EFF'S SURVEILLANCE SELF-DEFENSE

របៀបដើម្បីជៀសផុតពីការវាយប្រហារដោយបន្លំ

https://ssd.eff.org/en/about-surveillance-self-defense

LOCALIZATION LAB

https://ssd.eff.org/en/module/how-avoid-phishing-attacks
ត្រួតពិនិត្យចុងក្រោយ៖ ១១-២៦-២០១៩ (**Last reviewed:** 11-26-2018)

នៅលើដំណើរការដើម្បីធ្វើឱ្យប្រសើរឡើងនូវសន្តិសុខឌីជីថលរបស់អ្នក អ្នកអាចនឹងជួបមនុស្សមិនល្អដែលប៉ុនប៉ងធ្វើឱ្យប៉ះពាល់ដល់គោលដៅសន្តិសុខរបស់អ្នក។ យើងហៅអ្នកទាំងនេះថាជាសត្រូវ។ នៅពេលដែលមានគូបដិបក្ខ បញ្ជូនអ៊ីមែល ឬតំណភ្ជាប់ដែលមើលទៅដូចជាធម្មតា ប៉ុន្តែតាមពិត វាមានភាពពិសពុលដែលគេហៅថាការបន្លំ។ ការវាយប្រហារដោយការបន្លំ ជាធម្មតា វាគឺមកជាទម្រង់នៃសារដើម្បីបញ្ចុះបញ្ចូលអ្នកឲ្យ៖

- ចុចលើតំណភ្ជាប់
- បើកឯកសារ
- ដំឡើងកម្មវិធីនៅលើឧបករណ៍របស់អ្នក ឬ
- បញ្ចូលឈ្មោះប្រើប្រាស់ និងពាក្យសម្ងាត់របស់អ្នកទៅក្នុងវេបសាយដែលត្រូវមើលទៅដូចជាគេហទំព័រពិតប្រាកដ។

ការវាយប្រហារដោយបន្លំ អាចបញ្ឆោតអ្នកឱ្យប្រគល់ពាក្យសម្ងាត់របស់អ្នក ឬបញ្ឆោតអ្នកឱ្យដំឡើងមេរោគនៅលើឧបករណ៍របស់អ្នក។ អ្នកវាយប្រហារ អាចប្រើមេរោគដើម្បីគ្រប់គ្រងឧបករណ៍របស់អ្នកពីចម្ងាយ លួចព័ត៌មាន ឬលួចតាមដានអ្នក។

គោលការណ៍ណែនាំនេះ នឹងជួយអ្នកក្នុងការកំណត់អត្តសញ្ញាណការវាយប្រហារដោយបន្លំនៅពេលអ្នកឃើញវា និងរៀបរាប់ពីវិធីជាក់ស្តែងមួយចំនួន ដើម្បីជួយការពារប្រឆាំងនឹងការវាយប្រហារបែបនេះ។

ប្រភេទនៃការវាយប្រហារដោយបន្លំ

ការបន្លំយកពាក្យសម្ងាត់ (មានន័យដូចគ្នានឹងការប្រមូលទិន្នន័យផ្ទាល់ខ្លួនរបស់អ្នក)

អ្នកវាយប្រហារដោយបន្លំ អាចបញ្ឆោតអ្នកឱ្យផ្តល់ឱ្យពួកគេនូវពាក្យសម្ងាត់របស់អ្នក ដោយធ្វើឱ្យអ្នកនូវតំណភ្ជាប់បញ្ឆោត។ អាសយដ្ឋានវេបសាយនៅក្នុងសារប្រហែលជាមានគោលដៅមួយ ប៉ុន្តែវានាំទៅគោលដៅមួយផ្សេងទៀត។ នៅលើកុំព្យូទ័ររបស់អ្នក ជាទូទៅអ្នកអាចមើលគោលដៅរបស់ URL ដោយដាក់កូនកណ្តុរលើតំណភ្ជាប់។ ប៉ុន្តែតំណភ្ជាប់អាចត្រូវបានបន្លំបន្ថែមទៀតជាមួយនឹងតួអក្សរដែលមើលទៅដូចជាពិត ឬដោយប្រើឈ្មោះវេបសាយដែលមានតួអក្សរមួយខុសពីឈ្មោះវេបសាយផ្លូវការរបស់គេ និងអាចនាំអ្នកទៅវេបសាយដែលហាក់ដូចជាចូលទៅកាន់សេវាកម្មដែលអ្នកប្រើប្រាស់ ដូចជា Gmail ឬ Dropbox ជាដើម។ ផ្ទាំងចូលក្លែងក្លាយទាំងនេះ ជាទូទៅមើលទៅមានលក្ខណៈដូចរបស់ពិត ដែលវាជាការទាក់ទាញក្នុងការវាយបញ្ចូលឈ្មោះអ្នកប្រើ និងពាក្យ
សម្ងាត់របស់អ្នក។ ប្រសិនបើអ្នកធ្វើដូច្នេះ អ្នកនឹងផ្ញើព័ត៌មានរបស់អ្នកទៅឱ្យអ្នកវាយប្រហារ។

