គមជាកន្លែងដែលព័ត៌មានផ្ទាល់ខ្លួនត្រូវបានចែករំលែកដោយបើកចំហ ហើយក៏ជាគោលដៅចម្បងសម្រាប់ឧក្រិដ្ឋជនបច្ចេកវិទ្យាផងដែរ។

ការការពារកេរ្តិ៍ឈ្មោះ

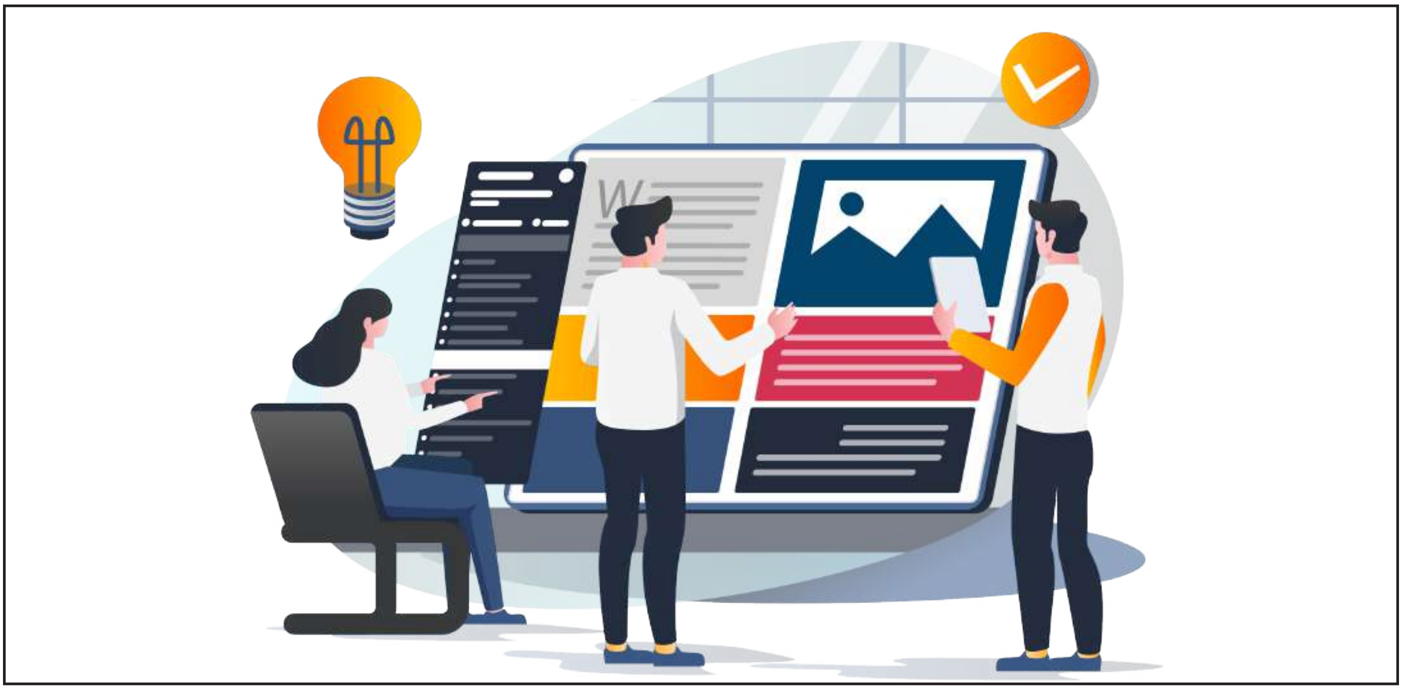
នៅពេលដែលអត្តសញ្ញាណឌីជីថលត្រូវបានគេលួចបន្លំ ជនខិលខូចអាចប្រើប្រាស់គណនីបណ្តាញសង្គម ឬអ៊ីមែលរបស់ជនរងគ្រោះទៅប្រព្រឹត្តសកម្មភាពអវិជ្ជមាន ដូចជា ផ្ញើសារបោកប្រាស់សាច់ញាតិ និងមិត្តភក្តិ ឬបង្កើតមាតិកាខុសច្បាប់ ដែលធ្វើឱ្យប៉ះពាល់ដល់កិត្តិយស និងកេរ្តិ៍ឈ្មោះរបស់ជនរងគ្រោះ។ ដូច្នេះ ការពង្រឹងសុវត្ថិភាពអត្តសញ្ញាណឌីជីថល គឺមិនត្រឹមតែការពារទិន្នន័យផ្ទាល់ខ្លួនប៉ុណ្ណោះទេ ប៉ុន្តែក៏ជាខែលការពារកេរ្តិ៍ឈ្មោះ ភាពស្អាតស្អំ និងទំនុកចិត្តដែលបុគ្គលម្នាក់បានកសាងមកផងដែរ។



ការធានានិរន្តរភាពការងារ និងឱកាសអាជីវកម្ម

សម្រាប់បុគ្គលិក និងម្ចាស់អាជីវកម្មក្នុងយុគសម័យឌីជីថលនេះ គណនីការងារ, អ៊ីមែលផ្លូវការ និងអត្តសញ្ញាណឌីជីថល គឺជាឧបករណ៍យុទ្ធសាស្ត្រក្នុងការប្រាស្រ័យទាក់ទង និងធ្វើប្រតិបត្តិការអាជីវកម្ម។ ការការពារអត្តសញ្ញាណឌីជីថលបានល្អ ជួយការពារទិន្នន័យសម្ងាត់របស់ក្រុមហ៊ុន/ស្ថាប័ន, ជៀសវាងការខាតបង់ឱកាសអាជីវកម្មដោយសារការផ្អាកដំណើរការប្រព័ន្ធ, ទទួលបាន

ទំនុកចិត្តពីអតិថិជន, មានការអនុលោមតាមបទប្បញ្ញត្តិត្រឹមត្រូវ និងការពារមិនឱ្យដៃគូពាណិជ្ជកម្ម បាត់បង់ទំនុកចិត្តមកលើរូបអ្នក ឬស្ថាប័នរបស់អ្នកឡើយ។



