EFF'S SURVEILLANCE SELF-DEFENSE

របៀបធ្វើ៖ ការពារកម្មវិធីទូរស័ព្ទអាយហ្វូន

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

LOCALIZATION LAB

https://ssd.eff.org/en/module/how-encrypt-your-iphone
ត្រួតពិនិត្យចុងក្រោយ៖ ៣-២៦-២០១៨ (**Last reviewed:** 3-26-2018)

បើសិនជាអ្នកមានទូរសព្ទអាយហ្វូន 3GS និងជំនាន់ក្រោយៗដូចជា អាយផត់ថាច់ (iPod Touch) ជំនាន់ទី៣ និងជំនាន់ក្រោយៗ ឬគ្រប់អាយផេត (iPad) អ្នកអាចការពារទិន្នន័យលើឧបករណ៍របស់អ្នក ដោយប្រើកូដនីយកម្ម។ វិធីនេះមានន័យថា បើនរណាម្នាក់បានគ្រប់គ្រងឧបករណ៍អ្នកទាំងស្រុង គេនឹងត្រូវការ លេខសម្ងាត់ពីអ្នកដើម្បីវិកូដនីយកម្មលើទិន្នន័យដែលមាននៅក្នុងឧបករណ៍ រួមទាំងលេខទំនាក់ទំនង សារ ប្រវត្តិការហៅចេញ ចូល និងអ៊ីមែល។

ឧបករណ៍ទំនើបៗរបស់ អេផល (Apple) បានធ្វើកូដនីយកម្មលើទិន្នន័យដោយស្វ័យប្រវត្តិជាមួយនឹងកម្រិត នៃសុវត្ថិភាពផ្សេងៗ។ ប៉ុន្តែអ្នកគួរតែធ្វើកូដនីយកម្មដោយដាក់ឃ្លាសម្ងាត់ ឬលេខកូដដែលគ្មានអ្នកផ្សេងដឹង ដើម្បីការពារកុំឱ្យនរណាម្នាក់លួចយកទិន្នន័យ ដោយការលួចយកឧបករណ៍។ សូមមើលខាងក្រោមពីការ ណែនាំអំពីរបៀបធ្វើកូដនីយកម្ម៖

លើឧបករណ៍ដែលប្រើប្រព័ន្ធប្រតិបត្តិការ iOS 4 - iOS 7៖

១. ចូលទៅ ការកំណត់ទូទៅ (General settings) ហើយរើសយកលេខសម្ងាត់ (Passcode) ឬ អាយថាច់ & លេខសម្ងាត់ (iTouch & Passcode)។
២. ហើយធ្វើតាមការណែនាំដើម្បីបង្កើតលេខសម្ងាត់។

លើឧបករណ៍ដែលប្រើប្រព័ន្ធប្រតិបត្តិការ iOS 8 - iOS 11៖

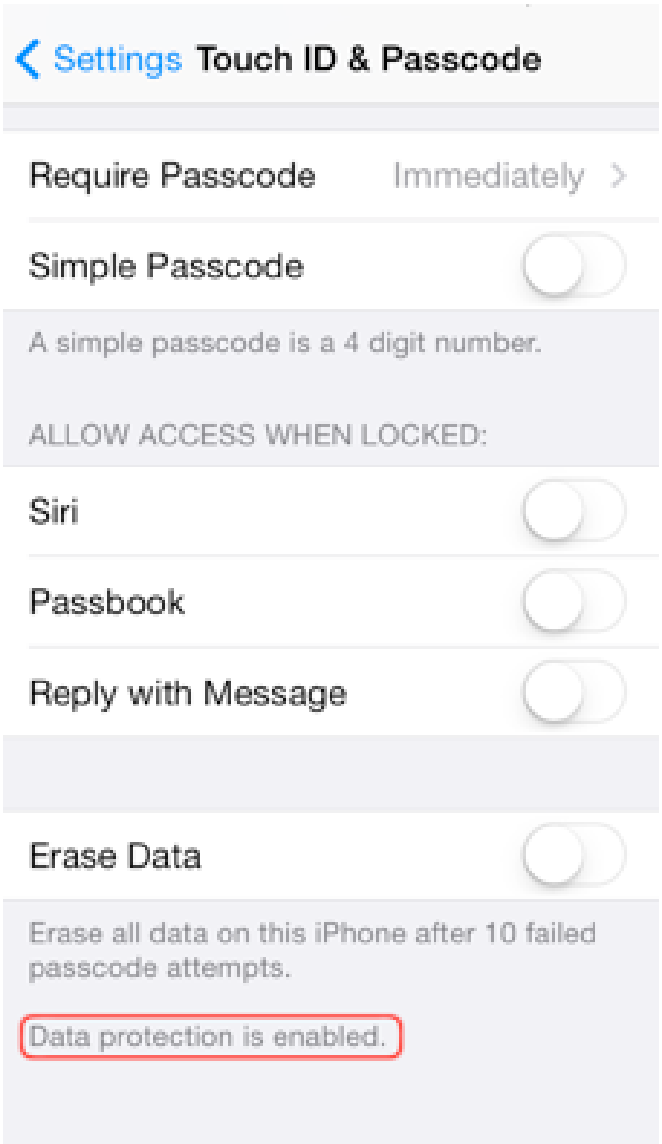
១. បើកម្មវិធី ការកំណត់
២. ចុចលើ Touch ID & Passcode
៣. ហើយធ្វើតាមការណែនាំដើម្បីបង្កើតលេខសម្ងាត់។

