ចូរមានការប្រយ័ត្នប្រយែងអំពី
សន្តិសុខព័ត៌មាន
និងសប្បាយចិត្តក្នុងការប្រើប្រាស់
អ៊ិនធឺណិត

ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍
អគ្គនាយកដ្ឋានបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន
នាយកដ្ឋានសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន
www.mptc.gov.kh

ASEAN · JAPAN
Information Security Awareness

ចូរមានការយល់ដឹង | មានសន្តិសុខ | និងប្រយ័ត្នប្រយែង

សន្តិសុខព័ត៌មាន

ប្រើប្រាស់អ៊ិនធឺណិតជាមួយនឹងការជឿជាក់

សន្តិសុខលើទូរសព្ទ័ទំនើប(Smartphone)

- ទូរស័ព្ទទំនើបបានក្លាយជាការពេញនិយមច្រើនឡើងនៅទូទាំងពិភពលោកហើយចំនួនភាគរយនៃ ទូរសព្ទ័ទំនើបនៅក្នុងការ លក់ទូរស័ព្ទចល័តកំពុងតែមានការកើនឡើង។
- ទូរស័ព្ទទំនើបគឺជាឧបករណ៍ដែលមានលក្ខណៈស្មុគស្មាញខ្ពស់បើប្រៀបធៀបទៅនឹងទូរស័ព្ទចល័តធម្មតា។ ពួកវាអាចឱ្យយើង បើកមើលវិបសាយដែលបានរចនាឡើងសម្រាប់កុំព្យូទ័រ និងប្រភេទផ្សេងៗគ្នានៃកម្មវិធីជាច្រើនដែលអាចត្រូវបានទាញយកនិងប្រើ ដោយសេរី។
- កំណែថ្មីដែលបានធ្វើឱ្យទាន់សម័យនៃប្រព័ន្ធប្រតិបត្តិការនិងកម្មវិធីនៅលើទូរស័ព្ទទំនើបត្រូវបានផ្តល់ជាទៀងទាត់។ ភាពទាន់សម័យទាំងនេះអាចផ្តល់នូវមុខងារជាច្រើនហេតុដូចនេះ ហើយទើបបង្កើនឱ្យមានភាពស្មុគស្មាញ ឬជាការធ្វើឲ្យប្រសើរឡើងសន្តិសុខនៃទូរស័ព្ទទំនើប ។

※ OS គឺជាអក្សរកាត់នៃ Operating System (ប្រព័ន្ធប្រតិបត្តិការ) ដែលជាកម្មវិធីសម្រាប់ធ្វើការគ្រប់គ្រងកុំព្យូទ័រឬ ទូរស័ព្ទ។ ឧទាហរណ៍នៅក្នុងកុំព្យូទ័រ, ប្រព័ន្ធប្រតិបត្តិការធ្វើការគ្រប់គ្រងមុខងារច្រើនប្រភេទដូចជាមុខងារ Input/Output (បញ្ចូល/ បញ្ចេញ) ដែលគ្រប់គ្រងការបញ្ចូលពីក្តារចុច (keyboards) ឬលទ្ធផលដើម្បីបង្ហាញ ឬម៉ាស៊ីនបោះពុម្ព។
※ Application គឺជាកម្មវិធីមួយសម្រាប់គោលបំណងជាក់លាក់ដូចជាការវាយអត្ថបទសៀវភៅ ឬការធ្វើបញ្ជី។ អ្នកប្រើអាចជ្រើសកម្មវិធី ដែលពួកគេត្រូវការ ហើយប្រើកម្មវិធីទាំងនោះបន្ទាប់ពីបង្កើតពួកវានៅក្នុងប្រព័ន្ធប្រតិបត្តិការ ដែលមានមុខងារជាមូលដ្ឋានជាទូទៅត្រូវបានប្រើដោយគ្រប់កម្មវិធីទាំងអស់។
※ Update មានន័យថាការធ្វើបច្ចុប្បន្នភាពលើកម្មវិធី ដើម្បីជួសជុលកំហុសឬដើម្បីផ្តល់ជូននូវការធ្វើឱ្យប្រសើរលើមុខងារមួយចំនួន។ អ្នកប្រើប្រាស់អាចរក្សាកម្មវិធីរបស់ពួកគេឱ្យមានភាពទាន់សម័យ ហើយវាក៏ជាការសំខាន់ផងដែរ ក្នុងការធ្វើឱ្យបច្ចុប្បន្នភាពកម្មវិធី ឱ្យមានសន្តិសុខសម្រាប់សន្តិសុខពត៌មាន។

1 ចំនួននៃមេរោគដែលផ្តោតសំខាន់ទៅលើទូរស័ព្ទទំនើបទាំងនោះគឺកំពុងតែកើនឡើង។ ប្រសិនបើឧបករណ៍របស់អ្នកត្រូវបានឆ្លង មេរោគ ទិន្នន័យដែលមានក្នុងសៀវភៅអាសយដ្ឋាន ឬពត៌មានផ្ទាល់ខ្លួនដទៃទៀតអាចនឹងត្រូវបានផ្ញើទៅកាន់ម៉ាស៊ីនមេខាងក្រៅ ឬក៏ការកាត់ទឹកប្រាក់ដោយគ្មានការអនុញ្ញាតអាចនឹងកើតមានឡើង។

