Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

សៀវភៅណែនាំស្តីពីសន្តិសុខអ៊ីនធឺណិតសម្រាប់អាជីវកម្មខ្នាតតូច

ភាពស្មុគស្មាញនៃខ្លឹមសារ
សាមញ្ញ ●○○

cyber.gov.au

សេចក្តីផ្តើម

សម្រាប់អាជីវកម្មខ្នាតតូច សូម្បីតែឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិតតូចតាច ក៏អាចបង្កការខូចខាតធ្ងន់ធ្ងរដែរ។ សៀវភៅណែនាំនេះរួមបញ្ចូលវិធានការសន្តិសុខជាមូលដ្ឋានដើម្បីជួយការពារអាជីវកម្មរបស់អ្នក ប្រឆាំងនឹងការគំរាមកំហែងសន្តិសុខអ៊ីនធឺណិតទូទៅ។ ជាចំណុចចាប់ផ្តើម យើងសូមណែនាំលើវិធានការបីដូចខាងក្រោម៖

- បើកការផ្ទៀងផ្ទាត់ពហុកត្តា
- ធ្វើបច្ចុប្បន្នភាពកម្មវិធីសូហ្វវែររបស់អ្នក
- ថតចម្លងទុកព័ត៌មានរបស់អ្នក

សៀវភៅណែនាំនេះអាចរួមបញ្ចូលវិធានការដែលមិនពាក់ព័ន្ធនឹងអាជីវកម្មរបស់អ្នក ឬអាជីវកម្មរបស់អ្នកអាចមានតម្រូវការស្មុគស្មាញជាងនេះ។ បន្ទាប់ពីបញ្ចប់សៀវភៅណែនាំនេះ យើងសូមណែនាំអាជីវកម្មខ្នាតតូចឱ្យអនុវត្តយុទ្ធវិធីបន្ទូរបន្ថយកម្រិតទី១ នៃដំណាក់កាលសំខាន់ៗទាំងប្រាំបី (Maturity Level One of the Essential Eight)។ ប្រសិនបើអ្នកមានសំណួរអំពីដំបូន្មាននេះ ឬអំពីសន្តិសុខអ៊ីនធឺណិតកាន់តែទូលំទូលាយ យើងសូមណែនាំឱ្យអ្នកនិយាយជាមួយអ្នកជំនាញផ្នែកព័ត៌មានវិទ្យា (IT) ឬទីប្រឹក្សាដែលគួរឱ្យទុកចិត្តម្នាក់។

ចូលទៅកាន់គេហទំព័រ cyber.gov.au ដើម្បីអានសៀវភៅណែនាំពេញលេញរបស់យើង រួមទាំងដំបូន្មានអំពីវិធីសាស្ត្រអនុវត្តសម្រាប់វិធានការនីមួយៗ។

តារាងមាតិកា

ការគំរាមកំហែងដល់អាជីវកម្មខ្នាតតូច 4

សារបោកបញ្ឆោត 4

ការវាយប្រហារតាមអ៊ីមែល 5

កម្មវិធីសូហ្វវែរព្យាបាទ 6

ធានាសន្តិសុខគណនីរបស់អ្នក 7

បើកការផ្ទៀងផ្ទាត់ពហុកត្តា 7

ប្រើពាក្យសម្ងាត់ ឬឃ្លាសម្ងាត់រឹងមាំ 7

គ្រប់គ្រងគណនីដែលបានចែករំលែក 7

អនុវត្តការត្រួតពិនិត្យការចូលដំណើរការ 7

ការពារឧបករណ៍ និងព័ត៌មានរបស់អ្នក 8

ធ្វើបច្ចុប្បន្នភាពកម្មវិធីសូហ្វវែររបស់អ្នក 8

ថតចម្លងទុកព័ត៌មានរបស់អ្នក 8

ប្រើកម្មវិធីសូហ្វវែរសន្តិសុខ 8

ធានាឱ្យបាននូវសន្តិសុខបណ្តាញ និងសេវាកម្មខាងក្រៅរបស់អ្នក 9

ពង្រឹងសន្តិសុខគេហទំព័ររបស់អ្នក 9

កំណត់ឧបករណ៍របស់អ្នកឡើងវិញ មុននឹងលក់ ឬបោះចោលវា 9

រក្សាឧបករណ៍របស់អ្នកឱ្យជាប់សោ និងការពារសន្តិសុខជាក់ស្តែង 10

ការពារទិន្នន័យអាជីវកម្មរបស់អ្នក 10

រៀបចំបុគ្គលិករបស់អ្នក 11

អប់រំបុគ្គលិក 11

រៀបចំផែនការសង្គ្រោះបន្ទាន់ 11

តាមដានព័ត៌មាន 11

ការគំរាមកំហែងដល់អាជីវកម្មខ្នាតតូច

សារបោកបញ្ឆោត

ការបោកបញ្ឆោតគឺជាមធ្យោបាយទូទៅ ដែលឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតកំណត់គោលដៅអាជីវកម្មខ្នាតតូច។ គោលដៅរបស់ពួកគេគឺដើម្បីបោកបញ្ឆោតអ្នក ឬបុគ្គលិករបស់អ្នកឱ្យចូលទៅក្នុង៖

- ការផ្ញើប្រាក់ ឬកាតអំណោយ
- ការចុចលើតំណភ្ជាប់ព្យាបាទ ឬឯកសារភ្ជាប់ព្យាបាទ
- ការផ្តល់ព័ត៌មានរសើប ដូចជាពាក្យសម្ងាត់។

ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតអាចព្យាយាម និងអាជីវកម្មរបស់អ្នកតាមរយៈអ៊ីមែល សារជាអក្សរ ការហៅទូរសព្ទ និងប្រព័ន្ធផ្សព្វផ្សាយសង្គម។ ជារឿយៗ ពួកគេនឹងតាំងខ្លួនជាបុគ្គល ឬស្ថាប័នដែលអ្នកទុកចិត្ត។

ការវាយប្រហារបោកបញ្ឆោតតាមអ៊ីមែល

ការព្រួយបារម្ភជាពិសេសចំពោះអាជីវកម្មខ្នាតតូច គឺ **ការវាយប្រហារបោកបញ្ឆោតតាមអ៊ីមែល។** ការបោកបញ្ឆោតទាំងនេះច្រើនតែមានតំណភ្ជាប់ទៅកាន់គេហទំព័រក្លែងក្លាយ ជាកន្លែងដែលអ្នកត្រូវបានលើកទឹកចិត្តឱ្យបើកចូលទៅក្នុងគណនីមួយ ឬបញ្ចូលព័ត៌មានលម្អិតសម្ងាត់។

ការវាយប្រហារបោកបញ្ឆោតតាមអ៊ីមែល ជាធម្មតាសម្របសម្រួលដល់ពាក្យសម្ងាត់នៃគណនីរបស់អ្នក។ ជារឿយៗ ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត ប្រើវិធីនេះដើម្បី “គ្រប់គ្រង” គណនីប្រព័ន្ធផ្សព្វផ្សាយសង្គមរបស់អាជីវកម្មខ្នាតតូច ហើយទុកពួកគេដើម្បីជំរិតទារប្រាក់។

មធ្យោបាយបន្ធូរបន្ថយ

ប្រសិនបើសារមកពីអង្គភាពមួយដែលគេស្គាល់ ហើយហាក់ដូចជាគួរឱ្យសង្ស័យ សូមប្រើការប្រុងប្រយ័ត្ន។ ទាក់ទងបុគ្គល ឬអាជីវកម្មដោយឡែកពីគ្នា ដើម្បីពិនិត្យមើលថាតើសារនោះស្របច្បាប់ដែរឬទេ។ ប្រើប្រាស់ព័ត៌មានលម្អិតនៃទំនាក់ទំនងដែលអ្នករកឃើញតាមរយៈប្រភពស្របច្បាប់មួយ ឧទាហរណ៍ តាមរយៈការចូលមើល គេហទំព័រផ្លូវការរបស់អាជីវកម្ម ហើយមិនមែនព័ត៌មានដែលមាននៅក្នុងសារគួរឱ្យសង្ស័យនោះទេ។

ស្វែងយល់បន្ថែមអំពីការកំណត់អត្តសញ្ញាណការបោកបញ្ឆោត និងការវាយប្រហារបោកបញ្ឆោតតាមអ៊ីមែល ដោយប្រើធនធាននានាខាងក្រោម៖

- ទទួលស្គាល់ និងរាយការណ៍ពីការបោកបញ្ឆោត
- ស្វែងយល់ពីរបៀបកត់សម្គាល់ការបោកបញ្ឆោតតាមអ៊ីមែល
- ការរកឃើញសារដែលបង្កើតដោយសង្គម។

