ដំបូន្មានសម្រាប់ការប្រើប្រាស់វ៉ាយហ្វាយសាធារណៈប្រកបដោយសុវត្ថិភាព

ជនអាក្រក់អាចទាញយកអត្តប្រយោជន៍ពីអ្នកតាមអនឡាញបាន។ សូមអានដំបូន្មានដែលត្រូវពិចារណាមួយចំនួនខាងក្រោម ប្រសិនបើអ្នកត្រូវការប្រើប្រាស់វ៉ាយហ្វាយសាធារណៈ។

ដើម្បីឆ្លើយតបទៅនឹងការផ្ទុះឡើងនៃមេរោគកូរ៉ូណានិងការបិទអាជីវកម្មនិងបណ្ណាល័យ ពួកយើងជាច្រើនកំពុងចំណាយពេលវេលាអនឡាញច្រើនឡើងៗ។ ជាលទ្ធផល យើងអាចនឹងត្រូវការប្រើវ៉ាយហ្វាយសាធារណៈ ដើម្បីភ្ជាប់អ៊ីនធឺណិត។ ប្រសិនបើអ្នកយល់ថាខ្លួនអ្នកត្រូវការប្រើវ៉ាយហ្វាយសាធារណៈ សូមពិចារណាលើអនុសាសន៍ ពីប្រធានឯកជនភាពប្រចាំរដ្ឋ ក្នុងការជួយការពារទិន្នន័យរបស់អ្នក ដូចខាងក្រោម៖

១. បញ្ជាក់ថាអ្នកពិតជាមានបណ្តាញត្រឹមត្រូវ។

ត្រូវប្រាកដថាអ្នកកំពុងភ្ជាប់ទៅបណ្តាញត្រឹមត្រូវ។ ជនអាក្រក់អាចបង្កើតបណ្តាញដែលមើលទៅដូចជាគ្មានបង្គគ្រោះថ្នាក់ ដោយផ្អែកលើឈ្មោះរបស់ពួកគេ ប៉ុន្តែតាមពិតគឺនឹងនាំអ្នកឱ្យភ្ជាប់ជាមួយបណ្តាញដែលបង្កើតឡើងដើម្បីមើលការប្រើអ៊ីនធឺណិតរបស់អ្នក។ នេះមានសេចក្តីថា ប្រសិនបើអ្នកបញ្ចូលព័ត៌មានឬពាក្យសម្ងាត់ចូលទៅវេយសាយនានា ហោកយ័រនឹងអាចលួចយកព័ត៌មានរបស់អ្នកបាន។ ដើម្បីការពារពីករណីនេះ សូមអានឈ្មោះបណ្តាញដោយយកចិត្តទុកដាក់បំផុត ហើយប្រសិនបើអាចធ្វើទៅបាន សូមសួរបុគ្គលិកណាម្នាក់ឬពិនិត្យមើលសញ្ញារបស់អាជីវកម្មនោះ ដើម្បីឱ្យប្រាកដថាបណ្តាញនោះស្របច្បាប់។

បណ្តាញពេញនិយម ដូចជាបណ្តាញកាហ្វេដែលធ្លាប់ស្គាល់ ទំនងជាមិនមានការសង្ស័យទេ ពីព្រោះក្រុមហ៊ុននោះកំពុងប្រតិបត្តិការបណ្តាញនេះជាសេវារួមជាមួយអាជីវកម្មរបស់ពួកគេទៅហើយ។

បណ្តាញដែលគេស្គាល់ជាទូទៅមានសុវត្ថិភាពជាងបណ្តាញវ៉ាយហ្វាយឥតគិតថ្លៃចៃដន្យ
ដែលអាចបង្ហាញនៅលើទូរសព្ទរបស់អ្នកនៅកន្លែងសាធារណៈណាមួយ។