2 ក្រៅពីការឆ្លងមេរោគនោះនៅពេលដែលទាញយកកម្មវិធីនានា កម្មវិធីទាំងនោះអាចស្នើសុំដើម្បីអោយប្រើប្រាស់ពត៌មានអំពីឧបករណ៍ ឬសំណើរសុំទិន្នន័យនៅក្នុងសៀវភៅអាសយដ្ឋានដែលត្រូវបានផ្ញើទៅកាន់ម៉ាស៊ីនមេខាងក្រៅ។ ឧទាហរណ៍ មានករណីនៃកម្មវិធីដែលអះអាងថាត្រូវបានរចនាឡើងដើម្បីបង្កើនគុណភាពថ្មប៉ុន្តែតាមការពិតទៅវាព្យាយាមដើម្បីផ្ញើទិន្នន័យសៀវភៅអាសយដ្ឋានដែលមិនទាក់ទងទៅនឹងការប្រើប្រាស់កម្មវិធីទៅកាគីខាងក្រៅ។

យន្តការឆ្លើយតប៖

- ធ្វើបច្ចុប្បន្នកម្មប្រព័ន្ធប្រតិបត្តិការ កម្មវិធីនិងកម្មវិធីប្រឆាំងមេរោគ នៅលើទូរស័ព្ទទំនើប ឲ្យបានដល់កំណែថ្មីចុងក្រោយគេបំផុត។ ដោយសារតែទូរស័ព្ទទំនើបមានពត៌មានអំពីសៀវភៅអាសយដ្ឋាន និង ពត៌មានសំខាន់ៗផ្សេង ទៀតភាពប្រុងប្រយ័ត្ន បន្ថែមទៀតគឺជាការចាំបាច់។
- នៅពេលដែលមានការទាញយកកម្មវិធី អ្នកត្រូវតែប្រាកដថាវិបសាយអាចជឿទុកចិត្តនិងអ្នកណាជាផលិតកម្មវិធីនោះ។ ដូចគ្នានេះផងដែរនៅពេលដែលទាញយកកម្មវិធី អ្នកត្រូវធ្វើការពិនិត្យមើលលើកិច្ចព្រមព្រៀងឬលក្ខខណ្ឌនៃសេវាកម្មសម្រាប់ព័ត៌មានដែលប្រមូលបាន និងថាតើវានឹងត្រូវបានប្រើដោយរបៀបណាមុនពេលធ្វើការយល់ព្រមឬប្រើកម្មវិធីទាំងនោះ។

សន្តិសុខបណ្តាញឥតខ្សែ
(Wireless LAN Security)

ក្នុងរយៈពេលប៉ុន្មានឆ្នាំចុងក្រោយនេះកុំព្យូទ័រមានទម្ងន់កាន់តែស្រាលជាងមុនហើយទូរស័ព្ទទំនើបកាន់តែមានការ ពេញនិយមបន្ថែមទៀត ដែលបានបង្កើនល្បឿនក្នុងការប្រើប្រាស់" បណ្តាញឥតខ្សែ" ហើយដែលអនុញ្ញាតឱ្យ យើងភ្ជាប់ទៅកាន់អ៊ីនធឺណិតតាមរយៈការទំនាក់ទំនងឥតខ្សែខាងក្នុង និងក្រៅផ្ទះ ឬការិយាល័យ។

លើសពីសេវាដែលបានបង់ថ្លៃដោយអ្នកផ្តល់សេវា, សេវាកម្មឥតគិតថ្លៃជាសាធារណៈ បានផ្តល់ជូននៅ ឯព្រលានយន្តហោះ ស្ថានីយ៍រថភ្លើង និងអគារពាណិជ្ជកម្មនានាក៏មានការកើនឡើងផងដែរ។

ហានិភ័យនិងការគំរាមកំហែង៖

1 ដោយសារតែបណ្តាញឥតខ្សែនៅក្នុងផ្ទះ ឬការិយាល័យអាចត្រូវបានតភ្ជាប់ដោយសេរីនៅក្នុងតំបន់ដែល គ្របដណ្តប់ដោយរលកវិទ្យុ, វាល់ទំនាក់ទំនងអាចត្រូវបានគេលួចចាប់យក ដ៏ាបណាទាល់តែមានវិធានការ សន្តិសុខត្រូវបានយកបានយកមកអនុវត្តន៍អោយបានត្រឹមត្រូវ។

2 ដូចគ្នានេះដែរការភ្ជាប់ចូលដោយគ្មានការអនុញ្ញាតទៅក្នុងបណ្តាញឥតខ្សែ អាចឈានទៅដល់ការជ្រាបចេញនូវព័ត៌មានផ្ទាល់ខ្លួនឬព័ត៌មានសំងាត់ក្រុមហ៊ុន ឬក៏អាចត្រូវបានគេប្រើប្រាស់ធ្វើជាឈ្នាន់សម្រាប់ការវាយប្រហារ នៅលើម៉ាស៊ីនមេ ។