ប្រសិនបើឧបករណ៍ដែលប្រើប្រព័ន្ធប្រតិបត្តិការ iOS 8 អ្នកត្រូវបិទ Simple Passcode ដើម្បីបង្កើត លេខកូដដែលវែងជាង ៤ខ្ទង់។ នៅក្នុងប្រព័ន្ធប្រតិបត្តិការ iOS 9 ផលិតផលរបស់អេផល បានកំណត់ឱ្យប្រើ លេខកូដសម្ងាត់ ៦ខ្ទង់ដោយស្វ័យប្រវត្តិ។

បើសិនជាអ្នកជ្រើសរើសលេខកូដសម្ងាត់ជាលេខសុទ្ធ អ្នកនឹងទទួលបានក្តារចុច ជាលេខ នៅពេលអ្នកត្រូវការដោះសោទូរសព្ទ ដែលវាងាយស្រួលក្នុងការវាយជាង អក្សរ ឬសញ្ញាលើក្តារចុចសប្បនិម្មិតតូច។ ទោះជាយ៉ាងណា យើងផ្តល់ យោបល់ឱ្យជ្រើសយកលេខកូដសម្ងាត់ដែលមានលាយលេខ និងអក្សរ ហើយវែង ជាង ៦ខ្ទង់ ដោយសារវាពិបាកក្នុងការជ្រៀតចូល បើទោះជាផ្នែករឹងរបស់ ផលិតផលអេផល ត្រូវបានរចនាឡើងដែលធ្វើឱ្យមានការពិបាកដល់ឧបករណ៍ បំបែកពាក្យសម្ងាត់។

ដើម្បីប្តូរលេខកូដសម្ងាត់តាមបំណងរបស់អ្នក សូមជ្រើសរើស “Passcode Options” និង "Custom Alphanumeric Code"។ ប្រសិនបើអ្នកចង់ផ្លាស់ប្តូរលេខកូដសម្ងាត់ដែលមានរួចហើយ សូមជ្រើសរើសយក “Change Passcode” ហើយបន្ទាប់មកជ្រើសយក “Passcode Options”។ អ្នកគួរតែជ្រើសរើសយកការកំណត់ការចាក់សោ “Require passcode” ទៅ “Immediately” ដូច្នេះឧបករណ៍របស់អ្នកនឹងចាក់សោនៅពេលអ្នកមិនប្រើវា។

នៅពេលអ្នកបានកំណត់នូវលេខកូដសម្ងាត់ហើយ សូមអូសចុះទៅក្រោមនៃផ្ទាំងការកំណត់លេខកូដសម្ងាត់។ លោកអ្នកនឹងបានឃើញនូវសារមួយដែលបង្ហាញថា ការការពារទិន្នន័យត្រូវបានបើកដំណើរការ “Data protection is enabled” ដែលមានន័យថា កូដនីយកម្មនៃឧបករណ៍របស់អ្នកត្រូវបានភ្ជាប់ទៅនឹងលេខកូដសម្ងាត់របស់អ្នក ហើយទិន្នន័យភាគច្រើននឹងត្រូវការលេខកូដដើម្បីដោះសោ។



នេះគឺជាមុខងារមួយចំនួនរបស់ប្រព័ន្ធប្រតិបត្តិការ iOS ដែលអ្នកគួរគិតអំពីការប្រើប្រាស់វា បើសិនជាអ្នកចង់ការពារទិន្នន័យឯកជនរបស់អ្នក៖