ការចូលរួមចំណែកកសាងសេដ្ឋកិច្ច-សង្គមឌីជីថល ដែលមានសុវត្ថិភាព

នៅពេលដែលបុគ្គលម្នាក់ៗមានអក្ខរកម្មឌីជីថល និងចេះការពារអត្តសញ្ញាណរបស់ខ្លួន នឹងបង្កើតបានជាខែលការពាររួមមួយសម្រាប់សហគមន៍ទាំងមូល។ ការប្រុងប្រយ័ត្នផ្ទាល់ខ្លួន នឹងកាត់បន្ថយឱកាសនៃការរីករាលដាលនៃហានិភ័យបណ្ដាលមកពីការឆបោកផ្សេងៗ ដែលធ្វើឱ្យប្រព័ន្ធអេកូឡូស៊ីនៃសេដ្ឋកិច្ច និងសង្គមឌីជីថលទាំងមូលមានភាពរឹងមាំ និងឆ្លើយតបទៅនឹងស្តង់ដាសុវត្ថិភាពសកល ដែលជាបច្ច័យជួយទាក់ទាញការវិនិយោគ និងបង្កើនទំនុកចិត្តដល់សាធារណជនគ្រប់រូប។

V. ករណីសិក្សា

ប្រទេសកម្ពុជា

ការកសាងប្រព័ន្ធអត្តសញ្ញាណឌីជីថលនៅកម្ពុជា ស្ថិតក្នុងដំណាក់កាលនៃការអនុវត្តដំបូងនៅឡើយ ប៉ុន្តែយើងបានសង្កេតឃើញការរីកចម្រើនគួរឱ្យកត់សម្គាល់ ផ្នែកហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យា និងក្របខណ្ឌគោលនយោបាយ ដែលគាំទ្រដល់ដំណើរការការអភិវឌ្ឍ និងការជំរុញការប្រើប្រាស់អត្តសញ្ញាណឌីជីថល។ ប៉ុន្តែ ប្រព័ន្ធនេះនៅតែត្រូវការការជំរុញបន្ថែមលើការចូលរួមប្រើប្រាស់ពីសាធារណជន និងការរៀបចំច្បាប់ការពារទិន្នន័យឱ្យបានពេញលេញ ដើម្បីធានាបាននូវប្រព័ន្ធអេកូឡូស៊ីឌីជីថលដែលមានសុវត្ថិភាព និងបរិយាបន្ន។ ក្នុងន័យនេះ រាជរដ្ឋាភិបាលបានចាត់ទុកការកសាងអត្តសញ្ញាណឌីជីថលជាអាទិភាពជាតិមិនអាចខ្វះបាន ក្នុងការធ្វើបរិវត្តកម្មឌីជីថល សំដៅកសាងសេដ្ឋកិច្ច-សង្គមឌីជីថល។ ដើម្បីឆ្លើយតបនឹងគោលដៅនេះ ស្ថាប័នពាក់ព័ន្ធបាននិងកំពុងអនុវត្តកិច្ចការគន្លឹះៗយ៉ាងសកម្ម តាមរយៈកិច្ចខិតខំប្រឹងប្រែង ដូចជា៖

- **ច្បាប់ស្តីពីអត្រានុកូលដ្ឋាន ស្ថិតិអត្រានុកូលដ្ឋាន និងអត្តសញ្ញាណកម្ម**

ច្បាប់នេះត្រូវបានរដ្ឋសភាអនុម័តកាលពីថ្ងៃទី១២ ខែមិថុនា ឆ្នាំ២០២៣ ក្នុងការកំណត់អំពីវិធាន និងនីតិវិធីដែលទាក់ទងនឹងការចុះបញ្ជីអត្រានុកូលដ្ឋាន, ការចុះបញ្ជីស្នាក់នៅ, ការរៀបចំស្ថិតិអត្រានុកូលដ្ឋាន, ការចុះបញ្ជីអត្តសញ្ញាណបុគ្គល និងការរៀបចំនិងការគ្រប់គ្រងបញ្ជីប្រជាជន ក្នុងគោលបំណងដើម្បីធានាឱ្យមានការចុះបញ្ជីអត្រានុកូលដ្ឋាន, ការចុះបញ្ជីស្នាក់នៅ និងការចុះបញ្ជីអត្តសញ្ញាណបុគ្គលជាសកល ដោយជាប់លាប់និងជាអចិន្ត្រៃយ៍ និងធានាឱ្យមនុស្សគ្រប់រូបមានអត្តសញ្ញាណខាងផ្លូវច្បាប់ ដោយបុគ្គលម្នាក់ត្រូវបានផ្តល់លេខកូដសម្គាល់អត្តសញ្ញាណបុគ្គលមួយ។ ច្បាប់នេះក៏បានគិតគូរអំពីការប្រើប្រាស់ទិន្នន័យ, ការការពារឯកជនភាពបុគ្គល និងសន្តិសុខទិន្នន័យ។ ទាំងអស់នេះ នឹងចូលរួមចំណែកយ៉ាងសំខាន់ជាមូលដ្ឋានឈានទៅការកសាង និងអភិវឌ្ឍអត្តសញ្ញាណឌីជីថលដែលជាគោលដៅរបស់រាជរដ្ឋាភិបាលផងដែរ។

- **សេចក្តីព្រាងច្បាប់ស្តីពីកិច្ចការពារទិន្នន័យបុគ្គលនៃព្រះរាជាណាចក្រកម្ពុជា**

ច្បាប់នេះកំណត់អំពីគោលការណ៍ វិធាន និងយន្តការគ្រប់គ្រងនៃការធ្វើប្រព្រឹត្តកម្មទិន្នន័យបុគ្គលដោយមានការទទួលខុសត្រូវ តម្លាភាព និងប្រកបដោយក្រមសីលធម៌ ក្នុងគោលបំណងការពារសិទ្ធិរបស់ប្រធានទិន្នន័យ និងលើកកម្ពស់បរិយាកាសវិនិយោគ ការប្រកួតប្រជែង និងការអភិវឌ្ឍពាណិជ្ជកម្មជាតិ និងអន្តរជាតិក្នុងបរិបទនៃសេដ្ឋកិច្ច និងសង្គមឌីជីថល។

- **សេចក្តីព្រាងច្បាប់ស្តីពីរដ្ឋាភិបាលឌីជីថលនៃព្រះរាជាណាចក្រកម្ពុជា**

ច្បាប់នេះកំណត់អំពីគោលការណ៍ វិធាន និងយន្តការកសាងរដ្ឋាភិបាលឌីជីថល តាមរយៈការប្រើប្រាស់បច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន ក្នុងគោលបំណងអភិវឌ្ឍសេវាឌីជីថល ហេដ្ឋារចនាសម្ព័ន្ធ