២. បិទមុខងារភ្ជាប់ដោយស្វ័យប្រវត្តិ។

ឧបករណ៍ជាច្រើន (ស្មាតហ្វូន លេបថប និងថេប្លេត) មានការកំណត់តំណភាពដោយស្វ័យប្រវត្តិ។
ការកំណត់នេះអនុញ្ញាតឱ្យឧបករណ៍របស់អ្នកភ្ជាប់ទៅនឹងបណ្តាញក្បែរៗបានយ៉ាងងាយស្រួល។
ករណីនេះមិនមានបញ្ហាអ្វីទេជាមួយបណ្តាញដែលទុកចិត្ត ប៉ុន្តែវាក៏អាចភ្ជាប់ឧបករណ៍របស់អ្នកទៅ
នឹងបណ្តាញដែលអាចនឹងមិនមានសុវត្ថិភាពផងដែរ។ អ្នកអាចបិទមុខងារនេះបានតាមរយៈ
មុខងារកំណត់លើឧបករណ៍របស់អ្នក។ សូមរក្សាការកំណត់ទាំងនេះនៅបិទជានិច្ច ជាពិសេស
នៅពេលអ្នកធ្វើដំណើរទៅកន្លែងដែលអ្នកមិនស្គាល់។ ជាវិធានការប្រុងប្រយ័ត្នបន្ថែម អ្នកអាចពិនិត្យមើល
"បំភ្លេចបណ្តាញ" បន្ទាប់ពីប្រើវ៉ាយហ្វាយសាធារណៈបាន។

អ្នកក៏គួរតែត្រួតពិនិត្យ Bluetooth របស់អ្នក ខណៈពេលកំពុងនៅទីសាធារណៈផងដែរ។ តំណភាព
Bluetooth អនុញ្ញាតឱ្យឧបករណ៍ផ្សេងៗប្រាស្រ័យទាក់ទងគ្នាបាន ហើយហេកឃ័រអាចរកមើលសញ្ញា
Bluetooth បើកចំហ ដើម្បីចូលទៅប្រើឧបករណ៍របស់អ្នកបាន។ សូមរក្សាមុខងារនេះលើទូរសព្ទរបស់
អ្នកនិងឧបករណ៍ផ្សេងទៀតឱ្យបិទជានិច្ច នៅពេលអ្នកស្ថិតក្នុងតំបន់ដែលអ្នកមិនស្គាល់។

៣. បិទមុខងារចែករំលែកឯកសារ។

ត្រូវប្រាកដថាបានបិទជម្រើសចែករំលែកឯកសារ ខណៈពេលកំពុងប្រើវ៉ាយហ្វាយសាធារណៈ។ អ្នកអាច
បិទមុខងារចែករំលែកឯកសារពីផ្ទៃចំណូលចិត្តប្រព័ន្ធឬផ្ទាំងបញ្ជាអាស្រ័យលើប្រព័ន្ធប្រតិបត្តិការរបស់អ្នក
។ AirDrop គឺជាឧទាហរណ៍នៃមុខងារចែករំលែកឯកសារដែលអ្នកគួរតែបិទ។ ប្រព័ន្ធប្រតិបត្តិការមួយចំនួន
ដូចជា Windows/កុំព្យូទ័រ នឹងបិទមុខងារចែករំលែកឯកសារជូនអ្នក ដោយជ្រើសរើសជម្រើស
"សាធារណៈ" នៅពេលភ្ជាប់ទៅនឹងបណ្តាញសាធារណៈថ្មីជាលើកដំបូង។

ជំហានដើម្បីបិទមុខងារចែករំលែកឯកសារ

លើកុំព្យូទ័រ៖

1. ទៅកាន់ Network and Sharing Center។
2. បន្ទាប់មក ផ្លាស់ប្តូរការកំណត់ចែករំលែកកម្រិតខ្ពស់។
3. បិទមុខងារចែករំលែកឯកសារនិងម៉ាស៊ីនព្រីន។

សម្រាប់ Macs៖

1. ចូលទៅកាន់ ផ្នែកចំណូលចិត្តប្រព័ន្ធ។
2. ជ្រើសរើស Sharing។
3. ដោះជម្រើសគ្រប់យ៉ាងចោល។
4. បន្ទាប់មកនៅក្នុង Finder សូមចុចលើ AirDrop ហើយជ្រើសរើស Allow me to be discovered by: No One។