ករណីសិក្សា៖

បុគ្គលិកម្នាក់នៅក្រុមហ៊ុននាំសំបុត្រមួយបានទទួលអ៊ីមែលពីបុគ្គលិកប្រតិបត្តិម្នាក់របស់ពួកគេ ដោយស្នើសុំឱ្យពួកគេទិញកាតឥណទានបង់ប្រាក់ជាមុនចំនួន 6 x $500។ នាយកប្រតិបត្តិបានប្រាប់នាងឱ្យរក្សាជាការសម្ងាត់ ពីព្រោះថាកាតឥណទានទាំងនោះនឹងក្លាយជាកាតអំណោយជាទឹកប្រាក់សម្រាប់សមាជិកបុគ្គលិក។ នៅពេលទិញរួច បុគ្គលិកនោះត្រូវបានស្នើសុំឱ្យថតរូបកាតទាំងសងខាង ហើយផ្ញើវាទៅនាយកប្រតិបត្តិជាភស្តុតាងនៃការទិញ។

ដូចដែលបានណែនាំ បុគ្គលិកនោះបានទៅការិយាល័យប្រៃសណីយ៍ ហើយបានប្រើប្រាស់កាតឥណទានផ្ទាល់ខ្លួនរបស់នាង ដើម្បីទិញកាតអំណោយ។ នាងបានឆ្លើយតបទៅអ៊ីមែលរបស់នាយកប្រតិបត្តិ ហើយបានផ្ញើរូបថតនៃកាតអំណោយទាំងនោះជាភស្តុតាង។

បន្ទាប់ពីត្រឡប់មកពីការិយាល័យប្រៃសណីយ៍វិញ បុគ្គលិកនោះក៏បានប្រគល់កាតនោះផ្ទាល់ដល់នាយកប្រតិបត្តិ ដែលគាត់មិនបានដឹងអំពីរឿងនោះទាល់តែសោះ។ នៅពេលពិនិត្យ **អ៊ីមែលទាំងអស់អំពីកាតអំណោយគឺផ្ញើមកពីអាសយដ្ឋានអ៊ីមែលចៃដន្យមួយ ហើយមិនមែនមកពីគណនីអ៊ីមែលស្របច្បាប់របស់នាយកប្រតិបត្តិនោះទេ។ ក្រុមហ៊ុនត្រូវបានគេបោកបញ្ឆោត។**

ការវាយប្រហារតាមអ៊ីមែល

បន្ថែមពីលើការបោកបញ្ឆោតដូចជាការបោកបញ្ឆោតតាមអ៊ីមែល ការវាយប្រហារតាមអ៊ីមែលទូទៅ ប្រឆាំងនឹងអាជីវកម្មខ្នាតតូច **គឺការសម្របសម្រួលអ៊ីម៉ែលអាជីវកម្មខ្នាតតូច** (Business email compromise BEC)។ ឧក្រិដ្ឋជនអាចក្លែងធ្វើជាតំណាងអាជីវកម្មដោយប្រើប្រាស់គណនីអ៊ីមែលដែលបានសម្របសម្រួល ឬតាមរយៈមធ្យោបាយផ្សេងទៀត - ដូចជាការប្រើឈ្មោះអាសយដ្ឋានគេហទំព័រ (domain name) មួយដែលមើលទៅស្រដៀងនឹងអាជីវកម្មពិតប្រាកដ។ ក្រៅពីការលួចព័ត៌មានគោលដៅនៃការវាយប្រហារទាំងនេះ ជាធម្មតាគឺដើម្បីបោកបញ្ឆោតជនរងគ្រោះឱ្យផ្ញើប្រាក់ទៅគណនីធនាគារមួយ ដែលដំណើរការដោយអ្នកបោកបញ្ឆោតនោះ។

មធ្យោបាយបន្ធូរបន្ថយ

ការការពារដ៏ល្អបំផុតប្រឆាំងនឹងការវាយប្រហារតាមអ៊ីមែល គឺការបណ្តុះបណ្តាល និងការយល់ដឹងសម្រាប់បុគ្គលិករបស់អ្នក។ ធានាឱ្យបានថាបុគ្គលិករបស់អ្នកដឹងពីការប្រុងប្រយ័ត្នជានិច្ច ចំពោះអ៊ីមែលដែលមានខ្លឹមសារដូចខាងក្រោម៖

- សំណើសុំឱ្យទូទាត់ប្រាក់ ជាពិសេសក្នុងករណីបន្ទាន់ ឬហួសកាលកំណត់
- ការផ្លាស់ប្តូរព័ត៌មានលម្អិតរបស់ធនាគារ
- អាសយដ្ឋានអ៊ីមែលដែលមើលទៅមិនត្រឹមត្រូវ ដូចជាឈ្មោះអាសយដ្ឋានគេហទំព័រ មិនត្រូវគ្នានឹងឈ្មោះក្រុមហ៊ុនរបស់អ្នកផ្គត់ផ្គង់។

ខណៈពេលដែលការវាយប្រហារទាំងនេះអាចបង្កការខូចខាតធ្ងន់ធ្ងរ វិធានការបន្ធូរបន្ថយគឺមានភាពងាយស្រួល ហើយស្ទើរតែគ្មានការចំណាយអ្វីទាំងអស់។ **នៅពេលបុគ្គលិកទទួលបានអ៊ីមែលបែបនេះ ការបន្ធូរបន្ថយដ៏មានប្រសិទ្ធភាពបំផុតគឺការហៅទូរសព្ទទៅអ្នកផ្ញើ ដើម្បីបញ្ជាក់ថាតើពួកគេស្របច្បាប់ឬអត់។** កុំប្រើប្រាស់ព័ត៌មានលម្អិតនៃទំនាក់ទំនងដែល ត្រូវបានគេផ្ញើមកអ្នក ពីព្រោះទាំងនេះអាចជាការក្លែងបន្លំ។ ណែនាំពីដំណើរការផ្លូវការសម្រាប់បុគ្គលិកដើម្បីអនុវត្តតាម នៅពេលទទួលបានសំណើទូទាត់ប្រាក់ ឬព័ត៌មានលម្អិតអំពីធនាគារត្រូវបានផ្លាស់ប្តូរ។

ស្វែងយល់អំពីការការពារអាជីវកម្មរបស់អ្នកពីការបោកបញ្ឆោត BEC និងការសម្របសម្រួលអ៊ីមែលជាមួយនឹងធនធានខាងក្រោម៖

- ការសម្របសម្រួលអ៊ីម៉ែលអាជីវកម្ម
- ការពារអាជីវកម្មរបស់អ្នកពីការក្លែងបន្លំ និងការបង្កគ្រោះថ្នាក់តាមអ៊ីម៉ែល
- អ្វីដែលត្រូវធ្វើប្រសិនបើអាជីវកម្មរបស់អ្នកត្រូវបានកំណត់ជាគោលដៅដោយការក្លែងបន្លំតាមអ៊ីមែល ឬការសម្របសម្រួល។

ករណីសិក្សា៖

អាជីវកម្មសំណង់តូចមួយបានទទួលអ៊ីមែលពីអ្នកផ្គត់ផ្គង់របស់ពួកគេដោយនិយាយថា ពួកគេបានផ្លាស់ប្តូរធនាគារ។ អ្នកផ្គត់ផ្គង់បានផ្តល់ព័ត៌មានលម្អិតអំពីគណនីថ្មីសម្រាប់ការទូទាត់វិក្កយបត្រ។ ដោយសារតែអ៊ីមែលនោះមើលទៅហាក់ដូចជាស្របច្បាប់ **អាជីវកម្មសំណង់នោះមិនបានហៅទូរសព្ទទៅអ្នកផ្គត់ផ្គង់ ដើម្បីបញ្ជាក់ពីការផ្លាស់ប្តូរព័ត៌មានលម្អិតនៃគណនីធនាគារនោះទេ។**

អាជីវកម្មបានទូទាត់វិក្កយបត្រដែលទទួលបានពីអ្នកផ្គត់ផ្គង់ជាង $70,000។ នៅថ្ងៃបន្ទាប់ បុគ្គលិកម្នាក់ទៀតបានទូទាត់វិក្កយបត្រដដែលម្តងទៀត ដោយការភាន់ច្រឡំ ក្នុងចំនួនទឹកប្រាក់បន្ថែមជាង $70,000។ សរុបមក ទឹកប្រាក់ចំនួនជាង $150,000 ត្រូវបានទូទាត់ចូលគណនីធនាគារថ្មីនោះ។

