សុវត្ថិភាពឌីជីថល

សៀវភៅណែនាំសម្រាប់គ្រូបណ្តុះបណ្តាល

២០១៩

Internews

ប្រែសម្រួលដោយ៖ DigitalHub.COM
www.digitalhub101.com

មាតិកា

	សេចក្តីថ្លែងអំណរគុណ Acknowledgment	១
១	ការវាយតម្លៃពីតម្រូវការ Needs Assessment	៤
២	ការវាយតម្លៃហានិភ័យ Risk Assessment	៦
៣	មូលដ្ឋានគ្រឹះសុវត្ថិភាពនៅលើកុំព្យូទ័រ និងគណនីនៅលើអ៊ីនធឺណិត Device Hygiene and Account Security	៩
៤	សុវត្ថិភាពលើទូរស័ព្ទស្មាតហ្វូន Mobile Security	១៥
៥	សុវត្ថិភាពក្នុងការរក្សាទុកទិន្នន័យ Secure Information Storage	១៩
៦	ការបម្រុងទុកឯកសារ Backups	២២
៧	សុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត Online Safety	២៦
៨	សុវត្ថិភាពក្នុងការទាក់ទងនៅលើអ៊ីនធឺណិត និងសុវត្ថិភាពនៅលើអ៊ីមែល Secure Communication and Email Hygiene	៣០
៩	ការយល់ដឹង និងការការពារពីការវាយប្រហារដោយបញ្ឆោតនៅលើអ៊ីនធឺណិត Phishing: Understanding and Preventing Attacks	៣២
១០	ធនធានសំខាន់ៗសំរាប់គ្រូបណ្តុះបណ្តាល Useful Resources for Trainers	៣៥

សេចក្តីថ្លែងអំណរគុណ

សៀវភៅណែនាំនេះ ត្រូវបានរៀបរៀង និងនិពន្ធឡើងដោយ Natasha Msonza ជនជាតិហ្ស៊ីមបាវេ ជាអ្នកឯកទេសផ្នែកសុវត្ថិភាពប្រព័ន្ធឌីជីថល។

ខ្ញុំបានបង្កើតមាតិកានេះឡើង ដោយផ្អែកតាមបទពិសោធន៍របស់ខ្ញុំ ជាគ្រូបណ្តុះបណ្តាលអស់ជាច្រើនឆ្នាំមកហើយ ហើយសៀវភៅនេះបានរួមបញ្ចូលប្រភេទមាតិកា និងជំបូន្មាននានាដែលខ្ញុំបានទទួលកន្លងមក ដែលធ្វើអោយការបង្រៀនរបស់ខ្ញុំកាន់តែមានភាពងាយស្រួលឡើង។

ខ្ញុំសូមធ្វើការថ្លែងអំណរគុណជាពិសេសដល់បណ្តាអង្គការ និងបុគ្គលទាំងឡាយដែលធ្វើអោយសៀវភៅនេះលេចជារូបរាងឡើង រួមមាន៖ Internews ដែលគាំទ្រការផលិតសៀវភៅនេះរហូតក្លាយទៅជាសមិទ្ធិផលជាក់ស្តែង ដែលនឹងប្រើប្រាស់ដោយអង្គការ Safe Sisters ព្រមទាំងគ្រូបណ្តុះបណ្តាលដ៏ទៃទៀតដែលចាប់អារម្មណ៍ចង់បង្រៀនបន្តពីកម្រិតមូលដ្ឋានមក។ គម្រោង ISC ដែលជួយជម្រុញទឹកចិត្តពីខាងក្រោយ ចំពោះគំរូវិធីសាស្រ្តបណ្តុះបណ្តាល ជាជំហានសាកល្បងនៅក្នុងប្រទេសហ្ស៊ីមបាវេ។ Defend Defenders ដែលផ្តល់ការគាំទ្រផ្សេងៗ រួមទាំងការសាកល្បងសៀវភៅនេះនៅក្រុមគោលដៅផងដែរ។

ខាងក្រោមនេះជាឈ្មោះបុគ្គលទាំងឡាយដែលចំណាយពេលវេលាដ៏មានតម្លៃពិនិត្យសៀវភៅនេះនិងផ្តល់មតិយោបលត្រលប់មកវិញ៖

- **Helen Nyinakiiza** (អូហ្គង់ដា)
- **Sonia Karungi** (អូហ្គង់ដា)
- **Azeenarh Mohammed** (នីហ្សេរីយ៉ា)
- **Aumarh Ikwueme** (នីហ្សេរីយ៉ា)
- **Szeming Ming** (ម៉ាឡេស៊ី)
- **Soraya Okuda** (អាមេរិច)
- **Norman Shamas** (អាមេរិច)
- **Tawanda Mugari** (ហ្ស៊ីមបាវេ)

សៀវភៅណែនាំត្រូវបានសាកល្បងជាលើកតំបូងនៅសិក្ខាសាលាគ្រូបណ្តុះបណ្តាលរបស់អង្គការ **Safe Sister** នៅ **Entebbe** ប្រទេសអូហ្គង់ដា ខែមេសា ឆ្នាំ២០១៨។ សូមអរគុណជាអនេក ដល់អង្គការ **Safe Sister** ដែលបានសាកល្បងប្រើប្រាស់សៀវភៅណែនាំនេះ និងផ្តល់មតិយោបល់ដ៏មានតម្លៃ។

ជាចុងក្រោយក្រុមការងារ DigitalHub សូមថ្លែងអំណរគុណយ៉ាងជ្រាលជ្រៅចំពោះអ្នកនិពន្ធ អង្គការ និងបុគ្គលនានា ជាពិសេសអង្គការSafe Sisters ដែលគាំទ្រអោយសៀវភៅនេះលេចចេញជារូបរាងបាន។ ក្រុមការងារយើងខ្ញុំសូមអធ្យាស្រ័យ និងការយោគយល់ទុកជាមុនប្រសិនបើការបកប្រែរបស់យើងខ្ញុំមានការខ្វះខាត មិនគ្រប់ជ្រុងជ្រោយត្រង់កន្លែងណាមួយ។ ទោះបីជាយ៉ាងណាក៏ដោយ យើងខ្ញុំសង្ឃឹមថាសៀវភៅនេះនឹងក្លាយជាគ្រូពិគ្រោះយោបល់ដ៏មានសារៈសំខាន់ ចំពោះអ្នកដែលមានបំណងចង់បង្រៀន ឬចែករំលែកចំណេះដឹងបន្ត។

សៀវភៅណែនាំនេះ ត្រូវបានរៀបរៀង ឡើងដោយ៖

- ធ្វើអោយវិធីសាស្ត្របណ្តុះបណ្តាលកាន់តែសាមញ្ញ តាមរយៈការរៀបចំប្រធានបទទៅតាម លំដាប់លំដោយចាប់ពី កម្រិតមូលដ្ឋាន ទៅកម្រិតមធ្យមចំពោះរបៀបវារៈបណ្តុះបណ្តាលចន្លោះពី ពីរទៅបីថ្ងៃចំពោះអ្នកចូលរួមតំបូងៗប្រមាណតែ ១០នាក់ប៉ុណ្ណោះ ក្នុងមួយវគ្គ។
- គ្រូបណ្តុះបណ្តាលត្រូវតែមានចំនេះដឹងជាមុន ឬប្រើប្រាស់ជំនាញបច្ចេកទេស និងកម្មវិធីមួយចំនួន ព្រមទាំងភ្ជាប់ប្រធានបទទៅនឹងប្រភពឯកសារដែលមានស្រាប់ជាដើម។
- រៀបចំចំនុចដែលត្រូវនិយាយដើម្បីជៀសវាងការជាប់គាំងពេលចាប់ផ្តើមឬពេលកំពុងបង្រៀនជាដើម ។
- ផ្តល់នូវគន្លឹះផ្សេងៗទាក់ទងនឹងវិធីសាស្ត្រនៃការចែករំលែកចំណេះដឹងចំពោះប្រធានបទជាក់លាក់ អោយបានត្រឹមត្រូវ និងមានប្រសិទ្ធិភាព។ (គ្រប់មេរៀនមិនចាំបាច់ប្រើបទបង្ហាញទាំងអស់នោះទេ)
- ផ្តល់នូវគន្លឹះក្នុងការប្រើប្រាស់ និងគ្រប់គ្រងពេលវេលាចំពោះប្រធានបទនីមួយៗ។ វាជួយសម្រួល អោយគ្រូបណ្តុះបណ្តាលដឹងពីរបៀបធ្វើផែនការបង្រៀនច្បាស់លាស់ជាពិសេសយល់កាន់តែច្បាស់ នូវចំនុចដែលគួរឬមិនគួរបង្ហាញឬពន្យល់បន្ថែមចំពោះពេលវេលាដែលនៅសល់។

គន្លឹះសំខាន់ៗសម្រាប់ គ្រូបណ្តុះបណ្តាល

១ យក USB តាមខ្លួនជានិច្ច ដែលផ្ទុកគ្រប់កម្មវិធី និងApps (ជាប្រភេទបើកទូលាយ និងមិនគិតថ្លៃ) ដែលអ្នកនឹងប្រើប្រាស់ ឬជារបស់យោង។ វាជួយអ្នកនៅពេលដែល អ៊ីនធឺណិតដើរយឺតនៅកន្លែងដែលអ្នកបង្រៀន។ ករណីនេះអ្នកគួរមាន USBសម្រាប់អ្នកចូលរួមម្នាក់ៗ (បើសិនជាអាច) ដើម្បីចៀសវាងការចម្លងមេរោគតាមរយៈការដោតUSB។

២ ត្រៀមខ្លួនទុកជាមុន បើមានករណីមិនអាចប្រើប្រាស់ប្រព័ន្ធអេឡិចត្រូនិចណាមួយ ឧទាហរណ៍ដូចជាProjector ឈប់តំណើរការឬដាច់ភ្លើងជាដើម។

៣ យើងស្នើសុំអោយគោរពទៅតាមស្តង់ដារចំនួន អ្នកចូលរួមប្រមាណ១០នាក់ ជាអតិបរមាក្នុងមួយវគ្គ។ ប្រសិនមានអ្នកចូលរួមលើសពីនេះ គួរតែមានគ្រូជំនួយជាពិសេសនៅពេលដែលមានលំហាត់ច្រើន។

៤ កុំមានការខ្មាស់អៀនអី ប្រសិនបើអ្នកមិនអាចឆ្លើយរាល់សំណួររបស់អ្នកចូលរួមបាន ព្រោះវាប្រសើរជាងធ្វើចេះ ឬក៏ឆ្លើយកុហក។ អ្នកអាចឆ្លើយយ៉ាងសាមញ្ញថា អ្នកមិនច្បាស់ចំពោះចម្លើយ ប៉ុន្តែអ្នករីករាយនឹងសាកសួរគ្រូបណ្តុះបណ្តាលផ្សេងទៀត ឬស្រាវជ្រាវបន្ថែមទៀត ហើយនឹងយកចម្លើយច្បាស់លាស់មួយត្រឡប់មកវិញ។

៥ ចៀសវាងបង្រៀនឧបករណ៍ប្រភេទ Database ច្រើនជាងមួយក្នុងថ្ងៃតែមួយ ឧទាហរណ៍ KeepassXC និង Veracrypt ព្រោះអ្នកចូលរួមងាយស្រួលច្រលំ នៅពេលព្យាយាមចាំថាមួយណាជាមួយណា។

១

ការវាយតម្លៃពីតម្រូវការ

Needs Assessment

ការធ្វើការវាយតម្លៃពីតម្រូវការ

ជារឿយៗយើងបង្រៀនក្រុមមនុស្សដែលយើងមិនដឹងពីទម្លាប់ និងសមត្ថភាពរបស់ពួកគេពាក់ព័ន្ធនឹងសុវត្ថិភាព និងបច្ចេកវិទ្យានោះទេ។ ម្លោះហើយការដឹងជាមុនថាអ្នកចូលរួមជានរណាគឺមានសារៈសំខាន់ណាស់ ព្រោះវាជួយអោយយើងអាចរៀបចំវគ្គបណ្ដុះបណ្ដាលបានល្អប្រសើរ។

ជាទូទៅការវាយតម្លៃពីតម្រូវការគឺផ្អែកទៅលើការវិភាគទាំងបញ្ហាដែលត្រូវដោះស្រាយ និងចំណេះដឹងដែលត្រូវកសាងឡើង។ គោលបំណងរបស់វាគឺដើម្បីរកព័ត៌មានពេលវេលា និងធនធានដែលសមស្របសម្រាប់បំពេញបន្ថែមអោយវគ្គបណ្ដុះបណ្ដាលទទួលជោគជ័យ។ ការធ្វើការវាយតម្លៃពីតម្រូវការជាមូលដ្ឋានមុនពេលវគ្គបណ្ដុះបណ្ដាលនឹងធ្វើអោយកម្មវត្ថុនៃវគ្គបណ្ដុះបណ្ដាលនោះអោយទៅជាការពិតជាក់ស្ដែងបាន។

យើងមានវិធីសាស្រ្តជាច្រើនដើម្បីដឹងពីតម្រូវការរបស់អ្នកចូលរួម។ ទោះបីជាមានវិធីសាស្រ្តច្រើនយ៉ាងណាក៏ដោយ វិធីគន្លឹះនោះគឺត្រូវពិគ្រោះជាមួយអ្នកចូលរួម និងហៅពួកគាត់អោយចូលរួមក្នុងតំណើរការនោះផងដែរ។

សរុបមកអ្នកត្រូវធ្វើការវាយតម្លៃអោយបានមុនវគ្គបណ្ដុះបណ្ដាលព្រោះវាជួយអ្នកអោយស្គាល់ពីប្រភេទមនុស្សដែលត្រូវចូលរួម និងជួយអ្នកកំណត់យកសម្ភារៈ និងឧបករណ៍ដែលត្រូវបង្រៀនរួមទាំងកម្មវិធី (Software) ផ្សេងៗ ជាពិសេសជួយក្នុងការបែងចែកពេលវេលាក្នុងមេរៀននីមួយៗ

ការធ្វើការវាយតម្លៃពីតម្រូវការ

១. មុនពេលវគ្គបណ្ដុះបណ្ដាលអ្នកត្រូវរៀបចំសំណួរស្ទាបស្ទង់ខ្លីមួយដែលសួរពាក់ព័ន្ធនឹងព័ត៌មានរបស់អ្នកចូលរួម។ ឧទាហរណ៍ដូចជា តើអ្នកធ្វើការងារអ្វី? តើអ្នកប្រើប្រាស់ប្រព័ន្ធប្រតិបត្តិការអ្វីនៅលើកុំព្យូទ័ររបស់អ្នក? តើអ្នកមានអារម្មណ៍ថាមានសុវត្ថិភាពឬទេ នៅពេលប្រើប្រាស់កុំព្យូទ័រ?

២. បើអាចទៅរួចអ្នកអាចចែកសំណួរវាយតម្លៃប្រហែលមួយឬពីរសប្ដាហ៍មុនពេលវគ្គបណ្ដុះបណ្ដាលមកដល់។ អ្នកអាចចែកសំណួរតាមរយៈអ៊ីមែល ឬផ្ញើតំណភ្ជាប់ជាដើម។ បន្ទាប់មកអ្នកត្រូវយកការឆ្លើយតបរបស់អ្នកចូលរួមដើម្បីកំណត់ប្រធានបទដែលត្រូវបង្រៀនហើយយកមតិយោបល់ត្រឡប់ជាមួយនឹងការវាយតម្លៃពីហានិភ័យរបស់អ្នកចូលរួម ដើម្បីចាប់ផ្ដើមគ្រោងរបៀបវារៈបង្រៀន។ អ្នកត្រូវចាំពីលំហូរនៃការបង្រៀនពីប្រធានបទមួយទៅប្រធានបទមួយជាមួយនឹងពេលវេលាដែលមានចំពោះវគ្គបណ្ដុះបណ្ដាលទាំងមូល។

គន្លឹះសំខាន់ៗ

គ្រូបណ្តុះបណ្តាល គួរតែទុកចន្លោះពេលនៅសេសសល់ខ្លះនៅក្នុងរបៀបវារៈ ដើម្បីអាចធ្វើការបត់បែនទៅតាមស្ថានភាពជាក់ស្តែងរបស់អ្នកចូលរួម។ ក្បិតអីអ្នកខ្លះឆាប់ចាប់បាន តែអ្នកខ្លះចាប់បានយឺត។

