National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

ការរក្សាសុវត្ថិភាពនៅលើបណ្តាញអ៊ីនធឺណិត

ហេតុអ្វីបានជាសន្តិសុខតាម (កុំព្យូទ័រ បណ្តាញកុំព្យូទ័រ និង) អ៊ីនធឺណិតមានសារៈសំខាន់សម្រាប់ខ្ញុំ?

អ៊ីនធឺណិតនិងប្រព័ន្ធផ្សព្វផ្សាយសង្គមគឺជាវេទិកាដ៏អស្ចារ្យមួយដែលជួយយើងចែករំលែកព័ត៌មាន និងរក្សាទំនាក់ទំនងជាមួយមិត្តភក្តិ និងក្រុមគ្រួសារ។

ទោះជាយ៉ាងណាក៏ដោយ ឧក្រិដ្ឋជន និងអង្គការមិនស្របច្បាប់ផ្សេងទៀតក៏ប្រើអ៊ីនធឺណិតនិងប្រព័ន្ធទាំងនេះដើម្បីព្យាយាមយកលុយរបស់អ្នក ព័ត៌មានរបស់អ្នក ឬដើម្បីបំភិតបំភ័យអ្នកផងដែរ។

ពួកគេអាចដំណើរការពីគ្រប់ទិសទីក្នុងពិភពលោក និយាយភាសាភាគច្រើនយ៉ាងស្ទាត់ជំនាញ និងបង្កើតគេហទំព័រក្លែងក្លាយដែលអាចគួរឱ្យជឿបាន។ ពួកគេនឹងទាក់ទងទៅអ្នកតាមរយៈអ៊ីមែល ប្រព័ន្ធផ្សព្វផ្សាយសង្គម និងសារជាអក្សរ ហើយពួកគេនឹងព្យាយាមធ្វើឱ្យអ្នកមានអារម្មណ៍ភ័យខ្លាច ឬព្រួយបារម្ភ ដូច្នេះអ្នកគិតអ្វីៗមិនច្បាស់លាស់នោះទេ។

ទាំងអស់នេះមានន័យថា អ្នកត្រូវរៀបចំខ្លួនឱ្យស្រេច និងតែងតែដឹងពីល្បិចកលដែលពួកគេប្រើប្រាស់។

តើបញ្ហាទូទៅអ្វីខ្លះដែលខ្ញុំអាចជួបប្រទះនៅលើអ៊ីនធឺណិត?

ទាំងនេះគឺជាស្ថានភាពទូទៅមួយចំនួនដែលយើងឃើញ។

- អ្នកទទួលបានអ៊ីមែលគួរឱ្យសង្ស័យមួយ ឬសារជាអក្សរសុំឱ្យអ្នកចុចលើតំណភ្ជាប់មួយ។
    - តំណភ្ជាប់ទាំងនេះច្រើនតែនាំទៅដល់គេហទំព័រក្លែងក្លាយ ដែលត្រូវបានរចនារៀបចំឡើងដើម្បីលួចចូល (your login) ឬលួចព័ត៌មានលម្អិតហិរញ្ញវត្ថុរបស់អ្នក។
- អ្នកទទួលបានការហៅទូរសព្ទគួរឱ្យសង្ស័យដែលសួររកព័ត៌មានផ្ទាល់ខ្លួន។
    - ដូចករណីខាងលើ អ្នកហៅទូរស័ព្ទនឹងក្លែងខ្លួនថាមកពីធនាគាររបស់អ្នក ហើយសួរព័ត៌មាន។
- អ្នកទទួលបានការប្រាស្រ័យទាក់ទងពីនរណាម្នាក់ដែលធ្វើពុតបន្លំជាបុគ្គលដែលមានអំណាច ដោយព្យាយាមឱ្យអ្នកធ្វើអ្វីមួយ។
    - ជារឿយៗ បុគ្គលនោះបង្កការគំរាមកំហែងខ្លះ។
- មាននរណាម្នាក់ចូលទៅក្នុងគណនីអនឡាញមួយ ឬច្រើនរបស់អ្នក (ឧទាហរណ៍៖ អ៊ីមែល ឬប្រព័ន្ធផ្សព្វផ្សាយសង្គម)។
    - ប្រសិនបើនរណាម្នាក់ចូលទៅក្នុងគណនីអនឡាញរបស់អ្នក ពួកគេអាចលួចព័ត៌មាន ឬទិសនៃការទូទាត់ថវិកានិងអាចកំណត់គោលដៅមិត្តភ័ក្តិ ឬក្រុមគ្រួសាររបស់អ្នកដោយក្លែងធ្វើជាអ្នក។
- ព័ត៌មានលម្អិតអំពីប័ណ្ណឥណទាន (credit card details) របស់អ្នកត្រូវបានលួច ឬអ្នកត្រូវបានគេបោកប្រាស់យកប្រាក់អស់នៅក្នុងការលក់ ឬការវិនិយោគក្លែងក្លាយមួយ។