ដូច្នេះ មុនពេលវាយពាក្យសម្ងាត់ សូមមើលរបារអាសយដ្ឋាននៃកម្មវិធីរុករករបស់អ្នក វានឹងបង្ហាញឈ្មោះគេហទំព័រពិតរបស់ទំព័រ។ ប្រសិនបើវាមិនដូចគ្នានឹងគេហទំព័រដែលអ្នកគិតថាអ្នកចង់ចូលនោះ សូមកុំបន្តទៀត! សូមចងចាំថា ការមើលស្លាកសញ្ញាសម្គាល់ក្រុមហ៊ុននៅលើទំព័រនេះ មិនបញ្ជាក់ថាគេហទំព័រនោះពិតប្រាកដទេ។ នរណាម្នាក់អាចថតចម្លងស្លាកសញ្ញាសម្គាល់ ឬរចនានៅលើទំព័រផ្ទាល់ខ្លួនរបស់ពួកគេ ដើម្បីបញ្ឆោតអ្នក។

អ្នកវាយប្រហារដោយបន្លំមួយចំនួន ប្រើទំព័រដែលមើលទៅដូចជាទំព័រដែលគេពេញនិយម ដើម្បីបន្លំភ្នែកអ្នក៖ https://wwwpaypal.com/ គឺខុសពី https://www.paypal.com/។ ដូចគ្នានេះដែរ https://www.paypal.com/ (ជាមួយអក្សរធំ "i" ជំនួសអក្សរ "L") ខុសពី https://www.paypal.com/។ មនុស្សជាច្រើនប្រើវិធីការបង្រួញ URL ដើម្បីបង្រួញ URL ដែលវែងមកជាងាយស្រួលអាន ឬវាយបញ្ចូល ប៉ុន្តែ URL ទាំងនេះអាចត្រូវបានប្រើដើម្បីលាក់បាំងគោលដៅដែលមានគ្រោះថ្នាក់។ ប្រសិនបើអ្នកទទួលបាន URL ដែលខ្លី ដូចតំណពី Twitter សូមសាកល្បងដាក់វានៅលើវេបសាយ https://www.checkshorturl.com/ ដើម្បីមើលថា តើវាទៅណាឲ្យពិតប្រាកដ។

សូមចងចាំថា វាមានភាពងាយស្រួលក្នុងការបន្លំអ៊ីមែលដែលបង្ហាញអាសយដ្ឋានត្រឡប់មិនពិត។ នេះមានន័យថា ការពិនិត្យមើលអាសយដ្ឋានអ៊ីមែលជាក់ស្តែងរបស់អ្នកផ្ញើ គឺមិនគ្រប់គ្រាន់ដើម្បីបញ្ជាក់ថា អ៊ីមែលមួយណាត្រូវបានបញ្ជូនដោយអ្នកណាពិតប្រាកដនោះទេ។

ការវាយប្រហារបន្លំដែលមានឈ្មោះថា Spearphishing

ការវាយប្រហារដោយបន្លំភាគច្រើនចែកចាយយ៉ាងទូលំទូលាយតាមបណ្តាញផ្សេងៗ។ អ្នកវាយប្រហារអាចផ្ញើអ៊ីមែលទៅមនុស្សរាប់រយ ឬរាប់ពាន់នាក់ដែលអះអាងថា មានវីដេអូគួរឱ្យចាប់អារម្មណ៍ ឯកសារសំខាន់ៗ ឬការទូទាត់វិក្កយបត្រ។