ឌីជីថល និងអភិបាលកិច្ចទិន្នន័យ សម្រាប់រដ្ឋាភិបាលទាំងមូល ដើម្បីលើកកម្ពស់គុណភាពជីវិត និងទំនុកចិត្តប្រជាពលរដ្ឋតាមរយៈការបម្រើសេវាសាធារណៈឱ្យកាន់តែល្អប្រសើរ។

ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា ឆ្នាំ២០២១-២០៣៥

រាជរដ្ឋាភិបាលបានដាក់ចេញនូវ **ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា ២០២១ - ២០៣៥** ជាមួយចក្ខុវិស័យច្បាស់លាស់មួយគឺ "ការកសាងសេដ្ឋកិច្ច និងសង្គមឌីជីថលរស់រវើក តាមរយៈការរៀបចំមូលដ្ឋានគ្រឹះជំរុញការទទួលយក និងបរិវត្តកម្មឌីជីថល នៅក្នុងគ្រប់តួអង្គសង្គម ទាំងរដ្ឋ ទាំងពលរដ្ឋ និងទាំងធុរជន ដើម្បីជំរុញសន្ទុះកំណើនសេដ្ឋកិច្ចថ្មី និងលើកកម្ពស់សុខុមាលភាពសង្គម តាមគន្លងប្រក្រតីភាពថ្មី"។ ដើម្បីកសាងសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជាតាមចក្ខុវិស័យនេះ ក្របខណ្ឌគោលនយោបាយនេះបានកំណត់យកគោលដៅចម្បងចំនួន ៥ រួមមាន៖ ការអភិវឌ្ឍហេដ្ឋារចនាសម្ព័ន្ធ, ការកសាងទំនុកចិត្ត និងភាពជឿជាក់លើប្រព័ន្ធឌីជីថល, ការកសាងពលរដ្ឋឌីជីថល, ការកសាងរដ្ឋាភិបាលឌីជីថលឌីជីថល និងការជំរុញធុរកិច្ចឌីជីថល។ ក្នុងនោះមានការអនុវត្តវិធានការជាក់លាក់មួយចំនួនទាក់ទងនឹងការរៀបចំ និងជំរុញការប្រើប្រាស់អត្តសញ្ញាណឌីជីថលឱ្យបានទូលំទូលាយ ទាំងចំពោះប្រជាពលរដ្ឋ, ស្ថាប័នឯកជន និងស្ថាប័នសាធារណៈ។

គោលនយោបាយរដ្ឋាភិបាលឌីជីថលកម្ពុជា ២០២២-២០៣៥

រាជរដ្ឋាភិបាលបានដាក់ចេញនូវ គោលនយោបាយរដ្ឋាភិបាលឌីជីថលកម្ពុជា ២០២២-២០៣៥ ក្នុងគោលបំណងកសាងរដ្ឋាភិបាលឆ្លាត ដោយឈរលើមូលដ្ឋាននៃការប្រើប្រាស់ហេដ្ឋារចនាសម្ព័ន្ធ និងបច្ចេកវិទ្យាជាប្រព័ន្ធអេកូឡូស៊ី សម្រាប់ការធ្វើទំនើបកម្មប្រព័ន្ធអភិបាលកិច្ច និងការកែទម្រង់ប្រកបដោយតម្លាភាព និងភាពជឿទុកចិត្ត ដើម្បីអភិវឌ្ឍសេដ្ឋកិច្ច និងសង្គមឌីជីថលប្រកបដោយបរិយាបន្ន។ ដើម្បីសម្រេចបាននូវចក្ខុវិស័យនេះ រាជរដ្ឋាភិបាលបានដាក់ចេញគោលដៅជាយុទ្ធសាស្រ្តចំនួន ៤ និងយុទ្ធសាស្រ្តចំនួន ១០ ព្រមទាំងសកម្មភាពជាអាទិភាពនៃយុទ្ធសាស្រ្តជាច្រើន ដោយក្នុងនោះមានការរៀបចំ និងពង្រឹងហេដ្ឋារចនាសម្ព័ន្ធអត្តសញ្ញាណឌីជីថល ដើម្បីគាំទ្រដល់ការគ្រប់គ្រងការប្រើប្រាស់ និងការផ្ទៀងផ្ទាត់អត្តសញ្ញាណរូបវន្តបុគ្គល និងនីតិបុគ្គលក្នុងទម្រង់ឌីជីថល សម្រាប់ធ្វើប្រតិបត្តិការលើថ្នាលឌីជីថលទាំងក្នុងក្របខណ្ឌរដ្ឋាភិបាលឌីជីថលនិងវិស័យឯកជន។

ផែនការយុទ្ធសាស្រ្តជាតិស្តីពីអត្តសញ្ញាណកម្ម ឆ្នាំ២០១៧-២០២៦

ផែនការយុទ្ធសាស្រ្តនេះត្រូវបានរាជរដ្ឋាភិបាលអនុម័តកាលពីខែមិថុនា ឆ្នាំ២០១៦ និងជាផែនការដ៏មានសារៈសំខាន់មួយដោយមានទស្សនៈវិស័យយូរអង្វែង ក្នុងការដឹកនាំតម្រង់ទិសដៅទៅលើការងារគ្រប់គ្រងទិន្នន័យ អត្តសញ្ញាណកម្មប្រជាពលរដ្ឋ តាមប្រព័ន្ធព័ត៌មានវិទ្យាបែបទំនើប និងការប្រើប្រាស់ទិន្នន័យអត្តសញ្ញាណកម្ម ដើម្បីលើកកម្ពស់ប្រសិទ្ធភាពផ្តល់សេវាសាធារណៈជូនប្រជាពលរដ្ឋ។

ផែនការយុទ្ធសាស្ត្រជាតិស្តីពីអត្តសញ្ញាណកម្ម ដំណាក់កាលទី២ ឆ្នាំ២០២៦-២០៣៥ (NSPI 2.0)