យន្តការឆ្លើយតប៖

- ប្រើបណ្តាញឥតខ្សែនៅក្នុងផ្ទះ ឬការិយាល័យ បន្ទាប់ពីមានការតំឡើងទិន្នន័យបំលែង (WPA2) ដូច្នេះហើយទំនាក់ទំនង ដែលមានលក្ខណៈជាអត្ថបទធម្មតា គឺមិនអាចត្រូវបានគេលួចចាប់យក និងជាការការពារមិនឲ្យមានការភ្ជាប់ដោយគ្មានការអនុញ្ញាតដែរ។ ជាមួយគ្នានេះផងដែរ ការកំណត់នូវឧបករណ៍ ដែលអាចភ្ជាប់មកជាមួយបាន (ដោយប្រើប្រាស់ចម្រោះ MAC Address) នៅលើឧបករណ៍ Routers, Access Point, ... ដែលធ្វើឲ្យអ្នកទីបីដែលគ្មានការសិទ្ធ មិនអាចតភ្ជាប់បានទេ។
- នៅពេលប្រើប្រាស់បណ្តាញឥតខ្សែជាសាធារណៈ: ចូរប្រើប្រាស់វិបសាយណាដែលមានការបំលែងដោយ SSL (គឺជាវិបសាយណាដែលចាប់ផ្តើមដោយ https://) និងធ្វើការត្រួតពិនិត្យទៅលើកុំព្យូទ័រដែលអ្នកប្រើប្រាស់ថាតើមុខងារចែករំលែកឯកសារត្រូវបានបិទជាស្រេច មុនពេលប្រាស់សេវាកម្មនេះ។

※ SSL មកពីពាក្យថា Secure Socket Layer ដែលគឺជា Protocol មួយសម្រាប់ធ្វើការបំលែងទិន្នន័យ (encrypted) ដែលធ្វើតាមអ៊ិនធឺណែត។

ការក្លែងបន្លំឱ្យចុច(One-Click Fraud)

ការក្លែងបន្លំឱ្យចុចសំដៅទៅលើការបោកបញ្ឆោតជាទឹកប្រាក់ដោយបង្ហាញលើអេក្រង់នូវរឹកំយប័ត្រសំរាប់ការបង់ថ្លៃឬការប្រើប្រាស់សេវាបង់ថ្លៃបន្ទាប់ពីចុចលើរូបភាពឬដៃអូនៅលើវិបសាយ។

បច្ចុប្បន្ននេះមានការក្លែងបន្លំដោយអោយចុចដោយប្រើប្រាស់កម្មវិធីក្នុងទូរស័ព្ទនិងសេវាកម្មប្រព័ន្ធផ្សព្វផ្សាយសង្គមដូចជាប្លុកជាដើម ។

ក្រៅពីករណី "ការបន្លំអោយចុច" អេក្រង់ដែលបានបង្ហាញនូវរឹកំយប័ត្រអាចត្រូវបានបង្ហាញបន្ទាប់ពីការចុចពីរបីដងដូចជាការ ផ្ទៀងផ្ទាត់អាយុ។ នៅក្នុងករណីមួយចំនួនផ្សេងទៀតបច្ចេកទេសដែលបានប្រើគឺក្លាយជារឿងទុច្ចរិតនិងទំនើបដូចជាអេក្រង់ដែលបង្ហាញនូវរឹកំយប័ត្រនោះមិនបាត់ទៅវិញទេសូម្បីតែបន្ទាប់ពីថាមពល ត្រូវបានបិទនៅលើឧបករណ៍នោះ។

※1 Blog គឺមកពីពាក្យថា Weblog ដែលអ្នកប្រើអាចសរសេរដោមតិឬជាចំណាប់អារម្មណ៍របស់ពួកគេ ដូចជាទិនានុប្បវត្តិនិងអ្នកមក ទស្សនាដោយសេរីអាចផ្តល់នូវមតិយោបល់របស់ពួកគេនៅលើកន្លែងប្រកាសរបស់ពួកគេ។

※2 SNS គឺជាអក្សរកាត់នៃ Social Network Service (សេវាបណ្តាញសង្គម) ដែលផ្តល់នូវវិបសាយដែលមានមុខងារដោប្រើនដូចជាការ បើកអាល់ប៊ុមកំណត់ហេតុប្រចាំថ្ងៃឬរូបថតរបស់យើងដល់សាធារណៈជនឬធ្វើឱ្យនៅក្នុងសហគមន៍ដែលអ្នកប្រើអាចផ្លាស់ប្តូរគំនិត របស់ពួកគេដោយសេរី។

ហានិភ័យនិងការគំរាមកំហែង៖

1 ការចុចលើរូបភាពឬដៃអូតគិតថ្លៃដែលគួរឱ្យចាប់អារម្មណ៍ អាចនាំទៅដល់ការស្នើរឱ្យបងប្រាក់ដែលគ្មានការអនុញ្ញាត ឬទៅ វិបសាយក្លែងបន្លំ។

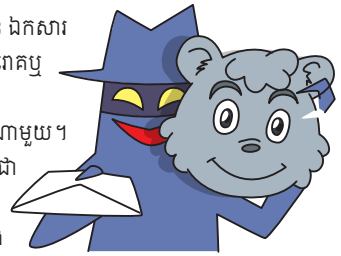
2 មានករណីមួយចំនួនដែល IP Address ឬអ្នកផ្តល់សេវាព័ត៌មានត្រូវបានបង្ហាញនៅក្នុងបញ្ជីនៅលើអេក្រង់កំព្យូទ័រ ដើម្បីធ្វើឱ្យមានអារម្មណ៍ភ័យខ្លាច ដោយសារការធ្វើឱ្យវាមើលទៅដូចថា បុគ្គលដែលត្រូវបានគេកំណត់អត្តសញ្ញាណរួចហើយ។