ប៉ុន្តែ ជួនកាលការវាយប្រហារដោយបន្លំ ត្រូវបានកំណត់គោលដៅដោយផ្អែកលើអ្វីដែលអ្នកវាយប្រហារបានដឹងរួចមកហើយអំពីព័ត៌មានរបស់បុគ្គលម្នាក់នោះ។ នេះត្រូវបានគេហៅថា "Sphearphishing" ។ សូមស្រមៃថា អ្នកទទួលអ៊ីមែលពីពូរបស់អ្នកឈ្មោះ បូរីស ដែលសរសេរថា មានរូបភាពកូនៗរបស់គាត់។ ពូ បូរីស ពិតជាមានកូន ហើយមើលទៅដូចជាផ្ញើមកពីអាសយដ្ឋានរបស់គាត់ទៀត ហើយអ្នកបើកវា។ នៅពេលដែលអ្នកបើកអ៊ីមែលមានឯកសារ PDF ភ្ជាប់ វាបានបង្ហាញរូបភាពកូនរបស់ពូ បូរីស ប៉ុន្តែវាក៏ដំឡើងកម្មវិធីមេរោគស្ងាត់ៗនៅលើឧបករណ៍របស់អ្នកដែលអ្នកបានប្រើប្រាស់ ដើម្បីឃ្លាំមើលអ្នក។ ពូ បូរីស មិនបានផ្ញើអ៊ីមែលនោះទេ ប៉ុន្តែអ្នកដែលបានស្គាល់អ្នកថាអ្នកជាក្មួយរបស់ពូ បូរីស (ហើយគាត់មានកូន) ជាអ្នកធ្វើវា។ ឯកសារ PDF ដែលអ្នកបានចុច វាបានចាប់ផ្តើមកម្មវិធី PDF reader របស់អ្នក ប៉ុន្តែវាបានទាញយកប្រយោជន៍ពីក្នុងកម្មវិធីនោះ ដើម្បីដំណើរការកូដផ្ទាល់។ បន្ថែមពីលើការបង្ហាញ PDF ដល់អ្នក វាក៏បានទាញយកមេរោគចូលទៅក្នុងកុំព្យូទ័ររបស់អ្នកផងដែរ។ មេរោគនោះអាចទាញយកទំនាក់ទំនងរបស់អ្នក និងកត់ត្រាអ្វីដែលកាមេរ៉ារបស់អ្នកមើលឃើញ និងកត់ត្រាអ្វីដែលមីក្រូហ្វូនរបស់អ្នកស្តាប់។

មធ្យោបាយល្អបំផុតដើម្បីការពារខ្លួនអ្នកពីការវាយប្រហារដោយបន្លំ គឺមិនត្រូវចុចលើតំណភ្ជាប់ណាមួយ ឬបើកឯកសារភ្ជាប់ណាមួយឡើយ។ ប៉ុន្តែដំបូន្មាននេះ គឺមិនប្រាកដសម្រាប់មនុស្សភាគច្រើននោះទេ។ ខាងក្រោមនេះជាមធ្យោបាយអនុវត្តជាក់ស្តែងមួយចំនួន ដើម្បីការពារប្រឆាំងនឹងការបន្លំ។

របៀបនៃការជួយការពារការប្រឆាំងនឹងការវាយប្រហារដោយបន្លំ

ធ្វើបច្ចុប្បន្នភាពកម្មវិធីរបស់អ្នក

ការវាយប្រហារដោយបន្លំដែលប្រើប្រាស់មេរោគ ជាញឹកញាប់ពឹងផ្អែកលើកំហុសកម្មវិធីដើម្បីទទួលបានមេរោគលើម៉ាស៊ីនរបស់អ្នក។ ជាធម្មតា នៅពេលដែលកំហុសត្រូវបានគេស្គាល់ អ្នកផលិតកម្មវិធីនឹងចេញផ្សាយបច្ចុប្បន្នភាពដើម្បីជួសជុលវា។ មានន័យថា កម្មវិធីចាស់មានកំហុសជាសាធារណៈដែលអាចត្រូវបានប្រើដើម្បីជួយដំឡើងមេរោគ។ ការរក្សាកម្មវិធីរបស់អ្នកឱ្យបច្ចុប្បន្នភាព អាចកាត់បន្ថយហានិភ័យនៃការឆ្លងមេរោគ។

ប្រើប្រាស់កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ដែលបំពេញដោយស្វ័យប្រវត្តិ

កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ដែលបំពេញពាក្យសម្ងាត់ដោយស្វ័យប្រវត្តិ តាមដានគេហទំព័រណាដែលមានពាក្យសម្ងាត់ជាកម្មសិទ្ធិ។ ខណៈដែលវាងាយស្រួលសម្រាប់មនុស្សត្រូវបានហោកបញ្ឆោត ដោយចូលទំព័រក្លែងក្លាយ អ្នកគ្រប់គ្រងពាក្យសម្ងាត់ មិនត្រូវបានហោកបញ្ឆោតតាមរបៀបដូចគ្នានេះទេ។ ប្រសិនបើអ្នកប្រើកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ (រួមបញ្ចូលកម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់ដែលមានស្រាប់នៅក្នុងកម្មវិធីរុករករបស់អ្នក) ហើយវាបដិសេធដើម្បីបំពេញពាក្យសម្ងាត់ដោយស្វ័យប្រវត្តិ អ្នកគួរតែស្ទាក់ស្ទើរ និងពិនិត្យមើលហើយមើលទៀតលើគេហទំព័រដែលអ្នកកំពុងប្រើ។ ប្រសើរជាងនេះទៅទៀត ប្រើពាក្យសម្ងាត់ដែលបង្កើតដោយចៃដន្យ ដូច្នេះអ្នកត្រូវបានបង្ខំឱ្យពឹងផ្អែកលើការបំពេញដោយស្វ័យប្រវត្តិ ហើយទំនងជាមិនវាយបញ្ចូលពាក្យសម្ងាត់របស់អ្នកចូលទៅក្នុងទំព័រក្លែងក្លាយ។

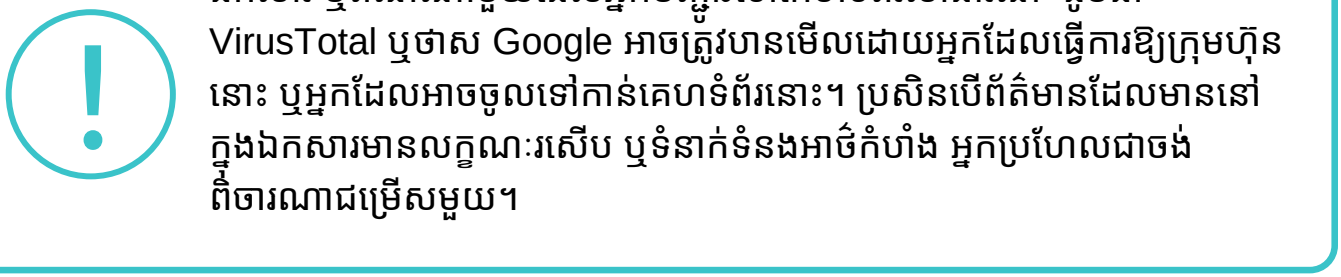
បញ្ជាក់អ៊ីមែលជាមួយអ្នកផ្ញើ

មធ្យោបាយមួយក្នុងការកំណត់ប្រសិនបើអ៊ីមែលគឺជាអ៊ីមែលវាយប្រហារដោយបន្លំ គឺអាចត្រួតពិនិត្យមើលតាមរយៈប៉ុស្តិ៍ផ្សេងៗគ្នាជាមួយអ្នកដែលសង្ស័យថាបានផ្ញើវា។ ប្រសិនបើអ៊ីមែលនោះត្រូវបានគេអះអាងថាបានផ្ញើចេញពីធនាគាររបស់អ្នក កុំចុចលើតំណនៅក្នុងអ៊ីមែល។ ដោយជំនួសទូរសព្ទទៅកាន់ធនាគាររបស់អ្នក ឬបើកកម្មវិធីរុករករបស់អ្នក ហើយវាយបញ្ចូល URL នៃគេហទំព័រធនាគាររបស់អ្នក។ ដូចគ្នានេះដែរ បើសិនជាពូ បូរីស របស់អ្នកផ្ញើអ៊ីមែលដោយភ្ជាប់ឯកសារមក សូមទូរសព្ទទៅគាត់ ហើយសួរគាត់ថា តើគាត់បានផ្ញើរូបភាពកូនៗរបស់គាត់មកទេ មុនពេលអ្នកបើកវា។