   - អ្នកបោកប្រាស់សង្ឃឹមថាអ្នកនឹងឃើញការលក់ទិញក្នុងតម្លៃសមរម្យដ៏ល្អមួយ ហើយអ្នកចង់បង់ប្រាក់ដោយមិនគិតវែងឆ្ងាយ។ ឬប្រហែលជាគេហទំព័រពិតមួយត្រូវបានជាប់ជាមួយនៅក្នុងការរំលោភទិន្នន័យ ហើយព័ត៌មានលម្អិតរបស់អ្នកត្រូវបានបែកធ្លាយតាមអ៊ីនធឺណិត។

មានវិធីសាស្រ្តច្រើនទៀតនៅទីនេះ៖

ទទួលបានជំនួយឥឡូវនេះ - ធ្វើជាម្ចាស់លើអ៊ីនធឺណិតរបស់អ្នក

តើខ្ញុំរក្សាសុវត្ថិភាពតាមអ៊ីនធឺណិតដោយរបៀបណា?

- ពាក្យសម្ងាត់វែង និងតែមួយគត់
   - ពាក្យសម្ងាត់ណាដែលកាន់តែវែង វាកាន់តែរឹងមាំ។
   - បង្កើតពាក្យសម្ងាត់ដែលគួរឱ្យចងចាំបានលើសពី ១៦ តួអក្សរដោយភ្ជាប់ពាក្យចៃដន្យចំនួនបួនជាមួយគ្នា (ឧទាហរណ៍៖ TriangleRhinoOperationShoes) និងការបន្ថែមលេខ អក្សរធំ និងនិមិត្តសញ្ញាប្រសិនបើចាំបាច់ (ឧទាហរណ៍៖ Triangle&"Rhino"Operation2Shoes)។
   - សំខាន់បំផុត កុំប្រើពាក្យសម្ងាត់របស់អ្នកដែលប្រើរួចហើយ ម្តងទៀត។ ប្រសិនបើឧក្រិដ្ឋជនទទួលបានពាក្យសម្ងាត់ណាមួយរបស់អ្នក ពួកគេនឹងសាកល្បងប្រើពាក្យសម្ងាត់នោះនៅលើគណនីផ្សេងទៀតផងដែរ។
   - បង្កើតពាក្យសម្ងាត់ល្អ - ធ្វើជាម្ចាស់លើអ៊ីនធឺណិតរបស់អ្នក
- បើកការផ្ទៀងផ្ទាត់ពីរកត្តា (have two-factor authentication turned on)
   - នេះគឺជាព័ត៌មានបន្ថែមមួយទៀត - ជាធម្មតាលេខកូដនៅលើទូរស័ព្ទរបស់អ្នក - អ្នកត្រូវចូលទៅក្នុងគេហទំព័រមួយ។
   - បច្ចេកទេសនេះគឺមានប្រសិទ្ធិភាពខ្លាំង ហើយអាចបញ្ឈប់ការប៉ុនប៉ងភាគច្រើនដើម្បីចូលទៅក្នុងគណនីរបស់អ្នក។
   - យើងសូមណែនាំឱ្យប្រើ 'កម្មវិធីផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវ' (authenticator app) ដែលនេះត្រូវបានគាំទ្រមួយដែរ។
   - បង្កើតការផ្ទៀងផ្ទាត់ពីរកត្តា (2FA) - ធ្វើជាម្ចាស់លើអ៊ីនធឺណិតរបស់អ្នក
- រក្សាភាពឯកជននៅលើអ៊ីនធឺណិត
   - ជម្រើសដ៏ល្អបំផុតដើម្បីរក្សាសុវត្ថិភាពនៅលើប្រព័ន្ធផ្សព្វផ្សាយសង្គមគឺត្រូវបើកការកំណត់ឯកជនភាពនៅក្នុងកុំព្យូទ័ររបស់អ្នក (have your privacy settings turned on)។
   - នេះនឹងបញ្ឈប់មនុស្សចៃដន្យ រួមទាំងឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត មិនអាចមើលការបង្ហោះរបស់អ្នក ឬផ្ញើសារមកអ្នកបានទេ។
   - ការពារភាពឯកជនរបស់អ្នកនៅលើអ៊ីនធឺណិត - ធ្វើជាម្ចាស់លើអ៊ីនធឺណិតរបស់អ្នក
- រក្សាអ្វីៗគ្រប់យ៉ាងឱ្យបានថ្មីៗបំផុត។
   - នៅពេលអ្នកធ្វើបច្ចុប្បន្នភាព (update) ទូរស័ព្ទ កុំព្យូទ័រ ឬកម្មវិធីកម្មវិធីកុំព្យូទ័ររបស់អ្នក នេះដោតខ្សែចូលជិតរន្ធណាមួយដែលអាចមាននៅក្នុងសុវត្ថិភាពកុំព្យូទ័រផងដែរ។
   - ឧក្រិដ្ឋជនតែងតែស្វែងរកមធ្យោបាយដើម្បីចូលទៅ និងធ្វើបច្ចុប្បន្នភាពជួសជុលភាពងាយរងគ្រោះ។
   - បន្តធ្វើបច្ចុប្បន្នភាពរបស់អ្នក - ធ្វើជាម្ចាស់លើអ៊ីនធឺណិតរបស់អ្នក