រាជរដ្ឋាភិបាលត្រៀមអនុវត្ត**ផែនការយុទ្ធសាស្ត្រជាតិស្តីពីអត្តសញ្ញាណកម្ម ដំណាក់កាលទី២ ឆ្នាំ២០២៦-២០៣៥** ក្រោយដំណាក់កាលទី១ ឆ្នាំ២០១៧-២០២៦ ដែលជិតត្រូវបានបញ្ចប់។ ផែនការនេះ គឺជាមូលដ្ឋានគ្រឹះដ៏រឹងមាំ និងជាសសរស្តម្ភលើការរៀបចំហេដ្ឋារចនាសម្ព័ន្ធសាធារណៈឌីជីថល (DPI) និងអត្តសញ្ញាណឌីជីថលនៅកម្ពុជា។ ផែនការយុទ្ធសាស្ត្រដំណាក់កាលទី២នេះ និងបន្តដោះស្រាយបញ្ហាប្រឈមដែលនៅសេសសល់ ពីការអនុវត្តផែនការយុទ្ធសាស្ត្រដំណាក់កាលទី១ ព្រមទាំងដាក់ចេញនូវផែនការកែទម្រង់ ដោយបង្កើតនូវ **«អត្តសញ្ញាណស្របច្បាប់សម្រាប់ប្រជាពលរដ្ឋខ្មែរគ្រប់រូប និងមនុស្សគ្រប់រូបដែលរស់នៅក្នុងប្រទេសកម្ពុជា»** ព្រមទាំងការកសាងនូវអត្តសញ្ញាណឌីជីថលជាតិមួយ ដែលមានសុវត្ថិភាព និងអាចជឿទុកចិត្តបាន សម្រាប់ប្រជាពលរដ្ឋខ្មែរប្រើប្រាស់ក្នុងការទទួលសេវាសាធារណៈ និងសេវាឯកជន។

ថ្នាលផ្លាស់ប្តូរទិន្នន័យកម្ពុជា (CamDX)

ថ្នាលនេះត្រូវបានអភិវឌ្ឍ និងដាក់ឱ្យប្រើប្រាស់ក្នុងឆ្នាំ២០១៩ ក្នុងគោលបំណងសម្រាប់ផ្លាស់ប្តូរទិន្នន័យដោយប្រើប្រាស់សន្ទានកម្មនៃកម្មវិធីកុំព្យូទ័រ (Application Programming Interface - API) រវាងប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានមួយ និងប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មានមួយទៀតក្នុងវិស័យសាធារណៈ និងជាមួយវិស័យឯកជន ដែលជាសមាជិក CamDX ប្រកបដោយសុវត្ថិភាពតាមរយៈប្រព័ន្ធអ៊ីនធឺណិត ឬបណ្តាញតភ្ជាប់ឌីជីថលផ្សេងៗ។ សេវាសន្ទានកម្មនៃកម្មវិធីកុំព្យូទ័រ (API) ដែលមានលើ ថ្នាល CamDX មានដូចជា សេវាផ្ទៀងផ្ទាត់ទិន្នន័យអត្តសញ្ញាណបុគ្គល [Electronic Know-Your-Customer (e-KYC) APIs], សេវាកំណត់អត្តសញ្ញាណសហគ្រាស [Electronic Know-Your-Business (e-KYB) APIs], សេវាបំប្លែងព័ត៌មានពីរូបភាពទៅជាអក្សរ [Optical Character Recognition (OCR) APIs] និង API សម្រាប់ផ្ទៀងផ្ទាត់ទិន្នន័យបណ្ណបើកបររបស់ក្រសួងសាធារណការ និងដឹកជញ្ជូន។

ថ្នាលសម្គាល់អត្តសញ្ញាណអតិថិជនឌីជីថលកម្ពុជា (CamDigikey)

ថ្នាលនេះត្រូវបានបង្កើតឡើងក្នុងឆ្នាំ២០១៩ ដើម្បីសម្គាល់អត្តសញ្ញាណអតិថិជនឌីជីថល ដែលផ្តោតលើភាពងាយស្រួល និងសុវត្ថិភាពសម្រាប់អ្នកប្រើប្រាស់។ CamDigiKey ផ្តល់ជូននូវសេវាកម្មជាច្រើន រួមមាន កម្មវិធីទូរសព្ទដៃ, សេវាកម្មធ្វើយថាភូតកម្មតែមួយដង/យថាភូតកម្មរួម (Single Sign-On Service), ការធ្វើយថាភូតកម្មជាមួយពាក្យ/លេខសម្ងាត់តិច (Password-less authentication), ការផ្តល់ Open APIs សម្រាប់ការផ្ទៀងផ្ទាត់អត្តសញ្ញាណអតិថិជន (Open KYC Verification APIs)។

បណ្ណបើកបរឌីជីថល

រាជរដ្ឋាភិបាលបានសម្រេចដាក់ឱ្យប្រើប្រាស់ **«បណ្ណបើកបរឌីជីថល»** ដែលអាចផ្ទៀងផ្ទាត់

ភាពត្រឹមត្រូវតាមរយៈថ្នាលផ្ទៀងផ្ទាត់ឯកសារ verify.gov.kh កាលពីថ្ងៃទី១៣ ខែឧសភា ឆ្នាំ២០២៦។ សាធារណជនអាចស្នើសុំបណ្ណបើកបរឌីជីថល ដាក់ក្នុង Personal Wallet លើ DG SuperApp របស់ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍ និងអាចប្រើប្រាស់រហូតដល់បណ្ណផុតសុពលភាព ដែលនេះបានជួយសន្សំសំចៃពេលវេលា, កាត់បន្ថយចំណាយ, កាត់បន្ថយការខកចិត្តដែលបណ្តាលមកពីការរង់ចាំយូរ និងការក្លែងបន្លំអត្តសញ្ញាណ។

- **យុទ្ធនាការផ្ទៀងផ្ទាត់អត្តសញ្ញាណស៊ីមកាត ជាមួយនឹងគណនីធនាគារ/គណនីទូទាត់សងប្រាក់របស់អ្នកប្រើប្រាស់**