※3 IP Address គឺជាអាស័យដ្ឋានដែលមានតែមួយគត់ដើម្បីកំណត់អត្តសញ្ញាណឧបករណ៍ ឬក៍កុំព្យូទ័រដែលភ្ជាប់ទៅកាន់អ៊ិនធឺណែត។

យន្តការឆ្លើយតប៖

- ចូរធ្វើការបង្ខាំងការព្យាយាមតភ្ជាប់ទៅកាន់វិបសាយមិនល្អដោយប្រើកម្មវិធីច្រោះ(filtering software) ឬកម្មវិធីសុវត្ថិភាពផ្សេងទៀតចុងក្រោយបំផុត។ ដូចគ្នានេះផងដែរ ត្រូវតែប្រាកដថាទាញយកកម្មវិធីទូរស័ព្ទពីវិបសាយ ដែលជឿទុកចិត្ត។
- ត្រូវដឹងថានៅពេលដែលប្រើកុំព្យូទ័រ ការចុចតែមួយនឹងមិនកំណត់អត្តសញ្ញាណខ្លួនអ្នកទេ ដូច្នេះមិនត្រូវឆ្លើយតបទៅនឹងការប៉ុនប៉ង សម្រាប់ការបង់ប្រាក់នោះទេ។ ចំពោះទូរស័ព្ទទំនើបត្រូវប្រុងប្រយ័ត្នថា អាស្រ័យលើកម្មវិធី, ពត៌មានទុកនៅលើឧបករណ៍ដូចជាព័ត៌មាន ទំនាក់ទំនងផ្ទាល់ខ្លួនរបស់អ្នកឬពត៌មាន ផ្សេងៗទៀតនៅក្នុងសៀវភៅអាសយដ្ឋាន អាចនឹងត្រូវបានបញ្ចេញ។
- ប្រសិនបើអ្នកបានទាក់ទងជាមួយវិបសាយណាមួយ ការស្នើរឱ្យបងប្រាក់ដោយគ្មានការអនុញ្ញាតនៅតែបន្ត ឬប្រសិនបើអ្នកទទួលបាននូវ សេចក្តីបង្គាប់របស់តុលាការ សូមពិគ្រោះជាមួយអាជ្ញាធរមានសមត្ថកិច្ច (ការប្រឹក្សាយោបល់ផ្នែករដ្ឋបាលឬពិគ្រោះយោបល់មេធាវីដោយឥតគិតថ្លៃជាដើម) សំរាប់ជាជំហ៊ុនាន។

ការវាយប្រហារគោលដៅតាមអ៊ីម៉ែល ឬក៏ Spear Phishing Attack



ការវាយប្រហារគោលដៅតាមអ៊ីម៉ែល គឺជាការវាយប្រហារមួយ ដែលអ៊ីមែលនោះត្រូវបានគេធ្វើបន្លំថាបានធ្វើពីមនុស្សដែលស្គាល់គ្នា។ អ៊ីមែលនោះទំនងជាមាន ឯកសារភ្ជាប់មិនល្អ នៅពេលដែលអ្នកប្រើប្រាស់ចុចបើកឯកសារ នោះនឹងអាច ឆ្លងមេរោគឬ Trojan ចូលក្នុងប្រព័ន្ធ។

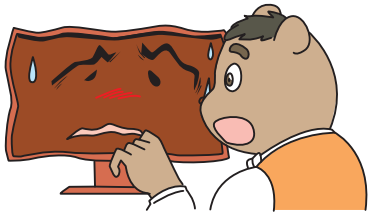
ឧទាហរណ៍ដ៏សាមញ្ញគឺថាគោលដៅគឺជាអង្គការឬអ្នកប្រើប្រាស់ជាក់លាក់ណាមួយ។ អ៊ីម៉ែលភ្ជាប់ជាមួយឯកសារ មានមេរោគត្រូវបានផ្ញើពីអ្នកវាយប្រហារដែលក្លែងជាភាគី ពាក់ព័ន្ធឬជាមិត្តរួមការងាររបស់អង្គការនោះ។

មានករណីដែលត្រូវបានរាយការណ៍ ដែលពាក្យសម្ងាត់ត្រូវបានលួចឬការឆ្លងមេរោគ ដែលបង្កមកពីការវាយប្រហារគោលដៅតាមអ៊ីម៉ែល។

ហានិភ័យនិងការគំរាមកំហែង៖

1 នៅក្នុងការវាយប្រហារកាលពីថ្មីៗនេះ វិធីសាស្ត្រដែលត្រូវបានប្រើក្នុងគោលបំណងដើម្បីបន្លំ ដូចជាអ៊ីម៉ែលមួយ ដែលជឿទុកចិត្ត បានក្លាយជាការស្ទុះគ្រស្មាញនិងមានកម្រិតខ្ពស់។ ឈ្មោះរបស់នាយកដ្ឋាន ឬបុគ្គលដែលមាន ពិតប្រាកដត្រូវបានគេប្រើ បន្ថែមទៅលើការប្រើប្រាស់មាតិកាឬពត៌មានដែលភាគីពាក់ព័ន្ធចង់ដឹង។

2 ប្រសិនបើមេរោគមួយត្រូវបានភ្ជាប់ ការបើកឯកសារភ្ជាប់នឹងធ្វើឲ្យមានការតភ្ជាប់ដោយស្វ័យប្រវត្តិ ទៅកាន់ម៉ាស៊ីនមេខាងក្រៅ និងព័ត៌មាននៅក្នុងកុំព្យូទ័ររបស់អ្នកនឹងត្រូវបានលេចធ្លាយ។