សម្រាប់ Ios គ្រាន់តែរក AirDrop នៅក្នុង Control Center ហើយបិទវាទៅ។

៤. ប្រើប្រាស់ VPN។

ពិចារណាដំឡើង VPN (បណ្តាញឯកជននិម្មិត) នៅលើឧបករណ៍របស់អ្នក។ VPN គឺជាជម្រើសដែលមានសុវត្ថិភាពបំផុតសម្រាប់ឯកជនភាពឌីជីថលនៅលើវ៉ាយហ្វាយសាធារណៈ។ វាធ្វើកូដនីយកម្មលើទិន្នន័យរបស់អ្នក នៅពេលវាឆ្លងកាត់ទៅនិងពីឧបករណ៍របស់អ្នក ហើយដើរតួជា "រូង" ការពារមួយ ដើម្បីឱ្យទិន្នន័យរបស់អ្នកមិនអាចមើលឃើញបាន នៅពេលវាឆ្លងកាត់បណ្តាញ។

៥. ការព្រមានរបស់ FBI អំពីគេហទំព័រដែលបានធ្វើកូដនីយកម្ម - HTTPS។

FBI បានព្រមានអំពីវេបសាយដែលមានអាសយដ្ឋានចាប់ផ្តើមជាមួយ "https"។ វត្តមានរបស់ពាក្យ "https" និងរូបសញ្ញាសោគឺដើម្បីសន្មតបង្ហាញថាចរាចរណ៍វេបត្រូវបានធ្វើកូដនីយកម្ម និងថាអ្នកចូលមើលអាចចែកចាយទិន្នន័យបានដោយសុវត្ថិភាព។ ទោះយ៉ាងណា ឧក្រិដ្ឋជនអ៊ិនធឺណិតឥឡូវនេះកំពុងទាញចំណូលពីការទុកចិត្តពីសាធារណជន ដោយបញ្ឆោតឱ្យមនុស្សចូលមើលគេហទំព័រមិនល្អដែលមានបញ្ចូលអក្សរ https និងមើលទៅដូចជាមានសុវត្ថិភាព ដែលធាតុពិតមិនមានឡើយ។

អនុសាសន៍របស់ FBI៖

- សូមកុំជឿទុកចិត្តលើឈ្មោះលើអ៊ីមែល៖ សូមចោទសំណួរអំពីចេតនានៃខ្លឹមសារអ៊ីមែល។
- ប្រសិនបើអ្នកទទួលបានអ៊ីម៉ែលគួរឱ្យសង្ស័យដែលមានបញ្ជាប់ពីបណ្តាញទំនាក់ទំនងដែលស្គាល់មួយ សូមបញ្ជាក់ថាសារនោះពិតជាត្រឹមត្រូវ ដោយហៅទូរសព្ទឬផ្ញើអ៊ីមែលទៅបណ្តាញទំនាក់ទំនងនោះ។ សូមកុំឆ្លើយតបដោយផ្ទាល់ទៅអ៊ីមែលដែលគួរឱ្យសង្ស័យនោះ។

- សូមពិនិត្យកំហុសអក្ខរាវិរុទ្ធឬដែនខុសក្នុងបញ្ហាប់ (ឧទា. ប្រសិនបើអាសយដ្ឋានមួយគួរតែបញ្ចប់ដោយ ".gov" តែបែរជាបញ្ចប់ដោយ ".com" ទៅវិញ)។
- សូមកុំទុកចិត្តវេបសាយ ដោយគ្រាន់តែវាមានរូបសញ្ញាសោឬមានអក្សរ "https" នៅក្នុងរបាអាសយដ្ឋានរបស់កម្មវិធីរុករក។