នៅពេលដែលអាជីវកម្មហៅទូរសព្ទទៅកាន់អ្នកផ្គត់ផ្គង់របស់ពួកគេ ដើម្បីសួរថាតើពួកគេអាចសងប្រាក់ដែលបានទូទាត់ពីរដងនោះមកវិញបានឬទេ អ្នកផ្គត់ផ្គង់បានណែនាំថា ព័ត៌មានលម្អិតអំពីធនាគារទាំងនោះមិនត្រឹមត្រូវទេ។ ការស៊ើបអង្កេតមួយត្រូវបានចាប់ផ្តើមអនុវត្តភ្លាមៗ ហើយអ្នកផ្គត់ផ្គង់បានរកឃើញថាគណនីអ៊ីមែលមួយរបស់ពួកគេ ត្រូវបានគេលួចចូល ហើយកំពុងផ្ញើព័ត៌មានលម្អិតនៃគណនីធនាគារក្លែងបន្លំ។ **ប្រាក់មិនត្រូវបានប្រមូលមកវិញទេ។**

កម្មវិធីសូហ្វវែរព្យាបាទ

[កម្មវិធីផ្ទុកមេរោគដើម្បីលួចចូលប្រព័ន្ធកុំព្យូទ័រ (Malware)] គឺជាពាក្យទូលំទូលាយមួយសម្រាប់កម្មវិធីសូហ្វវែរព្យាបាទ ដែលត្រូវបានរចនាឡើងដើម្បីបង្កគ្រោះថ្នាក់ដូចជា កម្មវិធីផ្ទុកមេរោគចាប់ជំរិត (ransomware), មេរោគ (viruses), កម្មវិធីប្រមូលព័ត៌មានសម្ងាត់ពីគេហទំព័រ (spyware) និងកម្មវិធីបំផ្លាញទិន្នន័យកុំព្យូទ័រ (trojans)។ Malware អាច៖

- លួច ឬចាក់សោឯកសារនៅលើឧបករណ៍របស់អ្នក
- លួចលេខធនាគារ ឬលេខកាតឥណទានរបស់អ្នក
- លួចឈ្មោះអ្នកប្រើប្រាស់ និងពាក្យសម្ងាត់របស់អ្នក
- គ្រប់គ្រង ឬយកការណ៍សម្ងាត់លើកុំព្យូទ័ររបស់អ្នក។

Malware អាចបញ្ឈប់ឧបករណ៍របស់អ្នកពីដំណើរការបានត្រឹមត្រូវ លុប ឬធ្វើឱ្យខូចឯកសាររបស់អ្នក ឬអនុញ្ញាតឱ្យអ្នកដទៃចូលប្រើប្រាស់ព័ត៌មានផ្ទាល់ខ្លួន ឬអាជីវកម្មរបស់អ្នក។ ប្រសិនបើឧបករណ៍របស់អ្នកបានឆ្លង Malware អ្នកអាចងាយរងការវាយប្រហារផ្សេងទៀត។ Malware ក៏អាចរីករាលដាលទៅដល់ឧបករណ៍ផ្សេងទៀត នៅលើបណ្តាញរបស់អ្នកផងដែរ។

ឧបករណ៍របស់អ្នកអាចឆ្លង malware
តាមវិធីជាច្រើន រួមមាន៖

- ការចូលមើលគេហទំព័រដែលត្រូវបានឆ្លង malware
- ការទាញយកឯកសារ ឬកម្មវិធីសូហ្វវែរដែលឆ្លងមេរោគពីអ៊ីនធឺណិត
- ការបើកឯកសារភ្ជាប់ក្នុងអ៊ីមែលដែលបានឆ្លងមេរោគ។

កម្មវិធីផ្ទុកមេរោគចាប់ជំរិត

Ransomware គឺជាប្រភេទនៃ malware ជាទូទៅ និងមានគ្រោះថ្នាក់មួយ។ វាធ្វើការដោយការចាក់សោ ឬដាក់លេខកូដពិសេសកុំឱ្យគេចូលមើលបាន (Encrypt) ទៅលើឯកសាររបស់អ្នក ដូច្នេះអ្នកមិនអាចចូលប្រើវាបានតទៅទៀតទេ។ ការជំរិតទារប្រាក់ ជាធម្មតានៅក្នុងទម្រង់នៃរូបិយប័ណ្ណឌីជីតថលគ្រីបតូ (Cryptocurrency) ត្រូវបានទាមទារដើម្បីស្តារការចូលប្រើឯកសារឡើងវិញ។ ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតក៏អាចគំរាមបោះពុម្ពផ្សាយ ឬលក់ទិន្នន័យតាមអ៊ីនធឺណិតផងដែរ លុះត្រាតែមានការបង់ប្រាក់សម្រាប់ការជំរិតទារប្រាក់នោះ។

មធ្យោបាយបន្ធូរបន្ថយ

ខណៈពេលដែលកម្មវិធីសូហ្វវែរកម្ចាត់មេរោគ ឬកម្មវិធីសូហ្វវែរសន្តិសុខអាចជួយការពារអ្នកពី malware គ្មានកម្មវិធីសូហ្វវែរណាមួយមានប្រសិទ្ធភាព 100% នោះទេ។ បុគ្គលិកត្រូវតែមានការប្រុងប្រយ័ត្នជាមួយនឹងអ៊ីមែល គេហទំព័រ និងការទាញយកឯកសារនានា ហើយត្រូវធ្វើបច្ចុប្បន្នភាពឧបករណ៍របស់ពួកគេឱ្យបានទៀងទាត់ ដើម្បីរក្សាសន្តិសុខ។

សូមមើលធនធានខាងក្រោមសម្រាប់ព័ត៌មានបន្ថែមស្តីពីការការពារអាជីវកម្មរបស់អ្នកពី ransomware៖

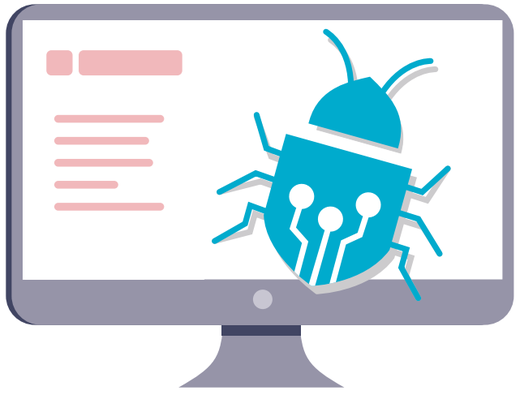
- Ransomware
- ការពារខ្លួនអ្នកពីការវាយប្រហារដោយ ransomware
- អ្វីដែលត្រូវធ្វើប្រសិនបើអ្នកត្រូវបានជំរិតទារប្រាក់

ករណីសិក្សា៖

បុគ្គលិកនៃហាងលក់គ្រឿងបន្លាស់រថយន្តមួយបានចូលមកធ្វើការនៅព្រឹកមួយ ហើយមិនអាចចាប់ផ្តើមដំណើរការកុំព្យូទ័រម៉ាស៊ីនមេរបស់ពួកគេបានទេ។ នៅពេលដែលអ្នកផ្តល់សេវាកម្មផ្នែកព័ត៌មានវិទ្យា (IT) របស់ពួកគេបានចូលប្រើម៉ាស៊ីនមេ ពួកគេបានរកឃើញបង្អួចមួយបើកដែលនិយាយថា ទិន្នន័យកុំព្យូទ័រទាំងអស់ត្រូវបានដាក់លេខកូដពិសេសកុំឱ្យគេចូលមើលបាន (Encrypt)។ សារខ្លីមួយទាមទារឱ្យពួកគេបង់ប្រាក់ជំរិតជា រូបិយប័ណ្ណឌីជីតថលប៊ីតខញ (Bitcoin) ដើម្បីដោះសោឯកសារទាំងនោះ។

ថាសកុំព្យូទ័រសម្រាប់ថតចម្លងទុកដែលដោតចូលទៅក្នុងកុំព្យូទ័រ ក៏ត្រូវបានដាក់លេខកូដពិសេសកុំឱ្យគេចូលមើលបាន (Encrypt) ផងដែរ។ ពួកគេបានព្យាយាមភ្ជាប់ថាសកុំព្យូទ័រសម្រាប់ថតចម្លងទុកបន្ថែមទៀត ប៉ុន្តែឯកសារនានាត្រូវបានដាក់លេខកូដពិសេសកុំឱ្យគេចូលមើលបាន (Encrypt) ដោយស្វ័យប្រវត្តិក្នុងរយៈពេលប៉ុន្មានវិនាទីប៉ុណ្ណោះ។ ពួកគេបានបរាជ័យក្នុងការកំចាត់ ransomware មុនពេលព្យាយាមសង្គ្រោះទិន្នន័យរបស់ពួកគេ ហើយបានបាត់បង់រាល់ឯកសារថតចម្លងទុកដែលពួកគេមាន។