- iTunes មានជម្រើសមួយសម្រាប់ចម្លងទិន្នន័យពីទូរសព្ទ ទៅកាន់កុំព្យូទ័រ។ iTunes មិនបានធ្វើកូដនីយកម្មក្នុងសកម្មភាពរបស់អ្នកដោយស្វ័យប្រវត្តិទេ។ ប្រសិនបើអ្នកជ្រើសរើសយក “Encrypt backup” នៅលើផ្ទាំង Summary នៃឧបករណ៍របស់អ្នកនៅក្នុង iTunes នោះ iTunes នឹងធ្វើកូដនីយកម្មលើព័ត៌មានសម្ងាត់ផ្សេងៗទៀតដូចជាពាក្យសម្ងាត់របស់ Wi-Fi និងអ៊ីមែលជាដើម ប៉ុន្តែវាធ្វើកូដនីយកម្មមុនពេលចម្លងទៅកាន់កុំព្យូទ័រ។ ដូច្នេះត្រូវប្រាកដថា អ្នករក្សាទុកពាក្យសម្ងាត់កន្លែងដែលមានសុវត្ថិភាព។ វាជារឿងកម្រដែលអ្នកត្រូវទាញយកទិន្នន័យដែលបានចម្លងទុករបស់យើងមកវិញ តែបើសិនជាអ្នកមិនចាំពាក្យសម្ងាត់ដើម្បីដោះសោទិន្នន័យនៅក្នុងភាពអាសន្ននោះ ទើបជារឿងដែលឈឺចាប់បំផុត។

- បើសិនជាអ្នកចម្លងទិន្នន័យ iCloud នៅលើឧបករណ៍ អេផល អ្នកគួរតែប្រើឃ្លាសម្ងាត់ដែលវែង ដើម្បីការពារទិន្នន័យ ហើយត្រូវទុកឃ្លាសម្ងាត់ឱ្យមានសុវត្ថិភាព។ ខណៈដែលអេផល ធ្វើកូដនីយកម្មលើទិន្នន័យភាគច្រើននៅក្នុងឯកសារចម្លងទុកទាំងនោះ វាក៏ប្រហែលជាអាចប្រើប្រាស់ព័ត៌មាននោះដើម្បីបម្រើឱ្យការអនុវត្តច្បាប់នានាផងដែរ ដោយសារតែក្រុមហ៊ុនអេផល គ្រប់គ្រងសោសម្រាប់កូដនីយកម្មរបស់ iCloud។

- បើសិនជាអ្នកបើកឱ្យមានការការពារទិន្នន័យដូចដែលបានរៀបរាប់ខាងលើ អ្នកនឹងអាចលុបទិន្នន័យលើឧបករណ៍របស់អ្នកបានដោយសុវត្ថិភាព ហើយលឿន។ នៅក្នុងការកំណត់របស់ Touch ID & Passcode អ្នកអាចកំណត់ឱ្យឧបករណ៍របស់អ្នកអាចលុបទិន្នន័យទាំងអស់ បន្ទាប់ពីបរាជ័យដាក់បញ្ចូលលេខកូដចំនួន ១០ដង។ បើអ្នកកំណត់បែបនេះនៅលើឧបករណ៍ អ្នកត្រូវប្រាកដថា ទិន្នន័យក្នុងទូរសព្ទរបស់អ្នកត្រូវបានថតចម្លងទុកក្នុងករណីដែលមានអ្នកណាម្នាក់មានចេតនាបញ្ចូលលេខសម្ងាត់ខុស។

- តាមរយៈ គោលការណ៍អនុវត្តច្បាប់ចាស់របស់ក្រុមហ៊ុន អេផល “ក្រុមហ៊ុនអេផល អាចទាញយកនូវបណ្តុំព័ត៌មានទិន្នន័យសកម្មមួយចំនួនពីឧបករណ៍ iOS ដែលជាប់លេខកូដសម្ងាត់។ ជាពិសេស អ្នកប្រើប្រាស់ដែលបានបម្លែងឯកសារដែលមានសកម្មភាពលើឧបករណ៍ iOS ហើយនៅក្នុងកម្មវិធីដែលមានស្រាប់នៅក្នុងឧបករណ៍ដែលមិនបានធ្វើកូដនីយកម្មដោយប្រើប្រាស់លេខកូដសម្ងាត់។ ក្រុមហ៊ុនអាចទាញយកព័ត៌មានទាំងនេះមកក្រៅ ហើយផ្តល់ទៅឱ្យអ្នកអនុវត្តន៍ច្បាប់។ ក្រុមហ៊ុនអេផល អាចដំណើរការទាញយកទិន្នន័យរបៀបនេះនៅលើឧបករណ៍ដែលមានប្រព័ន្ធប្រតិបត្តិការ iOS ៤ និងប្រព័ន្ធប្រតិបត្តិការចុងក្រោយ។ សូមចាំថា មានតែបណ្តុំព័ត៌មានទិន្នន័យសកម្មប៉ុណ្ណោះដូចជា៖ សារ រូបថត វីដេអូ បញ្ជីទំនាក់ទំនង ការថតសំឡេង និងប្រវត្តិការហៅចេញចូល ដែលអាចត្រូវបានផ្តល់ទៅកាន់អ្នកអនុវត្តន៍ច្បាប់ ឬដឹកាឆែកឆេរផ្លូវការណាមួយ។ ក្រុមហ៊ុនអេផល មិនអាចផ្តល់នូវ៖ អ៊ីមែល ការបញ្ជូលប្រតិទិន ឬក៏ទិន្នន័យពីកម្មវិធីរបស់ភាគីទីបី។”

