

រក្សាអង្គការរបស់អ្នកឱ្យមានសុវត្ថិភាពតាមអ៊ីនធឺណិត

ហេតុអ្វីបានជាសន្តិសុខតាមអ៊ីនធឺណិតមានសារៈសំខាន់សម្រាប់ ក្រុមសហគមន៍ និង អង្គការនានា?

ទំព័រនេះមានជំនួយនិងជំហានមួយចំនួនដែលអ្នកអាចអនុវត្តដើម្បីការពារក្រុម ឬអង្គការសហគមន៍របស់អ្នកពីការគំរាមកំហែងសន្តិសុខតាមអ៊ីនធឺណិត។ ទំព័រនេះក៏មានវិធីសាស្ត្រដាច់ដោយឡែកសម្រាប់បុគ្គលម្នាក់ៗ ដើម្បីរក្សាសុវត្ថិភាពលើអ៊ីនធឺណិតផងដែរ។

ជំនួយនេះគឺផ្អែកលើការគំរាមកំហែងទូទៅ និង ធ្ងន់ធ្ងរបំផុត

ការអាប់ដេត (ធ្វើបច្ចុប្បន្នភាព)

រក្សាកម្មវិធីនៅលើឧបករណ៍របស់អ្នកឱ្យទាន់សម័យដើម្បីជួសជុលរន្ធណាមួយនៅក្នុងសុវត្ថិភាព (អ៊ីនធឺណិត)។

- រក្សាឧបករណ៍របស់ក្រុមសហគមន៍ ឬអង្គការរបស់អ្នកឱ្យទាន់សម័យ។ នេះរាប់បញ្ចូលទាំងទូរសព្ទ កុំព្យូទ័រ រ៉ោតទ័រវ៉ាយហ្វាយ (WiFi routers) និងអ្វីៗផ្សេងទៀតដែលភ្ជាប់អ៊ីនធឺណិតរួមទាំងឧបករណ៍ឆ្លាតវៃផងដែរ។
- ប្រើការអាប់ដេតដោយស្វ័យប្រវត្តិ ប្រសិនបើអាចធ្វើទៅបាន។

ការផ្ទៀងផ្ទាត់ពីរកត្តា (Two-factor authentication / 2FA)

បន្ថែមសុវត្ថិភាពថែមទៀតដល់គណនីរបស់អ្នកដោយទាមទារពាក្យសម្ងាត់ និងជំហានមួយបន្ថែមទៀត ដូចជាលេខកូដពីកម្មវិធីនៅលើទូរស័ព្ទរបស់អ្នកផងដែរ។

- ចំណាំ៖ នេះត្រូវបានគេហៅថាការផ្ទៀងផ្ទាត់ពហុកត្តា (multi-factor authentication / MFA) ការផ្ទៀងផ្ទាត់ពីរជំហាន (two-step verification / 2SV) និងឈ្មោះផ្សេងៗជាច្រើនទៀត។
- បើកកម្មវិធី 2FA លើគណនីក្រុមសហគមន៍ ឬអង្គការរបស់អ្នក។
- ប្រសិនបើអាចធ្វើបាន សូមសាកល្បងប្រើទម្រង់ 2FA ដែលធន់នឹងការបន្លំ (phishing resistant) ដែលមានន័យថាអ្នកមិនអាចចាញ់បោកគេបានទេ។ នេះអាចជាសារូបវន្តសុវត្ថិភាពមួយ ឬអ្វីមួយ ដូចជាស្នាមម្រាមដៃ ឬលេខសម្គាល់មុខ (face ID)។

តាមដានគណនីអនឡាញរបស់អ្នក

ត្រូវប្រាកដថា អតីតសមាជិកមិនរក្សាទុកការចូលប្រើគណនីរបស់ពួកគេ បន្ទាប់ពីចាកចេញពីក្រុមសហគមន៍ ឬអង្គការ។