បើកឯកសារដែលគួរឱ្យសង្ស័យនៅក្នុងថាស Google

មនុស្សខ្លះរំពឹងថានឹងទទួលបានឯកសារភ្ជាប់ពីមនុស្សដែលមិនស្គាល់។ ឧទាហរណ៍៖ ជាទូទៅ អ្នកសារព័ត៌មានទទួលឯកសារពីប្រភពជាច្រើន។ ប៉ុន្តែវាអាចជាការពិបាកក្នុងការផ្ទៀងផ្ទាត់ថាឯកសារ Word, Excel spreadsheet ឬឯកសារ PDF មិនមានមេរោគ។

ក្នុងករណីទាំងនេះ សូមកុំចុចទ្វេដងលើឯកសារដែលបានទាញយក។ ផ្ទុយទៅវិញ សូមបញ្ជូនវាទៅក្នុងថាស Google ឬកម្មវិធីអានឯកសារអនឡាញផ្សេងទៀត។ វានឹងក្លាយទៅជារូបភាព ឬ HTML ដែលស្ទើរតែនឹងរារាំងវាពីការដំឡើងមេរោគនៅក្នុងឧបករណ៍របស់អ្នក។ ប្រសិនបើអ្នកងាយស្រួលក្នុងការរៀនកម្មវិធីថ្មី ហើយមានឆន្ទៈចំណាយពេលវេលាក្នុងការបង្កើតបរិយាកាសថ្មីសម្រាប់ការអានអ៊ីមែល ឬឯកសារបរទេស នោះមានប្រព័ន្ធប្រតិបត្តិការដែលបានរចនាឡើងដើម្បីកំណត់ពីប្រសិទ្ធភាពនៃមេរោគ។ TAILS គឺជា ប្រព័ន្ធប្រតិបត្តិការលីនុច (Linux-based OS) ដែលលុបខ្លួនវាបន្ទាប់ពីអ្នកប្រើវា។ Qubes គឺជាប្រព័ន្ធប្រតិបត្តិការលីនុចមួយផ្សេងទៀត ដែលបំបែកកម្មវិធីដោយប្រុងប្រយ័ត្ន ដើម្បីកុំឱ្យពួកគេជ្រៀតជ្រែកគ្នាទៅវិញទៅមកដោយកំណត់នូវប្រសិទ្ធភាពនៃមេរោគ។ ប្រព័ន្ធប្រតិបត្តិការទាំងពីរនេះ ត្រូវបានរចនាឡើងដើម្បីធ្វើការលើកុំព្យូទ័រយួរដៃឬកុំព្យូទ័រលើតុ។ អ្នកក៏អាចដាក់តំណភ្ជាប់ដែលមិនទុកចិត្ត និងឯកសារទៅ VirusTotal ដែលជាសេវាកម្មអនឡាញដែលពិនិត្យមើលឯកសារ និងតំណភ្ជាប់ប្រឆាំងនឹងម៉ាស៊ីនកម្ចាត់មេរោគខុសៗគ្នាជាច្រើន ហើយរាយការណ៍ពីលទ្ធផល។ នេះមិនមែនជាកម្មវិធីកម្ចាត់មេរោគទេ ដែលជារឿយៗមិនអាចរកឃើញមេរោគថ្មី ឬការវាយប្រហារគោលដៅនោះទេ ប៉ុន្តែវាប្រសើរជាងគ្មានអ្វីទាំងអស់។



ឯកសារ ឬតំណណាមួយដែលអ្នកបញ្ជូនទៅគេហទំព័រសាធារណៈ ដូចជា VirusTotal ឬថាស Google អាចត្រូវបានមើលដោយអ្នកដែលធ្វើការឱ្យក្រុមហ៊ុននោះ ឬអ្នកដែលអាចចូលទៅកាន់គេហទំព័រនោះ។ ប្រសិនបើព័ត៌មានដែលមាននៅក្នុងឯកសារមានលក្ខណៈរសើប ឬទំនាក់ទំនងអាថ៌កំបាំង អ្នកប្រហែលជាចង់ពិចារណាជម្រើសមួយ។