ការវាយតម្លៃហានិភ័យ

Risk Assessment

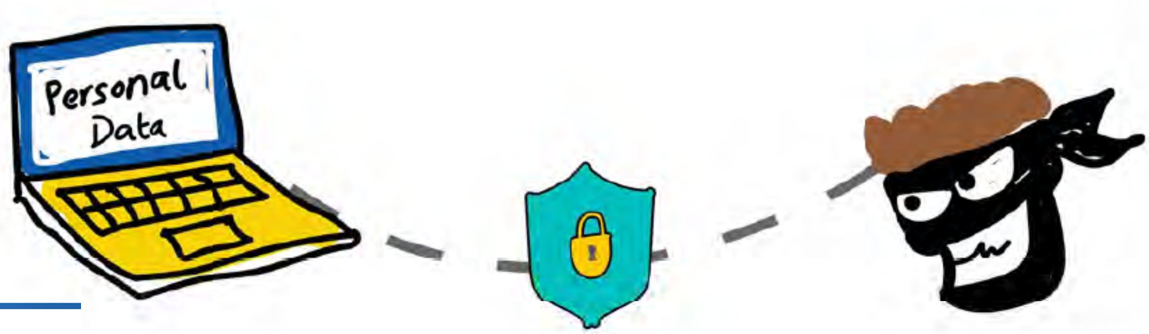
ការវាយតម្លៃហានិភ័យ

មុនពេលចូលទៅកាន់មេរៀនសុវត្ថិភាពប្រព័ន្ធឌីជីថល វាមានសារៈសំខាន់ណាស់ក្នុងការស្វែងយល់ពីគំរូនៃការគំរាមកំហែងរបស់អ្នកចូលរួម។ គ្រូបណ្តុះបណ្តាលអាចធ្វើលំហាត់មួយគឺ ការវាយតម្លៃហានិភ័យនៅមុនពេលចូលទៅកាន់មេរៀន។ ទោះបីជាវានៅគៀកម៉ោងបង្រៀននៅថ្ងៃដំបូងក៏ដោយ ការធ្វើលំហាត់នេះមានសារៈសំខាន់ណាស់ក្នុងការត្រលប់ទៅមើលនិងកែប្រែរបៀបវារៈមួយចំនួនបើសិនជាអាច។ សូមចងចាំថា របៀបវារៈបង្រៀនត្រូវមានភាពបត់បែន និងអាចកែប្រែបានទៅតាមស្ថានភាពនិងកត្តាផ្សេងៗដែលកើតឡើង។

ការធ្វើការវាយតម្លៃហានិភ័យមានន័យថាអ្នកប្តេជ្ញាចិត្តដើម្បីបង្កើតរបៀបវារៈមួយដែលសមស្រប មានភាពពាក់ព័ន្ធគ្នា និងផ្តល់ដំណោះស្រាយចំពោះតម្រូវការជាក់លាក់របស់អ្នកចូលរួមផងដែរ។ ដូចនេះ ការធ្វើលំហាត់នេះជួយអ្នកចូលរួមកំណត់និងយល់ពីការគំរាមកំហែងនៅលើប្រព័ន្ធឌីជីថលដែលពួកគេកំពុងប្រឈមតាមរយៈការងាររបស់ពួកគេ ជាពិសេសគោលដៅចុងក្រោយ គឺរកវិធីដើម្បីទប់ទល់។

នៅកម្រិតមូលដ្ឋាននៃការធ្វើសំណាក (គំរូ) នៃការគំរាមកំហែង (threat model) គឺគេធ្វើការបែងចែកប្រភេទនៃការគំរាមកំហែង ភាពងាយរងគ្រោះ (ចំនុចខ្សោយអ្នកចូលរួម) និងហានិភ័យ ដើម្បីសម្រេចថាអ្វីដែលមានគ្រោះថ្នាក់ខ្លាំងជាងគេ ហើយអាចកើតឡើងខ្ពស់ជាងគេ។ ការធ្វើដូចនេះ ជាដំណើរការដែលអ្នកចូលរួមគួរធ្វើអោយបានទៀងទាត់ ដោយសារការគំរាមកំហែងប្រឆាំងនឹងបុគ្គល និងស្ថាប័នតែងតែវិវត្តជានិច្ច។ដោយសារមានវិធីជាច្រើនក្នុងការធ្វើការវាយតម្លៃហានិភ័យ ដូចនេះយើងសូមលើកវិធីសាស្រ្តមួយដែលសាមញ្ញមកពិភាក្សាដូចខាងក្រោម៖

វិធីសាស្រ្តក្នុងការបង្រៀន	ធ្វើការពិភាក្សាក្រុមធំដើម្បីយកគំនិតសំខាន់ៗ
សំភារៈប្រើប្រាស់ក្នុងការបង្រៀន	ក្រដាសសរសេរ(ធំ) ហ្វឺត កូនក្រដាសតូចៗសម្រាប់កត់ត្រាស្អិតជាដើម
រយៈពេលបង្រៀន	១២០នាទី
ឧទាហរណ៍ប្រៀបធៀប	សំណាក(គំរូ)នៃការគំរាមកំហែង៖ វាដូចជាការធ្វើចំនាត់ថ្នាក់បញ្ហាផងដែរ ថាតើអ្នកនឹងផ្តល់អាទិភាពអោយហានិភ័យមួយណាជាងគេដោយប្រៀបធៀបជាមួយនឹងផលវិបាក និងភាពដែលអាចកើតឡើងរបស់វា ឧទាហរណ៍អ្នកត្រូវបើកបរយ៉ាងលឿនដើម្បីទៅការិយាល័យរបស់អ្នកព្រោះអ្នកបារម្ភមានគេចូលយកឯកសារព្រោះអ្នកភ្លេចចាក់សោរ។ដូចនេះរវាងសុវត្ថិភាពក្នុងពេលបើកបរនិងការបាត់ឯកសារមួយណាសំខាន់ជាង។
ប្រភពឯកសារពាក់ព័ន្ធ (ជាភាសាអង់គ្លេស)	https://rorypecktrust.org/getmedia/f8-ca7438-3202-4890-89e3-c1d8dba80bad/Rory-Pe



វាពិតជាមិនអាចទៅរួចទេប្រសិនបើអ្នកចង់ការពារប្រឆាំងគ្រប់ទម្រង់នៃការវាយប្រហារឬក៏ល្បិចបោកបញ្ឆោតទាំងអស់ដូចនេះអ្នកត្រូវរិះគិតហើយផ្ទង់អារម្មណ៍ថាតើនរណាប្រហែលជាចង់បានទិន្នន័យរបស់អ្នក តើពួកគេចង់បានអ្វីពីអ្នក ហើយគេអាចយកវាបានដោយរបៀបណា។

ដោយ៖ Electronic Frontier Foundation

១. ជំហានទី១ នៅក្នុងការធ្វើការវាយតម្លៃហានិភ័យ គឺត្រូវពិគ្រោះជាមួយអ្នកចូលរួមដោយផ្ទាល់ដើម្បីស្រង់យកបទពិសោធជាក់ស្តែងដែលប្រឈមចេញពី បរិបទជុំវិញការងាររបស់ពួកគេ ដើម្បីទុកជាធាតុចូលក្នុងវគ្គបណ្តុះបណ្តាល។

២. ជំហានទី២ គឺកំណត់ពីការគំរាមកំហែងដែលអ្នកចូលរួមកំពុងប្រឈមអោយបានជាក់លាក់។

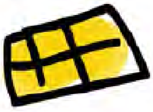
នីតិវិធី

ចែកក្រដាសកត់ត្រាខ្នាតតូចអោយអ្នកចូលរួម ៥-៧ សន្លឹកក្នុងម្នាក់

ប្រាប់អ្នកចូលរួមម្នាក់ៗអោយកំណត់ឬគិតពីហានិភ័យ(ការគម្រាមកំហែងដែលអាចកើតឡើងថ្ងៃអនាគត) អំពីបញ្ហានានាដែលពួកគាត់បារម្ភបំផុត ទាក់ទងនឹងសុវត្ថិភាពនៅលើប្រព័ន្ធឌីជីថល និងបច្ចេកវិទ្យាហើយអោយពួកគាត់សរសេរនៅលើក្រដាសដែលបានចែក។ គ្រូបណ្តុះបណ្តាលត្រូវប្រាប់ពួកគាត់ ឬសរសេរនៅលើក្តារខៀន នូវសំណួរណែនាំដូចខាងក្រោម ដើម្បីជាជំនួយដល់ការគិតៈ

- **តើអ្នកចង់ការពារអ្វីខ្លះ?**
- **តើអ្នកចង់ការពាររបស់ទាំងនោះពីនរណាខ្លះ?**
- **តើមានផលប៉ះពាល់/ផលវិបាកអ្វីខ្លះ បើអ្នកមិនអាចការពារពីអ្នកទាំងនោះបាន?**
- **តើបច្ចុប្បន្ននេះ អ្នកមានសមត្ថភាព ឬអសមត្ថភាពកម្រិតណា ដើម្បីទប់ទល់នឹងហានិភ័យទាំងពួងដែលអាចកើតឡើងបាន?**

ទុកពេលអោយអ្នកចូលរួមធ្វើប្រមាណ១៥នាទី បន្ទាប់មកប្រមូលក្រដាសកិច្ចការពីពួកគាត់។គ្រូត្រូវកត់ត្រាទុកហានិភ័យដែលបានកំណត់ដោយអ្នកចូលរួម។ហានិភ័យទាំងឡាយអាស្រ័យទៅលើការងាររបស់ពួកគេមានដូចជាៈការបាត់ឧបករណ៍អេឡិចត្រូនិចដោយសារចោរលួច ការបែកធ្លាយព័ត៌មាន ការលួចចូលអ៊ីមែល ឬការឆ្លងមេរោគជាដើម។



គូរតារាងវិភាគហានិភ័យ និងពន្យល់អ្នកចូលរួមពីរបៀបប្រើប្រាស់តារាងនោះ។

តារាងវិភាគហានិភ័យ

ការវិភាគហានិភ័យ				ផែនការសុវត្ថិភាព	
ការគំរាមកំហែង	កំរិតនៃភាពដែលអាចកើតឡើង	កំរិតនៃផលប៉ះពាល់	ផលគុណនៃកំរិតនៃភាពដែលអាចកើតឡើងនិងកំរិតនៃផលប៉ះពាល់	យុត្តិសាស្ត្រក្នុងការទប់ស្កាត់ហានិភ័យ	ការឆ្លើយតបក្នុងករណីកើតឡើង

៣. ជំហានទី៣ គឺការពិភាក្សាគ្នាក្នុងថ្នាក់ទាំងមូលដើម្បីរកដំណោះស្រាយដែលអាចទៅរួច ដើម្បីទប់ទល់នឹងហានិភ័យដែលបានកំណត់រួច។

៤. ជំហានទី៤ គឺជាជំហានចុងក្រោយ ដើម្បីរកមើលបញ្ហានានា ដែលប្រហែលជាត្រូវបានរកដំណោះស្រាយតាមរយៈវគ្គបណ្តុះបណ្តាលហើយគណៈគ្រប់គ្រងស្ថាប័នអាចសម្រេចថាទទួលយកវាតែម្តងឬក៏ទុកពិចារណាសិន ដើម្បីរកធនធានមនុស្ស និងការបែងចែកថវិការដើម្បីដោះស្រាយបញ្ហាទាំងនោះ។

មូលដ្ឋានគ្រឹះសុវត្ថិភាព
កុំព្យូទ័រ និងគណនីនៅលើអ៊ីនធឺណិត

Device Hygiene and Account Security

មូលដ្ឋានគ្រឹះសុវត្ថិភាពកុំព្យូទ័រ និងគណនីនៅលើអ៊ីនធឺណិត

អ្វីដែលអ្នកត្រូវចេះមុនពេលចាប់ផ្តើមមេរៀននេះ

មេរៀននេះតម្រូវអោយអ្នកចូលរួមមានចំណេះដឹងស្រាប់ពីរបៀបក្នុងការប្រើប្រាស់ Password Manager ដូចជា KeepassXC។
ចង់ដឹងពីរបៀបប្រើប្រាស់ KeepassXC សូមចូលទៅកាន់តំណភ្ជាប់នេះ៖
https://securityinabox.org/en/guide/keepassxc/windows/

នេះជាកន្លែងដែលសុវត្ថិភាពលើប្រព័ន្ធឌីជីថលចាប់ផ្តើមតំបូងគឺរៀនពីកម្រិតមូលដ្ឋានទៅដូចជារបៀបដែលមនុស្សទូទៅធ្វើអោយកុំព្យូទ័រ/ទូរស័ព្ទរបស់គេមានសុវត្ថិភាព ការប្រើប្រាស់កម្មវិធីកម្ចាត់មេរោគ (ប្រសិនបើមាន) ហើយថាតើពួកគេដឹងពីកន្លែង និងរបៀបដើម្បីពិនិត្យមើលចំនុចសំខាន់ទាក់ទងនឹងសុវត្ថិភាពដែរឬទេ។

នេះគឺជាប្រធានបទមួយក្នុងចំនោមប្រធានបទនានាជាច្រើនដែលអ្នកត្រូវពិភាក្សាគ្នាមុនពេលបង្រៀនថាតើអ្នកចូលរួមយល់ដឹង និងអាចដោះស្រាយបញ្ហាសុវត្ថិភាពដែលពួកគេកំពុងប្រើប្រាស់នាពេលបច្ចុប្បន្ននេះ។

Device hygiene and maintenance គឺជាការលើកកម្ពស់ការយល់ដឹងពីកន្លែងសុវត្ថិភាពសំខាន់ៗរបស់អ្នកប្រើប្រាស់ ពីរបៀបប្រើប្រាស់ និងរបៀបកំណត់ការប្រើប្រាស់ជាដើម។ មានវិធីសាស្រ្តជាច្រើនទាក់ទងនឹង device hygiene។ នៅក្នុងសៀវភៅណែនាំនេះ យើងនឹងផ្តល់ឧទាហរណ៍ និងវិធីសាស្រ្តដែលធ្លាប់បានសាកល្បងប្រើ ហើយជាទូទៅវាដំណើរការបាន។

សូមបញ្ជាក់ថា៖ ឧទាហរណ៍នៅក្នុងមេរៀននេះ ភាគច្រើនតម្រូវសម្រាប់អ្នកប្រើប្រាស់ Windows ដោយសារភាគច្រើននៃអ្នកចូលរួមនិយមប្រើប្រាស់កុំព្យូទ័រ Windows។ ទោះបីជាយ៉ាងណាក៏ដោយ អ្នកប្រើប្រាស់Macក៏ត្រូវបានរួមបញ្ចូលនៅក្នុងវគ្គបណ្តុះបណ្តាលផងដែរ។ គ្រូបណ្តុះបណ្តាល គួរតែពន្យល់ការកំណត់ផ្នែកសុវត្ថិភាពជារួមសម្រាប់អ្នកប្រើប្រាស់ទាំងពីរ (Mac និង Windows) ។

ផែនការបង្រៀន

វិធីសាស្រ្តបង្រៀន	ប្រើប្រាស់ Window Action Center ហើយបង្ហាញស្រ្កីនកុំព្យូទ័ររបស់អ្នក (LCD Projector) ព្រមទាំងសរសេរពាក្យបច្ចេកទេសសំខាន់សម្រាប់ការពិភាក្សាគ្នា
សំភារៈប្រើប្រាស់ក្នុងការបង្រៀន	Projector ផ្ទាំងក្រដាសធំ ហ្វឺត
រយៈពេលបង្រៀន	៩០ នាទី
ឧទាហរណ៍ប្រៀបធៀប	**Password Manager:** គឺដូចជាការទុកស៊ុតរបស់អ្នកទាំងអស់ទៅក្នុងកន្ត្រកមួយ (database) ប៉ុន្តែយើងមានយន្តការសុវត្ថិភាពដើម្បីធានាថាស៊ុតទាំងនោះ (password) នឹងមិនបែក។
ប្រភពឯកសារពាក់ព័ន្ធ (ជាភាសាអង់គ្លេស)	https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords

នីតិវិធីក្នុងការបង្រៀន

ចាប់ផ្តើមការពិភាក្សាគ្នាដោយសួរថា តើប៉ុន្មាននាក់មានប្រើពាក្យសំងាត់ នៅលើកុំព្យូទ័ររបស់ពួកគេ។ សួររបៀបក្រៅផ្លូវការ មុនចាប់ផ្តើមមេរៀនជាមួយសំណួរពញ្ញាក់ស្មារតីដូចជា៖

ហេតុអ្វីបានជាអ្នកមិនប្រើពាក្យសំងាត់?

ហេតុអ្វីបានជាអ្នកប្រើពាក្យសំងាត់?