យន្តការឆ្លើយតប៖

- កុំបើកឯកសារភ្ជាប់ភ្ជាប់មកជាមួយអ៊ីមែលណាមួយគួរឱ្យសង្ស័យឬ URL។
- ប្រសិនបើអ្នកបើកអ៊ីម៉ែលដែលគួរឱ្យសង្ស័យរួចហើយ សូមកុំកិតភ័យនិងកុំបិទឧបករណ៍ឲ្យសោះ គាត្រែតែផ្តាច់ខ្សែបណ្តាញនិងសុំជំនួយពីអ្នកគ្រប់គ្រងប្រព័ន្ធ។
- ជំឡើងកម្មវិធីប្រឆាំងមេរោគ និងធ្វើឱ្យប្រាកដថាវាគឺបានធ្វើបច្ចុប្បន្នកម្មជាទៀងទាត់។
- កំណត់ពេលធ្វើបច្ចុប្បន្នកម្មវិធីផ្សេងៗ បន្ថែមទៅលើការធ្វើបច្ចុប្បន្នកម្មប្រព័ន្ធប្រតិបត្តិការ។

ការវាយប្រហារ DDoS

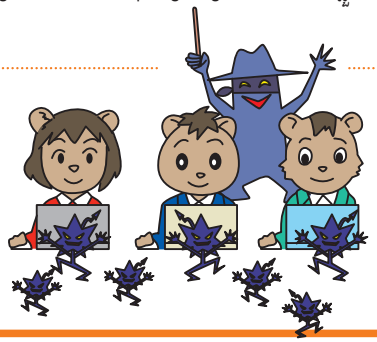
DDoS (Distributed Dinial of Service) គឺជាការវាយប្រហារមួយ ដែលម៉ាស៊ីនមេណាមួយត្រូវបានរំខានពីចំនួនដ៏ធំមួយនៃកំព្យូទ័រពីបណ្តាញជាច្រើន រហូតដល់បណ្តាញទំនាក់ទំនងបានកើនឡើងច្រើនពេក ហើយធ្វើអោយម៉ាស៊ីនមេឈប់ដំណើរតែម្តង ។

※1 Distributed Denial of Service

ហានិភ័យនិងការគំរាមកំហែង៖

1 អ្នកវាយប្រហារដំឡើងនូវកម្មវិធីដើម្បីធ្វើការវាយប្រហារទៅលើកុំព្យូទ័រដែលមិនទាក់ទងនឹងគោលដៅវាយប្រហារចុងក្រោយ ។ ដូច្នេះអ្នកប្រើប្រាស់អាចធ្វើការវាយប្រហារទៅលើម៉ាស៊ីនផ្សេងទៀតដោយមិនដឹងខ្លួន ។

2 កុំព្យូទ័រដែលបានឆ្លងរួចហើយ អាចធ្វើការវាយប្រហារផ្សេងទៀតក្រៅពី DDoS មានដូចជាការចម្លងមេរោគទៅកាន់ កុំព្យូទ័រផ្សេងទៀត, ការធ្វើអ៊ីម៉ែលឥតបានការ ឬធ្វើការកែប្រែមុខមាត់វិបសាយ (web defacement) ។



យន្តការឆ្លើយតប៖

- ធ្វើបច្ចុប្បន្នកម្ម ប្រព័ន្ធប្រតិបត្តិការនៅលើកុំព្យូទ័រ ទូរស័ព្ទ ឬឧបករណ៍ណាផ្សេងៗទៀតដែលនឹងតភ្ជាប់ទៅកាន់អ៊ីនធឺណិតឲ្យដល់ជំនាន់ចុងក្រោយបំផុត ។
- ដំឡើងកម្មវិធីកម្មវិធីប្រឆាំងនឹងមេរោគហើយត្រូវតែប្រាកដថាវាបានធ្វើបច្ចុប្បន្នកម្មបានទៀងទាត់ ។
- កំណត់ពេលធ្វើបច្ចុប្បន្នកម្មវិធីផ្សេងៗ បន្ថែមទៅលើការធ្វើបច្ចុប្បន្នកម្មប្រព័ន្ធប្រតិបត្តិការ ។

ការអនុវត្តន៍ល្អៗនៅពេលយើងប្រើប្រាស់អ៊ិនធឺណែត

ដោយសារតែការកើនឡើងនៃការប្រើប្រាស់ សេវាបណ្តាញសង្គម (Social Network), បញ្ហានៅលើអ៊ិនធឺណែតដែលមិនត្រូវបាន គិតពីមុន បែរជាមានការកើតឡើង ។

មាននូវករណីមួយចំនួនដែលអ្នកប្រើប្រាស់ដាក់ព័ត៌មានផ្ទាល់ខ្លួនលើអ៊ិនធឺណែត ដែលជាកន្លែងដែលព័ត៌មានបុគ្គលត្រូវបានគេ និយាយបង្ខូច អាចត្រូវបានកំណត់អត្តសញ្ញាណ ឬជាកន្លែងដែលក្រុមហ៊ុនចេញសេចក្តីសុំទោសជាសាធារណៈ ។