រាជរដ្ឋាភិបាលបើក**យុទ្ធនាការផ្ទៀងផ្ទាត់ អត្តសញ្ញាណស៊ីមកាត ជាមួយនឹងគណនីធនាគារ/គណនីទូទាត់សងប្រាក់របស់អ្នកប្រើប្រាស់** កាលពីថ្ងៃទី១៧ ខែមិថុនា ឆ្នាំ២០២៦ ក្នុងគោលបំណងការពារសុវត្ថិភាពឌីជីថលរបស់ប្រជាពលរដ្ឋ និងកាត់ផ្តាច់ឫសគល់នៃបទល្មើសតាមប្រព័ន្ធបច្ចេកវិទ្យា ដើម្បីឈានទៅដល់ការលុបបំបាត់ ស៊ីមកាតគ្មានអត្តសញ្ញាណអ្នកប្រើប្រាស់ច្បាស់លាស់ និងកំពុងត្រូវបានប្រើប្រាស់នៅក្នុងប្រព័ន្ធធនាគារ។ ប្រជាពលរដ្ឋអាចផ្ទៀងផ្ទាត់អត្តសញ្ញាណស៊ីមកាតក្នុងកម្មវិធី SIM Verifier Mini App ដែលមាននៅក្នុងថ្នាលសេវាឌីជីថលរួម DG SuperApp ដែលបានតភ្ជាប់ប្រព័ន្ធស្វ័យប្រវត្តិកម្មរបស់គ្រឹះស្ថានធនាគារនិងហិរញ្ញវត្ថុ។ គំនិតផ្តួចផ្តើមនេះ ក៏នឹងរួមចំណែកក្នុងការជំរុញការធ្វើបរិវត្តកម្ម និងនវានុវត្តន៍ឌីជីថលនៅក្នុងវិស័យទូរគមនាគមន៍ និងវិស័យធនាគារ ដែលជាគន្លឹះគាំទ្រដល់សេដ្ឋកិច្ចនិងសង្គមឌីជីថលនៅកម្ពុជាផងដែរ។

- **ការប្រើប្រាស់បច្ចេកវិទ្យា Electronic Know Your Customer (e-KYC) យ៉ាងទូលំទូលាយ**

e-KYC គឺជាបច្ចេកវិទ្យាមួយដែលអាចឱ្យស្ថាប័នមួយអាចផ្ទៀងផ្ទាត់ឯកសារអតិថិជនជាឌីជីថល ជាមួយនឹងមូលដ្ឋានទិន្នន័យដែលបានផ្ទៀងផ្ទាត់ពីមុន។ សមត្ថភាព e-KYC គឺដើម្បីលើកកម្ពស់ការយល់ដឹង និងលើកកម្ពស់ការប្រើប្រាស់បច្ចេកវិទ្យា និងនវានុវត្តន៍ថ្មីៗ ជាពិសេសដើម្បីជំរុញការប្រើប្រាស់ e-KYC ក្នុងវិស័យធនាគារ និងហិរញ្ញវត្ថុ។ គ្រឹះស្ថានធនាគារ និងហិរញ្ញវត្ថុនៅកម្ពុជាជាច្រើន រួមទាំងប្រព័ន្ធទូទាត់បាគង (Bakong) បានផ្លាស់ប្តូរមកប្រើប្រាស់ការផ្ទៀងផ្ទាត់ជីវមាត្រ (Biometrics) ដូចជា ស្កេនផ្ទៃមុខ និងស្កេនអត្តសញ្ញាណប័ណ្ណ ដើម្បីបើកគណនី និងធ្វើប្រតិបត្តិការហិរញ្ញវត្ថុដោយសុវត្ថិភាព។

ប្រទេស Estonia

ប្រទេសអេស្តូនី ត្រូវបានទទួលស្គាល់យ៉ាងទូលំទូលាយថាជាប្រទេសមួយដែលមានរដ្ឋាភិបាលឌីជីថលជឿនលឿនបំផុតនៅសកលលោក។ ក្នុងនោះ ជំហានសំខាន់ពីរ បានសម្រួល និងជំរុញអត្តសញ្ញាណឌីជីថលក្នុងប្រទេសអេស្តូនី គឺទី១. ការផ្តល់លេខអត្តសញ្ញាណផ្ទាល់ខ្លួនដែលហៅថា «Isikukood» ជូនដល់ប្រជាពលរដ្ឋ និងអ្នកស្នាក់នៅក្នុងប្រទេសអេស្តូនីគ្រប់រូប និងទី២. ការចេញលិខិតឆ្លងដែនដែលមានសុពលភាព ១០ឆ្នាំ។ អេស្តូនី បានអនុវត្តវិធីសាស្ត្រ «ឌីជីថលជាចម្បង»

ដែលអនុញ្ញាតឱ្យប្រជាជនអាចធ្វើអ្វីៗគ្រប់យ៉ាង ចាប់តាំងពីការបោះឆ្នោតតាមអនឡាញ រហូតដល់ការធានាថាក្រុមគ្រូពេទ្យអាចចែករំលែកកំណត់ត្រាវេជ្ជសាស្ត្រ និងវេជ្ជបញ្ជាជាមួយឱសថការីបានយ៉ាងរលូន។ តាមរយៈការធ្វើសមាហរណកម្មអត្តសញ្ញាណឌីជីថលយ៉ាងពេញលេញក្នុងជីវភាពរស់នៅប្រចាំថ្ងៃ ប្រទេសអេស្តូនីបានបង្កើតសង្គមឌីជីថលមួយដែលមានសុវត្ថិភាព, ប្រសិទ្ធភាព និងបរិយាបន្នដែលជាការកំណត់ស្តង់ដាកម្រិតសកល។

ប្រវត្តិនៃការចាប់ផ្តើមអត្តសញ្ញាណឌីជីថល

ធនាគារបានបង្កើតសេវាផ្ទៀងផ្ទាត់អត្តសញ្ញាណឌីជីថល (ឆ្នាំ១៩៩៦)

នៅក្នុងឆ្នាំ១៩៩៦ នៅពេលដែលសេវាធនាគារតាមអ៊ីនធឺណិត (Internet Banking) ត្រូវបានដាក់ឱ្យប្រើប្រាស់ អាចចាត់ទុកថាជាការចាប់ផ្តើមដំបូងបង្អស់នៃអត្តសញ្ញាណឌីជីថលនៅក្នុងប្រទេសអេស្តូនី។ ធនាគារនានាបានបង្កើតសេវាផ្ទៀងផ្ទាត់អត្តសញ្ញាណឌីជីថល ដែលបុគ្គលម្នាក់ៗអាចប្រើប្រាស់ ដើម្បីធ្វើប្រតិបត្តិការជាមួយធនាគារតាមអនឡាញ ហើយក្រោយមកសេវានេះត្រូវបានផ្តល់ជូនអាជ្ញាធរពន្ធដារ សម្រាប់ការបំពេញ និងដាក់លិខិតប្រកាសពន្ធលើប្រាក់ចំណូលផងដែរ។