គោលគំនិតនៃការពិភាក្សានេះ គឺដើម្បីជួយអ្នកចូលរួមអោយយល់ ហេតុអ្វីការធ្វើអោយកុំព្យូទ័រ ឬទូរស័ព្ទរបស់ពួកគេមានសុវត្ថិភាព គឺមានសារៈសំខាន់។

បង្ហាញកុំព្យូទ័ររបស់អ្នកអំពី Windows Action Center ហើយជាទូទៅគេអាចរកវាបានតាមរយៈការចូលទៅកាន់ប្រអប់ស្វែងរកហើយវាយពាក្យ Action Center ឬចូលទៅកាន់ Control Panel ។ Action Center មានផ្នែកការកំណត់ Security and Maintenance ។ គ្រូមិនចាំបាច់បង្ហាញ និងពន្យល់គ្រប់ចំនុចនៅក្នុងការកំណត់សុវត្ថិភាពនោះទេ (Security Setting) ដោយហេតុថាអ្នកចូលរួមអាចពិនិត្យ និងកំណត់មុខងារសុវត្ថិភាពសំខាន់ៗដោយខ្លួនឯង។ សូមចំណាំថាខណៈពេលកម្មវិធី (Software) កុំព្យូទ័រចេញមកថ្មី Action Center ក៏មិនមានការប្រែប្រួលពេកនោះដែរ យើងនៅតែអាចរកឃើញនៅកន្លែង Security and Maintenance នៅក្នុង Control Panel បាន ។

ចំនុចសំខាន់ៗដែលត្រូវយកចិត្តទុកដាក់

- មើលព័ណ៌កូដះឧទាហរណ៍ព័ណ៌ក្រហមជាធម្មតាចង្អុលបង្ហាញថាអ្វីមួយមានបញ្ហាដែលមិនអាចមើលរំលងបានទេ។ នេះគឺជាវិធីដ៏ល្អមួយ សម្រាប់អ្នកប្រើប្រាស់ ដើម្បីត្រួតពិនិត្យមើលភាពមិនប្រក្រតីរបស់ System ហើយយកចិត្តទុកដាក់ពិនិត្យមើលបញ្ហានៅកន្លែង Security and Maintenance។

- Action Center មានកន្លែងដែលត្រូវពិភាក្សាគ្នា ក្រោមទិដ្ឋភាពសុវត្ថិភាពដូចខាងក្រោមនេះ៖

ការធ្វើបច្ចុប្បន្នភាព Windows

- សរសេរពាក្យUpdates(បច្ចុប្បន្នភាព)នៅលើក្រដាសហើយសួរអ្នកចូលរួមអោយកំណត់និយមន័យពាក្យនេះ។ ធ្វើការអង្កេត និងពិភាក្សាជាមួយអ្នកចូលរួមហេតុអ្វីបានជាពួកគេមួយចំនួនមិនធ្វើបច្ចុប្បន្នភាព។

- ពន្យល់ពីគោលបំណងនៃការធ្វើបច្ចុប្បន្នភាព និងផ្តល់ការណែនាំដល់ពួកគេ អោយធ្វើការកំណត់ការទាញយក និងតម្លើងការធ្វើបច្ចុប្បន្នភាពដោយស្វ័យប្រវត្តិ។

- នៅពេលដំណាលគ្នានោះ ពិភាក្សាគ្នាពីការកំណត់ Check for updates ដែលផ្តល់តំណឹងដល់អ្នកប្រើប្រាស់ពីការធ្វើបច្ចុប្បន្នភាពកម្មវិធី (Software) ណាដែលមិនសូវចាំបាច់ ព្រមទាំងសម្រាប់ Windows និងកម្មវិធីនានារបស់ Microsoft។

ការពារមេរោគ និង Malware

- សរសេរពាក្យ Malware នៅលើក្រដាស ហើយសួរអ្នកចូលរួមអោយកំណត់និយមន័យរបស់វា។

- ពន្យល់អ្វីទៅជា Malware (ចេញមកពីការរួមបញ្ចូលគ្នារវាងពាក្យពីរគឺ “malicious” និង “software” ហើយវាបង្ហាញខ្លួនជា Trojans, Worms, spyware, adware, ransomare, rootkit ជាដើម។

- សរសេរពាក្យ “Virus” នៅលើក្រដាស ហើយសួរអ្នកចូលរួមអោយកំណត់និយមន័យពាក្យនេះ ពិភាក្សាគ្នាគ្រប់ទម្រង់នៃមេរោគ និងពីរបៀបដែលវាវាយប្រហារ។ កុំព្យូទ័រ/ទូរស័ព្ទជាច្រើនឆ្លងមេរោគដោយសារអ្នកប្រើប្រាស់ចូលទៅមើលគេហទំព័រដែលគ្មានសុវត្ថិភាពឬក៏ទាញយកកម្មវិធីដែលមានមេរោគបង្កប់នៅក្នុងនោះ។

- ពិភាក្សាពីរោគសញ្ញាដែលអាចកំណត់ថាមានវត្តមានមេរោគនៅក្នុងកុំព្យូទ័រព្រមទាំងការរីករាលដាលនៃមេរោគនៅពេលដែលការការពារប្រឆាំងនឹងមេរោគមិនត្រូវបានតម្លើងបិទចោលឬក៏មិនបានធ្វើបច្ចុប្បន្នភាព។

- ពិភាក្សាពីការផ្តល់អនុសាសន៍ដើម្បីតម្លើងកម្មវិធីប្រឆាំងមេរោគ ហើយបង្ហាញអ្នកចូលរួមពីរបៀបបើកកម្មវិធីកម្ចាត់មេរោគ (ប្រសិនបើតម្លើងរួច) ឬក៏ធ្វើបច្ចុប្បន្នភាព។

ការពិភាក្សាគ្នាផ្សេងៗទៀតដែលមានប្រយោជន៍

- របៀបពិនិត្យមើលកម្មវិធីកម្ចាត់មេរោគដែលមាននៅក្នុងកុំព្យូទ័រ
- របៀបជ្រើសរើសយកកម្មវិធីកម្ចាត់មេរោគណាល្អប្រសើរ ដោយផ្អែកទៅតាមអនុសាសន៍យោងពីគេហទំព័រ av-test.org (ជាគេហទំព័រដែលបានចង្អុលបង្ហាញ ធ្វើតេស្តសាកល្បង និងប្រៀបធៀបកម្មវិធីកម្ចាត់មេរោគដែលពេញនិយម)។
- សារៈសំខាន់នៃការប្រើកម្មវិធីកម្ចាត់មេរោគបើទោះបីជាមិនគិតថ្លៃក៏ដោយ។ចំណាយពេលពន្យល់អ្នកចូលរួមថាមិនមែនបានន័យថាកម្មវិធីមិនគិតថ្លៃមិនសូវមានប្រសិទ្ធិភាពជាងកម្មវិធីដែលគិតថ្លៃនោះទេ។ វាគ្រាន់តែកម្មវិធីដែលទិញមានអត្ថប្រយោជន៍បន្ថែម ដូចជាទទួលបានការសេវាគាំទ្រអតិថិជនបន្ថែម ឬក៏ backupជាដើម។
- ចង្អុលបង្ហាញថាកម្មវិធីកម្ចាត់មេរោគដែលសមស្របអាស្រ័យទៅតម្រូវការរបស់អ្នកប្រើប្រាស់ផងដែរ។ ឧទាហរណ៍ អ្នកប្រើប្រាស់ម្នាក់ដែលចំណាយពេល ដ៏ច្រើននៅលើ បណ្តាញអ៊ីនធឺណិតប្រហែលជាជ្រើសរើសយកម្មវិធីណាដែលមានសមត្ថភាពខ្ពស់ក្នុងការការពារសុវត្ថិភាពលើប្រព័ន្ធអ៊ីនធឺណិត។ ណែនាំអ្នកចូលរួមផងដែរនូវមុខងារសំខាន់ៗ ដែលកម្មវិធីកម្ចាត់មេរោគមួយគួរតែមាន ហើយបើកអោយវាតំណើរការដោយស្វ័យប្រវត្តិ និងធ្វើការស្កេនអោយទៀងទាត់ ព្រមទាំងបញ្ជាក់ពីផលប៉ះពាល់តិចតួចបំផុតចំពោះដំណើរការរបស់កុំព្យូទ័រ។
- ពិភាក្សាពីឈុតកម្មវិធី (Software) endpoint security (ដូចជា Sophos ឬ Kaspersky) និងលក្ខណៈសម្បត្តិដែលគេផ្តល់អោយ។ ជាទូទៅ គេផ្តល់ជូនច្រើនជាងមុខងារការពារមេរោគដោយបញ្ចូលមុខងារបន្ថែមទៀតដូចជា Checking patching ជាដើម។
- និយាយអំពីហេតុអ្វីបានជាអ្នកចូលរួមមិនគួរតម្លើងកម្មវិធីកម្ចាត់មេរោគពីរនៅក្នុងកុំព្យូទ័រតែមួយ។ នេះដោយសារជារឿយអ្នកប្រើប្រាស់មានអារម្មណ៍ថាការដាក់កម្មវិធីបន្ថែមជួយបំពេញបន្ថែមមុខងារអោយគ្នាទៅវិញទៅមក។ នោះគឺមិនពិតនោះទេ ព្រោះកម្មវិធីកម្ចាត់មេរោគពី រព្យាយាមបំពេញមុខងារដូចគ្នា នឹងធ្វើអោយកុំព្យូទ័រដើរយឺត ហើយជាលទ្ធផលធ្វើឲ្យវាប្រឆាំងគ្នាធ្វើអោយគ្មានការការពារអ្វីទាំងអស់។ ខណៈពេលដែលគ្មានកម្មវិធីកម្ចាត់មេរោគណាល្អឥតខ្ចោះនោះ អ្នកប្រើប្រាស់អាចជ្រើសរើសយកកម្មវិធីមួយណាដែលផ្តល់អោយពួកគេនូវការពារបានប្រសើរបំផុតតាមដែលអាចធ្វើបាន។
- ជាចុងក្រោយ តែងមានការយល់ច្រឡំជារួមថា កុំព្យូទ័រ Mac គឺមានភាពស៊ាំប្រភេទមេរោគផ្សេងៗបាន។ យកពេលពន្យល់អ្នកចូលរួមថា ទោះបីជា Mac មានភាពធន់ជាង ក៏វាមិនមានភាពស៊ាំទៅនឹងការវាយប្រហាររបស់មេរោគនោះដែរ។ កាលពីមុនមេរោគមួយចំនួន ត្រូវបានបង្កើតឡើងដើម្បីសម្រាប់វាយប្រហារប្រព័ន្ធប្រតិបត្តិការរបស់ Mac តែដោយសារMac មានតម្លៃថ្លៃ មនុស្សតិចតួចណាស់អាចទិញវាមកប្រើបាន។ ដូចនេះហើយអ្នកដែលបង្កើតមេរោគ មិនសូវចំណេញនោះទេ។ ទោះបីជាយ៉ាងណាក៏ដោយ យើងឃើញមានការកើនឡើងមេរោគ ដែលមានគោលដៅវាយប្រហារ Mac ដោយសារតែមានការកើនឡើងអ្នកទិញផលិតផលក្រុមហ៊ុនApple កាន់តែច្រើន។ មានកម្មវិធីទាំងយកថ្លៃ និងមិនគិតថ្លៃ សម្រាប់Mac OS។

Network Firewall

- សរសេរពាក្យ 'firewall' នៅលើក្រដាស ហើយសួរអ្នកចូលរួមអោយកំណត់និយមន័យពាក្យនេះ។
- ពន្យល់អ្វីទៅជា firewall ហើយវាមានសារៈប្រយោជន៍ដូចម្តេចខ្លះ រួមទាំងការកំណត់អោយវាបើកដំណើរការ (Turn On)។ ប្រើពាក្យប្រដូច៖ Firewall មួយដូចជាអ្នកចាំបើកទ្វារសម្ងាត់ ឬភ្នាក់ងារសន្តិសុខដែលចាំសង្កេតរាល់ចរាចរណ៍ចេញចូលនិងបញ្ឈប់ចរាចរណ៍ណាដែលសង្ស័យលួចចូលដោយស្វ័យប្រវត្តិ។
- Firewall មានប្រយោជន៍ក្នុងការសម្គាល់ពពួកមេរោគ។

ការចាក់សោរកុំព្យូទ័រ

- សួរអ្នកចូលរួមប្រសិនបើពួកគេកំណត់ការចាក់សោរអេក្រង់កុំព្យូទ័ររបស់ពួកគេដោយតម្រូវអោយវាយពាក្យសម្ងាត់ដើម្បីការពារការចូលដោយគ្មានការអនុញ្ញាត។ពិភាក្សាពីសារៈសំខាន់នៃការចាក់សោរអេក្រង់កុំព្យូទ័រនៅពេលដែលអ្នកប្រើប្រាស់ដើរចេញពីមុខកុំព្យូទ័រឬទុកកុំព្យូទ័រចោលមិនប្រើប្រាស់។ការដោះសោរកុំព្យូទ័រគឺជារឿងងាយស្រួលទេប៉ុន្តែវាត្រូវបានគេមើលរំលងជារឿយៗពីវិធីធ្វើអោយឯកសារមានសុវត្ថិភាព។
- ជម្រើសខាងក្រោមនេះអាចប្រើបាន ចំពោះកុំព្យូទ័រដែលប្រើWindows ៖
  - **រួមបញ្ចូលគ្នារវាង Ctrl+Alt+Del**
  - **ប្រើ Control Panel និងជ្រើសរើសយក a screen saver ដែលតម្រូវអោយវាយពាក្យសម្ងាត់ដើម្បីប្រើប្រាស់កុំព្យូទ័រម្តងទៀត**
  - **ចុច Windows Key + L**
  - **ចុច Start + L**

ពាក្យសម្ងាត់

នេះគឺជាមេរៀនដ៏មានសារៈសំខាន់សម្រាប់ការពិភាក្សាគ្នាពីព្រោះពាក្យសម្ងាត់គឺជាខ្សែការពារតំបូងគេនៅក្នុងការការពារ ទាំងកុំព្យូទ័រ/ទូរស័ព្ទ និងគណនីនានានៅលើប្រព័ន្ធអនឡាញ។

- សួរអ្នកចូលរួមថាតើធាតុផ្សំអ្វីខ្លះបង្កើតបានជាពាក្យសម្ងាត់រឹងមាំ។ អ្នកចូលរួមនឹងព្យាយាមផ្តល់ចម្លើយពីការរួមបញ្ចូលគ្នារវាងអក្សរធំ លេខ និងសញ្ញា។ដូចនេះពាក្យសម្ងាត់ដែលរឹងមាំគឺ៖
  - មានតែមួយ៖ មិនប្រើពាក្យសម្ងាត់តែមួយជាមួយគណនីច្រើន
  - វែង៖ ស្តង់ដារពាក្យសម្ងាត់ដ៏រឹងមាំចេញដោយNIST សង្កត់ធ្ងន់ថាប្រវែងកាន់តែវែង គឺជាកត្តាសំខាន់បំផុត
  - បង្កើតឡើងដោយភាសាណាមួយ(vernacular)ជាជាងប្រើភាសាអង់គ្លេស។ឧបករណ៍បំបែកលេខកូដសម្ងាត់ភាគច្រើនប្រើភាសាអង់គ្លេស។
  - ងាយស្រួលចាំ៖ ប្រើអក្សរនៅខាងដើមនៃពាក្យនីមួយៗមកធ្វើជាពាក្យសម្ងាត់។

ដោយសារតែពាក្យសម្ងាត់សម្រាប់គណនី នីមួយៗត្រូវតែរឹងមាំ និងមានតែមួយ ហើយដោយសារតែមនុស្សម្នាក់ៗមានគណនីច្រើន ដូចនេះវាប្រហែលជាមិនចាំបាច់អោយ យើងប្រើវិធីនេះដើម្បីបង្កើតពាក្យសម្ងាត់រឹងមាំ នៅគ្រប់គណនីនោះទេ។ នេះមានន័យថាយើងមិនចាំបាច់ទៅចាំគ្រប់ពាក្យសម្ងាត់នៅលើគណនីផ្សេងៗគ្នានោះទេ។ មកដល់ត្រឹមនេះ យើងនឹងឈានដល់ការពិភាក្សាគ្នាមួយទៀតគឺកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager)។

ចំនុចដ៏មានសារៈសំខាន់ដែលគ្រូបណ្តុះបណ្តាលអាចចង្អុលបង្ហាញបន្ថែមទៀតគឺស្តង់ដាពាក្យសម្ងាត់ពី NIST។ នៅពេលដែលបង្កើតស្តង់ដារណែនាំនេះ ស្តង់ដារមួយចែងថាពាក្យសម្ងាត់ត្រូវតែផ្លាស់ប្តូរនៅពេលមានហេតុផលល្អមួយដើម្បីផ្លាស់ប្តូរវា (ដូចជានៅពេលមានពាក្យសម្ងាត់មួយ ត្រូវបានបំបែកបាន នៅលើអ្នកផ្តល់សេវាកម្មគណនីអនឡាញរបស់អ្នកប្រើប្រាស់)

កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager)

- សួរអ្នកចូលរួមប្រសិនបើពួកគេកំពុងប្រើប្រាស់កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager)។ ពន្យល់អ្វីទៅជាកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager)៖ ជាកម្មវិធីដែលសម្រាប់បង្កើតនិងផ្ទុកពាក្យសម្ងាត់នានារបស់អ្នកហើយទុកនៅកន្លែងដែលមានសុវត្ថិភាព។កម្មវិធីនេះប្រាប់អ្នកថាពាក្យសម្ងាត់របស់អ្នកនីមួយៗរឹងមាំយ៉ាងណា។កម្មវិធីគ្រប់គ្រងពាក្យ សម្ងាត់(Pass wordManager)ខ្លះប្រាប់អ្នកភ្លាមៗនៅពេលដែលក្រុមហ៊ុនផ្តល់សេវាកម្មរបស់គណនីអនឡាញដែលអ្នកប្រើប្រាស់ត្រូវបានគេបំបែកបានហើយប្រាប់ថាតើព័ត៌មានផ្ទាល់ខ្លួនអ្នកត្រូវបានបង្ហាញ។
- ពិភាក្សាគ្នាពីរបៀបប្រើប្រាស់កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់(Password Manager) ដោយមិនចាំ បាច់ប្រើអ៊ីនធឺណិត ឬប្រើវានៅលើគេហទំព័រហើយអោយ ឧទាហរណ៍ដែលជាទូទៅ គេអាចទុកចិត្តបានដែលមានដូចជា (1Password, LastPass)។ 1Password ជាដៃគូជាមួយ haveibeenpwned.com ហើយផ្តល់តំណឹងដល់អ្នកប្រើប្រាស់ណាម្នាក់ប្រសិនបើពាក្យសម្ងាត់របស់គេត្រូវបានគេបំបែកបាន។ ប៉ុន្តែកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager)មួយចំនួនគឺគិតថ្លៃ។
- ទោះបីជាកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager) នៅលើគេហទំព័រមួយចំនួនល្អ ក៏ដោយគ្រូបណ្តុះបណ្តាលត្រូវណែនាំអោយជ្រើសរើសយកជម្រើសដោយតម្លើងកម្មវិធីនៅលើកុំព្យូទ័រ/ទូរស័ព្ទផ្ទាល់ជាដំណោះស្រាយដ៏ល្អ។ ព័ត៌មានផ្ទុកនៅលើអនឡាញ ងាយស្រួលបែកធ្លាយ ខណៈពេលដែលកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (Password Manager) ដែលបើកទូលាយ (open source) ទំនងជាមាននិរន្តភាពយូរអង្វែងជាងទៅថ្ងៃអនាគត។
- បង្ហាញអេក្រង់កុំព្យូទ័ររបស់អ្នក ហើយពន្យល់ពីរបៀប KeepassXC តំណើរការដើម្បីបង្កើត និងផ្ទុកពាក្យសម្ងាត់នៅលើកុំព្យូទ័រ និងពីរបៀបទាញយកពាក្យសម្ងាត់ពី database សម្រាប់ប្រើប្រាស់នៅលើគណនីនានា។
- និយាយអំពី KeepassDroid/MiniKeepass និងកម្មវិធីនានាដែលអាចប្រើប្រាស់ជំនួសបាន ចំពោះទូរស័ព្ទដើម្បីដោះស្រាយក្តីបារម្ភផ្សេងៗ។Databaseអាចរក្សាទុកដោយចាក់សោរ(encrypted)ឬមិនចាក់សោរ(unencrypted)នៅUSBឬនៅលើcloud។ដូចនេះយើងអាចយកវាមកប្រើប្រាស់នៅពេលដែលត្រូវការបាន។ទោះបីជាយ៉ាងណាក៏ដោយអ្នកប្រើប្រាស់ត្រូវការពារវាជាមួយពាក្យសម្ងាត់ដ៏រឹងមាំមួយ និងថតចម្លងកម្មវិធី (Software) KeepassXC មួយដើម្បីអាចបើក database។