ហានិភ័យនិងការគំរាមកំហែង៖

1 មានករណីដែលអាចកើតមានឡើង នៅពេលដែលការដាក់ព័ត៌មានធម្មតានៅលើសេវាបណ្តាញសង្គម អាចនាំទៅរកព័ត៌មានផ្ទាល់ ខ្លួនត្រូវបានគេបញ្ចេញ ឬបទបរិហារកេរ្តិ៍របស់អ្នកដទៃ ឬការរំលោភបំពានលើភាពជាឯកជន ។

2 ជាធម្មតាការប្រកាសនៅលើអ៊ិនធើណែត អាចបណ្តាលមានតម្រូវការនៃការបង់ប្រាក់សម្រាប់ការខូចខាត, ដែលត្រូវផ្តន្ទាទោសតាមច្បាប់ ឬឈានដល់ការចាប់ខ្លួន ។

យន្តការឆ្លើយតប៖

- ត្រូវមានការប្រុងប្រយ័ត្នក្នុងការបញ្ចេញព័ត៌មានផ្ទាល់ខ្លួនដែលមិនចាំបាច់នៅលើអ៊ិនធើណែតាមរយៈ: សេវាបណ្តាញសង្គម, ប្លុក ឬ ប្លុកតូចៗ ។ល។ ការដាក់រូបភាពអាចបង្ហាញពត៌មានទីតាំង ដូច្នេះអ្នកគួរតែមានការប្រុងប្រយ័ត្ន ។
- ទោះបីជា នៅលើអ៊ិនធើណែតក៏ដោយ ក៏អ្នកត្រូវគិត គូរដល់ភាពជាឯកជនរបស់មនុស្សដទៃនិងសេចក្តីថ្លៃថ្នូរ និងពិនិត្យមើលព័ត៌មាននោះមុនពេលដាក់បង្ហាញ ។

ការកំណត់និងគ្រប់គ្រងឲ្យបានត្រឹមត្រូវ នូវ ID និង Password

ក្នុងគោលបំណងដើម្បីប្រើប្រាស់អ៊ីអ៊ែម៉ែល ការទិញតាមអ៊ីធឺណិត ដំណើរការគណនីធនាគារតាមអ៊ិនធឺណែត និងសេវាកម្មផ្សេងទៀត នៅលើអ៊ិនធឺណែត ប្រកបដោយសុវត្ថិភាពមានប្រភេទជាច្រើននៃគ្រោងការណ៍ការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវ គឺខណៈពេលមួយដែលពេញនិយមបំផុត គឺជាការបន្សំលេខសម្គាល់ (ID) / ពាក្យសម្ងាត់ (Password)។

មានការកើនឡើងនៅក្នុងការវាយប្រហារតាមអ៊ិនធើណែតដែលមានគោលដៅទៅលើគណនីអ្នកប្រើប្រាស់ ដូចជាលេខសម្គាល់ និងពាក្យសម្ងាត់។

ហានិភ័យនិងការគំរាមកំហែង៖

1 ភាគីទីបីអាចក្លែងខ្លួនជាអ្នក និងបញ្ចេញពត៌មាន ឬបង្កឱ្យមានការខូចខាតដល់រូបិយវត្ថុប្រសិនបើលេខសម្គាល់ ឬពាក្យសម្ងាត់គឺ ជាការរួមបញ្ចូលគ្នាយ៉ាងសាមញ្ញបែបនេះ (ដូចជា 4 ខ្ទង់នៃថ្ងៃខែឆ្នាំកំណើត, ឬ "9999" ជាដើម) ឬប្រសិនបើវាត្រូវបាន គ្រប់គ្រង ដោយមិនមានការប្រុងប្រយ័ត្ន (ឧទហរណ៍ពាក្យសម្ងាត់បានបិទជាប់នឹងអេក្រង់កុំព្យូទ័រដោដើម)។

2 ប្រសិនបើប្រើលេខសម្គាល់ ឬពាក្យសម្ងាត់ដូចគ្នាសម្រាប់វិបសាយច្រើន ហើយបើសិនជាពត៌មានដែលត្រូវបានលេចធ្លាយ ពីវិបសាយមួយ, លទ្ធភាពនៃការក្លាយជាជនរងគ្រោះនៃការវាយប្រហារតាមអ៊ិនធើណែតទៅលើវិបសាយមួយផ្សេង ទៀតនឹងកើនមានឡើង។

3 ប្រសិនបើព័ត៌មានផ្ទាល់ខ្លួន ឬព័តមានដែលមានសារៈសំខាន់ត្រូវហានបញ្ចូលទៅក្នុងកុំព្យូទ័រដែលបើកជាសាធារណៈ ពត៌មានអាចនឹងត្រូវបានគេលួច។

យន្តការឆ្លើយតប៖

- កំណត់ពាក្យសម្ងាត់ជាមួយតួអក្សរដែលមិនអាចទាយទុកជាមុនបាន គឺយ៉ាងហោចណាស់ ៨ តួអក្សរដែលមានលាយលេខ អក្សរធំនិងតូច និងនិមិត្តសញ្ញា។ ជាមួយគ្នានោះដែរត្រូវផ្លាស់ប្តូរពាក្យសម្ងាត់ជាទៀងទាត់។
- កុំចែករំលែកពាក្យសម្ងាត់ជាមួយនឹងមនុស្សផ្សេងទៀត ឬប្រើពាក្យសម្ងាត់ដូចគ្នាសម្រាប់សេវាផ្សេងទៀត។
- ជៀសវាងការវាយបញ្ចូលនូវព័ត៌មានផ្ទាល់ខ្លួន ទៅក្នុងកុំព្យូទ័រសាធារណៈ ដូចជានៅការហ្វេអ៊ិនធើណែត ឬកន្លែងផ្សេងៗទៀត