ការប្រើប្រាស់ Mandatory Digital Identity Smart Card

Mandatory Digital Identity Smart Card ត្រូវបានប្រកាសដាក់ឱ្យប្រើប្រាស់នៅឆ្នាំ២០០២។ ការដែលលិខិតឆ្លងដែនផុតសុពលភាពក្នុងរយៈពេល ១០ឆ្នាំ គឺជាដើមហេតុជំរុញឱ្យមានការសម្រេចចិត្តស្វែងរកឯកសារអត្តសញ្ញាណប្រភេទថ្មី ដោយក្រុមហ៊ុន Cybernetica បានធ្វើការសិក្សាសាកល្បងលើ Smart Card នៅចុងទសវត្សរ៍ឆ្នាំ១៩៩០ ជាហេតុនាំឱ្យមានការដាក់ចេញអត្តសញ្ញាណថ្មីនៅឆ្នាំ២០០២។ កត្តានេះ រួមជាមួយនឹងការអនុវត្ត Public Key Infrastructure (PKI) និងការបង្កើត X-Road (ប្រព័ន្ធផ្លាស់ប្តូរទិន្នន័យប្រកបដោយសុវត្ថិភាពពីឧបករណ៍មួយទៅឧបករណ៍មួយ ត្រូវបានអភិវឌ្ឍន៍ដោយ Cybernetica) បានធ្វើឱ្យអេស្តូនីចាប់ផ្តើមដើរតួនាទីជានិន្នាការដឹកនាំនៅលើឆាកសកល។

ការដាក់ឱ្យប្រើប្រាស់ X-Road និងអត្តសញ្ញាណឌីជីថល

ប្រព័ន្ធរដ្ឋាភិបាលឌីជីថលរបស់អេស្តូនី ត្រូវបានបំបែកចេញជាសមាសធាតុសំខាន់ពីរ គឺ X-Road និងអត្តសញ្ញាណឌីជីថល ដោយត្រូវបានដាក់ឱ្យប្រើប្រាស់ក្នុងពេលដំណាលគ្នា ហើយបានធ្វើការយ៉ាងស៊ីសង្វាក់ជាមួយគ្នា ដោយមានសំណើទិន្នន័យជិតមួយពាន់លានដងត្រូវបានបញ្ជូនទៅកាន់ X-Road ជារៀងរាល់ឆ្នាំ ហើយ **៩៥%** នៃសំណើទាំងនោះត្រូវបានធ្វើឡើងដោយស្វ័យប្រវត្តិ។ ដូច្នេះ អត្តសញ្ញាណឌីជីថល បានចាប់ផ្តើមដំបូងចេញពីធនាគារ ដែលសេវាផ្ទៀងផ្ទាត់អត្តសញ្ញាណដំបូងគេគឺកាតកូដ (Code Cards) និងបន្ទាប់មក គឺឧបករណ៍គណនាលេខ PIN (PIN Calculators)។

ដំណើរការនៃអត្តសញ្ញាណឌីជីថល

រដ្ឋាភិបាលអេស្តូនីមានគោលការណ៍ស្នូលតែមួយគត់នៃប្រព័ន្ធអត្តសញ្ញាណឌីជីថលរបស់ខ្លួន គឺផ្តល់ព័ត៌មានតែម្តងគត់ ហើយប្រជាពលរដ្ឋអេស្តូនីត្រូវផ្តល់ព័ត៌មានជាក់លាក់ណាមួយជូនរដ្ឋាភិបាលតែមួយលើកប៉ុណ្ណោះ។ នៅពេលដែលព័ត៌មាននោះត្រូវបានផ្ទៀងផ្ទាត់រួចរាល់ នឹងត្រូវបានចែករំលែកឆ្លងកាត់ហេដ្ឋារចនាសម្ព័ន្ធទូទាំងប្រទេស។ ហេតុនេះ ប្រសិនបើអ្នកបានផ្តល់ថ្ងៃ ខែ និងឆ្នាំកំណើតនៅពេលធ្វើលិខិតឆ្លងដែនថ្មី អ្នកមិនចាំបាច់ផ្តល់ព័ត៌មាននោះម្តងទៀតឡើយ នៅពេលអ្នកទៅធ្វើប័ណ្ណបើកបរឡើងវិញ។ នេះជាប្រព័ន្ធមួយដែលមាន «ភាពអាចប្រើប្រាស់ឡើងវិញបាន» ដែលជាដំណោះស្រាយបច្ចេកវិទ្យាពិសេសមួយ សម្រាប់ចែករំលែកទិន្នន័យរវាងក្រសួង និងស្ថាប័ន។ គោលការណ៍ស្នូលនៃ «ភាពអាចប្រើប្រាស់ឡើងវិញបាន» និង «ភាពជឿទុកចិត្តបាន» ទាំងនេះ បានបម្រើប្រយោជន៍យ៉ាងល្អប្រសើរដល់ប្រទេសអេស្តូនី។

ភាពជោគជ័យនៃអត្តសញ្ញាណឌីជីថល

នាពេលបច្ចុប្បន្ន សេវារដ្ឋបាល **៩៩%** អាចចូលប្រើប្រាស់បានតាមប្រព័ន្ធអនឡាញដោយប្រជាពលរដ្ឋ ហើយសេវាទាំងនោះកំពុងត្រូវបានប្រើប្រាស់យ៉ាងសកម្ម ដោយ **៩៨%** នៃប្រតិវេទន៍ពន្ធនៅអេស្តូនីត្រូវបានប្រកាសតាមអនឡាញ។ រដ្ឋាភិបាលអេស្តូនីប៉ាន់ប្រមាណថា ខ្លួនអាចសន្សំសំចៃបានប្រមាណ **២%** នៃទិន្នផលសេដ្ឋកិច្ចសរុប និងសន្សំពេលវេលាធ្វើការបានយ៉ាងច្រើនជារៀងរាល់ឆ្នាំដោយសារភាពជោគជ័យនេះ។ លើសពីនេះ អេស្តូនីត្រូវបានទទួលស្គាល់ថាជាប្រទេសមួយក្នុងចំណោមប្រទេសដែលមានភាពស្ទាត់ជំនាញខាងផ្នែកបច្ចេកវិទ្យាបំផុតនៅលើសកលលោក ដោយបង្ហាញពីរបៀបគ្រប់គ្រងរដ្ឋបាលបែបថ្មី ដែលសក្តានុពលនៃបច្ចេកវិទ្យាត្រូវបានទទួលយក ដោយគ្មានការភ័យខ្លាច។