៤

សុវត្ថិភាពលើទូរស័ព្ទស្មាតហ្វូន

Mobile Security

សុវត្ថិភាពលើទូរស័ព្ទស្មាតហ្វូន

ស្មាតហ្វូនស្ទើរតែក្លាយទៅជាឧបករណ៍ដែលមិនអាចខ្វះបានក្នុងជីវិតរស់នៅប្រចាំថ្ងៃទៅហើយ។ពីមួយថ្ងៃទៅមួយថ្ងៃ បច្ចេកវិទ្យាស្មាតហ្វូននេះ កាន់តែមានការរីកចម្រើន ដែលវាមិនត្រឹមតែ យកទៅប្រើសម្រាប់ការកម្សាន្ត និងការងារផ្ទាល់ខ្លួននោះទេ វាក៏ត្រូវបានប្រើប្រាស់សម្រាប់បំពេញការងារផងដែរ។ ដោយសារតែវាអាចប្រើប្រាស់បានយ៉ាងទូលំទូលាយដូចច្នេះហើយ ទើបធ្វើឱ្យអ្នកប្រើប្រាស់ជួបបញ្ហាជាច្រើនពីការប្រើប្រាស់ឧបករណ៍ទាំងនេះដែរ។

ការវិវត្តន៍នៃបច្ចេកវិទ្យាអ៊ីនធឺណិត និងស្មាតហ្វូននេះ ក៏ជាមូលហេតុធ្វើឱ្យមានការកើនឡើងនៃចំនួនឧក្រិដ្ឋជនអ៊ីនធឺណិតកាន់តែច្រើនជារៀងរាល់ថ្ងៃ។ពួកឧក្រិដ្ឋជនទាំងនោះព្យាយាមរកគ្រប់មធ្យោបាយដោយធ្វើការវាយប្រហារឧបករណ៍ណាដែលភ្ជាប់ទៅកាន់អ៊ីនធឺណិត លួចតាមដានសកម្មភាពនៃការប្រើអ៊ីនធឺណិត តាមរយៈមេរោគដែលពួកគេបានបង្កើតឡើងក្នុងគោលបំណងស្វែងរកប្រាក់ចំណេញ និងក្នុងគោលបំណងជាក់លាក់ផ្សេងៗទៀត។

ផែនការបង្រៀន

វិធីសាស្ត្រក្នុងការបង្រៀន	ភាគច្រើនផ្តោតលើការពិភាក្សា
សំភារៈប្រើប្រាស់ក្នុងការបង្រៀន	ទូរស័ព្ទស្មាតហ្វូន ផ្ទាំងក្រដាសធំ ហ្វឺត
រយៈពេលបង្រៀន	៦០ នាទី
ប្រភពឯកសារពាក់ព័ន្ធ (ជាភាសាអង់គ្លេស)	https://securityinabox.org/en/android https://level-up.cc/curriculum/mobile-safety

នីតិវិធីក្នុងការបង្រៀន

គ្រូបណ្តុះបណ្តាលអាចចាប់ផ្តើមដោយធ្វើការពិភាក្សាពីវិធីផ្សេងៗគ្នាដែលអ្នកចូលរួមតែងតែយកមកអនុវត្តដើម្បីធ្វើឱ្យទូរស័ព្ទដៃរបស់ពួកគេមានសុវត្ថិភាព។ ចំណុចដែលគួរតែយកមកបញ្ចូលក្នុងការពិភាក្សារួមមាន៖

- **ស្មាតហ្វូនដូចនឹងកុំព្យូទ័រដែរ៖** ប្រាប់ឱ្យអ្នកចូលរួមគិតថា ទូរស័ព្ទស្មាតហ្វូនប្រៀបដូចជាកុំព្យូទ័រដែរដូច្នេះអ្វីដែលពួកគេអាចយកទៅប្រើដើម្បីធ្វើឱ្យកុំព្យូទ័រមានសុវត្ថិភាពក៏គួរតែអាចយកមកប្រើជាមួយទូរស័ព្ទស្មាតហ្វូនបានដែរ។

- **កម្មវិធីកម្ចាត់មេរោគ៖** ប្រសិនបើទូរស័ព្ទដូចនឹងកុំព្យូទ័រ នោះមានន័យថា ទូរស័ព្ទក៏ត្រូវការការពារពីមេរោគផ្សេងៗដែរ។ កម្មវិធីកម្ចាត់មេរោគភាគច្រើន បង្កើតទាំងកម្មវិធី (Software) ដែលអាចយកទៅតម្លើងប្រើលើកុំព្យូទ័រ និងកម្មវិធីទូរស័ព្ទ (App)ដែលអាចប្រើបានជាមួយទូរស័ព្ទដែរ។

- **ចាក់សោអេក្រង់៖** គ្រូបណ្តុះបណ្តាលអាចរំលឹកពីចំណុចសំខាន់ៗពីមេរៀនពាក្យសម្ងាត់រឹងមាំមកនិយាយម្តងទៀត។ពន្យល់ពីសារសំខាន់នៃការប្រើពាក្យសម្ងាត់រឹងមាំគ្រូបណ្តុះបណ្តាលអាចឧបមាថា ប្រសិនបើទូរស័ព្ទ ឬកុំព្យូទ័ររបស់អ្នកចូលរួមត្រូវបានបាត់បង់ ឬត្រូវបានគេលួច នោះការចាក់សោរអេក្រង់ជាមួយនឹងពាក្យសម្ងាត់រឹងមាំអាចការពារទិន្នន័យនៅក្នុងឧបករណ៍នោះបាន។សម្រាប់ទូរស័ព្ទដៃ គ្រូបណ្តុះបណ្តាលគួរតែពន្យល់ពីភាពខុសគ្នារវាងការចាក់សោអេក្រង់ដោយប្រើមុខងារអូស (Pattern) លេខកូដ (PIN) និងដោយប្រើពាក្យសម្ងាត់ (Password) ជាដើម។ ខាងក្រោមនេះជាការពន្យល់ត្រួសៗពីមុខងារនិមួយៗ៖
  - **អូស (Pattern)៖** គឺជារបៀបនៃការចាក់សោរអេក្រង់ទូរស័ព្ទដោយប្រើម្រាមដៃអូសជាទម្រង់ផ្សេងៗ (ឧ.អូសជាទម្រង់អក្សរ Z N V ជាដើម) នៅលើអេក្រង់ទូរស័ព្ទ។ គុណវិបត្តិរបស់វាគឺ អ្នកផ្សេងអាចដឹងពីគំនូសដើម្បដោះសោ ប្រសិនគេផ្ទៀងមើលលើកញ្ចក់អេក្រង់នោះ ព្រោះគំនូសស្នាមម្រាមដៃដែលអូសនៅលើកញ្ចក់អេក្រង់ទូរស័ព្ទមិនរលុបភ្លាមៗទេ។គុណវិបត្តិមួយទៀតគឺវាមានភាពងាយស្រួលឱ្យអ្នកដទៃដឹងនិងចាំពីគំនូសនោះដោយគ្រាន់សង្កេតមើលការអូសលើកញ្ចក់អេក្រង់នៅពេលដែលម្ចាស់ទូរស័ព្ទយកទូរស័ព្ទនោះមកប្រើ។ ការចាក់សារដោយប្រើមុខងារអូសមិនមានសុវត្ថិភាពខ្ពស់ទេហើយគ្រូបណ្តុះបណ្តាលមិនគួរលើកទឹកចិត្តឱ្យអ្នកចូលរួមជ្រើសរើសយកជម្រើសមួយនេះទេ។

  - **លេខកូដ(PIN)៖** គឺជាមុខងារនៃការចាក់សោរអេក្រង់ដោយប្រើលេខទាំងអស់(មិនមានលាយអក្សរឬសញ្ញា)។បញ្ហារបស់មនុស្សភាគច្រើននៅពេលប្រើលេខកូដ(PIN)គឺពួកគេប្រើលេខដែលងាយស្រួលក្នុងការចងចាំដូចជា ប្រើលេខរៀង លេខគូរ ឆ្នាំកំណើតជាដើម។ ទោះជាយ៉ាងណាក៏ ការចាក់សោរដោយប្រើលេខកូដ (PIN) ល្អប្រសើរជាង មុខងារអូស (Pattern) ដែរ។ គ្រូបណ្តុះបណ្តាលអាចណែនាំឱ្យអ្នកចូលរួមប្រើជម្រើសនេះ ប្រសិនបើកម្រិតចំណេះដឹង របស់អ្នកចូលរួមទាប ឬពួកគាត់មិនស្គាល់ពីតួអក្សរភាសាអង់គ្លេសជាដើម។

  - **ពាក្យសម្ងាត់(Password)៖** គឺជាការចាក់សោរអេក្រង់ដែលយើងអាចលាយបញ្ចូលគ្នាបានទាំងលេខអក្សរនិមិត្តសញ្ញាផ្សេងៗនិងអាចដាក់ចំនួនតួអក្សរច្រើនតាមការចង់បានរបស់អ្នកបង្កើត។ ដោយសារតែវាអាចលាយអក្សរ លេខ និមិត្តសញ្ញាបញ្ចូលគ្នា និងអាចបង្កើតបានវែងនេះហើយទើបធ្វើឱ្យអ្នកផ្សេងពិបាកក្នុងការប៉ាន់ស្មាននិងចងចាំពាក្យសម្ងាត់ដែលបានបង្កើតនោះកត្តានេះហើយ បានជាការចាក់សោអេក្រង់ដោយប្រើពាក្យសម្ងាត់ (Password) ត្រូវបានចាត់ទុកថាមានសុវត្ថិភាពខ្លាំងនិងណែនាំឱ្យប្រើប្រាស់។ប៉ុន្តែគ្រូបណ្តុះបណ្តាលត្រូវមើលពីកម្រិតចំណេះដឹង និងស្ថានភាពជាក់ស្តែងរបស់អ្នកចូលរួមដែរ ទោះបីជាជម្រើសនេះល្អ តែវាក៏មានហានិភ័យច្រើនដែរ។ អ្នកចូលរួមអាចងាយនឹងភ្លេច ឬច្រឡំតួអក្សរណាមួយ នៅពេលបង្កើតពាក្យសម្ងាត់។ ដូច្នេះគ្រូបណ្តុះបណ្តាលត្រូវប្រុងប្រយ័ត្ន មុននឹងឱ្យអ្នកចូលរួមអនុវត្ត អាចឱ្យអ្នកចូលរួមសរសេរពាក្យសម្ងាត់ របស់ពួកចូលទៅក្នុងសៀវភៅ ឬកត់ចម្លងទុកនៅកន្លែងណាដែលមានសុវត្ថិភាព ហើយពួកគេអាចស្វែងរកវិញបានករណីដែលពួកគេភ្លេច។

- **Biometric៖** គឺជាការចាក់សោរអេក្រង់ដោយស្កេនខ្ទៀដៃ ឬស្កេនមុខជាដើម។ ការប្រើមុខងារនេះក៏ត្រូវបានគេចាត់ទុកមានសុវត្ថិភាពខ្ពស់ផងដែរ។ប៉ុន្តែពេលខ្លះវាក៏មានភាពងាយស្រួលនិងមិនចំណាយពេលយូរក្នុងការដោះសោអេក្រង់ទូរស័ព្ទ ប្រសិនបើម្ចាស់ទូរស័ព្ទត្រូវបានគេគំរាមកំហែងឱ្យដាក់ម្រាមដៃ ឬបើកភ្នែកមើលទូរស័ព្ទដើម្បីស្កេនដោះសោអេក្រង់ទូរស័ព្ទនោះ។

ចំណុចសំខាន់មួយដែរ ដែលគ្រូបណ្តុះបណ្តាលគួរបញ្ជាក់ គឺការកំណត់ពេលវេលាឱ្យទូរស័ព្ទចាក់សោរដោយខ្លួនឯងនៅពេលដែលមិនប្រើ

- **ការធ្វើបច្ចុប្បន្នភាព (Update)៖** ដូចគ្នានឹងកុំព្យូទ័រដែរ កម្មវិធីទូរស័ព្ទ (App) ផ្សេងៗ និងប្រព័ន្ធប្រតិបត្តិការ (Operating System) គឺត្រូវតែធ្វើបច្ចុប្បន្នភាពឱ្យបានទៀងទាត់ដែរ។ ភាពងាយរងគ្រោះ និងចំណុចខ្សោយផ្សេងៗនៃកម្មវិធី ត្រូវបានរកឃើញជាបន្តបន្ទាប់ ហើយវានឹងត្រូវបានជួលជុលឬធ្វើឱ្យប្រសើរឡើងវិញនៅពេលធ្វើបច្ចុប្បន្នភាពនេះឯង។ចំណុចសំខាន់ដែលគ្រូបណ្តុះបណ្តាលត្រូវបញ្ជាក់គឺរាល់ការធ្វើបច្ចុប្បន្នភាពចាំបាច់ត្រូវការភ្ជាប់ទៅកាន់អ៊ីនធឺណិត។គ្រូបណ្តុះបណ្តាលគួរតែណែនាំឱ្យអ្នកចូលរួមអនុវត្តការធ្វើបច្ចុប្បន្នភាព នៅពេលដែលពួកគេភ្ជាប់អ៊ីនធឺណិតជាមួយ WIFI។ការធ្វើបច្ចុប្បន្នភាពអាចមានទំហំធំប្រសិនបើពួកធ្វើបច្ចុប្បន្នភាពដោយប្រើកញ្ចប់អ៊ីនធឺណិតលើទូរស័ព្ទ(3Gឬ4G)អាចធ្វើឱ្យការទាញយកនោះយឺតនិងចំណាយថវិការក្នុងទូរស័ព្ទពួកគេច្រើន។ គ្រូបណ្តុះបណ្តាលគួរតែបញ្ជាក់ពីបញ្ហាទូរស័ព្ទដំណើរការយឺត ឬឧស្សាហ៍គាំង (បញ្ហាទាំងនេះមិនមែនសុទ្ធតែមកពីទូរស័ព្ទមិនបានធ្វើបច្ចុប្បន្នភាពទេ ក៏សមត្ថភាពទូរស័ព្ទមានដូចជា អង្គចងចាំ (RAM) ស៊ីភីយូ (CPU) ទំហំផ្ទុក (Storage) និងបញ្ហាផ្សេងៗជាច្រើនទៀត) ក៏អាចដោយសារការមិនដែលធ្វើបច្ចុប្បន្នភាពទូរស័ព្ទដែរ។

- **ទាញយកកម្មវិធីពីប្រភពច្បាស់លាស់៖** ប្រភពដែលអាចទុកចិត្ត និងមានសុវត្ថិភាពសម្រាប់ទូរស័ព្ទអែនដ្រយ (Android) គឺ Google Play Store ចំណែកចំពោះអ្នកប្រើ iPhone គឺ Apple Store។ ត្រង់ចំណុចនេះ គ្រូបណ្តុះបណ្តាលអាចលើកទឹកចិត្ត អ្នកចូលរួមឱ្យធ្វើការពិនិត្យ មើលនូវមតិយោបល់របស់អ្នកផ្សេងចំពោះកម្មវិធីនោះ ពិនិត្យមើលការផ្តល់ពិន្ទុពីអ្នកដែលបានទាញយក និងពីចំនួននៃការទាញយកកម្មវិធីនោះនៅលើ Google Play Store ឬ Apple Store ដើម្បីផ្ទៀងផ្ទាត់ថាកម្មវិធីនោះល្អ និងអាចទុកចិត្តបានដែរឬទេ។ គ្រូបណ្តុះបណ្តាលគួរតែបង្ហាញពីរបៀបក្នុងការទាញយកនិងពីរបៀបក្នុងការផ្ទៀងផ្ទាត់កម្មវិធី(App)ទៅកាន់អ្នកចូលរួម។ចំណុចសំខាន់ដែលគួរតែលើកមកពិភាក្សាគឺ សារៈសំខាន់នៃការពិនិត្យមើលឡើងវិញលើវិសាលភាពនៃការអនុញ្ញាតសិទ្ធិកម្មវិធី(App)ដែលស្នើរសុំចូលប្រើទិន្នន័យឬមុខងារនៅក្នុងទូរស័ព្ទដែលអ្នកចូលរួមចង់តំឡើង។កម្មវិធីខ្លះត្រូវការចូលទៅប្រើទិន្នន័យឬមុខងារមួយចំនួនដែលមិនទាក់ទងនឹងមុខងារនៃការដំណើរការកម្មវិធីនោះទាល់តែសោះ។ឧទាហរណ៍កម្មវិធីដែលទាក់ទងនឹងអាកាសធាតុមិនគួរស្នើរសុំចូលទៅប្រើរូបភាព ឬបញ្ជីទំនាក់ទំនង (Contact) នៅក្នុងទូរស័ព្ទនោះទេ។ វាមានសារៈសំខាន់ណាស់ក្នុងការពិនិត្យឡើងវិញនូវសិទ្ធិក្នុងការចូលប្រើព័ត៌មាន ឬទិន្នន័យរបស់កម្មវិធីនិមួយៗព្រោះនេះកម្មវិធីខ្លះបានលួចយកព័ត៌មានឬទិន្នន័យរបស់អ្នកក្នុងគោលបំណងធ្វើអាជីវកម្មណាមួយ ដែលរំលោភឯកជនភាពរបស់អ្នក។