- ប្រសិនបើអ្នកមានមនុស្សជាច្រើនចូលប្រើគណនីដូចគ្នា សូមប្រាកដថាពួកគេទាំងអស់មានការចូលផ្សេងៗគ្នា (different logins) ហើយអ្នកទាំងអស់នោះបានបើកកម្មវិធី 2FA ឡើង។
- រក្សាបញ្ជីនៃគណនីអ្នកប្រើប្រាស់ទាំងអស់ ហើយបិទដំណើរការណាមួយដែលមិនចាំបាច់ដូចជានៅពេលដែលបុគ្គលិកចាកចេញពីអង្គការរបស់អ្នក។
- រក្សាការចុះឈ្មោះឧបករណ៍ណាមួយដែលអ្នកបានផ្តល់ឱ្យសមាជិករបស់អ្នក ហើយចងចាំថាត្រូវយកមកវិញ ហើយកំណត់ឧបករណ៍ទាំងនោះឡើងវិញឲ្យដូច (ឧបករណ៍ទាំងនោះ) ចេញពីរោងចក្រ (factory reset) ប្រសិនបើបុគ្គលនោះចាកចេញពីអង្គការ។ អ្នកក៏ប្រហែលជាត្រូវផ្លាស់ប្តូរលេខកូដរូបវន្តសម្រាប់ការចូលប្រើប្រាស់អគារផងដែរ។

ពិនិត្យមើលថាតើអ្នកណាដែលអាចចូលប្រើគណនីអនឡាញរបស់អ្នក

មនុស្សនៅក្នុងក្រុម ឬស្ថាប័នរបស់អ្នក គួរតែមានសិទ្ធិចូលប្រើ តែអ្វីដែលពួកគេត្រូវការប៉ុណ្ណោះ។

- ប្រសិនបើគណនីរបស់បុគ្គលណាម្នាក់ត្រូវបានគេ 'hacked' (លួចចូល) ជំហានទាំងនេះអាចកាត់បន្ថយនូវគ្រោះថ្នាក់ដែលអ្នកវាយប្រហារអាចធ្វើបាន។
- ត្រួតពិនិត្យជាប្រចាំ និងលុបការអនុញ្ញាតណាដែលមិនចាំបាច់។

- ប្រសិនបើអ្នកមានគណនី "admin" តែមួយដែលមនុស្សជាច្រើនប្រើ ត្រូវតាមដានគណនី "admin" នោះដើម្បីរកសកម្មភាពដែលមិនធម្មតា។ ព្យាយាមកំណត់ការមានគណនីប្រភេទទាំងនេះ ជាពិសេសសម្រាប់កិច្ចការប្រចាំថ្ងៃ។
- ច្បាប់ទាំងនេះក៏អនុវត្តចំពោះការចូលប្រើរបស់អ្នកគ្រប់គ្រងទៅកាន់ឧបករណ៍ ដូចជា រ៉ោតទ័រ (routers) ជាដើម។

ពិនិត្យមើលកិច្ចសន្យារបស់អ្នកជាមួយអ្នកផ្តល់សេវា

ប្រសិនបើអ្នកបានជួលនរណាម្នាក់ឱ្យដំណើរការសេវាកម្ម IT (អាយធី) សម្រាប់អ្នក។

- ត្រូវប្រាកដថាពួកគេមានការការពារសន្តិសុខតាមអ៊ីនធឺណិត ដើម្បីបំពេញតម្រូវការរបស់ក្រុមសហគមន៍ ឬអង្គការរបស់អ្នក។