បញ្ហាប្រឈមនៃការប្រើប្រាស់អត្តសញ្ញាណឌីជីថល

អេស្តូនីហាក់បីដូចជាគោលដៅដ៏ទាក់ទាញសម្រាប់ជនខិលខូចដែលចង់សាកល្បងប្រព័ន្ធសុវត្ថិភាពនៃអត្តសញ្ញាណឌីជីថលរបស់ប្រទេសនេះ ប៉ុន្តែជាក់ស្តែង ប្រទេសនេះមិនធ្លាប់រងគ្រោះដោយការវាយប្រហារទ្រង់ទ្រាយធំណាមួយឡើយ។ នេះមិនមែនមានន័យថាគ្មានបញ្ហានោះទេ កាលពីឆ្នាំ២០១៧ អេស្តូនីបានស្ថិតក្នុងស្ថានភាពបិទខ្ទប់ប្រព័ន្ធបណ្តោះអាសន្ន បន្ទាប់ពីការរកឃើញចំណុចខ្សោយមួយដែលបង្កឱ្យមានហានិភ័យសុវត្ថិភាពធ្ងន់ធ្ងរ ដែលតម្រូវឱ្យផ្អាកប្រព័ន្ធដំណើរការ។ ប៉ុន្តែទោះជាយ៉ាងណាក៏ដោយ រដ្ឋាភិបាល និងនគរបាលអេស្តូនីបានបញ្ជាក់ថា មិនមានរបាយការណ៍ណាមួយត្រូវបានប្រើប្រាស់ក្នុងផ្លូវបោកប្រាស់នោះឡើយ។

បទពិសោធ និងមេរៀនពីអេស្តូនី

មេរៀន និងបទពិសោធ ដែលបណ្តាប្រទេសនានានៅលើសកលលោកអាចដកស្រង់ពីអេស្តូនីបាន មានដូចជា៖

◉ **ទី១.** ការធ្វើឱ្យទិន្នន័យក្នុងប្រព័ន្ធអាចប្រើប្រាស់ឡើងវិញបាន ផ្តល់នូវអត្ថប្រយោជន៍ជាច្រើនដល់អតិថិជន និងអាជីវកម្ម តាមរយៈការកាត់បន្ថយពេលវេលាដែលត្រូវខាតបង់ក្នុងការចែករំលែក និងផ្ទៀងផ្ទាត់ព័ត៌មានដដែលៗជាច្រើនលើកច្រើនសារ។

◉ **ទី២.** ការលើកកម្ពស់បរិយាបន្ន គឺជាផ្នែកមួយនៃផែនការដែលអេស្តូនីបានចាត់ទុកអ៊ីនធឺណិតដូចជា សិទ្ធិមនុស្សមូលដ្ឋាន ដោយធានាថាសូម្បីតែកោះតូចៗក៏មានបណ្តាញអ៊ីនធឺណិតដែលអាចទុកចិត្តបានផងដែរ និងតាមរយៈការបើកចំហប្រព័ន្ធនេះដល់ជនបរទេស និងប្រជាពលរដ្ឋអេស្តូនីដូចៗគ្នា ដោយពួកគេបានដាក់បរិយាបន្ននៅចំកណ្តាលនៃកិច្ចខិតខំប្រឹងប្រែងរបស់ខ្លួន។

◉ **ទី៣.** ការប្តេជ្ញាចិត្ត តាមរយៈការធ្វើឱ្យសេវារដ្ឋបាលភាគច្រើនអាចប្រើប្រាស់បានតាមប្រព័ន្ធអ៊ីនធឺណិត ដែលនេះបានធានាថាមនុស្សគ្រប់គ្នាមានហេតុផលក្នុងការប្រើប្រាស់ ជំនួសឱ្យការទុកសេវារដ្ឋបាលឱ្យនៅត្រឹមតែជាចំណាប់អារម្មណ៍របស់ក្រុមមនុស្សមួយចំនួនតូច។ កត្តានេះបានជួយកសាងទំនុកចិត្តលើប្រព័ន្ធ និងធានាថាអាជីវកម្មនានាអាចរីកចម្រើនជុំវិញប្រព័ន្ធនេះ ដោយមានទំនុកចិត្តថានឹងមិនត្រូវគេបោះបង់ចោលនៅពាក់កណ្តាលទីនោះឡើយ។

VI. សេចក្តីសន្និដ្ឋាន

ជារួម អត្តសញ្ញាណឌីជីថល បានប្រែប្រួលពីឧបករណ៍ផ្ទៀងផ្ទាត់សាមញ្ញ មកជាហេដ្ឋារចនាសម្ព័ន្ធគន្លឹះមិនអាចខ្វះបាន ក្នុងការគាំទ្រដល់ដំណើរការរបស់រដ្ឋ សេដ្ឋកិច្ច និងសង្គម។ ទន្ទឹមនឹងអត្ថប្រយោជន៍ដ៏ច្រើនលើសលប់លើការសម្រួលសេវាសាធារណៈ និងឯកជន ការកើនឡើងនៃបទល្មើសសាយប័រដូចជា ការលួចអត្តសញ្ញាណ និងការប្រើប្រាស់បច្ចេកវិទ្យា AI (Deepfakes) ដើម្បីបោកប្រាស់ បានក្លាយជាការគំរាមកំហែងយ៉ាងធ្ងន់ធ្ងរ។ ដូច្នេះ ការពង្រឹងសន្តិសុខអត្តសញ្ញាណឌីជីថល តាមរយៈវិធានការការពារបច្ចេកទេស និងការយល់ដឹងនិងការប្រុងប្រយ័ត្នផ្ទាល់ខ្លួន គឺជាកត្តាចាំបាច់ដើម្បីការពារទ្រព្យសម្បត្តិ ឯកជនភាព និងកេរ្តិ៍ឈ្មោះ។ បណ្តាប្រទេសលើសកលលោក បាននិងកំពុងជំរុញការអភិវឌ្ឍ និងការពង្រឹងប្រព័ន្ធសន្តិសុខអត្តសញ្ញាណឌីជីថលរបស់ខ្លួន។ ជាក់ស្តែង កម្ពុជាបើទោះបីជាស្ថិតក្នុងដំណាក់កាលដំបូងនៃការអនុវត្តនៅឡើយ ប៉ុន្តែការខិតខំប្រឹងប្រែងរបស់រាជរដ្ឋាភិបាល និងភាគីពាក់ព័ន្ធ ក្នុងការរៀបចំក្របខណ្ឌច្បាប់ គោលនយោបាយ និងការប្រើប្រាស់ថ្នាលឌីជីថលសម្រាប់កំណត់អត្តសញ្ញាណឌីជីថល កំពុងតែបង្កើតនូវមូលដ្ឋានគ្រឹះយ៉ាងរឹងមាំ។ កម្ពុជា ក៏ដូចជាបណ្តាប្រទេសដទៃក៏អាចសិក្សាពីប្រទេសដែលកំពុងឈានមុខគេ ដូចជា ប្រទេសអេស្តូនី ដែលមានការប្តេជ្ញាចិត្តខ្ពស់ និងមានប្រព័ន្ធរដ្ឋាភិបាលឌីជីថលមួយដែលរឹងមាំ និងមានបរិយាបន្ន។ ក្នុងន័យនេះ ការចូលរួមយ៉ាងសកម្មពីគ្រប់ភាគីទាំងរដ្ឋ ឯកជន និងសាធារណជនក្នុងការការពារ និងប្រើប្រាស់អត្តសញ្ញាណឌីជីថលប្រកបដោយទំនុកចិត្ត នឹងក្លាយជាកាតាលីករដ៏សំខាន់មួយ ដើម្បីជំរុញការកសាងសេដ្ឋកិច្ច-សង្គមឌីជីថលនៅកម្ពុជាឱ្យមានភាពរឹងមាំ, សុវត្ថិភាព និងមានចីរភាព៕