- **ប្រើមុខងារសុវត្ថិភាពដែលមានស្រាប់៖** ត្រង់ចំណុចនេះ គ្រូបណ្តុះបណ្តាលត្រូវប្រាប់ពីមុខងារសុវត្ថិភាពដែលមានស្រាប់នៅក្នុងទូរស័ព្ទរបស់ពួកគេ ចៀសវាងការទាញយកកម្មវិធី (App) បន្ថែមក្នុងករណីដែលមិនចាំបាច់។ មុខងារដែលមានស្រាប់ទាំងនោះមានដូចជា ការចាក់សោអេក្រង់ ការកំណត់ពេលវេលាចាក់សោរដោយស្វ័យប្រវត្តិតាមពេលវេលាកំណត់ការចាក់សោរម៉ាស៊ីនឬធ្វើកូដនីយកម្ម (Encryption) ទូរស័ព្ទជាដើម។ល។
- **បិទ GPS និង Bluetooth៖** GPS និង Bluetooth គួរតែបើកនៅពេលដែលត្រូវការប្រើតែប៉ុណ្ណោះ មិនគួរបើកវាចោលគ្រប់ពេលនោះទេ។ ការបិទ GPS អាចជួយការពារពីការ តាមដានលើទីតាំងឧបករណ៍របស់អ្នក និងការលួចចូលទៅគ្រប់គ្រងទិន្នន័យពីចម្ងាយតាមរយៈ Bluetooth។
- **ចៀសវាងការភ្ជាប់ទៅកាន់ WI-FI ដែលមិនមានសុវត្ថិភាព៖** អ៊ីនធឺណិតនៅទីសាធារណៈដូចជានៅផ្ទះសំណាក់ សណ្ឋាគារ ហាងការហ្វេ ព្រលានយន្តហោះ ឬទីកន្លែងសារណៈផ្សេងៗ ជាទូទៅមិនមានសុវត្ថិភាពនោះទេ។ អ្នកផ្សេង ឬជនខិលខូចអាចបង្កើត Wi-fi បានដោយងាយដោយគ្រាន់តែបើកមុខងារHotspot។ម្ចាស់wi-fiឬជនខិលខូចអាចធ្វើការតាមដានរាល់សកម្មភាពប្រើអ៊ីនធឺណិតនិងលួចយកទិន្នន័យសំខាន់ៗពីឧបករណ៍របស់អ្នកប្រើប្រាស់ នៅពេលដែលពួកគេភ្ជាប់ទៅកាន់បណ្តាញអ៊ីនធឺណិតនោះ។ ដើម្បីបង្ការហានិភ័យ អ្នកប្រើប្រាស់គួរតែពិនិត្យមើលឈ្មោះ Wi-fi ទាំងនោះឱ្យច្បាស់លាស់ ឬអាចទៅសុំឈ្មោះ Wi-fi និងពាក្យសម្ងាត់ពីអ្នកធ្វើការនៅទីនោះដោយផ្ទាល់។ គួរចៀសវាងចូលទៅកាន់គណនីធនាគារ ឬធ្វើការប្រតិបត្តិការលុយកាក់តាមមធ្យោបាយផ្សេងៗជាមួយនឹងអ៊ីនធឺណិតនៅកន្លែងនោះនិងគួរតែប្រើកម្មវិធីVPNប្រសិនបើចាំបាច់ត្រូវតែប្រើអ៊ីនធឺណិត។

គ្រូបណ្តុះបណ្តាលអាចបង្ហាញពីភាពងាយស្រួលក្នុងការបង្កើតwi-fiសម្រាប់ឱ្យអ្នកដទៃប្រើប្រាស់នៅលើទូរស័ព្ទដោយប្រើមុខងារ Hotspot របៀបក្នុងការដាក់ឈ្មោះ និងរបៀបក្នុងការប្តូរឈ្មោះ wi-fi ដែលបានបង្កើតនោះ។ គួររំលឹកអ្នកចូលរួមថា ប្រសិនបើពួកគេភ្ជាប់ទៅកាន់អ៊ីនធឺណិតនៅកន្លែងសារធារណៈពួកគេពិបាកក្នុងការកំណត់ឱ្យដឹងច្បាស់ថាមួយណាជាwi-fiពិតប្រាកដ និងមួយណាមិនពិតនោះទេ ដូច្នេះពួកគេអាចមានហានិភ័យច្រើនពីការប្រើអ៊ីនធឺណិតនោះ។

ចុងបញ្ចប់ គ្រូបណ្តុះបណ្តាលអាចណែនាំអ្នកចូលរួមឱ្យស្គាល់ពីកម្មវិធីទំនាក់ទំនងដែលមានសុវត្ថិភាពដូចជា Signal WhatsApp **និងកម្មវិធីវីភីអិន** (VPN) **ជាដើម។**

ការពិភាក្សានេះគួរតែពន្យល់ផងដែរអំពីកូដនីយកម្ម(end-to-end-encryption)**និងមុខងារសុវត្ថិភាពផ្សេងៗទៀត ដូចជាមុខងារស្រទាប់ការពារពីរជាន់** (two-factor authentication) **ជាដើម។ ការផ្ទៀងផ្ទាត់អត្តសញ្ញាណ**(fingerprint)**ជាមួយមនុស្សដែលទំនាក់ទំនងជាមួយយើងតាមរយៈកម្មវិធី**Signal**ជាដើមក៏ជាផ្នែកមួយដែលមានសារៈសំខាន់ដែរព្រោះអាចឱ្យអ្នកចូលរួមផ្ទៀងផ្ទាត់ដឹងថាតើមនុស្សដែលពួកកំពុងទាក់ទងឬផ្ញើសារទៅនោះពិតជាមនុស្សដែលពួកគេចង់ទាក់ទងប្រាកដមែន។**

៥

សុវត្ថិភាពក្នុងការរក្សាទុកទិន្នន័យ

Secure Information Storage

សុវត្ថិភាព ក្នុងការរក្សាទុកទិន្នន័យ

អ្វីដែលអ្នកត្រូវចេះមុនពេលចាប់ផ្តើមមេរៀននេះ

មេរៀននេះតម្រូវអោយគ្រូបង្រៀន ចេះពីរបៀបប្រើប្រាស់ឧបករណ៍ចាក់សោរឯកសារដូចជា Veracrypt។
រៀនពី **Veracrypt** នៅទីនេះ៖ https://securityinabox.org/en/guide/veracrypt/windows.

មេរៀននេះផ្តោតលើការការពារឯកសារសំខាន់ៗនៅលើកុំព្យូទ័រ ដោយប្រើប្រាស់ ការចាក់សោរ(បំលែងកូដ)ឬហៅម៉្យាងទៀតថាបច្ចេកវិទ្យាលាក់ឯកសារ។នៅពេលចាប់ផ្តើមវាពិតជាមានសារៈសំខាន់ណាស់ដើម្បីពិនិត្យមើលថាតើការប្រើប្រាស់បច្ចេកវិទ្យាបំលែងកូដ (Encryption Technology) ស្របច្បាប់នៅក្នុងប្រទេសរបស់អ្នកឬទេ។

ផែនការបង្រៀន

វិធីសាស្រ្តក្នុងការបង្រៀន	ការពិភាក្សាគ្នា និងការបង្ហាញអេក្រង់កុំព្យូទ័រ
សំភារៈប្រើប្រាស់ក្នុងការបង្រៀន	Projector **និងកម្មវិធី** (Software) Veracrypt
រយៈពេលបង្រៀន	១២០ នាទី
ឧទាហរណ៍ប្រៀបធៀប	**Encryption:** គឺ ដូចជាការរក្សាព័ត៌មានសំខាន់ៗនៅកន្លែងដែលចាក់សោរសុវត្ថិភាព។ វាអាចបើកប្រើប្រាស់ ជាមួយនឹងសោរមួយ ឬការរួមបញ្ចូលគ្នា នៃពាក្យសម្ងាត់រឹងមាំ (ឬpassphrase នៅក្នុងករណីកុំព្យូទ័រ) ហើយមានតែម្ចាស់ទេដែលដឹង និងចូលទៅមើលមាតិការខាងក្នុងបាន។
ប្រភពឯកសារពាក់ព័ន្ធ (ជាភាសាអង់គ្លេស)	របៀបប្រើ Veracrypt: https://securityinabox.org/en/guide/veracrypt/windows

នីតិវិធីក្នុងការបង្រៀន

- ចាប់ផ្តើមមេរៀនដោយ បំផុសការពិភាក្សាគ្នាថា តើស្ថិតក្នុងកាលៈទេសៈបែបណា ទើបអ្នកចូលរួមត្រូវការការពារឬលាក់ព័ត៌មានរសើបរួមបញ្ចូលទាំងប្រភេទព័ត៌មានបែបណាដែលយើងគួរតែរក្សាទុកអោយឆ្ងាយពីការលួចចូលមើលបាន។ការដាក់ពាក្យសម្ងាត់នៅលើអេក្រង់កុំព្យូទ័រទំនងជាមិនអាចការពារបានគ្រប់គ្រាន់នោះទេ ដោយសារវាងាយស្រួលគេលួចចូលបាន។
- ពន្យល់ត្រួសៗថានៅក្នុងប្រធានបទនេះនឹងផ្តោតសំខាន់លើការទប់ស្កាត់ការចូលទៅមើលព័ត៌មានរសើបដោយគ្មានការអនុញ្ញាត តាមរយៈការចាក់សោរ និងការលាក់ឯកសារសំខាន់ដោយប្រើ (Software) មិនអស់ថ្លៃហើយបើកទូលាយ (open source)។ សរសេរពាក្យ Encryption នៅលើក្រដាសហើយសួរអ្នកចូលរួមអោយកំណត់និយមន័យរបស់វា។
- ពន្យល់ថា Encryption គឺជាវិធីមួយដោយបំលែងឯកសារមួយ មិនអោយអានបានដោយអ្នកដ៏ទៃដោយគ្មានការអនុញ្ញាតិ ឬពាក្យសម្ងាត់ត្រឹមត្រូវ (passphrase)។ គ្រូបណ្តុះបណ្តាលអាចពន្យល់ដោយសង្ខេបពីជម្រើសនានាដែលអាចប្រើប្រាស់បានចំពោះអ្នកប្រើ Mac និងWindows។
- ទោះបីជាមានជម្រើសច្រើនក៏ដោយ គ្រូបណ្តុះបណ្តាលគួរតែណែនាំ Veracrypt ជាជម្រើសមួយដ៏ល្អ ដោយសារតែមុខងារឈានមុខរបស់វា។ Veracrypt គឺជាកម្មវិធីមួយ ដែលមិនយកថ្លៃ ហើយបើកទូលាយព្រមទាំងអនុញ្ញាតអោយអ្នកចូលរួមអាចបង្កើតកន្លែងផ្ទុកឯកសារសុវត្ថិភាពផ្ទាល់ខ្លួនផងដែរ (encrypted volumes)។
- អាស្រ័យលើរបៀបដែលអ្នកចែកចាយកម្មវិធីនេះទៅអោយអ្នកចូលរួម។អ្នកអាចបង្ហាញអ្នកចូលរួមតាំងពីរបៀបទាញយកវា របៀបតម្លើង និងរបៀបប្រើជាដើម។

គន្លឹះសំខាន់ៗ

ប្រសិនបើអ្នកជួបបញ្ហា អ្នកចូលរួមមួយចំនួនមិនអាចតម្លើងកម្មវិធីនេះបាន ឬក៏មិនចង់តម្លើងដោយមូលហេតុផ្សេងៗ អោយអ្នកទាំងនោះអង្គុយនៅជិត អ្នកដែលកំពុងធ្វើតាមការណែនាំរបស់អ្នក។ គ្រូបណ្តុះបណ្តាលគួរតែធានាថាគ្រប់អ្នកដែលមិនទាន់បានតម្លើងមានកម្មវិធីនោះនៅនឹងខ្លួនគេ ហើយអាចតម្លើងបានគ្រប់ពេលដែលគេត្រូវការ។

- ឥលូវអ្នកមានជម្រើសដើម្បីពន្យល់ពីរបៀបតម្លើង Veracrypt ពីរបៀបបង្កើតកន្លែងផ្ទុកឯកសារថ្មីមួយ (virtual container) រួចយកឯកសារដាក់នៅក្នុងនោះ ជាដើម។ ការចាក់សោរ disk ដោយផ្នែកៗជារឿយៗត្រូវបានណែនាំជាជំហានតំបូង។នីតិវិធីនៃការបង្រៀនមេរៀននេះនឹងដើរទៅដោយរលូនប្រសិនបើអ្នកបង្ហាញមួយជំហានម្តងៗ ហើយអោយអ្នកចូលរួមធ្វើតាមនៅលើកុំព្យូទ័ររបស់ពួកគេ។

- លើកទឹកចិត្តអ្នកចូលរួមអោយប្រើប្រាស់កន្លែងដែលផ្ទុកឯកសារថ្មីដែលមានសុវត្ថិភាពដើម្បីដាក់ឯកសារសំខាន់ៗហើយអោយពួកគេចងចាំឈ្មោះឯកសារដែលគេដាក់នោះ។កន្លែងសុវត្ថិភាពនេះអាចធ្វើការបម្រុងទុកឯកសារដូចជាឯកសារនានានៅលើកុំព្យូទ័រផងដែរហើយលម្អិតពីរបៀបចូលទៅកាន់វា អាចរក្សារទុកនៅក្នុងកម្មវិធី Password Manager។

- នៅចុងបញ្ចប់នៃមេរៀននេះ វាពិតជាមានសារៈសំខាន់មែនទែន ដោយចង្អុលបង្ហាញថា កន្លែងសុវត្ថិភាព ឬក៏ Veracrypt volume គួរតែ ‘unmounted’ នៅពេលដែលមិនប្រើវា ឬមុនពេលប្រើ USB/External hard drive ដែលមិនគួរទុកចិត្ត។

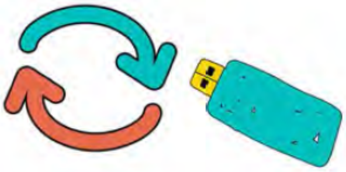
- ជួនកាលយើងអាចបង្វែរការចាប់អារម្មណ៍ដោយធ្វើការផ្លាស់ប្តូរឈ្មោះរបស់វាជាឯកសារត្រង់ៗទៅជាអ្វីផ្សេងទៀត ដូចជា .mp3 ជាដើម។ ធ្វើដូចនេះអ្នកនៅតែអាចប្រើវាបានធម្មតា មិនប៉ះពាល់ដល់ឯកសារនោះទេ។

៦

ការបម្រុងទុកទិន្នន័យ

Backups

ការបម្រុងទុកទិន្នន័យ



នៅពេលដែលនិយាយពីសុវត្ថិភាពលើប្រព័ន្ធឌីជីថល ការបម្រុងទុកទិន្នន័យ (Backup) គឺជាផ្នែកមួយសំខាន់បំផុតដែលគ្រប់គ្នាគួរតែយកចិត្តទុកដាក់។ប៉ុន្តែជាអកុសលប្រធានបទនេះត្រូវមនុស្សជាច្រើនមើលរំលង និងមិនត្រូវបានយកមកពិភាក្សាច្រើននោះទេ។

ការបម្រុងទុកទិន្នន័យ (Backup) សំដៅលើ ការថតចម្លងឯកសារដែលសំខាន់ពីច្បាប់ដើម យកទៅរក្សាទុកនៅកន្លែងផ្សេងទៀត ឬក្នុងឧបករណ៍ណាមួយដទៃទៀតដូចជានៅក្នុង USB Drive External Hard Drive និងនៅលើអ៊ីនធឺណិត (Cloud) ។ល។ ការធ្វើការបម្រុងទុកនេះ គឺដើម្បីការពារពីការបាត់បង់ឯកសារទាំងនោះដោយប្រការណាមួយ។ឧបករណ៍ខូច ឆ្លងមេរោគ បាត់ ចោរលួច ឬមានបញ្ហាណាមួយកើតឡើងដោយយថាហេតុជាដើម។