ព័ត៌មានខាងលើនេះ អនុវត្តតែចំពោះឧបករណ៍ដំណើរការដោយ iOS ដែលកំពុងដំណើរការកំណែមុន iOS 8.0 ប៉ុណ្ណោះ។

- ឥឡូវ ក្រុមហ៊ុនអេផល ហានលើកឡើងថា រាល់ឧបករណ៍ដែលមានប្រព័ន្ធប្រតិបត្តិការចាប់ពី iOS 8.0 ឡើងទៅ ក្រុមហ៊ុនអេផល មិនអាចបើកដំណើរការទាញយកទិន្នន័យហានទេ ព្រោះទិន្នន័យដែលអ្នកអនុវត្តន៍ច្បាប់ត្រូវការនោះ គឺត្រូវហានធ្វើកូដនីយកម្ម ហើយក្រុមហ៊ុនមិនមានសោកូដនីយកម្មនោះទេ។

ចំណុចត្រូវចងចាំ៖ ខណៈដែលក្រុមហ៊ុនអេផល មិនអាចទាញយកទិន្នន័យដោយផ្ទាល់ពីទូរសព្ទ តែបើសិនជាឧបករណ៍អ្នកភ្ជាប់ដំណើរការជាមួយ iCloud ឬហានចម្លងទុកនៅក្នុងកុំព្យូទ័រ នោះមានន័យថា ទិន្នន័យភាគច្រើននឹងអាចទាញយកដោយអ្នកអនុវត្តន៍ច្បាប់។ នៅក្នុងកាលៈទេសៈជាច្រើន កូដនីយកម្មនៅលើ iOS គឺមានប្រសិទ្ធភាពតែនៅពេលដែលឧបករណ៍ទើបតែបើកឡើងវិញ ហើយមិនទាន់ជាប់សោ។ អ្នកវាយប្រហារមួយចំនួន អាចទាញយកទិន្នន័យដែលមានតម្លៃពីអង្គចងចាំរបស់ឧបករណ៍អ្នកនៅពេលវាកំពុងបើក។ (ពួកគេថែមទាំងអាចយកទិន្នន័យនៅពេលវាទើបតែត្រូវហានបិទដែរ)។ សូមចាំថា ប្រសិនបើអាចធ្វើហាន សូមឱ្យប្រាកដថាឧបករណ៍របស់អ្នកត្រូវហានបិទដំណើរការ (ឬហានចាប់ផ្តើមឡើងវិញ ហើយមិនត្រូវហានចាក់សោ) ប្រសិនបើអ្នកជឿថាវាទំនងជាត្រូវហានរឹបអូស ឬលួច។ នៅពេលដែលគោលការណ៍នេះត្រូវហានហោះពុម្ពផ្សាយ ក្រុមហ៊ុនមួយចំនួនហានអះអាងថា ពួកគេអាចបំបែកកូដសម្ងាត់របស់ iPhone សម្រាប់ការអនុវត្តច្បាប់ ប៉ុន្តែព័ត៌មានលម្អិតជុំវិញការអះអាងទាំងនេះ មិនទាន់ច្បាស់លាស់ទេ។

- ប្រសិនបើអ្នកមានការព្រួយហារម្តថាឧបករណ៍របស់អ្នកអាចហាត់បង់ ឬត្រូវហានគេលួច អ្នកអាចកំណត់ឧបករណ៍អេផលរបស់អ្នក ដើម្បីឱ្យវាអាចត្រូវហានលុបចោលពីចម្ងាយដោយប្រើមុខងារ "Find My iPhone" ។ ចំណាំថា វានឹងអនុញ្ញាតឱ្យក្រុមហ៊ុន Apple ស្នើសុំពីចម្ងាយនូវទីតាំងនៃឧបករណ៍របស់អ្នកនៅពេលណាក៏ហាន។ អ្នកគួរតែថ្លឹងថ្លែងនូវអត្ថប្រយោជន៍នៃការលុបទិន្នន័យ ប្រសិនបើអ្នកហាត់បង់ការគ្រប់គ្រងលើឧបករណ៍របស់អ្នកជាមួយនឹងហានិភ័យនៃការបង្ហាញពីទីតាំងរបស់អ្នក។ (ទូរសព្ទចល័តបញ្ជូនព័ត៌មាននេះទៅក្រុមហ៊ុនទូរសព្ទ ខណៈឧបករណ៍ភ្ជាប់ Wi-Fi ដូចជា iPad និង iPod Touch មិនហានធ្វើដូច្នេះ។)