ឯកសារយោង

- Types of identity theft: risks and prevention strategies, ចេញផ្សាយថ្ងៃទី២៨ ខែវិច្ឆិកា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/u2t3s7rh
- សទ្ទានុក្រមបរធនបាលកិច្ច, ចូលអានថ្ងៃទី៨ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/8c477k9f
- Digital identity protection: a cornerstone of trust in the digital era, ចេញផ្សាយថ្ងៃទី២៦ ខែមីនា ឆ្នាំ២០២៦, ចូលអានថ្ងៃទី៨ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/52w4u3zn
- 10 smart ways to prevent identity theft, ចេញផ្សាយថ្ងៃទី២៤ ខែវិច្ឆិកា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី១៥ ខែកក្កដា ឆ្នាំ២០២៦, https://www.acronis.com/en/blog/posts/10-smart-ways-to-prevent-identity-theft/
- Benefits of Digital Identity Solutions, ចេញផ្សាយថ្ងៃទី២៣ ខែឧសភា ឆ្នាំ២០២៤, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/yu7p8j4a
- Identity Theft, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/ycka4xr
- What is identity theft protection? How it works and why it is so important?, ចេញផ្សាយថ្ងៃទី១៦ ខែសីហា ឆ្នាំ២០២៣, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/4p6b7dzc
- A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity, World Economic Forum, ចេញផ្សាយខែសីហា ឆ្នាំ២០១៦, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦
- Digital ID Overview, ចេញផ្សាយថ្ងៃទី២០ ខែមករា ឆ្នាំ២០២៦, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/3vrrnc6j
- ច្បាប់ស្តីពីអត្រានុកូលដ្ឋាន ស្ថិតិអត្រានុកូលដ្ឋាន និងអត្តសញ្ញាណកម្ម, ចេញផ្សាយឆ្នាំ២០២៣, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦
- សេចក្តីព្រាងច្បាប់ស្តីពីកិច្ចការពារទិន្នន័យបុគ្គលនៃព្រះរាជាណាចក្រកម្ពុជា, ចេញផ្សាយខែកក្កដា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦
- សេចក្តីព្រាងច្បាប់ស្តីពីរដ្ឋាភិបាលឌីជីថលនៃព្រះរាជាណាចក្រកម្ពុជា, ចេញផ្សាយខែកក្កដា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦
- ក្របខណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា ២០២១-២០៣៥, ចេញផ្សាយខែឧសភា ឆ្នាំ២០២១, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦
- គោលនយោបាយរដ្ឋាភិបាលឌីជីថលកម្ពុជា ២០២២-២០៣៥, ចេញផ្សាយខែមករា ឆ្នាំ២០២២, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦
- កិច្ចប្រជុំលើកទី៥ នៃគណៈកម្មាធិការជាតិដឹកនាំតម្រង់ទិសការងារអត្រានុកូលដ្ឋាន ស្ថិតិអត្រានុកូលដ្ឋាន និងអត្តសញ្ញាណកម្ម, ចេញផ្សាយថ្ងៃទី១៩ ខែកុម្ភៈ ឆ្នាំ២០២១, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/3ufhaanp
- ការត្រៀមអនុវត្តផែនការយុទ្ធសាស្ត្រជាតិស្តីពីអត្តសញ្ញាណកម្ម ដំណាក់កាលទី២, ចេញផ្សាយថ្ងៃទី២៤ ខែវិច្ឆិកា ឆ្នាំ២០២៥, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/yhuja53v

- ថ្នាលឌីជីថល, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/4pb2svwu
- បណ្ណបើកបរឌីជីថល, ចេញផ្សាយថ្ងៃទី១៣ ខែឧសភា ឆ្នាំ២០២៦, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/4dz5x5dp
- យុទ្ធនាការផ្ទៀងផ្ទាត់អត្តសញ្ញាណស៊ីមកាត ជាមួយនឹងគណនីធនាគារ/គណនីទូទាត់សងប្រាក់របស់អ្នកប្រើប្រាស់, ចេញផ្សាយថ្ងៃទី១៧ ខែមិថុនា ឆ្នាំ២០២៦, ចូលអានថ្ងៃទី២៧ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/22mdpkfk
- *The history of digital identity*, ចូលអានថ្ងៃទី២២ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/4ypsbe4b
- *Digital identity in practice – Estonia and the e-state*, ចូលអានថ្ងៃទី២១ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/b9cp2jcy
- e-Identity Story, ចូលអានថ្ងៃទី២២ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/562yyxdv
- *AI fraud drives identity verification toward continuous trust and layered assurance*, ចេញផ្សាយថ្ងៃទី២ ខែកក្កដា ឆ្នាំ២០២៦, ចូលអានថ្ងៃទី២៤ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/3zhfxkep
- *The History of Digital Identity in Estonia*, ចេញផ្សាយថ្ងៃទី២១ ខែកក្កដា ឆ្នាំ២០២១, ចូលអានថ្ងៃទី២៤ ខែកក្កដា ឆ្នាំ២០២៦, https://tinyurl.com/2mdhy7vt

---

កម្ពុជា ៤.0 - Cambodia 4.0

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

គាំទ្រដោយ