ផែនការបង្រៀន

វិធីសាស្រ្តក្នុងការបង្រៀន	ភាគច្រើនផ្តោតលើការពិភាក្សា
សំភារៈប្រើប្រាស់ក្នុងការបង្រៀន	ផ្ទាំងក្រដាសធំ ហ្វឺត ឧបករណ៍ផ្ទុកទិន្នន័យ (USB / External drive) Projector
រយៈពេលបង្រៀន	៦០ នាទី
ឧទាហរណ៍ប្រៀបធៀប	**ការបម្រុងទុកឯកសារ៖** ប្រៀបធៀបដូចជាការចម្លងកូនសោរផ្ទះអ្នកអ៊ីចឹងដែរ ប្រសិនបើអ្នកបាត់កូនសោរដើម អ្នកអាចប្រើកូនសោរដែលអ្នកបានចម្លងទុកនោះដើម្បីចូលទៅក្នុងផ្ទះបាន។
ប្រភពឯកសារពាក់ព័ន្ធ (ជាភាសាអង់គ្លេស)	https://level-up.cc/curriculum/protecting-data/data-backup-basics

នីតិវិធីក្នុងការបង្រៀន

- គ្រូបណ្តុះបណ្តាលអាចចាប់ផ្តើមដោយសួរអ្នកចូលរួមថាតើការបម្រុងទុកឯកសារឬBackupមានន័យដូចម្តេចសម្រាប់ពួកគេ? ស្តាប់ចម្លើយរបស់ពួកគាត់ និងព្យាយាមកត់ចំណាំចំណុចសំខាន់ៗដែលគាត់បានឆ្លើយ។ អ្នកអាចនឹងទទួលបានចំនុចសំខាន់ពីពួកគាត់ដែលត្រឹមត្រូវ និងបន្ថែមពីចំនុចដែលអ្នកមាន។

- គ្រូបណ្តុះបណ្តាល គួរធ្វើការពិភាក្សាពីជំហានសំខាន់ៗ ដែលអ្នកចូលរួមគួរធ្វើ មុននឹងធ្វើការបម្រុងទុក (Backup) ទិន្នន័យ។ ជំហានដំបូងដែលសំខាន់នោះគឺ ការកំណត់អោយដឹងពីទិន្នន័យដែលសំខាន់ជាមុនសិន។បន្ទាប់ពីដឹងថាទិន្នន័យណាជាទិន្នន័យសំខាន់និងត្រូវតែធ្វើការបម្រុងទុក (Backup)ហើយជំហានបន្ទាប់អាចជាការកំណត់ពីឧបករណ៍ឬទីកន្លែងដែលត្រូវទុកឯកសារបម្រុងទាំងនោះ។ ឧបករណ៍ និងទីកន្លែងទាំងនោះអាចជា USB ឬ External Hard Drive និងនៅលើអ៊ីនធឺណិត ដូចជានៅលើ Dropbox និង Google Drive ជាដើម។ ជំហានទាំងនេះសំខាន់ណាស់ ព្រោះបើយើងមិនបានបញ្ជាក់ឱ្យច្បាស់ពីឯកសារដែលសំខាន់នោះទេ អ្នកចូលរួមអាចនឹងយកឯកសាររបស់ពួកទាំងអស់ យកទៅបម្រុងទុកដែលឯកសារខ្លះមិនសូវសំខាន់ និងមានទំហំផ្ទុកធំថែមទៀតផង។ឧទាហរណ៍ដូចជាឯកសារប្រភេទវីឌីអូឬរូបភាពជាដើមដែលធ្វើឱ្យមានការលំបាកក្នុងការរកឧបករណ៍ផ្ទុកឱ្យបានគ្រប់គ្រាន់។ការកំណត់ពីទីកន្លែងក៏មានសារៈសំខាន់ដូចគ្នាត្បិតបើអ្នកចូលរួមដាក់ឯកសារបម្រុងទុកនៅកន្លែងមិនច្បាស់លាស់អាចធ្វើឱ្យមានការលំបាកក្នុងការយកមកប្រើវិញពេលត្រូវការ ឬអាចបាត់ឯកសារនោះផងក៏ថាបាន។
- សួរសំណួរបន្តគឺ តើសព្វថ្ងៃពួកគាត់បានធ្វើការបម្រុងទុក (Backup) ឯកសារដែរឬទេ? តើពួកគាត់បម្រុងទុកទិន្នន័យទាំងនោះយ៉ាងដូចម្តេច?ធ្វើដូចម្តេចដើម្បីឱ្យទិន្នន័យរបស់ពួកគាត់មានសុវត្ថិភាព? តើទិន្នន័យប្រភេទអ្វីខ្លះដែលពួកគាត់បានបម្រុងទុក (Backup)? ហេតុអ្វីបានជាពួកគាត់បម្រុងទុក(Backup) ទិន្នន័យទាំងនោះ? បន្ទាប់ពីពិភាក្សាចប់ គ្រូបណ្តុះបណ្តាលអាចឱ្យពួកគាត់ធ្វើបទបង្ហាញ និងធ្វើការសង្ខេប និងកែតម្រូវនូចចំនុចខ្វះខាត ដែលពួកគាត់បានពិភាក្សា។
- រំលឹកអ្នកចូលរួមឱ្យពួកគាត់យល់ឱ្យច្បាស់ពីការបម្រុងទុកឯកសារ ពីសារៈសំខាន់របស់វា និងណែនាំកុំឱ្យពួកគាត់ធ្វើការបម្រុងទុក(Backup)ឯកសារឬទិន្នន័យសំខាន់របស់ពួកគាត់តែនៅក្នុងឧបករណ៍ដែលគាត់កំពុងប្រើប្រាស់។ ប្រាប់ពួកគាត់ឱ្យចេះធ្វើការបម្រុងទុកឯកសារឱ្យបានញឹកញ៉ាប់ ប្រាប់ពួកគាត់ឱ្យទុកក្នុងឧបករណ៍ និងទីកន្លែងលើសពីមួយ ដូចជានៅក្នុង External Hard Drive ផង និងនៅលើអ៊ីនធឺណិតផងជាដើម។ ពិភាក្សាពីចំណុចវិជ្ជមាន និងអវិជ្ជមាន ពីរបៀបផ្សេងគ្នានៃការបម្រុងទុកឯកសារ។ ត្រូវចងចាំថា គ្មានវិធីសាស្រ្តបម្រុងទុកឯកសារមួយណាដែលល្អឥតខ្ចោះនោះទេ វិធីសាស្រ្តខ្លះអាចល្អសម្រាប់មនុស្សមួយចំនួន តែអាចមិនល្អសម្រាប់អ្នកផ្សេងទៀត។ វាអាស្រ័យទៅលើស្ថានភាពជាក់ស្តែង និងប្រភេទការងារ។ ខាងក្រោមនេះជាចំណុចដែលអាចមានប្រយោជន៍សម្រាប់បង្ហាញទៅអ្នកចូលរួមៈ

កន្លែងបម្រុងទុកទិន្នន័យ	ចំណុចវិជ្ជមាន	ចំណុចអវិជ្ជមាន
USB Flash Drive	• ងាយស្រួលក្នុងការយកតាម	• ងាយនឹងបាត់បង់ ទំហំផ្ទុកមានកំណត់ (ទំហំផ្ទុកតូច)
នៅលើអ៊ីនធឺណិត (Clould)	• ប្រើបានគ្រប់ពេលវេលា គ្រប់ទីកន្លែង គ្រប់ឧបករណ៍ ឱ្យតែមានអ៊ីនធឺណិត	• ចាំបាច់ត្រូវមានអ៊ីនធឺណិត • ទំហំផ្ទុកមានកំណត់ (បើចង់បានទំហំបន្ថែម ត្រូវតែចំណាយលុយទិញ) • ក្រុមហ៊ុនដែលរក្សាទុកទិន្នន័យភាគច្រើន មិនបានធានាទាំងស្រុងនូវសុវត្ថិភាពទិន្នន័យរបស់អ្នកនោះទេ។ វាមានការពិបាកក្នុងការទុកចិត្តថា តើទិន្នន័យសំខាន់របស់អ្នកត្រូវបានយកចិត្តទុកដាក់ថែរក្សាដោយក្រុមហ៊ុនកម្រិតណា។
CDs / DVDs	• មានតម្លៃថោក និងងាយស្រួលក្នុងការរកទិញ	• ងាយនឹងឆ្កូត និងមិនអាចទុកបានយូរ • ទំហំផ្ទុកមានកំណត់ • កុំព្យូទ័រជំនាន់ក្រោយៗ ភាគច្រើនមិនមានភ្ជាប់មកជាមួយនូវកន្លែងចាក់ CD និង DVD ទៀតទេ
External Hard Drive	• ជាឧបករណ៍ដែលត្រូវបានគេណែនាំឱ្យប្រើ • ងាយស្រួលក្នុងការទិញយកមកប្រើ	• ងាយស្រួលក្នុងការឆ្លងមេរោគនិងជួនកាលខូចមិនដំណើរការតែម្តង។ ប្រសិនបើអ្នកប្រើវាគួរតែប្រើសម្រាប់តែធ្វើការ Backup ឯកសារបានហើយ កុំចែករំលែកឱ្យអ្នកផ្សេងប្រើ ឬកុំប្រើវាដើម្បីផ្ទេរឯកសារពីកុំព្យូទ័រមួយ ទៅកុំព្យូទ័រមួយផ្សេងទៀត។

របៀបក្នុងការបម្រុងទុកឯកសារ

មានវិធីសាស្ត្រច្រើនក្នុងការបម្រុងទុកឯកសារ ឬទិន្នន័យ ដែលអ្នកខ្លះប្រើកម្មវិធីជំនួយ អ្នកខ្លះប្រើកម្មវិធីដែលមានស្រាប់នៅលើប្រព័ន្ធប្រតិបត្តិការ Windows ហើយអ្នកខ្លះទៀតគ្រាន់តែថតចម្លង (copy) ឯកសារដែលចង់បម្រុងទុក (Backup) និងយកទៅដាក់ (Pass) ទៅក្នុងឧបករណ៍ផ្សេង ឬកន្លែងផ្សេងដែលពួកគេគិតថាមានសុវត្ថិភាព។ គ្រូបណ្ដុះបណ្ដាលអាចណែនាំឱ្យអ្នកចូលរួមប្រើវិធីសាស្ត្រណាក៏បាន សំខាន់ត្រូវប្រាកដថាវិធីសាស្ត្រនោះ មានភាពងាយស្រួលសម្រាប់អ្នកចូលរួម ដែលពួកគេអាចធ្វើបានដោយខ្លួនឯង។

ប្រសិនបើមានកម្មវិធីដែលគ្រូបណ្ដុះបណ្ដាលយល់ថាមានសុវត្ថិភាព និងងាយស្រួលក្នុងការប្រើប្រាស់ គ្រូបណ្ដុះបណ្ដាលក៏គួរតែណែនាំ និងធ្វើការបង្ហាញពីកម្មវិធីនោះដែរ។ សម្រាប់អ្នកប្រើ Windows ពួកគេអាចធ្វើការ Backup ជាមួយកម្មវិធីដែលមានស្រាប់នៅលើ Windows។ គ្រូបណ្ដុះបណ្ដាលក៏អាចធ្វើការបង្ហាញអ្នកចូលរួមពីរបៀបក្នុងការបម្រុងទុកឯកសារដល់តាមរយៈកម្មវិធីដែលមានស្រាប់នៅលើ Windows នេះដែរ ប្រសិនបើគិតថាពួកគេអាចយកទៅប្រើប្រាស់បាន។

ចំណុចសំខាន់ៗដែលត្រូវបញ្ជាក់

- ការបម្រុងទុកទិន្នន័យដែលល្អបំផុត គឺវាអាស្រ័យទៅលើការកំណត់នូវឯកសារដែលសំខាន់ និងពីឧបករណ៍ ឬទីកន្លែងដែលពួកគេចង់បម្រុងទុកឯកសារសំខាន់ទាំងនោះ។
- គ្មានឧបករណ៍ឬកន្លែងណាដែលមានសុវត្ថិភាព១០០%នោះទេ ប្រសិនបើអ្នកចូលរួមគាត់មិនបានបារម្ភពីការរំលោភសិទ្ធិឯកជនភាព គាត់អាចរក្សាទុកឯកសាររបស់ពួកគាត់នៅលើអ៊ីនធឺណិត (Cloud)។ ប៉ុន្តែប្រសិនប្រសិនពួកគាត់បារម្ភខ្លាំងពីការរំលោភឯកជនភាព គាត់អាចស្វែងរកឧបករណ៍ដូចជា USB ឬ External Hard Drive ដើម្បីរក្សាទុកឯកសារទាំងនោះ។
- ការបម្រុងទុកឯកសារ (Backup) ឱ្យបានទៀងទាត់ជារឿងដែលគ្រប់គ្នាចាំបាច់ត្រូវតែធ្វើ។ វាមិនមានវិធីសាស្ត្រក្នុងការ Backup ណាដែលល្អជាងគេនោះទេ អ្នកអាច Backup តាមរបៀបណាក៏បានដែលគិតថាងាយស្រួល និងអាចធ្វើបានជាប្រចាំ។
- ត្រូវប្រាកដថាឯកសារដែលបានបម្រុងទុកនោះមានសុវត្ថិភាពនិងអាចយកមកប្រើវិញបាននៅពេលដែលត្រូវការ។ ឧស្សាហ៍ចូលទៅពិនិត្យនិងសាកល្បងបើកប្រើឡើងវិញចៀសវាងឯកសារដែលបានបម្រុងទុកនោះខូច ឬត្រូវបានមេរោគបំផ្លាញ។
- សូមធ្វើការបម្រុងទុកឯកសារឱ្យបានច្រើនកន្លែង និងច្រើនឧបករណ៍ (លើសពីមួយកន្លែង ឬក្នុងឧបករណ៍តែមួយ)។ ការទុកឯកសារក្នុងឧបករណ៍នៅកន្លែងតែមួយ មានហានិភ័យច្រើនណាស់ ប្រសិនបើមានរឿងចៃដន្យណាមួយកើតឡើង ឧបករណ៍នោះខូច បាត់ ឆ្លងមេរោគ នោះឯកសារសំខាន់ទាំងនោះក៏ត្រូវបាត់បង់ដូចគ្នា។
- បើសិនជាអាច គួរចាក់សោរ ឬធ្វើកូដនីយកម្ម (Encrypt) ឯកសារដែលបានបម្រុងទុកនោះ។ ការចាក់សោរ ឬធ្វើកូដនីយកម្ម (Encrypt) ជួយការពារអ្នកផ្សេងក្នុងការចូលទៅប្រើ ឬកែប្រែឯកសារទាំងនោះដោយគ្មានការអនុញ្ញាតពីម្ចាស់ដើម។ ប្រសិនបើឯកសារអ្នកបានធ្វើកូដនីយកម្មទោះបីជាអ្នកដទៃទទួលបានឯកសារនោះ ក៏មិនអាចប្រើប្រាស់ឯកសារនោះបានដែរ។

៧

សុវត្ថិភាពលើប្រព័ន្ធអ៊ីនធឺណិត

Online Safety

សុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត

ផែនការបង្រៀន

វិធីសាស្រ្តក្នុងការបង្រៀន	ការពិភាក្សា និងបទបង្ហាញ
សំភារៈប្រើប្រាស់ក្នុងការបង្រៀន	Projector ផ្ទាំងប្រដាសធំៗ និងប៊ិក
រយៈពេលបង្រៀន	៩០នាទី
ឧទាហរណ៍ប្រៀបធៀប	TOR: ឧទាហរណ៍ អ្នកចង់ធ្វើដំណើរពីផ្សារថ្មីទៅផ្សារអូឡាំពិច។ប៉ុន្តែអ្នករត់ម៉ូតូកង់បីបាននាំអ្នកពីផ្សារថ្មី រួចហើយកាត់តាមផ្សារអូរឫស្សី រួចបានទៅដល់ផ្សារអូរឡាំពិចដែលត្រូវចំណាយពេលយូរជាងធម្មតា។ ដូចនេះ TOR ហាក់ដូចជាអ្នករត់ម៉ូតូកង់បីអញ្ចឹងដែរ ព្រោះថា TOR ឆ្លងកាត់បណ្តាញជាច្រើនមុននាំទៅកាន់គេហទំព័រដែលអ្នកចង់ទស្សនា។ VPN: វាហាក់ដូចជាអ្នកពាក់ម៉ាស់ និងមួកការពារអញ្ចឹង។ ព្រោះថាវាធ្វើឲ្យបុគ្គលដទៃទៀតមិនអាចកំនត់អត្តសញ្ញាណអ្នកណាបានឡើយ។
ប្រភពឯកសារពាក់ព័ន្ធ (ជាភាសាអង់គ្លេស)	https://level-up.cc/curriculum/safer-browsing

សុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត

- គ្រប់គណនីទាំងអស់អ្នកត្រូវត្រួតពិនិត្យទៅលើ ការកំណត់ឯកជនភាព និងសុវត្ថិភាព(privacy and security setting)។ នៅពេលអ្នកបង្ហោះអ្វីមួយនៅលើអ៊ីនធឺណិត អ្នកអាចនឹងជួបហានិភ័យពាក់ព័ន្ធជាមួយព័ត៌មានដែលអ្នកចែករំលែកទៅកាន់ជនដែលមិនមានបំណងល្អលើរូបអ្នក។អ្នកគួរពិចារណាឡើងវិញ នៅពេលអ្នកចង់បង្ហោះ ឬចែករំលែកអ្វីមួយនៅលើអ៊ីនធឺណិត និងត្រួតពិនិត្យឡើងវិញ នូវការកំណត់ឯកជនភាព និងសុវត្ថិភាព(privacy and security setting)។ Google ឬ Facebook មានសេវាកម្ម “privacy check-up” ដើម្បីជួយលើឯកជនភាពរបស់អ្នកផងដែរ។