ជម្រើសតែមួយគត់ដែលនៅសេសសល់គឺការបង្ហូរទៅការដំឡើងពីរោងចក្រនូវម៉ាស៊ីនមេ ហើយចាប់ផ្តើមជាមួយប្រព័ន្ធថ្មីមួយ។ **អាជីវកម្មរបស់ពួកគេបានបាត់បង់ទិន្នន័យជាច្រើនឆ្នាំ ហើយត្រូវចាប់ផ្តើមឡើងវិញទាំងអស់។**



ធានាសន្តិសុខគណនីរបស់អ្នក

បើកការផ្ទៀងផ្ទាត់ពហុកត្តា

ការផ្ទៀងផ្ទាត់ពហុកត្តា (MFA) ធ្វើឱ្យឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតកាន់តែពិបាកក្នុងការចូលប្រើប្រាស់គណនីរបស់អ្នក។

MFA បន្ថែមស្រទាប់សន្តិសុខមួយទៀតទៅក្នុងគណនីរបស់អ្នក។ វាគឺជាវិធីដ៏មានប្រសិទ្ធភាពបំផុតមួយក្នុងការការពារគណនីរបស់អ្នកពីការចូលប្រើប្រាស់ដោយនរណាម្នាក់ ដូច្នេះអ្នកគួរតែប្រើប្រាស់វានៅកន្លែងណាដែលអាចធ្វើទៅបាន។ នរណាម្នាក់ដែលចូលទៅក្នុងគណនីរបស់អ្នក នឹងត្រូវផ្តល់អ្វីមួយផ្សេងទៀតបន្ថែមលើឈ្មោះអ្នកប្រើប្រាស់ និងពាក្យសម្ងាត់របស់អ្នក។ នេះអាចជាលេខកូដតែមួយគត់ពីសារជាអក្សរ ឬកម្មវិធី app ផ្ទៀងផ្ទាត់មួយ។ សម្រាប់ព័ត៌មានបន្ថែម សូមអានដំបូន្មានអំពី MFA របស់យើងដែលមាននៅលើគេហទំព័រ **cyber.gov.au/mfa**។

✓ **បើក MFA នៅគ្រប់ទីកន្លែងដែលអាចធ្វើទៅបាន ដោយចាប់ផ្តើមជាមួយគណនីដ៏សំខាន់បំផុតរបស់អ្នក។**

អនុវត្តការគ្រប់គ្រងការចូលប្រើប្រាស់

ការរឹតបន្តឹងការចូលប្រើរបស់អ្នកប្រើប្រាស់អាចកំណត់ការខូចខាតដែលបណ្តាលមកពីឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត។

ការគ្រប់គ្រងការចូលប្រើប្រាស់ គឺជាវិធីមួយដើម្បីកំណត់ការចូលប្រើឯកសារ និងប្រព័ន្ធជាក់លាក់មួយចំនួន។ ជាធម្មតា បុគ្គលិកមិនតម្រូវឱ្យមានការចូលប្រើដោយពេញលេញចំពោះទិន្នន័យ គណនី និងប្រព័ន្ធទាំងអស់នៅក្នុងអាជីវកម្មមួយនោះទេ។ ពួកគេគួរតែត្រូវបានអនុញ្ញាតឱ្យចូលប្រើប្រាស់តែអ្វីដែលពួកគេត្រូវការ ដើម្បីបំពេញភារកិច្ចរបស់ពួកគេប៉ុណ្ណោះ។

ការរឹតបន្តឹងការចូលប្រើប្រាស់ នឹងជួយកំណត់ការខូចខាតដែលបណ្តាលមកពីឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត។ ឧទាហរណ៍ ប្រសិនបើកុំព្យូទ័ររបស់បុគ្គលិកម្នាក់ត្រូវបានឆ្លង ransomware ជាមួយនឹងការគ្រប់គ្រងការចូលប្រើប្រាស់បានត្រឹមត្រូវ វាអាចប៉ះពាល់ដល់ឯកសារមួយចំនួនតូច ជាជាងអាជីវកម្មទាំងមូល។

✓ **ធានាឱ្យបានថាអ្នកប្រើប្រាស់ម្នាក់ៗអាចចូលប្រើប្រាស់តែអ្វីដែលពួកគេត្រូវការសម្រាប់តែតួនាទីរបស់ពួកគេប៉ុណ្ណោះ។**

ប្រើប្រាស់ពាក្យសម្ងាត់ ឬឃ្លាសម្ងាត់រឹងមាំ

ការពារគណនីរបស់អ្នកពីឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតដោយប្រើពាក្យសម្ងាត់ ឬឃ្លាសម្ងាត់មានសន្តិសុខ។

អាជីវកម្មខ្នាតតូចជាច្រើនប្រឈមមុខនឹងការវាយប្រហារតាមអ៊ីនធឺណិត ដែលជាលទ្ធផលនៃអាកប្បកិរិយាពាក្យសម្ងាត់មិនល្អ។ ឧទាហរណ៍ ការប្រើពាក្យសម្ងាត់ដូចគ្នាឡើងវិញនៅលើគណនីច្រើន។ អ្នកអាចប្រើទាំងកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ និងឃ្លាសម្ងាត់ដើម្បីបង្កើតពាក្យសម្ងាត់រឹងមាំ។

កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ បំពេញតួនាទីដូចជាសុវត្ថិភាពនិម្មិតសម្រាប់ពាក្យសម្ងាត់របស់អ្នក។ អ្នកអាចប្រើប្រាស់វាដើម្បីបង្កើត និងរក្សាទុកពាក្យសម្ងាត់រឹងមាំ ពាក្យសម្ងាត់ដែលមាន**លក្ខណៈពិសេសតែមួយ**សម្រាប់គណនីនីមួយៗរបស់អ្នក។ ប្រសិនបើអ្នកមានគណនីច្រើន វាដកបន្ទុកនៃការចងចាំពាក្យសម្ងាត់ដែលមានលក្ខណៈពិសេសតែមួយ ។ អ្នកមិនចាំបាច់ចាំពាក្យសម្ងាត់ ឬគណនីដែលត្រូវនឹងពាក្យសម្ងាត់នោះទេ ពីព្រោះទិន្នន័យទាំងអស់ត្រូវបានកត់ត្រាទុកនៅក្នុងកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់របស់អ្នក។

សម្រាប់គណនីដែលអ្នកបើកចូលជាប្រចាំ ឬអ្នកមិនចង់រក្សាទុកក្នុងកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ សូមពិចារណាប្រើឃ្លាសម្ងាត់ជាពាក្យសម្ងាត់របស់អ្នក។ ឃ្លាសម្ងាត់គឺជាការរួមបញ្ចូលគ្នានៃពាក្យចៃដន្យ ឧទាហរណ៍ ‘crystal onion clay pretzel’។ ពួកវាមានប្រយោជន៍នៅពេលអ្នកចង់បានពាក្យសម្ងាត់សន្តិសុខដែលងាយស្រួលចងចាំ។ ប្រើការលាយចៃដន្យនៃពាក្យបួន ឬច្រើន ហើយរក្សាវាជាលក្ខណៈពិសេស **- កុំប្រើឃ្លាសម្ងាត់ឡើងវិញ** នៅលើគណនីច្រើន។ សម្រាប់ព័ត៌មានបន្ថែម សូមអានដំបូន្មានអំពីឃ្លាសម្ងាត់ និងកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ របស់យើងដែលមាននៅលើគេហទំព័រ **cyber.gov.au/passphrases**។

✓ **ប្រើប្រាស់កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ដើម្បីបង្កើត និងរក្សាទុកពាក្យសម្ងាត់ដែលមានលក្ខណៈពិសេសសម្រាប់គណនីសំខាន់ៗនីមួយៗរបស់អ្នក។**

គ្រប់គ្រងគណនីដែលបានចែករំលែក

ការចែករំលែកគណនីអាចសម្របសម្រួលដល់សន្តិសុខ និងធ្វើឱ្យពិបាកក្នុងការតាមដានសកម្មភាពព្យាបាទ។

នៅក្នុងអាជីវកម្មខ្នាតតូច អាចមានហេតុផលស្របច្បាប់ដែលបុគ្គលិកត្រូវការចែករំលែកគណនី ប៉ុន្តែវាគួរតែត្រូវបានជៀសវាងតាមដែលអាចធ្វើទៅបាន។ នៅពេលដែលបុគ្គលិកច្រើននាក់ប្រើគណនីដូចគ្នា វាអាចពិបាកក្នុងការតាមដានសកម្មភាពត្រឡប់ទៅបុគ្គលិកជាក់លាក់ណាម្នាក់ ហើយរឹតតែពិបាកក្នុងការតាមដានឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតដែលលួចចូល។ លុះត្រាតែអ្នកផ្លាស់ប្តូរពាក្យសម្ងាត់ បុគ្គលិកនានាក៏អាចបន្តចូលប្រើគណនីបាន សូម្បីតែបន្ទាប់ពីពួកគេបានចាកចេញពីអាជីវកម្មក៏ដោយ។