សារអេឡិចត្រូនិចមិនបានការ (Spam E-mails)

អ៊ីអ៊ែម៉ែលគឺជាឧបករណ៍ទំនាក់ទំនងយ៉ាងងាយស្រួលដោយការផ្ញើនិងការទទួល អាចត្រូវបានអនុវត្តដោយមិនចាំបាច់គិតពីថាអ្នកទទួលនៅកន្លែងណា ឬនៅឆ្ងាយក៏ដោយ។ ទោះជាយ៉ាងណាក្នុងនាមជាអ្នកទទួលអ៊ីអ៊ែម៉ែល អ្នកនឹងទទួលបាននូវសារមិនបានការឬចាំបាច់ជាច្រើន ដែលយើងស្គាល់ថាជា "Spam Mail"។

ដោយសារតែចំនួនសារឥតបានការតាមអ៊ីអ៊ែម៉ែលដ៏ច្រើនត្រូវបានផ្ញើនោះវាធ្វើឲ្យមានបញ្ហាចំពោះអ្នកផ្តល់សេវាកម្ម ដោយសារតែ ឧបករណ៍ប្រើប្រាស់ត្រូវបានដំណើរការច្រើនហួសហេតុដែលបណ្តាលឲ្យមានការពន្យាពេលក្នុងការផ្ញើរ ឬទទួលអ៊ីអ៊ែម៉ែលដទៃទៀត ។

ហានិភ័យនិងការគំរាមកំហែង៖

1 មានករណីខ្លះ ដែលកុំព្យូទ័រធ្វើការបង្កើតនូវចំនួនអាស័យដ្ឋានអ៊ីអ៊ែម៉ែលយ៉ាងច្រើនហើយផ្ញើរសារអ៊ីមែលចេញ។ ដូច្នេះ ការប្រើប្រាស់អាសយដ្ឋានអ៊ីអ៊ែម៉ែលខ្លី និងឈ្មោះដែលពេញនិយមនៅក្នុងអាសយដ្ឋានទាំងនោះ អាចបណ្តាលឱ្យ មានលទ្ធភាពកាន់តែច្រើនឡើងនៃការទទួលបានសារអ៊ីអ៊ែម៉ែលឥតបានការ។

2 អាសយដ្ឋានអ៊ីអ៊ែម៉ែលមួយចំនួនដែលត្រឹមត្រូវ ដើម្បីផ្ញើសារឥតបានការ ត្រូវបានប្រមូលតាមរយៈការចុះឈ្មោះនៃសេវាក្លែងក្លាយមួយដោយឥតគិតថ្លៃ ឬតាមរយៈនីតិវិធីជាវសេវា (unsubscribe)។

3 លើសពីនេះទៀតការបើកឯកសារភ្ជាប់ជាមួយអ៊ីអ៊ែម៉ែល ឬចុចទៅលើតំណភ្ជាប់នៅក្នុងអ៊ីអ៊ែម៉ែលមួយអាចនាំទៅរកការទស្សនា វិបសាយមួយដែលគ្មានការអនុញ្ញាត ឬនាំឱ្យមានការឆ្លងមេរោគ។

យន្តការឆ្លើយតប៖

- អាសយដ្ឋានអ៊ីអ៊ែលគួរតែមានមួយចំនួននៃតួអក្សរច្រើន និងរួមបញ្ចូលលេខដើម្បីធ្វើឱ្យវាពិបាកក្នុងការទស្សន៍ទាយ។
- កុំមានការធ្វេសប្រហែស បញ្ចូលអាសយដ្ឋានអ៊ីអ៊ែលរបស់អ្នកចូលទៅក្នុងវិបសាយ ឬការបង្ហាញអាសយដ្ឋានអ៊ីអ៊ែលរបស់អ្នក នៅលើគេហទំព័រប្រសិនបើវាជាការមិនចាំបាច់ទេ។
- ប្រសិនគឺជាការចាំបាច់ដើម្បីប្រើវិបសាយដែលមិនគួរឱ្យទុកចិត្តទាំងស្រុង វាជាការប្រសើរក្នុងការប្រើប្រាស់អាសយដ្ឋានអ៊ីអ៊ែលឥតគិតថ្លៃ ដែលផ្ទុយទៅនឹងអាស័យដ្ឋានដែលផ្តល់ដោយអ្នកផ្តត់ផ្តង់។

សារអេឡិចត្រូនិចមិនបានការ (Spam E-mails) ❷

សារឥតបានការប្រហែលជាមិនត្រឹមតែបង្កឱ្យមានភាពមិនសប្បាយចិត្ត ចំពោះអ្នកដែលទទួលឬការផ្អាកការងារប៉ុណ្ណោះទេ ប៉ុន្តែវិធី សាស្ត្រនេះ បានក្លាយជាព្យាបាទកាន់តែខ្លាំងឡើង និងមានភាពប៉ិនប្រសព្វទៀតផង ដែលអាចនាំឱ្យអ្នកប្រើប្រាស់ចូលទៅកាន់ វិបសាយដែលគ្មានការអនុញ្ញាត ដែលជាកន្លែងដែលទឹកប្រាក់អាចនឹងត្រូវបានគេលួច ឬតាមរយៈការចូលទៅកំណត់ តម្រងសារឥតបានការក្នុងអ៊ីម៉ែល។