ប្រើប្រាស់សោនៃការផ្ទៀងផ្ទាត់ពីរកត្តាជាសកល (U2F) នៅពេលចូល

គេហទំព័រខ្លះអនុញ្ញាតឱ្យអ្នកប្រើនិមិត្តសញ្ញាផ្នែករឹងពិសេស ដែលមានសមត្ថភាពកម្រិតខ្ពស់ដើម្បីជៀសវាងការវាយប្រហារបន្លំ។ សោសម្ងាត់ (tokens) ទាំងនេះ (ឬកូនសោ) ទាក់ទងជាមួយកម្មវិធីរុករករបស់អ្នក ដើម្បីបង្កើតអត្តសញ្ញាណនៃគេហទំព័រសម្រាប់ការចូល។ វាត្រូវបានគេហៅថា ការផ្ទៀងផ្ទាត់ពីរ កត្តាជាសកល Universal 2nd Factor ឬ "U2F" ពីព្រោះវាជាវិធីស្តង់ដារដើម្បីតម្រូវឱ្យមានវិធីសាស្ត្រផ្ទៀងផ្ទាត់ទីពីរបន្ថែមលើ ឃ្លាសម្ងាត់ នៅពេលចូល។ អ្នកគ្រាន់តែចូលជាធម្មតា ហើយ (នៅពេលដែលបានបញ្ចូល) ភ្ជាប់សោទៅកុំព្យូទ័រ ឬស្មាតហ្វូនរបស់អ្នក ហើយចុចប៊ូតុងដើម្បីចូល។ ប្រសិនបើអ្នកកំពុងនៅលើបណ្តាញបន្លំ កម្មវិធីរុករកនឹងដឹង និងមិនឱ្យអ្នកចូលជាមួយព័ត៌មានដែលបានបង្កើតឡើងនៅលើគេហទំព័រស្របច្បាប់។ មានន័យថា សូម្បីតែអ្នកក្លែងបន្លំ ហោកបញ្ឆោតអ្នក ហើយលួចឃ្លាសម្ងាត់របស់អ្នកក៏ដោយ ក៏វាមិនធ្វើឱ្យខូចគណនីរបស់អ្នកដែរ។ Yubico (អ្នកផលិតកូនសោបែបនេះ) ផ្តល់ព័ត៌មានបន្ថែមអំពី U2F។

ជាទូទៅ មិនគួរច្រឡំចំពោះការផ្ទៀងផ្ទាត់ពីរកត្តាជាសកល ដែលអាច ឬមិនអាចផ្តល់ការការពារការ បន្លំនោះទេ។

សូមប្រុងប្រយ័ត្នចំពោះសេចក្តីណែនាំតាមរយៈអ៊ីមែល

អ៊ីមែលបន្លំមួយចំនួនអះអាងថាមកពីផ្នែកជំនួយផ្នែកកុំព្យូទ័រ ឬក្រុមហ៊ុនបច្ចេកវិទ្យា ហើយសុំឱ្យអ្នកឆ្លើយតបជាមួយពាក្យសម្ងាត់របស់អ្នក ឬដើម្បីអនុញ្ញាតឱ្យមនុស្សជួសជុលកុំព្យូទ័រចូលប្រើកុំព្យូទ័ររបស់អ្នក ឬបិទដំណើរការលក្ខណៈសុវត្ថិភាពមួយចំនួននៅលើឧបករណ៍របស់អ្នក។ អ៊ីមែលនេះអាចផ្តល់នូវការពន្យល់ជាក់ស្តែងថា ហេតុអ្វីបានជាវាចាំបាច់ ដោយអះអាងថាប្រអប់អ៊ីមែលរបស់អ្នកពេញ ឬកុំព្យូទ័ររបស់អ្នកត្រូវបានគេហេគ (hack)។ ជាអកុសល ការគោរពតាមការណែនាំបន្លំទាំងនេះ អាចអាក្រក់សម្រាប់សុវត្ថិភាពរបស់អ្នក។ សូមប្រុងប្រយ័ត្ន ជាពិសេសមុនពេលផ្តល់ទិន្នន័យបច្ចេកទេសទៅអ្នកណាម្នាក់ ឬធ្វើតាមការណែនាំបច្ចេកទេស លុះត្រាតែអ្នកអាចប្រាកដថាប្រភពស្នើសុំនោះពិតជាត្រឹមត្រូវ។

ប្រសិនបើមាននរណាម្នាក់ធ្វើអ៊ីមែល ឬតំណសង្ស័យមួយទៅអ្នក សូមកុំបើក ឬចុចលើវា រហូតដល់អ្នកបន្ធូរស្ថានការណ៍ដោយមានគន្លឹះខាងលើ ហើយអ្នកអាចជឿជាក់ថាវាមិនមានមេរោគ។