✓ **កំណត់ការប្រើប្រាស់គណនីដែលបានចែករំលែក និងធានាសន្តិសុខរាល់ការប្រើប្រាស់ណាមួយនៅក្នុងអាជីវកម្មរបស់អ្នក។**

ការពារឧបករណ៍និងព័ត៌មានរបស់អ្នក

ធ្វើបច្ចុប្បន្នភាពកម្មវិធីសូហ្វវែររបស់អ្នក

ការរក្សាកម្មវិធីសូហ្វវែររបស់អ្នកឱ្យទាន់បច្ចុប្បន្នភាព គឺជាវិធីដ៏ល្អបំផុតមួយដើម្បីការពារអាជីវកម្ម របស់អ្នកពីការវាយប្រហារតាមអ៊ីនធឺណិត។

ការធ្វើបច្ចុប្បន្នភាពអាចជួសជុលកំហុសសន្តិសុខនៅក្នុងប្រព័ន្ធ ប្រតិបត្តិការរបស់អ្នក និងកម្មវិធីសូហ្វវែរផ្សេងទៀត ដូច្នេះវាកាន់តែពិបាកសម្រាប់ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតក្នុងការលួចចូល។ កំហុសថ្មីៗត្រូវបានរកឃើញគ្រប់ពេលវេលា ដូច្នេះកុំព្រងើយកន្តើយនឹងការជំរុញឱ្យធ្វើបច្ចុប្បន្នភាព។ ការធ្វើបច្ចុប្បន្នភាពកម្មវិធីសូហ្វវែររបស់អ្នកជាទៀងទាត់ នឹងកាត់បន្ថយឱកាសនៃឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតដោយប្រើចំណុចខ្សោយដែលគេស្គាល់ ដើម្បីដំណើរការ malware ឬលួចចូលក្នុងឧបករណ៍របស់អ្នក។ ប្រសិនបើអ្នកត្រូវការជំនួយ ACSC បានចេញផ្សាយការណែនាំអំពីបច្ចុប្បន្នភាពនានា។

ប្រសិនបើឧបករណ៍ ឬកម្មវិធីសូហ្វវែររបស់អ្នកចាស់ពេក នោះការធ្វើបច្ចុប្បន្នភាពប្រហែលជាមិនអាចរកបានទេ។ ប្រសិនបើអ្នកផលិតបានឈប់គាំទ្រផលិតផលជាមួយនឹងការធ្វើបច្ចុប្បន្នភាព អ្នកគួរតែពិចារណាដំឡើងកំណែទៅផលិតផលថ្មីមួយដើម្បីរក្សាសន្តិសុខ។ ឧទាហរណ៍ នៃប្រព័ន្ធដែលលែងទទួលបានការធ្វើបច្ចុប្បន្នភាពសំខាន់ៗគឺ iPhone 7 និង Microsoft Windows 7។

សម្រាប់ព័ត៌មានបន្ថែម សូមអានការណែនាំរបស់យើងអំពីការធ្វើបច្ចុប្បន្នភាព ដែលមាននៅលើគេហទំព័រ cyber.gov.au/updates។

✓ បើកការធ្វើបច្ចុប្បន្នភាពដោយស្វ័យប្រវត្តិសម្រាប់ឧបករណ៍ និងកម្មវិធីសូហ្វវែររបស់អ្នក។

ប្រើប្រាស់កម្មវិធីសូហ្វវែរសន្តិសុខ

កម្មវិធីសូហ្វវែរសន្តិសុខដូចជា កម្មវិធីសូហ្វវែរកំចាត់មេរោគ និងការការពារ ransomware អាចជួយការពារឧបករណ៍របស់អ្នកបាន។

ប្រើប្រាស់កម្មវិធីសូហ្វវែរសន្តិសុខដើម្បីស្វែងរក និងកំចាត់ malware ចេញពីឧបករណ៍របស់អ្នក។ កម្មវិធីសូហ្វវែរកំចាត់មេរោគអាចត្រូវបានបង្កើតឡើងដើម្បីធ្វើការស្កែនឯកសារ និងកម្មវិធីដែលគួរឱ្យសង្ស័យជាទៀងទាត់។ នៅពេលរកឃើញការគំរាមកំហែងមួយ អ្នកនឹងទទួលបានការដាស់តឿន ហើយឯកសារដែលគួរឱ្យសង្ស័យនឹងត្រូវបានដាក់ឱ្យនៅដាច់ដោយឡែក ឬត្រូវបានកំចាត់។

អាជីវកម្មខ្នាតតូចជាច្រើនអាចប្រើប្រាស់ Windows Security ដើម្បីការពារពួកគេពីមេរោគ និង malware។ Windows Security ត្រូវបានភ្ជាប់មកជាមួយនៅក្នុងឧបករណ៍ដែលមាន Windows 10 និង Windows 11 ហើយរួមបញ្ចូលការការពារមេរោគ និងការគំរាមកំហែងដោយឥតគិតថ្លៃ។ អ្នកក៏អាចប្រើប្រាស់វាដើម្បីបើកមុខងារការពារ ransomware នៅលើឧបករណ៍របស់អ្នក។

សម្រាប់ផលិតផល និងជម្រើសផ្សេងទៀត សូមអានដំបូន្មានអំពីកម្មវិធីសូហ្វវែរកំចាត់មេរោគរបស់យើងដោយស្វែងរកពាក្យ *antivirus* នៅលើគេហទំព័រ cyber.gov.au។

✓ ដំឡើងកម្មវិធីសូហ្វវែរសន្តិសុខ ដើម្បីបំពេញការស្កែនជាប្រចាំនៅលើឧបករណ៍របស់អ្នក។

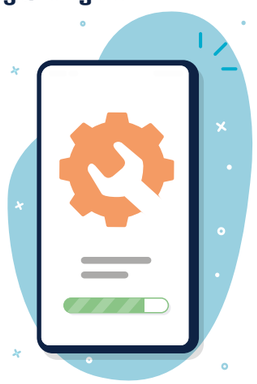
ថតចម្លងទុកព័ត៌មានរបស់អ្នក

ការថតចម្លងទុកជាទៀងទាត់អាចជួយអ្នកស្តារព័ត៌មានរបស់អ្នកឡើងវិញ ប្រសិនបើវាត្រូវបានបាត់បង់ ឬមានការសម្របសម្រួល។

ការថតចម្លងទុកព័ត៌មានសំខាន់ៗគួរតែជាការអនុវត្តជាប្រចាំ ឬដោយស្វ័យប្រវត្តិនៅក្នុងអាជីវកម្មរបស់អ្នក។ បើគ្មានការថតចម្លងទុកជាប្រចាំទេ វាមិនអាចទៅរួចសម្រាប់អ្នកក្នុងការស្តារព័ត៌មានរបស់អ្នកឡើងវិញ បន្ទាប់ពីការវាយប្រហារតាមអ៊ីនធឺណិតនោះទេ។

មានវិធីសាស្ត្រ និងផលិតផលជាច្រើនដែលអ្នកអាចប្រើដើម្បីថតចម្លងទុកព័ត៌មានរបស់អ្នក។ សម្រាប់ដំបូន្មានលម្អិតអំពីការថតចម្លងទុកអាជីវកម្មរបស់អ្នក សូមអានដំបូន្មានអំពីការថតចម្លងទុករបស់យើងដែលអាចរកបាននៅលើគេហទំព័រ cyber.gov.au/backups។ ជម្រើសដ៏ល្អបំផុតនឹងប្រែប្រួលសម្រាប់អាជីវកម្មនីមួយៗ ដូច្នេះសូមនិយាយជាមួយអ្នកជំនាញផ្នែកព័ត៌មានវិទ្យា(IT) ប្រសិនបើអ្នកមិនប្រាកដ។

✓ បង្កើត និងអនុវត្តផែនការដើម្បីថតចម្លងទុកព័ត៌មានរបស់អ្នកឱ្យបានទៀងទាត់។



ធានាឱ្យបាននូវសន្តិសុខបណ្តាញ និងសេវាកម្មខាងក្រៅរបស់អ្នក

ការពារអាជីវកម្មរបស់អ្នកពីការវាយប្រហារតាមអ៊ីនធឺណិត ដោយការដោះស្រាយភាពងាយរងគ្រោះដែលអាចកើតមាននៅក្នុងបណ្តាញរបស់អ្នក។