ដឹងពីរបៀបដែលគណនី និងប្រព័ន្ធទាំងអស់របស់អ្នកដំណើរការជាមួយគ្នា

ការយល់ដឹងអំពីការតភ្ជាប់ជួយអ្នកឱ្យដឹងពីកន្លែងដែលអ្នកវាយប្រហារអាចចូលទៅបាន។

- ពិនិត្យមើលការតភ្ជាប់រវាងប្រព័ន្ធរបស់អ្នក ឧទាហរណ៍ អ៊ីមែល កន្លែងផ្ទុកឯកសាររបស់ cloud (cloud storage) និង កម្មវិធីសម្រាប់គណនេយ្យជាដើម។
- ពិចារណាប្រើប្រាស់ Virtual Private Network / VPN (បណ្តាញឯកជននិម្មិត) សម្រាប់សុវត្ថិភាពបន្ថែមលើអ៊ីនធឺណិត។ ការប្រើប្រាស់ VPN ជួយលាក់សកម្មភាពអនឡាញរបស់អ្នកពីនរណាម្នាក់ដែលអាចព្យាយាមតាមដានអ្នក។ វិធីនេះគឺល្អណាស់ ប្រសិនបើសមាជិកណាមួយនៃក្រុម ឬអង្គការរបស់អ្នកតភ្ជាប់ពីចម្ងាយ។

ប្រាប់មនុស្សរបស់អ្នកឲ្យមានភាពឆ្លាតវៃ 'អ៊ីនធឺណិតឆ្លាតវៃ'

មនុស្សនៅក្នុងក្រុមសហគមន៍ ឬ អង្គការរបស់អ្នកទំនងជាត្រូវបានកំណត់គោលដៅ ជាងប្រព័ន្ធរបស់អ្នក។

- បណ្តុះបណ្តាលបុគ្គលិកទាំងអស់អំពីសន្តិសុខតាមអ៊ីនធឺណិតជាមូលដ្ឋាន។ គេហទំព័រ Own Your Online (ធ្វើជាម្ចាស់លើអ៊ីនធឺណិតរបស់អ្នក) [Own Your Online | NCSC](#) មានដំបូន្មាន និងគន្លឹះជាច្រើន ដើម្បីជួយរក្សាខ្លួនអ្នកឱ្យមានសុវត្ថិភាពតាមអ៊ីនធឺណិត និងរបៀបស្វែងរកការបោកប្រាស់។

- រំលឹកពួកគេថា នេះមានសារៈសំខាន់សម្រាប់គណនីផ្ទាល់ខ្លួនរបស់ពួកគេ ក៏ដូចជាគណនីដែលពួកគេប្រើសម្រាប់អង្គការរបស់អ្នក។
- [យើងមានការណែនាំសម្រាប់បុគ្គលក្នុងការរក្សាសុវត្ថិភាពលើអ៊ីនធឺណិតផងដែរ។](#)

រៀបចំផែនការសម្រាប់ឧប្បត្តិហេតុ

ការមានផែនការឆ្លើយតបជារឿងសំខាន់ដើម្បីកុំឱ្យមនុស្សមានការភិតភ័យ នៅពេលឧប្បត្តិហេតុកើតឡើង។

- ផែនការឆ្លើយតបឧប្បត្តិហេតុ គួសបញ្ជាក់ថា តើអ្នកណាធ្វើអ្វីក្នុងអំឡុងពេលឧប្បត្តិហេតុមួយ។ គំរូមាននៅទីនេះ (ការគ្រប់គ្រងឧប្បត្តិហេតុ) [Incident Management |NCSC](#)
- រួមបញ្ចូលផែនការសម្រាប់អ្វីដែលត្រូវធ្វើប្រសិនបើទូរស័ព្ទ កុំព្យូទ័រ ឬប្រព័ន្ធផ្សេងទៀតបរាជ័យ។ រក្សាផែនការនេះឱ្យបានទៀងទាត់បំផុត។
- រក្សាព័ត៌មានទំនាក់ទំនងលម្អិតរបស់អ្នកគ្រប់គ្នា នៅពេលចាំបាច់ និងព័ត៌មានលម្អិតបម្រុងទុក ប្រសិនបើវិធីចម្បងក្នុងការទាក់ទងពួកគេត្រូវខូច (ដូចជាអ៊ីមែល)។
- រក្សាទុកផែនការនៅកន្លែងណាមួយនៅខាងក្រៅប្រព័ន្ធរបស់អ្នកផងដែរ ក្នុងករណីដែលអ្នកមិនអាចយកផែនការនោះពីប្រព័ន្ធវិញបាន។