ទូរស័ព្ទទំនើបអាចត្រូវបានឆ្លងដោយមេរោគនៅក្នុងសារឥតបានការ ដោយបញ្ឆោតចំពីចម្ងាយ ដើម្បីផ្ញើនូវចំនួនដ៏ច្រើន នៃសារឥតបានការទៅអ្នកប្រើប្រាស់ដោយមិនដឹងខ្លួន។

❗ ហានិភ័យនិងការគំរាមកំហែង៖

1 មានករណីខ្លះ ដែលកុំព្យូទ័រធ្វើការបង្កើតនូវចំនួន អាស័យដ្ឋាន អ៊ីម៉ែលយ៉ាងច្រើនហើយផ្ញើសារអ៊ីមែលចេញ។ ដូច្នេះការ ប្រើប្រាស់អាសយដ្ឋានអ៊ីម៉ែលខ្លី និងឈ្មោះដែលពេញនិយមនៅ ក្នុងអាសយដ្ឋានទាំងនោះ អាចបណ្តាលឱ្យ មានលទ្ធភាពកាន់តែ ច្រើនឡើងនៃការទទួលបានសារអ៊ីម៉ែលឥតបានការ។

2 អាសយដ្ឋានអ៊ីម៉ែលមួយចំនួនដែលត្រឹមត្រូវ ដើម្បីផ្ញើសារឥតបានការ ត្រូវបានប្រមូលតាមរយៈ ការចុះឈ្មោះ នៃសេវាក្លែងក្លាយមួយដោយឥតគិតថ្លៃ ឬតាមរយៈនីតិវិធីជាវសេវា (unsubscribe)។

3 លើសពីនេះទៀតការបើកឯកសារភ្ជាប់ជាមួយអ៊ីម៉ែល ឬចុចទៅលើតំណភ្ជាប់នៅក្នុងអ៊ីម៉ែលមួយ អាចនាំទៅរកការទស្សនា វិបសាយមួយដែលគ្មានការអនុញ្ញាត ឬនាំឱ្យមានការឆ្លងមេរោគ។

យន្តការឆ្លើយតប៖

- ព្យាយាមបង្ខាំងសារឥតបានការដោយប្រើសេវាកម្មចាត់វិធានការលើសារឥតបានការ ដូចជាមុខងារបដិសេធ ឬមុខងារប្រឆាំងនឹង ការបន្លំ ដោយអ្នកផ្តល់សេវាអ៊ិនធឺណែតឬកម្មវិធីច្រោះ។
- ប្រសិនបើអ្នកទទួលបានសារឥតបានការ ចូរលុបវាដោយមិនចាំបាច់បើកវាទេឡើយ។ គួរបញ្ជាក់ផងដែរថា អ្នកមិន គួរបើក ឯកសារភ្ជាប់ ឬចូលជំណឿការ ភ្ជាប់ពីអ៊ីម៉ែលសង្ស័យ។ វាក៏អាចនឹងមានប្រសិទ្ធិភាពក្នុងការបញ្ជូនសារឥត បានការទៅអ្នកផ្តល់សេវារបស់អ្នកឬទីភ្នាក់ងារសាធារណៈរបស់អ្នក។
- អនុវត្តន៍វិធានការនៅលើទូរស័ព្ទទំនើបក៍ដូចជាកុំព្យូទ័រដែរ។

ការពារទូរស័ព្ទទំនើប (SmartPhone) និងកុំព្យូទ័រ ផ្ទាល់ខ្លួនរបស់អ្នក។

ទូរស័ព្ទទំនើបនិងកុំព្យូទ័រគឺជាឧបករណ៍មានប្រយោជន៍ប៉ុន្តែម្យ៉ាងវិញទៀត ពួកគេប្រឈមមុខនឹងគ្រោះថ្នាក់ជាច្រើនដូចជាការឆ្លងមេរោគកុំព្យូទ័រ។ ចូរចងចាំធ្វើតាមគន្លឹះល្អៗទាំងបីនៃសន្តិសុខពត៌មានដើម្បីជានាបាននូវ សុវត្ថិភាពនិងសន្តិសុខនៅពេលប្រើកុំព្យូទ័រនិងទូរស័ព្ទទំនើប។

គន្លឹះចំបងទាំង៣នៃសន្តិសុខព័ត៌មាន

ដោះស្រាយព័ត៌មានផ្ទាល់ខ្លួនសំខាន់ៗជាមួយនឹងការថែទាំ។

ការពារកុំព្យូទ័ររបស់អ្នកជាមួយនឹងការធ្វើបច្ចុប្បន្នភាពចុងក្រោយបំផុត។

កុំភ្ជាប់ទៅកាន់វិបសាយគួរឱ្យសង្ស័យឬអ៊ីម៉ែលមិនច្បាស់។

វិធានការសន្តិសុខពត៌មានអាចត្រូវបានប្រៀបធៀប ទៅនឹងខ្សែក្រវ៉ាត់ កៅអីរបស់យើងនៅ ពេលដែលយើងចេញទៅ ក្រៅនៅក្នុងឡាននោះ, ហើយវាជាអ្វីដែលយើងមិនត្រូវបំភ្លេចនៅពេលដែលយើងប្រើទូរស័ព្ទឬ កុំព្យូទ័រ។