- អ្នកគួរពន្យល់ឲ្យបានក្បោះក្បាយ នៅពេលអ្នកបង្រៀនអ្នកដទៃទៀតអំពីសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត។ឧទាហរណ៍ប្រសិនបើអ្នកចង់បង្រៀនអំពីសុវត្ថិភាពលើហ្វេសបុក(Facebook)អ្នកគួរពន្យល់ណែនាំពីចំនុចមួយៗដែលមាននៅលើការកំណត់ឯកជនភាព និងសុវត្ថិភាព (privacy and security setting) ឲ្យបានលម្អិត និងអនុវត្តផ្ទាល់ជាមួយពួកគេ។
- អ្នកគួរតែរំលឹកអ្នកចូលរួមថា វាពិតជាចាំបាច់ណាស់ក្នុងការត្រួតពិនិត្យព័ត៏មានដែលអ្នកមាននៅលើអ៊ីនធឺណិត។ពួកគេគួរតែដឹងថានៅពេលពួកគេមានព័ត៏មានច្រើនលើសលប់នៅលើអ៊ីនធឺណិត ព័ត៏មានទាំងនោះអាចត្រូវបានប្រមូលពីជនទី៣ទាំងពួកគេមិនដឹងខ្លួន។

Incognito Web Browsing មិនបានជួយលាក់អត្តសញ្ញាណរបស់អ្នកបានទេ។វាគ្រាន់តែជួយលុបការរុករក និងប្រវត្តិក្នុងការរុករករបស់អ្នកនៅលើអ៊ីនធឺណិតតែប៉ុណ្ណោះ (browsing activity and history) ។

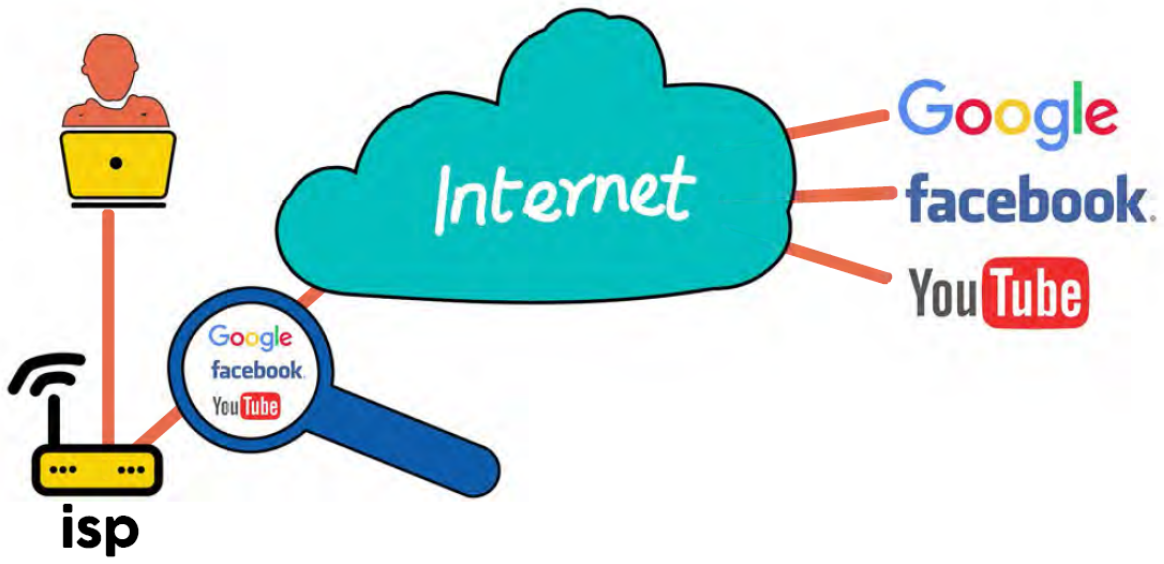
HTTP Vs HTTPS

- ពាក្យពេញរបស់ HTTP គឺ hyper-text transfer protocol។ នៅពេលអ្នកមើល គេហទំព័រដែលប្រើប្រាស់HTTPគឺជួនកាលវាមានផលប៉ះពាល់ដល់សុវត្ថិភាពនិងឯកជនភាព។ប៉ុន្តែអ្នកត្រូវចងចាំថាព័ត៏មានដែលអ្នកផ្តល់ឲ្យគេហទំព័រដែលប្រើប្រាស់ HTTP អាចត្រូវបានមើលឃើញពីជនទី៣។
- នៅពេលដែលអ្នកចូលមើលគេហទំព័រដែលប្រើប្រាស់ HTTP វាហាក់ដូចជាសំបុត្រដែលមិនបានដាក់ស្រោមសំបុត្រ ឲ្យបានត្រឹមត្រូវអញ្ចឹងដែរ។ ផ្ទុយពីគេហទំព័រដែលមាន HTTPS វាហាក់ដូចជាសំបុត្រដែលមានដាក់ស្រោមសំបុត្រត្រឹមត្រូវដើម្បីកុំឲ្យអ្នកដទៃដឹងពីអ្វីដែលអ្នកបានសរសេរក្នុងសំបុត្រនោះ។
- គេហទំព័រដែលគួរមាន HTTPS ត្រឹមត្រូវ គឺគេហទំព័រដែលពាក់ព័ន្ធជាមួយការទូរទាត់ប្រាក់តាមធនាគារ នៅលើអ៊ីនធឺណិត ឬគេហទំព័រដែលទាមទារនូវអត្តសញ្ញាណរបស់អ្នក ឬព័ត៏មានមានពីកាតធនាគាររបស់អ្នក។
- ពាក្យពេញរបស់ HTTPS គឺ hyper-text transfer protocol secure។ HTTPS គឺជាដំណោះស្រាយសំរាប់ឲ្យការប្រាស្រ័យទាក់ទង ឬផ្លាស់ប្តូរព័ត៏មាននៅលើ គេហទំព័រមានសុវត្ថិភាព។
- ជួនកាលគេហទំព័រដែលមានHTTPSប៉ុន្តែវាមិនបានបង្ហាញឲ្យយើងឃើញHTTPSដោយស្វ័យប្រវត្តិនោះទេ។ដូចនេះអ្នកគួរតែភ្ជាប់កម្មវិធីមួយនៅលើកម្មវិធីរុករករបស់អ្នក(browserextension)ដោយកម្មវិធីនោះមានឈ្មោះថា HTTPS Everywhere ដើម្បីជួយក្នុងការបង្ហាញគេហទំព័រដែលមាន HTTPS។

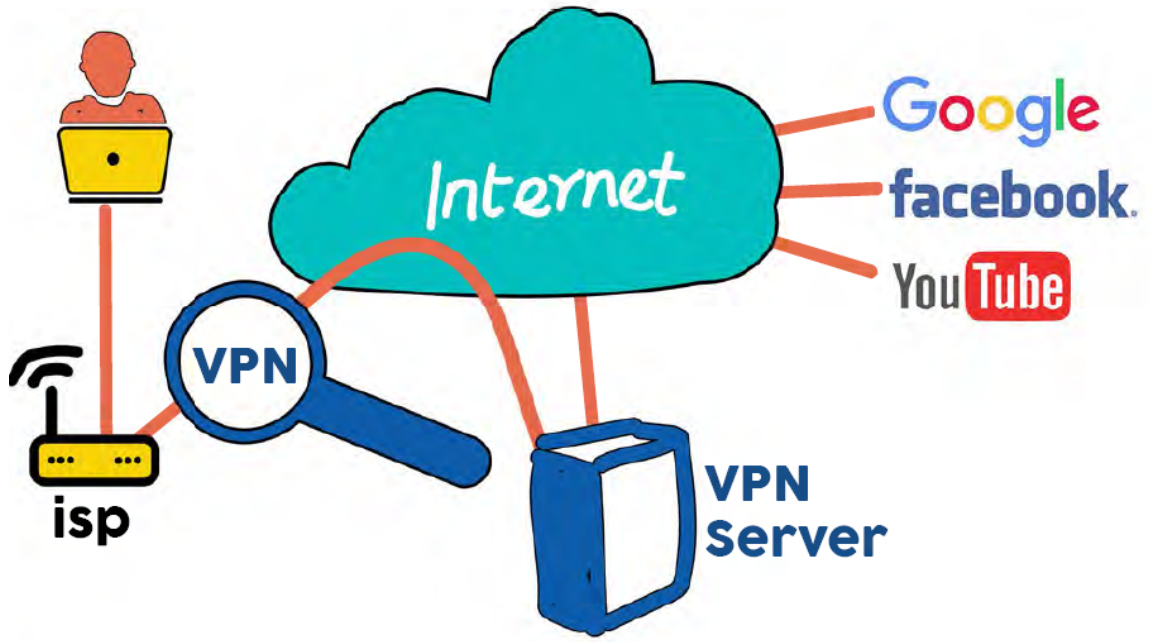
ការប្រើប្រាស់ VPNs (Virtual Private Networks)

- VPN បង្កើតឡើងក្នុងការការពារឯកជនភាពរបស់ អ្នកប្រើប្រាស់ដោយអ៊ីនគ្រីប នូវទិន្នន័យរបស់អ្នក (encrypting data) ផ្លាស់ប្តូរនូវទីកន្លែង និងការបង្ការការត្រួតពិនិត្យនៅលើអ៊ីនធឺណិតរបស់អ្នក (preventing censorship) ។
- អ្នកគួរតែបង្ហាញនូវរូបភាពខាងក្រោមនេះដើម្បីជាសេចក្តីផ្តើមរបស់ VPN។

ការភ្ជាប់អ៊ីនធឺណិតដោយគ្មានVPN



ការភ្ជាប់អ៊ីនធឺណិតដោយមានVPN



រូបភាពខាងលើបង្ហាញពីរបៀបដែលក្រុមហ៊ុនតាមដានពីគេហទំព័រដែលអ្នកចូលទស្សនា។

- ដើម្បីឲ្យកាន់តែលម្អិតជាងនេះទៅទៀតអ្នកគួរតែបង្ហាញមេរៀននេះដោយចូលទៅកាន់គេហទំព័រ iplocation.net ដើម្បីបង្ហាញពី IP Address (ទីតាំង) មុនពេលអ្នកភ្ជាប់ជាមួយ VPN។ បន្ទាប់មកភ្ជាប់ជាមួយ VPN ដើម្បីបង្ហាញពីទីតាំងរបស់អ្នក។ រួចប្រៀបធៀបពីភាពខុសគ្នារវាងមុនពេល និងក្រោយពេលភ្ជាប់ VPN។

- បង្ហាញអ្នកចូលរួមនូវ VPN មួយចំនួនដែលពួកគេអាចប្រើប្រាស់បានដោយឥតគិតថ្លៃ និងគិតថ្លៃ។ អ្នកគួរបង្ហាញពួកគេពីគុណវិបត្តិមួយចំនួនដែលមាននៅលើ VPN ដែលឥតគិតថ្លៃ ដូចជា ការរំខានដោយការផ្សាយពាណិជ្ជកម្ម និងការធ្វើល្បឿនអ៊ីនធឺណិតដើរយឺតផងដែរ។

ការប្រើប្រាស់ TOR ក្នុងការរុករកលើអ៊ីនធឺណិត

- បង្ហាញអ្នកចូលរួមពីការរុករកនៅលើអ៊ីនធឺណិតតាមរយៈTORដោយផ្តោតសំខាន់លើភាពខុសគ្នារវាងTOR,ChromeនិងFirefox។សំខាន់បំផុតអ្នកត្រូវផ្តោតលើចំនុចពិសេសរបស់TORគឺវាជួយការពារសុវត្ថិភាព និងឯកជនភាពរបស់អ្នកប្រើប្រាស់ដូចជា ការមិនរក្សាប្រវត្តិក្នុងការរុករកនៅលើអ៊ីនធឺណិត និងការផ្តាច់ Cookies ដោយស្វ័យប្រវត្តិ។

- អ្នកអាចធ្វើការតេស្តសាកល្បងតាមរយៈគេហទំព័រ iplocation.net ដើម្បីឃើញពីការផ្លាស់ប្តូរទីតាំងនៅពេលអ្នកប្រើប្រាស់កម្មវិធី TOR។

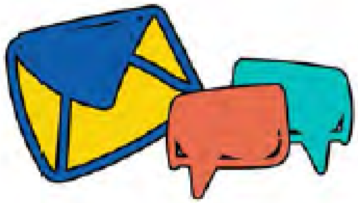
- កម្មវិធីTORគឺជាកម្មវិធីរុករកនៅលើអ៊ីនធឺណិតដែលមានសុវត្ថិភាពដែលជួយបំលែងទីតាំងរបស់អ្នក និងសកម្មភាពក្នុងការស្វែងរកព័ត៏មានរបស់អ្នកនៅលើអ៊ីនធឺណិត។ កម្មវិធី TOR ជាឧបសគ្គសម្រាប់បុគ្គលទី៣ ក្នុងការតាមដានអ្នកនៅលើអ៊ីនធឺណិត។

៨

សុវត្ថិភាពក្នុងការទាក់ទង នៅលើអ៊ីនធឺណិត និងសុវត្ថិភាព នៅលើអ៊ីមែល

Secure Communication and Email Hygien

សុវត្ថិភាពក្នុងការទាក់ទងនៅលើអ៊ីនធឺណិត និងសុវត្ថិភាពនៅលើអ៊ីមែល



អ្វីដែលអ្នកត្រូវចេះមុនពេលចាប់ផ្តើមមេរៀននេះ

ប្រធានបទនេះត្រូវការឲ្យអ្នកមានចំនេះដឹង និងបទពិសោធន៍មួចចំនួន ដូចជា ការតម្លើងការចាក់សោរពីរជាន់ (two-factor-authentication) និងរបៀបក្នុងការប្រើប្រាស់អ៊ីមែល អ៊ីនគ្រីបសិន Tutanota។

មេរៀនពាក់ព័ន្ធជាមួយ Tutanota: https://tutanota.com

មេរៀនពាក់ព័ន្ធជាមួយ ការចាក់សោរពីរជាន់ (Two-Factor-Authentication): https://sec.eff.org/topics/two-factor-authentica-tion.KNOW

អ៊ីមែល គឺប្រព័ន្ធទំនាក់ទំនងនៅលើអ៊ីនធឺណិតដ៏សំខាន់សម្រាប់បុគ្គលម្នាក់ៗ។ ការប្រើប្រាស់អ៊ីមែលដែលមានសុវត្ថិភាពគឺមានសារៈសំខាន់ណាស់ក្នុងការជៀសវាងនូវហានិភ័យនានាដែលអាចប៉ះពាល់ដល់សុវត្ថិភាព និងឯកជនភាពរបស់អ្នក។ នៅក្នុងមេរៀននេះ អ្នកនឹងយល់អំពីផ្នែកសំខាន់ៗរបស់អ៊ីមែល ដែលអាចជួយអ្នកក្នុងការការពារពីហានិភ័យទាំងនោះបាន។

ផែនការបង្រៀន

វិធីសាស្ត្រក្នុងការបង្រៀន	ការពិភាក្សា និងបទបង្ហាញ
សំភារៈប្រើប្រាស់ក្នុងការបង្រៀន	ផ្ទាំងប្រដាសធំៗ និងតូចៗ ប៊ិក
រយៈពេលបង្រៀន	៦០នាទី
ឧទាហរណ៍ប្រៀបធៀប	Two-Factor-Authentication គឺ ដូចជាសោរផ្ទះ អញ្ចឹងព្រោះបើនរណាម្នាក់ផ្លោះរបងផ្ទះអ្នកបានប៉ុន្តែគេត្រូវការសោរផ្ទះអ្នកមួយទៀតដើម្បីអាចចូលទៅក្នុងផ្ទះអ្នកបាន ។
ប្រភពឯកសារពាក់ព័ន្ធ (ជាភាសាអង់គ្លេស)	https://www.prxbx.com/email/

នីតិវិធីក្នុងការបង្រៀន

- អ្នកគួរចាប់ផ្ដើម ដោយសួរសំនួរមួយចំនួន ទៅកាន់អ្នកចូលរួម ដូចជាប្រភេទអ៊ីមែល ដែលពួកគេកំពុងប្រើប្រាស់សព្វថ្ងៃហើយបន្ទាប់មកកត់ចម្លើយនោះនៅលើក្ដារខៀន។បន្ទាប់មកសួរពួកគេមួយសំនួរទៀតថា មូលហេតុអ្វីបានជាពួកគេប្រើប្រាស់ប្រភេទអ៊ីមែលមួយនេះ។ អ្នកនឹងឃើញថាភាគច្រើនអ្នកចូលរួមប្រើប្រាស់ប្រភេទអ៊ីមែល ដូចជា Gmail, Yahoo និង Hotmail។