ឧបករណ៍ និងសេវាកម្មនៅក្នុងបណ្តាញរបស់អ្នក អាចជាគោលដៅចម្បងសម្រាប់ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត។ ប្រព័ន្ធទាំងនេះជាច្រើនអាចមានភាពស្មុគស្មាញក្នុងការធានាសន្តិសុខ ដូច្នេះសូមពិភាក្សាអំពីអនុសាសន៍ខាងក្រោម ជាមួយអ្នកជំនាញផ្នែកព័ត៌មានវិទ្យា។

- **ធានាសន្តិសុខម៉ាស៊ីនមេរបស់អ្នក៖** ប្រសិនបើអ្នកប្រើប្រាស់ NAS ឬម៉ាស៊ីនមេផ្សេងទៀតនៅក្នុងផ្ទះ ឬអាជីវកម្មរបស់អ្នក សូមប្រុងប្រយ័ត្នបន្ថែមទៀតដើម្បីធានាសន្តិសុខម៉ាស៊ីនមេទាំងនោះ។ ឧបករណ៍ទាំងនេះគឺជាគោលដៅទូទៅសម្រាប់ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត ព្រោះពួកវាជាញឹកញាប់រក្សាទុកឯកសារសំខាន់ៗ ឬអនុវត្តមុខងារសំខាន់ៗ។ មានយុទ្ធសាស្ត្របន្ថែមជាច្រើនដែលត្រូវការដើម្បីការពារឧបករណ៍ទាំងនេះ។ ឧទាហរណ៍ វាមានសារៈសំខាន់ណាស់ក្នុងការធានាថាម៉ាស៊ីនមេ ឬឧបករណ៍ NAS ត្រូវបានធ្វើបច្ចុប្បន្នភាពជាទៀងទាត់។ គណនីគ្រប់គ្រងគួរតែត្រូវបានធានាសន្តិសុខជាមួយនឹងឃ្លាសម្ងាត់ដ៏រឹងមាំ ឬការផ្ទៀងផ្ទាត់ពហុកត្តា។
- **កាត់បន្ថយស្នាមដានដែលប្រឈមពីខាងក្រៅ៖** ធ្វើសវនកម្ម និងធានាសន្តិសុខសេវាកម្ម អ៊ីនធឺណិតណាមួយដែលត្រូវបានដាក់ នៅលើបណ្តាញរបស់អ្នក។ វាអាចរាប់បញ្ចូលទាំងសេវាកម្ម ការត្រួតពិនិត្យកុំព្យូទ័រពីចម្ងាយ (Remote Desktop) , ការចែករំលែកឯកសារ (File Shares) , វ៉ិបមែល (Webmail) និងសេវាគ្រប់គ្រងពីចម្ងាយ។
- **ផ្ទេរទៅសេវាកម្មបណ្តាញម៉ាស៊ីនមេតាមប្រព័ន្ធអ៊ីនធឺណិត (cloud services)៖** ពិចារណាការប្រើប្រាស់សេវាកម្មតាមអនឡាញ ឬសេវាកម្មបណ្តាញម៉ាស៊ីនមេតាមប្រព័ន្ធអ៊ីនធឺណិត ដែលផ្តល់សន្តិសុខភ្ជាប់មកជាមួយ ជំនួសឱ្យការគ្រប់គ្រងដោយផ្ទាល់ខ្លួនរបស់អ្នក។ ឧទាហរណ៍ ប្រើប្រាស់សេវាកម្មតាមអនឡាញសម្រាប់អ្វីៗដូចជាការគ្រប់គ្រងអ៊ីមែល ឬគេហទំព័រ ជាជាងដំណើរការ និងធានាសន្តិសុខសេវាកម្មទាំងនេះដោយខ្លួនឯង។
- **កែលម្អសន្តិសុខនៃឧបករណ៍ភ្ជាប់បណ្តាញកុំព្យូទ័រ (Router) របស់អ្នក៖** អនុវត្តតាមការណែនាំរបស់យើងស្តីពីវិធីនានាដើម្បីធានាសន្តិសុខនៃឧបករណ៍ភ្ជាប់បណ្តាញកុំព្យូទ័រ (router) របស់អ្នក រួមទាំងការធ្វើបច្ចុប្បន្នភាពពាក្យសម្ងាត់លំនាំដើម ការបើក Wi-Fi “ភ្ញៀវ” សម្រាប់អតិថិជន ឬភ្ញៀវ និងការប្រើប្រាស់ពិធីសារដាក់លេខកូដពិសេសកុំឱ្យគេចូលមើលបា ន(Encryption protocols) ដ៏ខ្លាំងបំផុត។ ស្វែងរកពាក្យ router នៅលើគេហទំព័រ cyber.gov.au សម្រាប់ព័ត៌មានបន្ថែម។
- **ស្វែងយល់ពីខ្សែសង្វាក់ផ្គត់ផ្គង់តាមអ៊ីនធឺណិតរបស់អ្នក៖** អាជីវកម្មទំនើប ជាញឹកញយបញ្ចេញសេវាកម្មជាច្រើនទៅឱ្យក្រុមហ៊ុនខាងក្រៅគ្រប់គ្រងជំនួស។ ឧទាហរណ៍ ការប្រើប្រាស់ក្រុមហ៊ុនផ្តល់សេវាកម្មគ្រប់គ្រង ដើម្បីថែទាំព័ត៌មានវិទ្យារបស់ពួកគេ។ បញ្ហាសន្តិសុខជាមួយសេវាកម្ម ឬអ្នកផ្តល់សេវាទាំងនេះអាចជះឥទ្ធិពលយ៉ាងខ្លាំងដល់អាជីវកម្មរបស់អ្នក។ សម្រាប់ដំបូន្មានលម្អិតអំពីការគ្រប់គ្រងហានិភ័យនៃខ្សែសង្វាក់ផ្គត់ផ្គង់តាមអ៊ីនធឺណិត សូមអានការណែនាំអំពីខ្សែសង្វាក់ផ្គត់ផ្គង់តាមអ៊ីនធឺណិតរបស់យើងនៅលើគេហទំព័រ cyber.gov.au។

✓ និយាយទៅកាន់អ្នកជំនាញផ្នែកព័ត៌មានវិទ្យា អំពីវិធីនានាដើម្បីធានាសន្តិសុខបណ្តាញរបស់អ្នក។

ពង្រឹងសន្តិសុខគេហទំព័ររបស់អ្នក

គេហទំព័រគឺជាគោលដៅចម្បងសម្រាប់ការវាយប្រហារតាមអ៊ីនធឺណិត។

ការពារគេហទំព័ររបស់អ្នកពីការលួចយកមកគ្រប់គ្រង ដោយអនុវត្តតាមវិធានការសន្តិសុខជាមូលដ្ឋានមួយចំនួនដូចខាងក្រោម៖

- ធានាសន្តិសុខនៃការបើកចូលគេហទំព័ររបស់អ្នកជាមួយនឹងការផ្ទៀងផ្ទាត់ពហុកត្តា ឬពាក្យសម្ងាត់រឹងមាំ
- ធ្វើបច្ចុប្បន្នភាពជាប្រចាំនូវប្រព័ន្ធគ្រប់គ្រងខ្លឹមសារ និងកម្មវិធីបន្ថែមមុខងារ (plugins) នៃគេហទំព័ររបស់អ្នក។
- ថតចម្លងទុកគេហទំព័ររបស់អ្នកឱ្យបានទៀងទាត់ ដើម្បីឱ្យអ្នកអាចស្តារវាឡើងវិញបន្ទាប់ពីការវាយប្រហារតាមអ៊ីនធឺណិត។

ACSC មានធនធានបន្ថែមសម្រាប់ម្ចាស់គេហទំព័រ។ ស្វែងរកធនធានទាំងនេះនៅលើគេហទំព័រ **cyber.gov.au**៖

- កម្មវិធីឈ្នះរហ័ស (Quick Wins) សម្រាប់គេហទំព័ររបស់អ្នក
- ការអនុវត្តវិញ្ញាបនបត្រ TLS, HTTPS និង ឱកាសនិយម TLS
- សន្តិសុខប្រព័ន្ធឈ្មោះអាសយដ្ឋានគេហទំព័រ (Domain Name System Security) សម្រាប់ម្ចាស់ អាសយដ្ឋានគេហទំព័រ
- ការរៀបចំ និងការឆ្លើយតបទៅនឹងការវាយប្រហារដោយបដិសេធសេវាកម្ម