- ត្រូវប្រុងប្រយ័ត្នជានិច្ច
    - ដំបូន្មានដ៏ល្អបំផុតគឺត្រូវដឹងពីការបោកប្រាស់ទាំងនេះ ហើយតាមដានពួកគេ ប្រសិនបើឧក្រិដ្ឋជនព្យាយាម និងទាក់ទងអ្នកនៅលើវេទិកាអនឡាញណាមួយ។
    - ប្រសិនបើមានអ្វីមួយដែលគួរឲ្យសង្ស័យ សូមកុំទាក់ទងជាមួយអ្នកដែលបានទាក់ទងមកអ្នក។ ជាពិសេសត្រូវប្រយ័ត្នប្រសិនបើពួកគេសុំលុយ ទោះបីជាពួកគេហាក់ដូចជាមិត្តភាពក៏ដោយ។
    - រកមើលតំណភ្ជាប់ចម្លែកៗ និងអាសយដ្ឋានអ៊ីមែល (ឧទាហរណ៍៖ ធនាគាររបស់អ្នកនឹងមិនផ្ញើអ៊ីមែលមកអ្នកពីគណនី gmail ទេ)។
    - ប្រសិនបើមានការសង្ស័យ សូមទាក់ទងទៅអង្គការដោយផ្ទាល់ ហើយកុំធ្វើតាមតំណភ្ជាប់ណាមួយ ឬលេខទូរស័ព្ទដែលបានផ្ញើមកអ្នក។

តើខ្ញុំធ្វើដូចម្តេចប្រសិនបើខ្ញុំត្រូវបានគេបោកប្រាស់ ឬធ្វើអ្វីមកលើខ្ញុំដែលអាក្រក់ជាងនេះ?

មានកន្លែងជាច្រើនដែលអ្នកអាចទៅសុំជំនួយបាន។
អង្គការទាំងអស់នេះនឹងមិនចែករំលែកព័ត៌មានលម្អិតរបស់អ្នកជាមួយអ្នកណាម្នាក់ផ្សេងទៀតទេ លុះត្រាតែអ្នកផ្តល់ការយល់ព្រមជាមុនសិន។

- អ្នកអាចរាយការណ៍អំពីឧប្បត្តិហេតុតាមអ៊ីនធឺណិតទៅ NCSC តាមរយៈវិបផតថល CERT NZ (the CERT NZ portal) ហើយយើងអាចជួយ ឬទាក់ទងអ្នកជាមួយភ្នាក់ងារផ្សេងទៀត៖ [រាយការណ៍ពីឧប្បត្តិហេតុមួយ | CERT NZ]
- ប្រសិនបើអ្នកបានបាត់លុយ អ្នកគួរតែទាក់ទងទៅធនាគាររបស់អ្នកជាបន្ទាន់។
- សារអត្ថបទបោកប្រាស់អាចត្រូវបានបញ្ជូនបន្តដោយមិនគិតថ្លៃទៅកាន់លេខ 7726 ដែលជាសេវាកម្មដែលគ្រប់គ្រងដោយក្រសួងមហាផ្ទៃ (Department of Internal Affairs)។