៦. ការចូលមើលព័ត៌មានរសើបមិនត្រូវបានណែនាំឡើយ។

ទោះបីជាអ្នកមាន VPN ក៏ដោយ ក៏វានៅតែមិនត្រូវបានណែនាំឱ្យ ចូលប្រើគណនីធនាគារផ្ទាល់ខ្លួន ឬទិន្នន័យផ្ទាល់ខ្លួនប្រហាក់ប្រហែលដែលមានលក្ខណៈរសើប ដូចជាលេខសន្តិសុខសង្គម នៅលើបណ្តាញសាធារណៈដែលមិនមានសុវត្ថិភាពដែរ។ សូម្បីតែបណ្តាញសាធារណៈដែលមានសុវត្ថិភាពក៏អាចមានហានិភ័យដែរ។ សូមប្រើការវិនិច្ឆ័យល្អបំផុតរបស់អ្នក ប្រសិនបើអ្នកត្រូវតែចូលប្រើគណនីទាំងនេះនៅលើវ៉ាយហ្វាយសាធារណៈ។ សម្រាប់ប្រតិបត្តិការហិរញ្ញវត្ថុ វាអាចនឹងប្រសើរជាងក្នុងការប្រើមុខងារហាតស្ពតរបស់ស្មាតហ្វូនរបស់អ្នកជំនួសវិញ។

៧. ការពារសុវត្ថិភាព ទល់នឹង មិនការពារសុវត្ថិភាព។

ជាធម្មតា មានបណ្តាញវ៉ាយហ្វាយសាធារណៈពីរប្រភេទគឺការពារសុវត្ថិភាពនិងមិនការពារសុវត្ថិភាព។

បើអាច សូមភ្ជាប់ទៅនឹងបណ្តាញសាធារណៈដែលមានការពារសុវត្ថិភាពគ្រប់ពេល។ បណ្តាញដែលមិនមានការពារសុវត្ថិភាពអាចត្រូវបានភ្ជាប់ដោយគ្មានមុខងារសុវត្ថិភាព ដូចជាពាក្យសម្ងាត់ឬបញ្ជាប់ចូលអ្វីឡើយ។ បណ្តាញដែលមានការពារសុវត្ថិភាពជាធម្មតាតម្រូវឱ្យអ្នកប្រើប្រាស់យល់ព្រមតាមលក្ខខណ្ឌចុះឈ្មោះគណនី ឬវាយបញ្ចូលពាក្យសម្ងាត់ មុនពេលភ្ជាប់ទៅនឹងបណ្តាញ។

៨. សូមរក្សាជញ្ជាំងភ្លើងរបស់អ្នកឱ្យដំណើរការជានិច្ច។

ប្រសិនបើអ្នកកំពុងប្រើលេបថប់ សូមរក្សាជញ្ជាំងភ្លើងរបស់អ្នកឱ្យបើកជានិច្ច នៅពេលកំពុងប្រើវ៉ាយហ្វាយសាធារណៈ។ ជញ្ជាំងភ្លើងដើរតួជារបាំងការពារឧបករណ៍របស់អ្នកពីការគំរាមកំហែងដោយមេរោគទាំងឡាយ។ អ្នកប្រើអាចនឹងបិទជញ្ជាំងភ្លើង Windows ដោយសារតែសារជូនដំណឹងហើយបន្ទាប់មកក៏ភ្លេចវាទៅ។ ប្រសិនបើអ្នកចង់បើកវាឡើងវិញនៅលើកុំព្យូទ័រ នោះសូមចូលទៅកាន់ Control Panel រួច "System and Security" ហើយជ្រើសរើស "Windows Firewall"។ ប្រសិនបើអ្នកប្រើ

Mac សូមចូលទៅកាន់ “System Preferences” បន្ទាប់មក “Security & Privacy” រួចចុច “Firewall” ដើម្បីបើកដំណើរការមុខងារនេះ។

៩. ប្រើកម្មវិធីកម្ចាត់មេរោគ។

ត្រូវប្រាកដថាបានដំឡើងកម្មវិធីកម្ចាត់មេរោគចុងក្រោយបំផុតនៅលើលេបថបរបស់អ្នក។ កម្មវិធីកម្ចាត់មេរោគអាចជួយការពារអ្នក ខណៈពេលកំពុងប្រើវ៉ាយហ្វាយសាធារណៈបាន ដោយស្វែងរកមេរោគដែលអាចចូលក្នុងប្រព័ន្ធរបស់អ្នក ខណៈពេលកំពុងប្រើបណ្តាញរួមបាន។ សារដាស់តឿននឹងព្រមានអ្នកប្រសិនបើមេរោគដែលត្រូវបានស្គាល់ត្រូវបានដំណើរការលើឧបករណ៍របស់អ្នក ឬប្រសិនបើមានសកម្មភាពគួរឱ្យសង្ស័យ ការវាយប្រហារ ឬប្រសិនបើមេរោគចូលក្នុងប្រព័ន្ធរបស់អ្នក។