✓ សូមអានធនធានរបស់ ACSC អំពីសន្តិសុខគេហទំព័រ។

កំណត់ឧបករណ៍របស់អ្នកឡើងវិញមុននឹងលក់ ឬបោះចោលវា

ទិន្នន័យនៅលើឧបករណ៍ចាស់របស់អ្នក អាចត្រូវបានចូលប្រើដោយមនុស្សចម្លែក។

ប្រសិនបើអ្នកមិនបានបោះចោលឧបករណ៍របស់អ្នកដោយសន្តិសុខទេ ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតអាចចូលប្រើព័ត៌មានដែលផ្ទុកនៅលើវាបាន។ នេះអាចរួមបញ្ចូលអ៊ីមែល ឯកសារ និងទិន្នន័យអាជីវកម្មផ្សេងទៀត។ លុបព័ត៌មានទាំងអស់ចេញពីឧបករណ៍អាជីវកម្មរបស់អ្នក មុនពេលលក់ ជួញដូរ ឬបោះវាចោល។ ឧទាហរណ៍ ដោយធ្វើការកំណត់ឡើងវិញឱ្យដូចស្ថានភាពដើមពីរោងចក្រ។ ការធ្វើបែបនេះនឹងជួយលុបព័ត៌មានណាមួយ និងស្តារឧបករណ៍ទៅរកការកំណត់ភាពដើមរបស់វាវិញ។

សម្រាប់ដំបូន្មានអំពីការកំណត់ឧបករណ៍របស់អ្នកឡើងវិញ សូមអានការណែនាំរបស់យើងអំពីរបៀបបោះចោលឧបករណ៍របស់អ្នកដោយសន្តិសុខ។ ស្វែងរកពាក្យ dispose នៅលើគេហទំព័រ **cyber.gov.au**។

✓ ប្តូរទៅការដំឡើងពីរោងចក្រមុនពេលលក់ ឬបោះចោលឧបករណ៍អាជីវកម្ម។

រក្សាឧបករណ៍របស់អ្នកឱ្យជាប់សោ និងការពារសន្តិសុខជាក់ស្តែង

ការរឹតបន្តឹងការចូលប្រើឧបករណ៍អាជីវកម្មរបស់អ្នក នឹងកាត់បន្ថយឱកាសនានាសម្រាប់សកម្មភាពព្យាបាទ។

ការកំណត់ការចូលប្រើជាក់ស្តែងទៅកាន់ឧបករណ៍អាជីវកម្មរបស់អ្នក គឺជាវិធីសាមញ្ញមួយដើម្បីការពារទិន្នន័យពីការលួច ឬសកម្មភាពព្យាបាទផ្សេងទៀត។ មិនគួររក្សាទុកឧបករណ៍អាជីវកម្មនៅកន្លែងដែលបុគ្គលិកដែលពុំមានសិទ្ធិ ឬសមាជិកសាធារណៈអាចចូលប្រើបាននោះឡើយ។

ប្រើប្រាស់ការគ្រប់គ្រងសន្តិសុខ ដើម្បីការពារបន្ថែមនូវឧបករណ៍អាជីវកម្មរបស់អ្នក។ យ៉ាងហោចណាស់ឧបករណ៍ទាំងនោះគួរតែត្រូវបានចាក់សោដោយប្រើឃ្លាសម្ងាត់ លេខកូដ PIN ឬជីវមាត្រ (Biometrics)។ ធានាឱ្យបានថាឧបករណ៍ទាំងនេះត្រូវបានកំណត់ឱ្យចាក់សោដោយស្វ័យប្រវត្តិ បន្ទាប់ពីអសកម្មភាពរយៈពេលខ្លី។

✓ **កំណត់រចនាសម្ព័ន្ធឧបករណ៍ឱ្យចាក់សោដោយស្វ័យប្រវត្តិ បន្ទាប់ពីអសកម្មភាពរយៈពេលខ្លី។**

ការពារទិន្នន័យអាជីវកម្មរបស់អ្នក

ទិន្នន័យដែលកាន់កាប់ដោយអាជីវកម្មរបស់អ្នក គឺជាគោលដៅដ៏គួរឱ្យទាក់ទាញចំពោះឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត។

ការបំពានទិន្នន័យកំពុងមានការកើនឡើង - កុំអនុញ្ញាតឱ្យអាជីវកម្មរបស់អ្នកក្លាយជាជនរងគ្រោះ។ វាមានសារៈសំខាន់ណាស់ក្នុងការស្វែងយល់ ថាតើទិន្នន័យអាជីវកម្មរបស់អ្នកមានអ្វីខ្លះ និងនៅទីតាំងណាខ្លះ។ នៅពេលដែលអ្នកបានដឹងហើយ សូមប្រើអនុសាសន៍នានានៅក្នុងសៀវភៅណែនាំនេះ ដើម្បីជួយការពារទិន្នន័យរបស់អ្នកពីការចូលប្រើដោយឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត។ អាជីវកម្មខ្នាតតូចមួយចំនួនក៏អាចមានកាតព្វកិច្ចបន្ថែមតាមច្បាប់ផងដែរ។

- **បង្រួមទិន្នន័យអាជីវកម្មរបស់អ្នកចូលគ្នា។** អ្នកអាចមានទិន្នន័យផ្ទុកនៅលើឧបករណ៍ ឬសេវាកម្មជាច្រើន។ នៅពេលដែលទិន្នន័យត្រូវបានធ្វើវិមជ្ឈការ វាបង្កើនចំនួនប្រព័ន្ធដែលអ្នកត្រូវរក្សាសន្តិសុខ និងថតចម្លងទុក។ ការមានប្រព័ន្ធច្រើនក៏អាចបង្កើតឱកាសបន្ថែមទៀត សម្រាប់ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតដើម្បីវាយប្រហារផងដែរ។ កន្លែងណាដែលអាចធ្វើទៅបាន សូមរក្សាទុកទិន្នន័យអាជីវកម្មរបស់អ្នកនៅក្នុងទីតាំងកណ្តាលមួយដែលមានសន្តិសុខ ហើយថតចម្លងទុកជាប្រចាំ។ ការធ្វើមជ្ឈការទិន្នន័យរបស់អ្នក អាចបង្កើតការបំពានកាន់តែធំ ប្រសិនបើប្រព័ន្ធរបស់អ្នកត្រូវបានសម្របសម្រួល ដូច្នេះសូមប្រាកដថាទីតាំងកណ្តាលនេះត្រូវបានការពារយ៉ាងគ្រប់គ្រាន់ ជាមួយនឹងការកំណត់រចនាសម្ព័ន្ធសន្តិសុខ និងការចូលប្រើដែលបានរឹតបន្តឹង។ និយាយទៅកាន់អ្នកជំនាញផ្នែកព័ត៌មានវិទ្យា (IT) ឬសន្តិសុខអ៊ីនធឺណិតដើម្បីទទួលបានដំបូន្មាន។
- **ដឹងពីកាតព្វកិច្ចរបស់អ្នកសម្រាប់ការការពារទិន្នន័យ។** អាជីវកម្មខ្នាតតូចមួយចំនួនអាចមានកាតព្វកិច្ចតាមផ្លូវច្បាប់ សម្រាប់ការគ្រប់គ្រងព័ត៌មានផ្ទាល់ខ្លួនដែលពួកគេប្រមូលបាន។ ដើម្បីស្វែងយល់បន្ថែម សូមអានការណែនាំសម្រាប់អាជីវកម្មខ្នាតតូចរបស់ការិយាល័យស្នងការព័ត៌មានអូស្ត្រាលី ដែលមាននៅលើគេហទំព័រ **oaic.gov.au**។ សូមពិគ្រោះយោបល់ជាមួយអ្នកជំនាញផ្នែកច្បាប់ ប្រសិនបើអ្នកមិនប្រាកដ។

✓ **ស្វែងយល់អំពីទិន្នន័យដែលអាជីវកម្មរបស់អ្នកកាន់កាប់ និងទំនួលខុសត្រូវរបស់អ្នកដើម្បីការពារវា។**

រៀបចំបុគ្គលិករបស់អ្នក

អប់រំបុគ្គលិក

បុគ្គលិកដែលមានការអនុវត្តសន្តិសុខអ៊ីនធឺណិតល្អ គឺជាខ្សែការពារដំបូងរបស់អ្នកប្រឆាំងនឹងការវាយប្រហារតាមអ៊ីនធឺណិត។

បុគ្គលិករបស់អ្នកគួរតែមានការយល់ដឹងអំពីសន្តិសុខអ៊ីនធឺណិត រួមទាំងប្រធានបទនានាដូចខាងក្រោម៖