- បង្ហាញពីការ ការជ្រើសរើសប្រភេទអ៊ីមែល ដោយធ្វើការវិភាគឲ្យបានត្រឹមត្រូវទៅលើលទ្ធភាពដែលអ្នកអាចគ្រប់គ្រងលើឯកជនភាព និងសុវត្ថិភាព។ អ្វីដែលសំខាន់ជាងនេះទៅទៀត ការពង្រឹងសុវត្ថិភាព និងឯកជនភាពនៅលើអ៊ីមែល អាចត្រូវពិនិត្យលើបញ្ហាមួយចំនួន ដូចជា៖
  - មនុស្សគ្រប់គ្នាមិនបានចំណាយលុយក្នុងការប្រើប្រាស់អ៊ីមែលឡើយ។ តើអ្នកឆ្ងល់ដែរឬទេថា តើក្រុមហ៊ុនទាំងអស់នោះ អាចដំណើរការបានយ៉ាងដូចម្ដេច ប្រសិនបើការផ្ដល់សេវាកម្មទាំងនេះសុទ្ធតែមិនគិតថ្លៃ?អ្នកត្រូវដឹងថានៅពេលដែលអ្នកចុះឈ្មោះប្រើប្រាស់សេវាកម្មទាំងនោះអ្នកបានក្លាយជាផលិតផលសម្រាប់ពួកគេក្នុងការបង្កើតចំនូលរួចទៅហើយ។ ក្រុមហ៊ុនទាំងនោះរកកម្រៃតាមរយៈការលក់ទិន្នន័យរបស់អ្នកទៅកាន់ក្រុមហ៊ុនផ្សេងទៀតនិងការផ្សព្វផ្សាយផលិតផលតាមរយៈចំនង់ចំនូលចិត្តរបស់អ្នក ដោយផ្អែកលើទិន្នន័យ ដែលអ្នកបានផ្ដល់ឲ្យពួកគេ។
  - ប៉ុន្តែមិនមែនរាល់ក្រុមហ៊ុនអ៊ីមែលទាំងអស់សុទ្ធតែធ្វើដំណើរការតាមទម្រង់ខាងលើនេះទេ។ ក្រុមហ៊ុន Riseup រកប្រាក់តាមរយៈការស្វែងរកជំនួយដើម្បីធ្វើប្រតិបត្តិការក្រុមហ៊ុនរបស់គេ។

ការបំពាក់ផ្នែកសុវត្ថិភាពនៅលើអ៊ីមែល

- ដើម្បីធ្វើឲ្យអ៊ីមែលរបស់អ្នកកាន់តែមានសុវត្ថិភាពបន្ថែមទៀតនោះអ្នកត្រូវបំពាក់នូវការចាក់សោរពីរជាន់ (two-factor authentication) ដើម្បីទទួលបាននូវលេខកូដសម្ងាត់តាមរយៈសារ (SMS) ឬ App ដែលមាននៅលើទូរស័ព្ទរបស់អ្នក (Authentication App) និង កូនសោរ USB។

កូដនីយកម្ម ឬការចាក់សោរ ឬការបំលែងកូដ(Encryption)

- ក្រុមហ៊ុនអ៊ីមែល ភាគច្រើនបានធ្វើប្រតិបត្តិការដោយបំលែងកូដ (encrypt) នូវដំណើរការរវាងអ្នកប្រើប្រាស់ និងក្រុមហ៊ុនផ្ទាល់។ ប៉ុន្តែក្រុមហ៊ុនទាំងនោះភាគច្រើនមិនបានធ្វើការប្រតិបត្តិការបំលែងកូដ (encrypt) នៅលើសារនោះទេ។ ការធ្វើប្រតិបត្តិការដោយបំលែងកូដ (encrypt) នៅលើសារគឺការពារនូវឯកជនភាពនិងសុវត្ថិភាពរបស់អ្នកបញ្ជូនសារនិងអ្នកទទួលសារបានន័យថាក្រៅពីអ្នកផ្ញើ និងអ្នកទទួល ជនទីពមិនអាចមើលយល់បានឡើយ។

បន្ទាប់ពីអ្នកបង្ហាញចំនុចទូទៅរបស់ការបំលែងកូដ (encryption) នេះហើយ អ្នកអាចចាប់ផ្ដើមធ្វើការតេស្តសាកល្បងពីដំណើរការរបស់ ការបំលែងកូដ (encryption) និងបង្ហាញពីចំណុចពិសេសរបស់ការបំលែងកូដ (encryption)។ ទោះបីជាមានជម្រើសជាច្រើនក្នុងការប្រើប្រាស់អ៊ីមែលដែលបំលែងកូដ (email encryption) ជាដំបូងអ្នកគួរបង្ហាញពីជម្រើសដែលងាយស្រួល ដែលមានដូចជា Tutanota។ Tutanota គឺជាកម្មវិធីបើកទូលាយ (open source) និងបំពាក់ប្រព័ន្ធបំលែងកូដដោយស្វ័យប្រវត្តិ (automatically end-to-end encrypted)។ ក្រៅពី Tutanota មានជម្រើសការបំលែងកូដអ៊ីមែល (email encryption)ជាច្រើនទៀតដែលក្នុងនោះមានដូចជា Mailvelope, ProtonMail និង Enigmail ។

៩

ការយល់ដឹង និងការការពារ ពីការវាយប្រហារដោយបញ្ឆោត នៅលើអ៊ីនធឺណិត

Phishing: Understanding and Preventing Attack

ការយល់ដឹង និងការការពារពីការវាយប្រហារដោយបញ្ឆោតនៅលើអ៊ីនធឺណិត

គោលដៅចំបងនៅក្នុងមេរៀននេះគឺដើម្បីបង្កើននូវការប្រុងប្រយ័ត្នរបស់អ្នកពីការឆបោកនៅលើអ៊ីនធឺណិតតាមរយៈ អ៊ីមែល ឬតំណរភ្ជាប់ផ្សេងៗទៀត។

ផែនការបង្រៀន

វិធីសាស្រ្តក្នុងការបង្រៀន	ការពិភាក្សា
សំភារៈប្រើប្រាស់ក្នុងការបង្រៀន	ផ្ទាំងប្រដាសធំៗ និងតូចៗ ប៊ិក និងឧបករណ៍បញ្ចាំង
រយៈពេលបង្រៀន	៦០នាទី
ឧទាហរណ៍ប្រៀបធៀប	Phishing (ការបញ្ឆោតនៅលើអ៊ីនធឺណិត) គឺប្រៀបធៀបដូចជាជនឆបោកម្នាក់មកនិយាយជាមួយអ្នកដោយរូបគេធ្វើដូចជាធ្លាប់ស្គាល់អ្នកពីមុនមក។ប៉ុន្តែអ្វីដែរគេចង់បានគឺទូរស័ព្ទរបស់អ្នកនោះទេ។ ជនឆបោកម្នាក់នោះអាចបញ្ចេញកាយវិការដែលអ្នកអាចសង្ស័យបានថា គាត់មិនមានជាមនុស្សល្អនោះទេ។ ប៉ុន្តែប្រសិនបើជាអ្នកធ្វេសប្រហែស គាត់អាចលួចទូរស័ព្ទពីអ្នកបាន។
ប្រភពឯកសារពាក់ព័ន្ធ (ជាភាសាអង់គ្លេស)	https://phishingquiz.withgoogle.com/

គន្លឹះសំខាន់ៗ

- Phishingគឺជាប្រភេទសារឥតបានការ(spam)ដែលអាចមានលទ្ធភាពអាចចូលទាញយកព័ត៌មានរបស់អ្នកបានប្រសិនបើអ្នកចុចឬទាញយកពីតំណភ្ជាប់ពីក្នុងសាររបស់អ៊ីមែលនោះ។ឧទាហរណ៍ Phishing អ៊ីមែល អាចបញ្ឆោតឲ្យអ្នកផ្តល់នូវព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នក ដូចជា លេខកូដសម្ងាត់ ឬព័ត៌មានCreditCardរបស់អ្នក។វិធីសាស្រ្តដែលគេបញ្ឆោតអ្នកគឺតាមរយៈការទាញយកឯកសារ ឬព័ត៌មានតាមរយៈតំណរភ្ជាប់មិនមានប្រភពច្បាស់លាស់ ឬការតំឡើងកម្មវិធីនានាដែលមានមេរោគភ្ជាប់មកជាមួយ។

- ទោះបីជា Phishing អាចកើតឡើងក្នុងរូបភាពផ្សេងគ្នាក៏ដោយ ប៉ុន្តែភាគច្រើនវាកើតឡើងនៅលើ អ៊ីមែល ពីព្រោះជនខិលខូចទាំងនោះដឹងថា នៅក្នុងអ៊ីមែល របស់អ្នកមានទិន្នន័យជាច្រើន ដូចជា អ៊ីមែល របស់អ្នកភ្ជាប់ជាមួយគណនីសង្គមរបស់អ្នក (social media) និង គណនីធនាគាររបស់ អ្នកជាដើម។ អ្វីដែលសំខាន់ជាងនេះទៅទៀត អ៊ីមែល របស់អ្នកអាចកំនត់ឡើងវិញ នូវលេខកូដ សម្ងាត់របស់អ្នកបាន។

  ដូចនេះវាមានន័យថា ប្រសិនបើនរណាម្នាក់មានលទ្ធភាព ចូលទៅកាន់អ៊ីមែល របស់អ្នក អ្នកនឹង ប្រឈមមុខនឹងហានិភ័យជាច្រើន។

- វាពិតជាមានសារៈសំខាន់ណាស់ ក្នុងការពន្យល់ដោយមាន ឧទាហរណ៍ភ្ជាប់មកជាមួយដើម្បីទាញ ការចាប់អារម្មណ៍ពីអ្នកចូលរួម។អ្នកអាចចូលទៅកាន់គេហទំព័រនេះដើម្បីធ្វើការតេស្តសាកល្បងពី Phishing (https://phishingq-uiz.withgoogle.com/)។

វិធីសាស្ត្រ ក្នុងការ Phishing

- ការផ្ញើរតំណភ្ជាប់តាមរយៈអ៊ីមែល (link) ពីប្រភព ឬបុគ្គលមិនមានប្រភពច្បាស់លាស់ ដើម្បីស្នើរ សុំព័ត៏មានផ្ទាល់ខ្លួនរបស់អ្នក។
- ការទាញយកឯកសារ ឬព័ត៏មាន មាន (Attachment) ពីក្នុងអ៊ីមែល ។
- ការវាយអ៊ីមែល និងលេខកូដសម្ងាត់របស់អ្នក ទៅលើគេហទំព័រណាមួយដែលអ្នកមិនស្គាល់ ច្បាស់លាស់។

គន្លឹះក្នុងការការពារពី Phishing

- កុំវាយអ៊ីមែល ឬលេខកូដសម្ងាត់របស់អ្នកទៅកាន់គេហទំព័រដែលអ្នកមិនស្គាល់ច្បាស់លាស់។ ត្រួតពិនិត្យ URL របស់គេហទំព័ររបស់អ្នក។
- ត្រួតពិនិត្យ URL តាមរយៈគេហទំព័រ https://checkshorturl.com/ ដើម្បីពិនិត្យគោលដៅចុង ក្រោយរបស់តំណរភ្ជាប់នោះ។
- ត្រួតពិនិត្យតំណរភ្ជាប់ (link) ឲ្យបានច្បាស់លាស់មុននឹងចុច ឬទាញយកព័ត៏មានមានពីតំណរភ្ជាប់ នោះ។
- ទាក់ទងទៅកាន់អ្នកផ្ញើអ៊ីមែល មកអ្នក ដើម្បីឲ្យច្បាស់ថា បុគ្គលនោះពិតជាផ្ញើរអ្នកនូវឯកសារ ឬក៏ អ៊ីមែល ពិតប្រាកដមែន។
- ភ្ជាប់នូវការចាក់សោរពីរជាន់(two-factor authentication)ទៅលើអ៊ីមែល ឬគណនីផ្សេងៗ ទៀតរបស់អ្នក។

ការចាក់សោរពីរជាន់ (two-factor authentication)

- ការចាក់សោរពីរជាន់អាចធ្វើឲ្យគណនីរបស់អ្នកមានសុវត្ថិភាពជាងមុនតាមរយៈការបំពាក់នូវលេខកូដសម្ងាត់មួយជាន់ទៀត។នៅពេលដែលអ្នកចូលទៅកាន់គណនីរបស់អ្នកវានឹងត្រូវការលេខកូដសម្ងាត់មួយជាន់ទៀតដែលលេខកូដនោះមាន៦ខ្ទង់។អ្នកអាចទទួលបាននូវលេខកូដនោះតាមរយៈសារ ឬAppនៅលើទូរស័ព្ទរបស់អ្នក។ដូចនេះប្រសិនបើនរណាម្នាក់មានគណនី និងលេខកូដសម្ងាត់របស់អ្នក ពួកគេនៅត្រូវការលេខកូដសម្ងាត់ផ្សេងទៀតដើម្បីចូលទៅកាន់គណនីរបស់អ្នក។
- ធ្វើបច្ចុប្បន្នភាពនៅលើទូរស័ព្ទរបស់អ្នកជានិច្ច ពីព្រោះថា Phishing អាចបង្កប់មេរោគនៅក្នុងកម្មវិធីចាស់ ៗរបស់អ្នក។
-ជៀសវាងក្នុងការចែករំលែកព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នកច្រើនពេកនៅលើគណនីសង្គមរបស់អ្នក។
- ជៀសវាងក្នុងការប្រើប្រាស់អ៊ីមែល របស់អ្នកទៅចុះឈ្មោះ នៅលើសេវាកម្មអនឡាញផ្សេងៗ ព្រោះវាអាចធ្វើឲ្យអ្នកប្រឈមមុខ នឹងហានិភ័យដែលពាក់ព័ន្ធជាមួយឯកជនភាពរបស់អ្នក។

១០

ឯកសារសំខាន់ៗសំរាប់គ្រូបង្គោល

Useful Resources for Trainers

ធនធានសំខាន់ៗសំរាប់គ្រូបង្គោល

ការពង្រីកចំនេះដឹងរបស់គ្រូបង្គោលនៅលើប្រធានបទសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិតពិតជាមានសារៈសំខាន់ណាស់។ ការតាមដានព័ត៌មាន ការស្រាវជ្រាវ និងការតេស្តសាកល្បងនៅលើAppថ្មីៗគឺជាកាតព្វកិច្ចដ៏សំខាន់សម្រាប់គ្រូបង្គោលទាំងអស់។ធនធានទាំងអស់នេះអាចជួយអ្នកក្នុងការយល់ពីការផ្លាស់ប្តូរពីប្រព័ន្ធ បច្ចេកវិទ្យាដែលពាក់ព័ន្ធជាមួយ សុវត្ថិភាព និងឯកជនភាព។

ចំណងជើងអត្ថបទ	អ្នកផលិត	គោលបំណង
Digital Security Resources Index	@BeckLindsay and community owned	មូលដ្ឋានទិន្នន័យដែលផ្ទុកនូវធនធានសំខាន់ៗពាក់ព័ន្ធជាមួយសុវត្ថិភាពនៅប្រព័ន្ធអ៊ីនធឺណិត។មូលដ្ឋានទិន្នន័យនេះបានបោះពុម្ពផ្សាយជាច្រើនភាសា។
Guides and Training	Freedom of the Press Foundation	សេចក្តីណែនាំ និងឧបករណ៍សុវត្ថិភាពដែលមានសារៈសំខាន់សំរាប់អ្នកធ្វើការពាក់ព័ន្ធជាមួយវិស័យព័ត៌មាន។
Sideways dictionary	Jigsaw Washington Post	ន័យធៀបពាក់ព័ន្ធជាមួយសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត។
Level-up	Community owned, network maintained	ធនធានបើកទូលាយសំរាប់គ្រូ បណ្តុះបណ្តាលពាក់ព័ន្ធជាមួយ បច្ចេកវិទ្យា និងសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត។
Security in a Box	Tactical Technology Collective and Frontline Defenders	សេចក្តីណែនាំសំខាន់ៗសំរាប់គ្រូបង្គោល និងអ្នកប្រើប្រាស់ទូទៅ។សេចក្តីណែនាំនេះនិយាយពី កម្មវិធី (software) សម្រាប់ការពារសុវត្ថិភាពនៅលើទូរស័ព្ទ និងកុំព្យូទ័រ វិធី សាស្រ្តដើម្បីធ្វើឲ្យមានសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត និងជំហានទូទៅសម្រាប់ការពារឯកជនភាពរបស់អ្នកនៅលើអ៊ីនធឺណិត

ចំណងជើងអត្ថបទ	អ្នកផលិត	គោលបំណង
Security Education Companion	Electronic Frontier Foundation	ការណែនាំសម្រាប់គ្រូបណ្តុះបណ្តាលដំបូងពាក់ព័ន្ធជាមួយសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត។
Surveillance Self-Defense	Electronic Frontier Foundation	ព័ត៌មានពាក់ព័ន្ធជាមួយសុវត្ថិភាពក្នុងការទំនាក់ទំនងនៅលើប្រព័ន្ធអ៊ីនធឺណិតដែលរួមបញ្ចូលជាមួយការណែនាំស្តីពីសុវត្ថិភាពនិងឯកជនភាពនៅលើអនឡាញ។
Umbrella	Security First	Appសម្រាប់ជួយអ្នកក្នុងការពង្រឹងលើសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត។

ខាងក្រោមនេះគឺ ជាស្ថាប័ន និងបុគ្គលដែលអ្នកអាចគួរស្គាល់ដើម្បីជួយអ្នកក្នុងការតាមទាន់នូវព័ត៌មានទាក់ទងជាមួយសុវត្ថិភាពនៅលើប្រព័ន្ធអ៊ីនធឺណិត និងបច្ចេកវិទ្យា។

- **Electronic Frontier Foundation (twitter: @EFF)**
- **Tactical Technology Collective (twitter: @info_Activism)**
- **Frontline Defenders (twitter: @FrontLineHRD)**
- **The Engine Room (twitter: @EngnRoom)**
- **Internews (@internews)**
- **Access Now (@accessnow)**
- **Security First (@_SecurityFirst)**
- **Security Without Borders (@swborders)**
- **Privacy International (@privacyint)**
- **Internet Freedom Festival (@InternetFF)**
- **Open Technology Fund (OpenTechFund)**
- **Mozilla (@mozilla)**
- **The Tor Project (@torproject)**
- **Citizen Lab (@citizenlab)**