១០. ប្រើមុខងារផ្ទៀងផ្ទាត់ពីរជាន់ឬពហុជាន់។

សូមប្រើមុខងារផ្ទៀងផ្ទាត់ពហុជាន់ (MFA) នៅពេលភ្ជាប់ចូលទៅវេបសាយជាមួយព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នក។ នេះមានន័យថាអ្នកមានលេខកូដផ្ទៀងផ្ទាត់ទីពីរ (ដោយបានផ្ញើជាសារទៅទូរសព្ទរបស់អ្នក ឬផ្តល់ដោយកម្មវិធីឬឃីជាក់ស្តែងមួយ) ដែលការពារអ្នកបានបន្ថែមទៀត។ ដូច្នេះទោះបីជាហេកយ៉ូវមានឈ្មោះអ្នកប្រើនិងពាក្យសម្ងាត់ក៏ដោយ ក៏ពួកគេមិនអាចចូលប្រើគណនីរបស់អ្នកបានដែរ បើគ្មានលេខកូដផ្ទៀងផ្ទាត់នោះ។

១១. តាមដានឧបករណ៍ផ្ទាល់ខ្លួនរបស់អ្នកជាប់ជានិច្ច។

សូមកុំ ទុកលេបថប ថេប្លេត ឬស្មាតហ្វូនរបស់អ្នកចោល ដោយមិនមានអ្នកមើល នៅទីសាធារណៈ ឬក្នុងយានជំនិះណាមួយឱ្យសោះ។ ទោះបីជាអ្នកកំពុងប្រយ័ត្នប្រយែងនៅលើបណ្តាញវ៉ាយហ្វាយក៏ដោយ ក៏វានឹងមិនរារាំងនរណាម្នាក់ពីការលួចយកទ្រព្យសម្បត្តិរបស់អ្នកឬលួចមើលព័ត៌មានរបស់អ្នកបានដែរ។ ត្រូវដឹងពីជម្លដ្ឋានជុំវិញអ្នក ហើយយកចិត្តទុកដាក់អំពីមនុស្សជុំវិញអ្នក។

១២. ដំបូន្មានសុវត្ថិភាពអនឡាញផ្សេងទៀត។

នេះគឺជាដំបូន្មានមួយចំនួន ដើម្បីរក្សាសុវត្ថិភាពអនឡាញ ជាពិសេសប្រសិនបើអ្នកកំពុងប្រើតំណភ្ជាប់វ៉ាយហ្វាយសាធារណៈ៖

- ប្រើពាក្យសម្ងាត់រឹងមាំ។
- ធ្វើកូដនីយកម្មលើឧបករណ៍របស់អ្នក។
- ប្រយ័ត្ននឹងអ៊ីមែលបោកបញ្ឆោត។
- ប្រយ័ត្នអ្វីដែលអ្នកបង្ហោះលើបណ្តាញសង្គម។
  ព័ត៌មានផ្ទាល់ខ្លួនច្រើនពេកអាចជួយឱ្យពួកហាកយ័រទាយពាក្យសម្ងាត់អ្នកបាន។
- សូមលុបព័ត៌មានចាស់ៗដែលអ្នកលែងត្រូវការឱ្យអស់។
- ប្រសិនបើបណ្តាញមួយស្នើឱ្យអ្នកដំឡើងសុសវែរបន្ថែមឬឧបករណ៍បន្ថែមលើកម្មវិធីរុករក
  សូមកុំភ្លាប់ឱ្យសោះ។
- ត្រូវប្រាកដថា បំណះនិងកម្មវិធីអាប់ដេតចុងក្រោយបំផុតត្រូវបានដំឡើងនៅលើឧបករណ៍របស់អ្នក
  ដើម្បីការពារប្រឆាំងនឹងបញ្ហាដែលស្គាល់ទាំងឡាយ។