- ការគំរាមកំហែងផ្នែកសន្តិសុខអ៊ីនធឺណិតទូទៅ ដូចជាការសម្របសម្រួលអ៊ីមែលអាជីវកម្ម និង ransomware
- វិធានការការពារ រួមទាំងពាក្យសម្ងាត់ ឬឃ្លាសម្ងាត់ រឹងមាំ MFA និងការធ្វើបច្ចុប្បន្នភាពកម្មវិធីសូហ្វវែរ
- របៀបកត់សម្គាល់ការបោកបញ្ឆោតតាមអ៊ីមែល និងការវាយប្រហារបោកបញ្ឆោតតាមអ៊ីមែល
- គោលនយោបាយជាក់លាក់សម្រាប់អាជីវកម្ម (ឧទាហរណ៍ ដំណើរការសម្រាប់រាយការណ៍អ៊ីមែលដែលគួរឱ្យសង្ស័យ ឬសម្រាប់ការធ្វើសុពលភាពវិក្កយបត្រថាពិតប្រាកដ មុនពេលបង់ប្រាក់)
- អ្វីដែលត្រូវធ្វើនៅពេលមានករណីសង្គ្រោះបន្ទាន់។

គេហទំព័រ ACSC មានធនធានសម្រាប់ប្រធានបទទាំងនេះភាគច្រើននៅលើគេហទំព័រ cyber.gov.au/learn។ អ្នកអាចពិចារណាវិធីផ្សេងទៀតនៃការអប់រំបុគ្គលិករបស់អ្នក ឧទាហរណ៍ ជាមួយនឹងវគ្គសិក្សាផ្លូវការ ឬការបណ្តុះបណ្តាលផ្ទៃក្នុង។ ទោះជាអ្នកសម្រេចចិត្តបែបណាក៏ដោយ សូមចាំថា ការបណ្តុះបណ្តាលសន្តិសុខអ៊ីនធឺណិត មិនមែនជាតម្រូវការដែលធ្វើតែម្តងគត់នោះទេ ហើយគួរតែត្រូវបានធ្វើឡើងវិញដែលមានលក្ខណៈទៀងទាត់។

✓ **កំណត់ពីរបៀបដែលការយល់ដឹងអំពីសន្តិសុខអ៊ីនធឺណិត នឹងត្រូវបានបង្រៀននៅក្នុងអាជីវកម្មរបស់អ្នក។**

រៀបចំផែនការសង្គ្រោះបន្ទាន់

ផែនការសង្គ្រោះបន្ទាន់អាចកាត់បន្ថយផលប៉ះពាល់ នៃការវាយប្រហារតាមអ៊ីនធឺណិតលើអាជីវកម្មរបស់អ្នក។

នៅពេលឆ្លើយតបទៅនឹងឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត វាល់នាទីមានសារសំខាន់ណាស់។ ការមានផែនការសង្គ្រោះបន្ទាន់មានន័យថា បុគ្គលិករបស់អ្នកអាចចំណាយពេលតិចក្នុងការស្វែងរកអ្វីដែលត្រូវធ្វើ និងមានពេលវេលាកាន់តែច្រើនដើម្បីចាត់វិធានការ។

ពិចារណាសំណួរនានាខាងក្រោម នៅពេលបង្កើតផែនការសង្គ្រោះបន្ទាន់របស់អ្នក៖

- តើមានដំណើរការអ្វីខ្លះសម្រាប់បុគ្គលិករបស់អ្នកដើម្បីរាយការណ៍អំពី ឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិតដែលអាចកើតមាន?
- តើអ្នកទាក់ទងអ្នកណាសម្រាប់សុំជំនួយ? ឧទាហរណ៍ អ្នកជំនាញផ្នែកព័ត៌មានវិទ្យា និងធនាគាររបស់អ្នក។
- តើអ្នកនឹងប្រាស្រ័យទាក់ទងអំពីឧប្បត្តិហេតុទៅបុគ្គលិក អ្នកពាក់ព័ន្ធ ឬអតិថិជនរបស់អ្នក យ៉ាងដូចម្តេច?
- តើអ្នកនឹងគ្រប់គ្រងអាជីវកម្មដូចធម្មតាដោយរបៀបណា ប្រសិនបើប្រព័ន្ធសំខាន់ៗណាមួយគ្មានអ៊ីនធឺណិត?

ត្រូវប្រាកដថាបុគ្គលិករបស់អ្នកស្គាល់ច្បាស់ពីផែនការសង្គ្រោះបន្ទាន់ រួមទាំងតួនាទី ឬទំនួលខុសត្រូវដែលពួកគេអាចមាន។ រក្សាច្បាប់ចម្លងជាក្រដាស នៃផែនការក្នុងករណីដែលប្រព័ន្ធរបស់អ្នកគ្មានអ៊ីនធឺណិត នៅពេលដែលអ្នកត្រូវការវា។

✓ **បង្កើតផែនការសង្គ្រោះបន្ទាន់សម្រាប់ឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត។**

តាមដានព័ត៌មាន

ភ្ជាប់ជាដៃគូជាមួយ ACSC ដើម្បីទទួលបានព័ត៌មានចុងក្រោយពី ACSC។

តាមដានព័ត៌មានអំពីការគំរាមកំហែង និងភាពងាយរងគ្រោះតាមអ៊ីនធឺណិតចុងក្រោយបំផុត ដោយភ្ជាប់ជាដៃគូជាមួយ ACSC។ សេវាកម្មនេះនឹងផ្តើជូនអ្នកនូវព្រឹត្តិបត្រព័ត៌មានប្រចាំខែ និងការជូនដំណឹងនៅពេលដែលការគំរាមកំហែងតាមអ៊ីនធឺណិតថ្មីត្រូវបានកំណត់អត្តសញ្ញាណ។

សន្តិសុខអ៊ីនធឺណិតគឺជាវិស័យមួយមានការវិវឌ្ឍយ៉ាងឆាប់រហ័ស។ ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត កេងយកផលប្រយោជន៍យ៉ាងសកម្មពីភាពងាយរងគ្រោះ ក្នុងរយៈពេលប៉ុន្មាននាទីនៃការរកឃើញរបស់ពួកគេ។ តាមដានព័ត៌មានអំពីទិដ្ឋភាពសន្តិសុខអ៊ីនធឺណិត នឹងជួយឱ្យអាជីវកម្មរបស់អ្នកស្វែងយល់ពីការគំរាមកំហែងដែលវាទំនងជាប្រឈមមុខ និងរបៀបការពារប្រឆាំងនឹងពួកគេ។

✓ **ចុះឈ្មោះអាជីវកម្មរបស់អ្នកជាមួយកម្មវិធីភាពជាដៃគូរបស់ ACSC។**

ការបដិសេធការទទួលខុសត្រូវ
រូបភាពនៅក្នុងសៀវភៅណែនាំនេះគឺមានលក្ខណៈជាទូទៅ ហើយមិនគួរត្រូវបានចាត់ទុកថាជាដំបូន្មានផ្នែកច្បាប់ ឬពឹងផ្អែកលើ សម្រាប់ជាជំនួយក្នុងកាលៈទេសៈជាក់លាក់ណាមួយ ឬក្នុងស្ថានភាពសង្គ្រោះបន្ទាន់ឡើយ។ ក្នុងបញ្ហាសំខាន់ណាមួយ អ្នកគួរតែស្វែងរកដំបូន្មានដែលមានជំនាញវិជ្ជាជីវៈឯករាជ្យសមស្រប ទាក់ទងនឹងកាលៈទេសៈផ្ទាល់ខ្លួនរបស់អ្នក។

Commonwealth (ខុមុនវែល) មិនទទួលយកការទទួលខុសត្រូវ ឬបំណុលចំពោះការខូចខាត ការបាត់បង់ ឬការចំណាយណាមួយបណ្តាលមកពីការពឹងផ្អែកលើព័ត៌មានដែលមាននៅក្នុងសៀវភៅណែនាំនេះឡើយ។

រក្សាសិទ្ធិ។

ការប្រើប្រាស់សញ្ញាជាតិ។
លក្ខខណ្ឌនានាដែលសញ្ញាជាតិអាចត្រូវបានប្រើ គឺរៀបរាប់ជាលម្អិតនៅលើគេហទំព័ររបស់ក្រសួងនាយករដ្ឋមន្ត្រី និងគណៈរដ្ឋមន្ត្រី។
(www.pmc.gov.au/government/commonwealth-coat-arms)។

សម្រាប់ព័ត៌មានបន្ថែម ឬដើម្បីរាយការណ៍អំពីឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិត សូមទាក់ទងមកយើង៖
cyber.gov.au | 1300 CYBER1 (1300 292 371)
លេខនេះអាចប្រើបានតែក្នុងប្រទេសអូស្ត្រាលីប៉ុណ្ណោះ។

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre