បទបង្ហាញស្តីពី
សុវត្ថិភាពនៃការប្រើប្រាស់បណ្តាញសង្គម

រៀបរៀងដោយ ការិយាល័យគ្រប់គ្រងព័ត៌មានវិទ្យា

មាតិកា

១ ការវាយប្រហាររបស់សាយប័រ (CYBER ATTACK)

❖ អ្វីទៅជាការសាយប័រ (Cyber)?

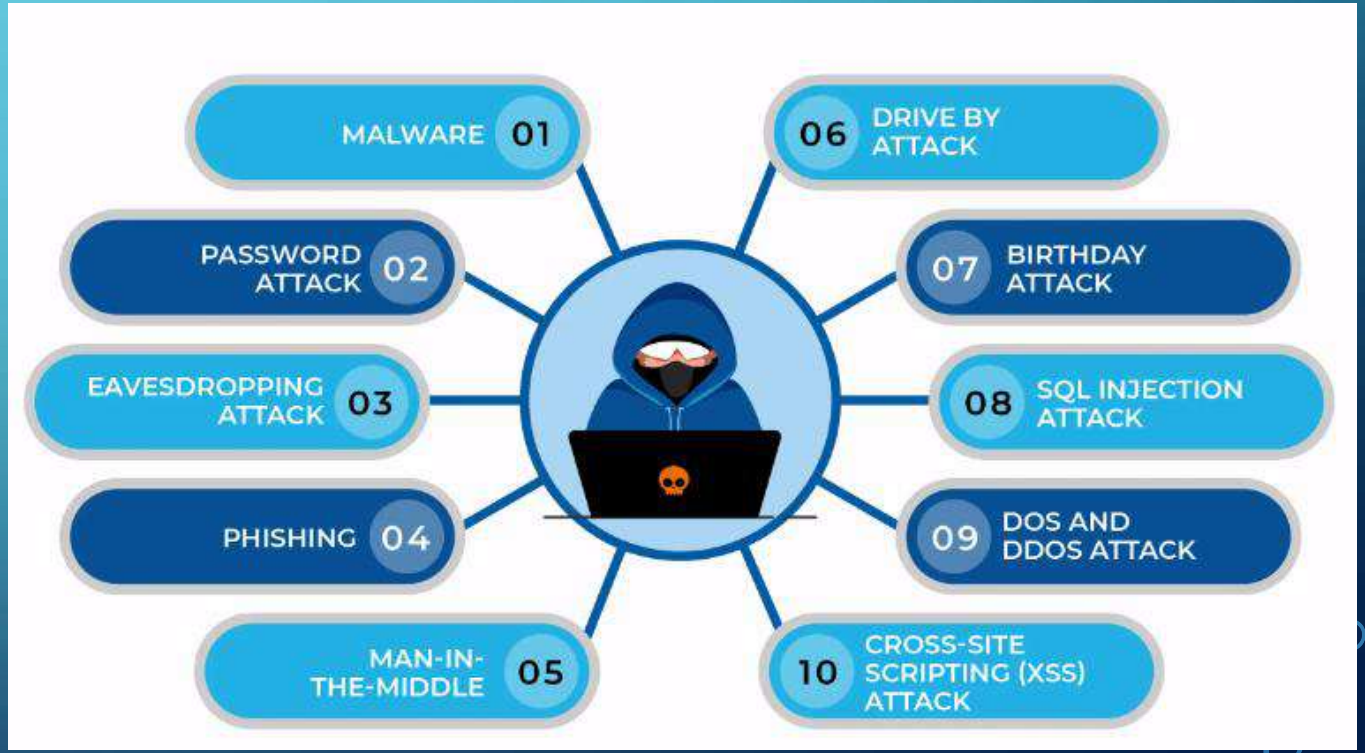
សាយប័រ (Cyber) គឺជាការបង្កើតជាមួយនឹងការផ្តោតអារម្មណ៍នៃបច្ចេកវិទ្យាជឿនលឿនដូចជាកុំព្យូទ័រ អ៊ីនធើណែត ដែលទាក់ទងទៅនឹងកុំព្យូទ័រជាទូទៅនៅលើដែនបច្ចេកវិទ្យាទំនើប។

1. Malware Attack
2. Denial-of-Service (DoS) Attacks
3. Phishing Attack
4. Spoofing
5. Identity-Based Attacks
6. Code Injection Attacks
7. Supply Chain Attacks
8. Insider Threats
9. DNS Tunneling
10. IoT-Based Attacks

ការវាយប្រហាររបស់សាយប័រ (CYBER ATTACK) (ត)

បច្ចុប្បន្នការវាយប្រហាតាមប្រព័ន្ធបច្ចេកវិទ្យាមានគ្រប់រូបភាពទៅតាមសកម្មភាពការងាររបស់ជនរងគ្រោះដែលជាអ្នកប្រើប្រាស់ប្រព័ន្ធបច្ចេកវិទ្យា។ ការវាយប្រហាភាគច្រើនទៅលើអ្នកប្រើប្រាស់បណ្តាញសង្គមដែលមានដូចជា÷

- ការវាយប្រហាតាមរយៈការផ្ញើរលើងក្លែងក្លាយ
- ការវាយប្រហាតាមរយៈសារអេឡិចត្រូនិច
- ការវាយប្រហាតាមរយៈ Message Verify Code OTP
- ការវាយប្រហាតាមរយៈ Password (Brute-force)
- ការវាយប្រហាតាមរយៈគេហទំព័រក្លែងក្លាយ
- ការវាយប្រហាតាមរយៈការបំបែកលេខសម្ងាត់ (hydra)
- ការវាយប្រហាតាមរយៈការ Download - ល -



២ វិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម

ចំណេះដឹងមូលដ្ឋានអំពីការប្រើប្រាស់បណ្តាញសង្គម និងបច្ចេកវិទ្យាឌីជីថលពិតជាមានសារៈសំខាន់សម្រាប់ការរស់នៅក្នុង យុគ-សម័យបច្ចុប្បន្ន។ ការយល់ដឹងអំពីចំណេះដឹងទាំងនេះ នឹងអាចជួយឱ្យអ្នកជៀសផុតពីការវាយប្រហារ និងការលួចទិន្នន័យផ្សេងៗដែលប៉ះពាល់ដល់ផលប្រយោជន៍ និងសុវត្ថិភាពផ្ទាល់ខ្លួន។ ទន្ទឹមនឹងនេះ យើងសង្កេតឃើញថា ក្នុងសង្គមកម្ពុជាបច្ចុប្បន្ន ករណីដែលអ្នកប្រើប្រាស់បណ្តាញសង្គម និងបច្ចេកវិទ្យាឌីជីថល បានទទួលរងនូវការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណែត ដែលឈានដល់ការលួចទិន្នន័យ និងទ្រព្យសម្បត្តិផ្ទាល់ខ្លួនមានច្រើនគួរឱ្យកត់សម្គាល់។ ចំណុចនេះសបញ្ជាក់ថា ប្រជាពលរដ្ឋកម្ពុជាមួយចំនួនធំចាំបាច់ត្រូវពង្រឹងចំណេះដឹងឌីជីថលរបស់ខ្លួនបន្ថែមទៀត។

❖ បណ្តាញសង្គមតេឡេក្រាម Telegram

ដើម្បីការពារគណនីតេឡេក្រាមឱ្យមានសុវត្ថិភាពសូមអនុវត្តដូចខាងក្រោម÷

១. ប្រើមុខងារផ្ទៀងផ្ទាត់ពីរជំហាន (Enable two-step-verification)

២. បិទលើមុខងារ People Nearby

៣. ពិនិត្យមើល Active Sessions

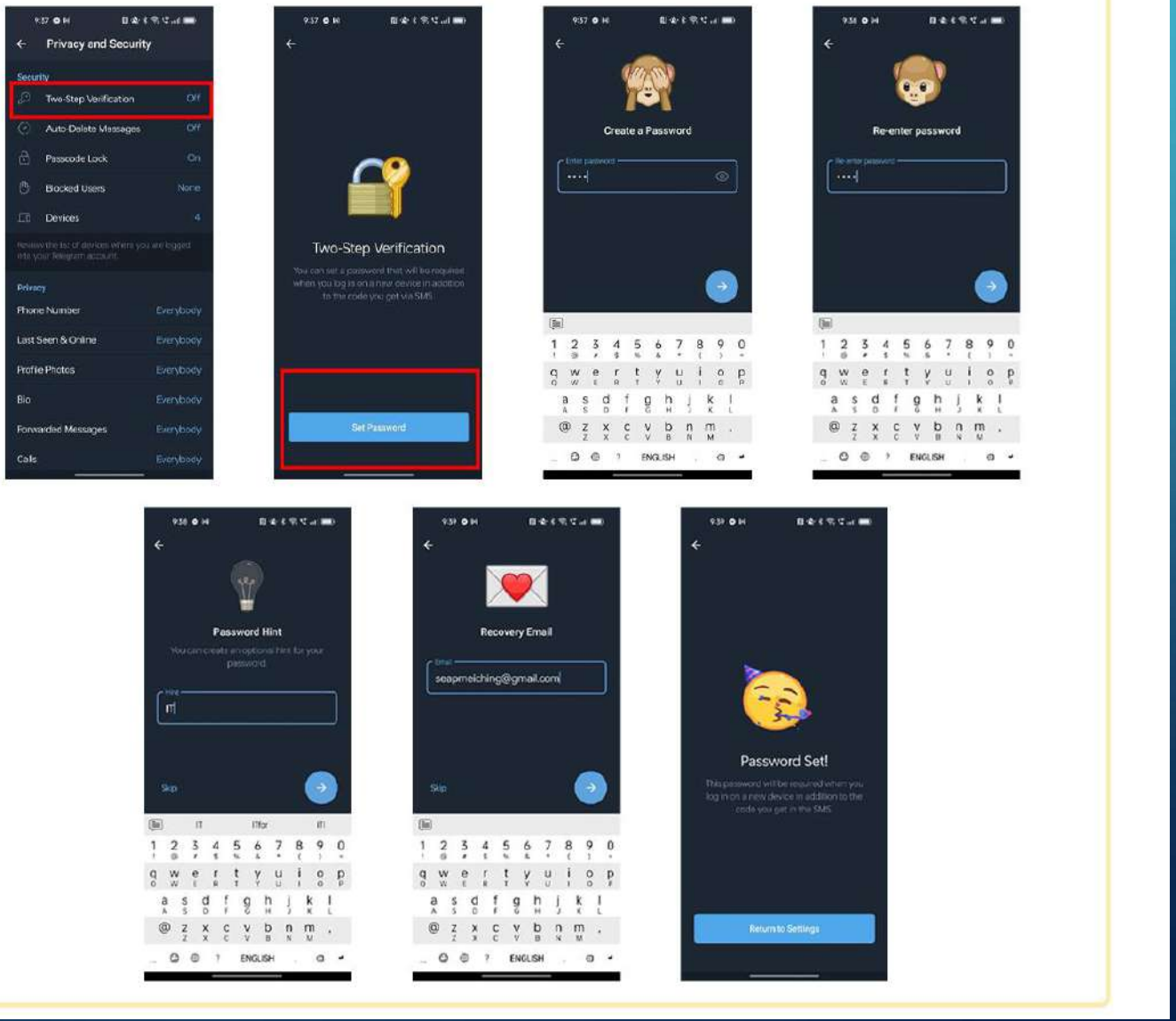
៤. បដិសេធនឹងសារក្លែងក្លាយ

៥. ប្រើពាក្យសម្ងាត់រឹងមាំ

៦. ប្រើមុខងារ Passcode Lock

២ វិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

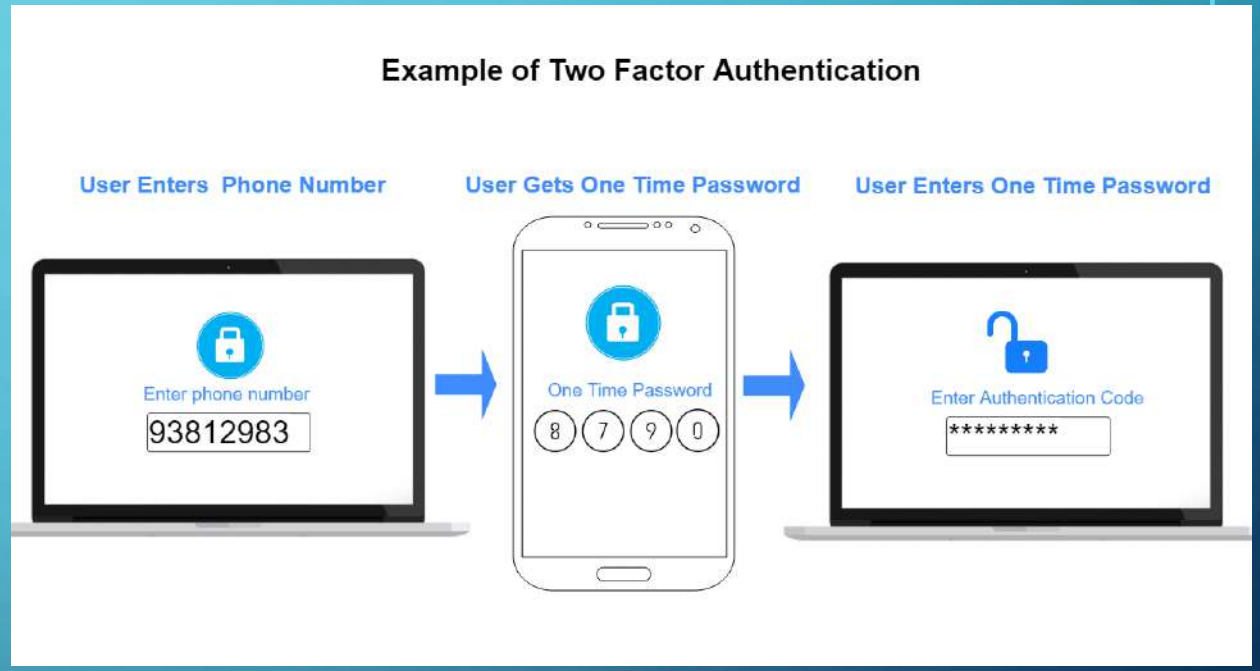
9. Enable two-step verification



២ វិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

- ស្វែងយល់អំពី 2 Factor Authentication (2FA)

2FA មាន២ទម្រង់ ដែលទម្រង់ទី១÷ គឺជាកំណត់អត្តសញ្ញាណដែលមានដូចជា Password ឬ PIN។ ទម្រង់ទី២÷ គឺជាការកំណត់អត្តសញ្ញាណដែលមានដូចជា Security Token ឬ Mobile Device (Authenticator app) ដែលអាចទទួលបានពាក្យសម្ងាត់តែម្តង (one time password) តាមរយៈ App ឬក៏ Text Message។



- អត្ថប្រយោជន៍នៃការប្រើប្រាស់ 2FA

✓ 2FA ធ្វើឱ្យអ្នកប្រើប្រាស់ដែលគ្មានការអនុញ្ញាតក្នុងការចូលប្រើប្រាស់គណនីរបស់អ្នកមានភាពលំបាកក្នុងការ Login។

✓ ជួយការពារប្រឆាំងនឹងការគំរាមកំហែងទូទៅដូចជាការវាយប្រហាតាមរយៈ Phishing Attack និង Password theft។

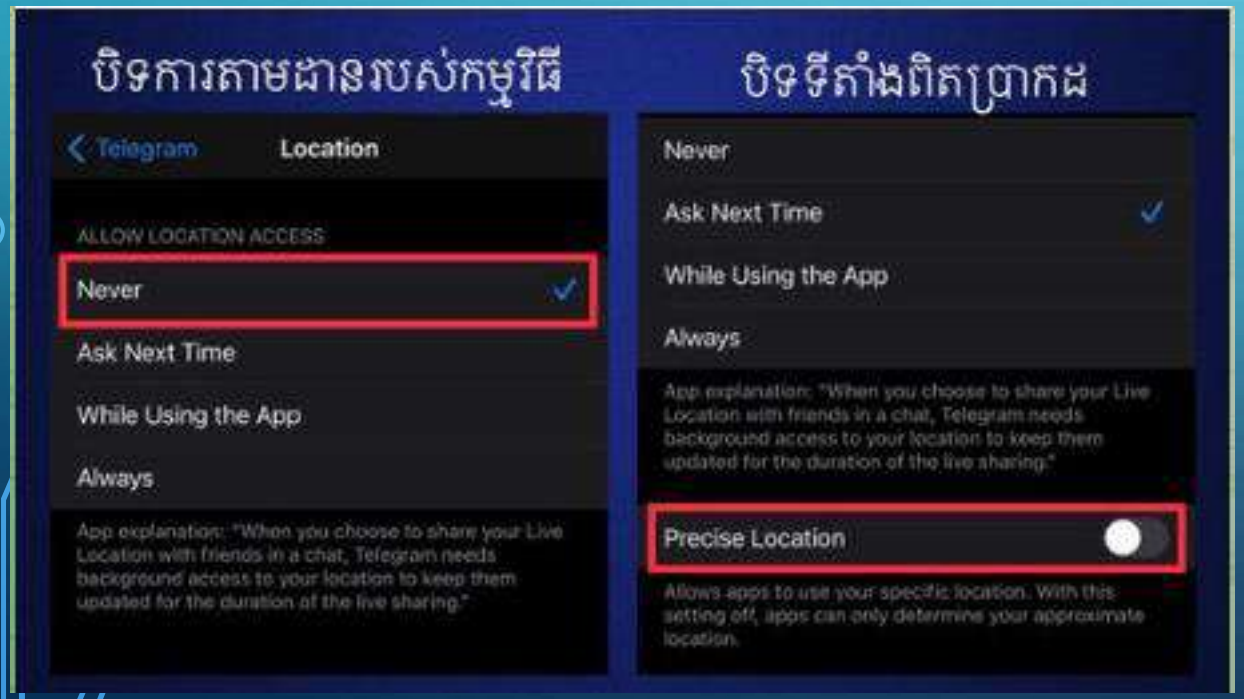
✓ អាចផ្តល់នូវកម្រិតបន្ថែមនៃការធានាដែលមានតែអ្នកប្រើប្រាស់ផ្ទាល់ (ម្ចាស់គណនី) ដែលមានការអនុញ្ញាតចូលប្រើ Sensitive information។

២ ទិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

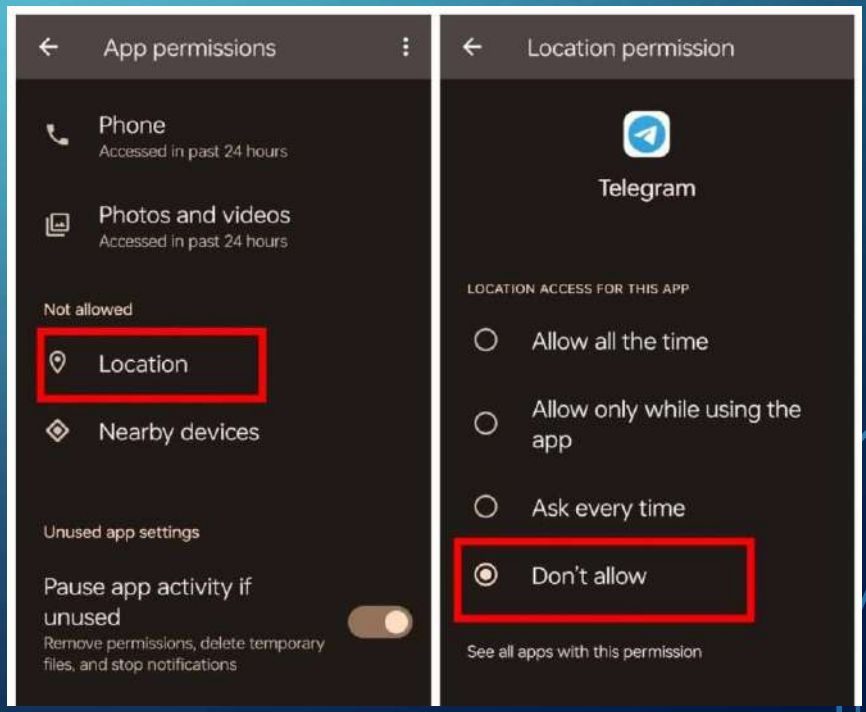
២. បិទលើមុខងារ People Nearby

សូមមានការប្រុងប្រយ័ត្នជាមួយនឹងការប្រើប្រាស់មុខងារ “People Nearby” របស់ Telegram ដែលអាចឱ្យជនខិលខូចដឹងទីតាំងពិតប្រាកដរបស់អ្នកបាន ប្រសិនបើលោកអ្នកបើកប្រើមុខងារនេះ គឺដូចគ្នាទៅនឹងការផ្សព្វផ្សាយអាយដ្ឋាន ឬ ទីតាំងរបស់លោកអ្នកនៅលើបណ្តាញទំនាក់ទំនងសង្គម ។ សម្រាប់លោកអ្នកដែលពុំដែលស្គាល់ឬប្រើមុខងារ "People Nearby" នោះ មុខងារនេះគឺដើម្បីអាចឱ្យអ្នកប្រើប្រាស់ធ្វើការទំនាក់ទំនងជាមួយនឹងអ្នកប្រើប្រាស់ដទៃទៀតដែលនៅក្បែរខ្លួន ឬដើម្បីស្វែងរកការពិភាក្សាជាក្រុម ប៉ុន្តែដើម្បីសុវត្ថិភាពសូមលោកអ្នកគួរតែបិទការប្រើប្រាស់មុខងារនេះប្រសិនបើពុំមានការចាំបាច់។

IOS



Android

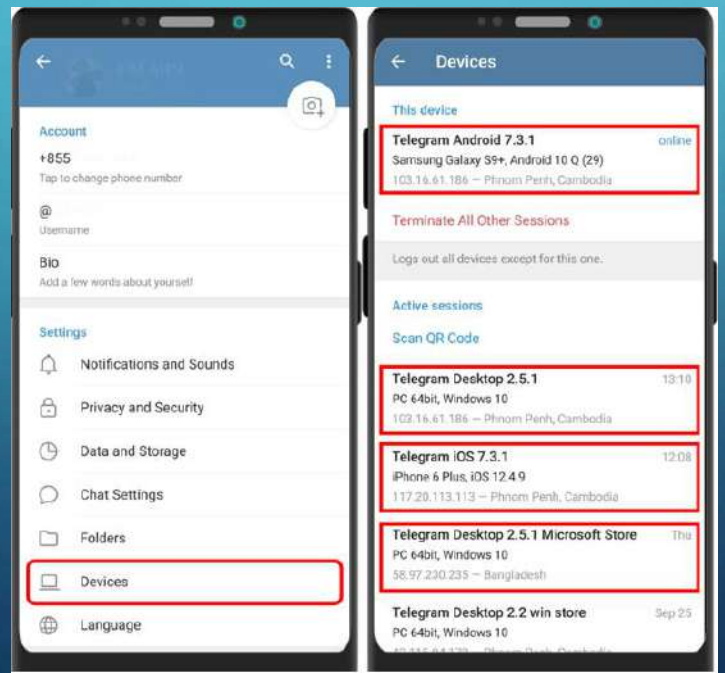


២ ទិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

៣. ពិនិត្យមើល Active Sessions

Active Sessions ជាមុខងារមួយដែលអាចឱ្យអ្នកប្រើប្រាស់មើលរាល់ Sessions ទាំងអស់ដែលកំពុងប្រើប្រាស់គណនីតេឡេក្រាមរបស់ខ្លួន អ្នកប្រើប្រាស់គួរពិនិត្យមើលថាតើមាន Active Sessions ណាមួយដែលគួរឱ្យសង្ស័យដែរឬទេ ដើម្បីពិនិត្យមើល សូមអនុវត្តតាមការណែនាំដូចខាងក្រោម÷

បើកកម្មវិធីតេឡេក្រាមហើយចូលទៅគណនីរបស់អ្នក ចូលទៅកាន់ “Settings” បន្ទាប់មកចុចលើ “Devices” ពិនិត្យលើ Sessions ឬឧបករណ៍ទាំងអស់ដែលកំពុងប្រើគណនីរបស់អ្នក បើឃើញមាន Sessions ឬឧបករណ៍ ដែលសង្ស័យមិនមែនជារបស់អ្នក សូមចុចលើ Sessions ឬឧបករណ៍ ហើយចុចលើ “TERMINATE” បន្ទាប់មកអ្នកត្រូវផ្លាស់ប្តូរលេខសម្ងាត់ផ្ទៀងផ្ទាត់ពីរជំហានហើយ បន្តធ្វើការតាមដានមើល Session ឬឧបករណ៍ តាមការណែនាំខាងលើជារឿយៗដើម្បីពិនិត្យលើការប្រើប្រាស់ដែលមែនជារបស់អ្នក។

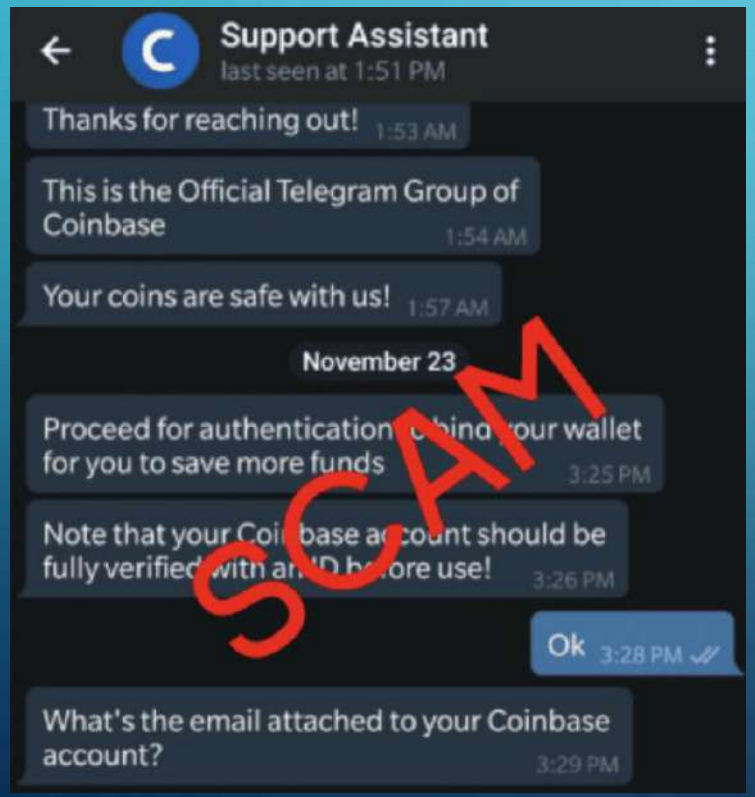


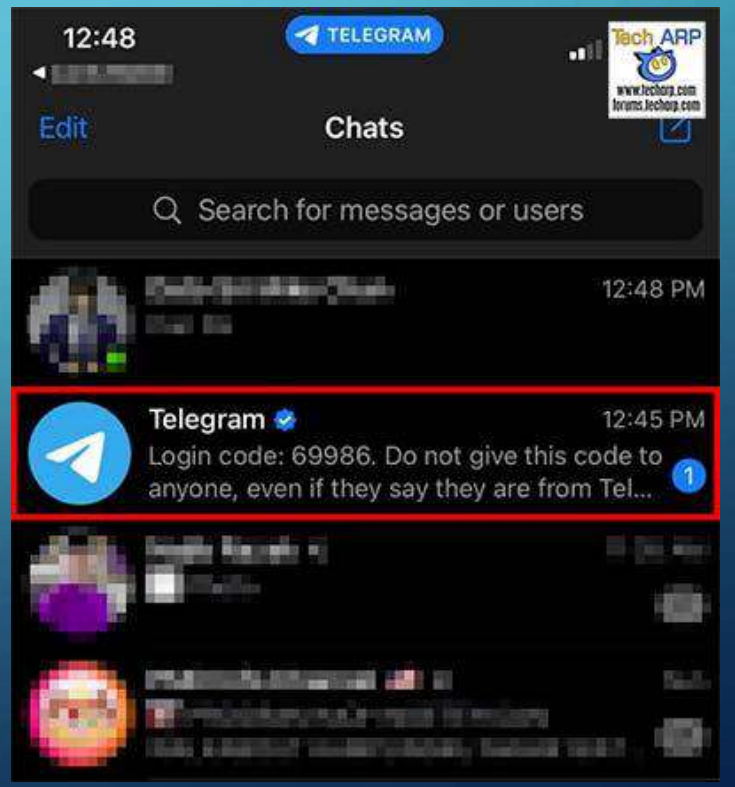
២ វិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

៤. បដិសេធនឹងសារក្លែងក្លាយ

ទី១. បោកបញ្ឆោតឲ្យថតផ្ទាំងសន្ទនាកម្មវិធីTelegram (screenshots chat screen) ÷

ជនអនាមិកប្រើប្រាស់គ្រប់មធ្យោបាយដើម្បីសន្ទនាជាមួយជនរងគ្រោះ (chat) និងទាមទារឲ្យជនរងគ្រោះថតផ្ទាំងសន្ទនានៃកម្មវិធីតេឡេក្រាមរបស់អ្នក ដើម្បីទទួលបានទូវលេខកូដ 6 ខ្ទង់ ដែលក្រុមហ៊ុនតេឡេក្រាមបានផ្ញើមកចូលក្នុងគណនីជនរងគ្រោះតាមរយៈគណនីឈ្មោះ “Telegram” (Official supports bot)។

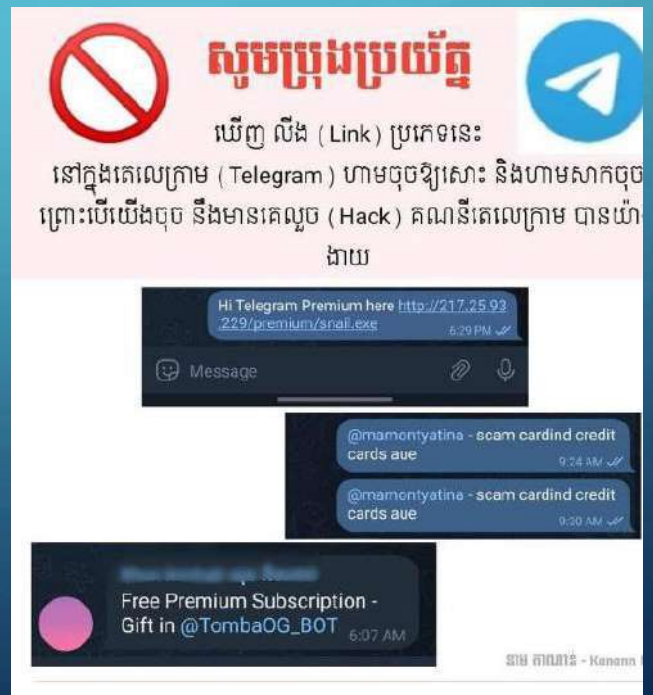


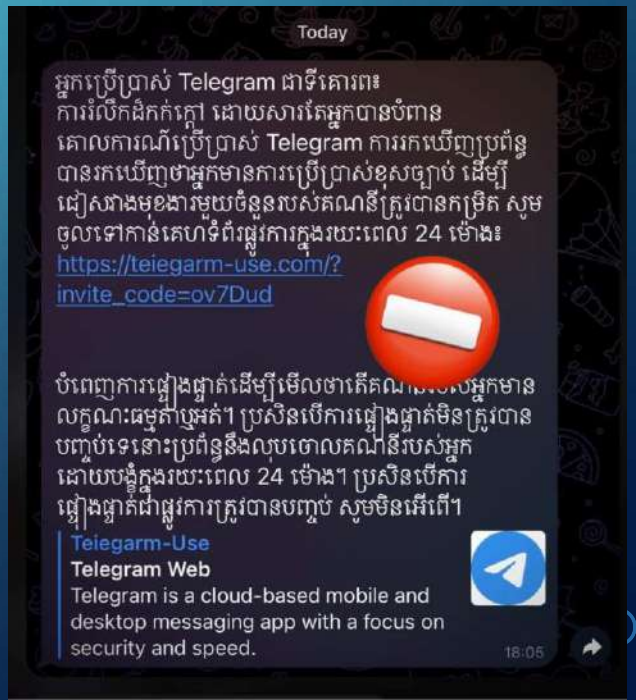


២ វិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

៤. បដិសេធនឹងសារក្លែងក្លាយ (ត)

ទី២. បោកបញ្ឆោតឲ្យចុចតំណភ្ជាប់ក្លែងក្លាយ (Fake Link)÷ ជនអនាមិកដើរតួជាក្រុមហ៊ុនតេឡេក្រាម ផ្ញើសារទៅកាន់ជនរងគ្រោះតាមរយៈសារទូរសព្ទ (SMS), សារអេឡិចត្រូនិក (Email), តេឡេក្រាម (Telegram chat) ជាដើម ដោយភ្ជាប់ជាមួយខ្លឹមសារជម្រុញអោយអ្នកចុចលើតំណភ្ជាប់នោះ ដើម្បីបំពេញព័ត៌មានាំពាក់ព័ន្ធនឹងគណនីរបស់ជនរងគ្រោះដើម្បីជនអាណាមិកអាចចូលទៅកាន់គណនីរបស់ជនរងគ្រោះបានតែម្តង។ ឧទាហរណ៍ដូចជា÷ ជនអានាមិកផ្ញើរសារដោយតម្រូវឲ្យជនរងគ្រោះធ្វើការបញ្ជាក់គណនី (Verify Telegram Account) លើតំណភ្ជាប់ក្លែងក្លាយបើមិនដូចនោះទេគណនីរបស់ជនរងគ្រោះនឹងត្រូវលុបចោល (Your account will be canceled if it has not been verified for a long time. Please complete if as soon as possible at Telegram.org.)

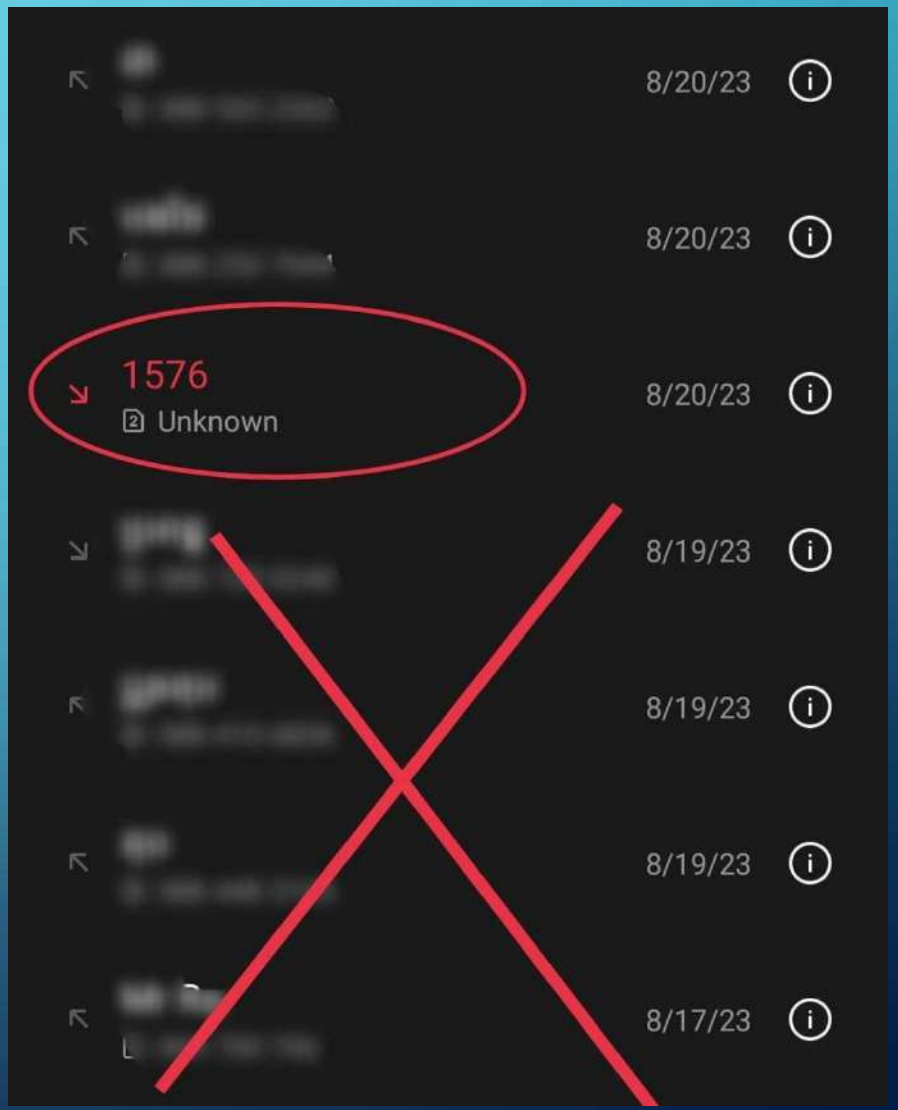




២ វិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

៤. បដិសេធនឹងសារក្លែងក្លាយ (ត)

ទី៣. បោកបញ្ឆោតតាមរយៈ Call scam ដែលជាប្រភេទវាយប្រហាតាមរយៈការខលទៅកាន់ទូរស័ព្ទរបស់អ្នក ដែលមានលេខត្រឹមតែ ៤ ឬ ៥ ខ្ទង់ប៉ុន្នោះ ប្រសិនបើលោកអ្នកធ្វើការទទួលការខលនេះ អាចនឹងមានបញ្ហានប៉ះពាល់ដល់គណនីដែលភ្ជាប់នឹងលេខទូរស័ព្ទរបស់លោកអ្នក។

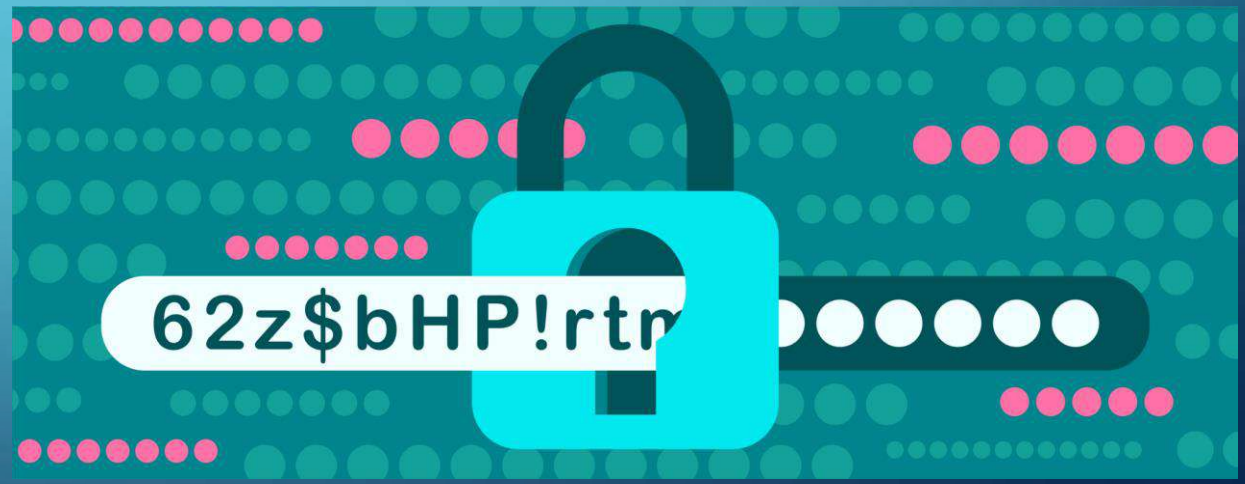


២ វិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

៥. ប្រើពាក្យសម្ងាត់រឹងមាំ

សព្វថ្ងៃនេះយើងឃើញមានគណនី តេឡេក្រាម ជាច្រើនត្រូវបានវាយប្រហារដោយ Hacker មូលហេតុសំខាន់មួយគឺការធ្វេសប្រហែសនិងការប្រើប្រាស់ពាក្យសម្ងាត់ទន់ខ្សោយ ដូច្នេះអ្នកគួរបង្កើតនិងប្រើប្រាស់ពាក្យសម្ងាត់រឹងមាំ ខាងក្រោមនេះគឺជាគន្លឹះ ៦ ចំណុច ក្នុងការបង្កើតពាក្យសម្ងាត់រឹងមាំ និងមិនងាយទាយដឹង÷

- បង្កើតលេខកូដសម្ងាត់របស់អ្នកអោយបានវែងយ៉ាងហោចណាស់ ១២ ខ្ទង់
- បញ្ចូលតួលេខរួម និមិត្តសញ្ញា និងអក្សរធំនិងអក្សរតូច
- ជៀសវាងការប្រើប្រាស់ព័ត៌មានផ្ទាល់ខ្លួន
- កុំប្រើឡើងវិញនូវពាក្យសម្ងាត់ដែលធ្លាប់ប្រើ
- រក្សាទុកពាក្យសម្ងាត់ឱ្យមានសុវត្ថិភាព
- ផ្លាស់ប្តូរពាក្យសម្ងាត់ឱ្យបានទៀងទាត់



២ ទិធីសាស្ត្រការពារសន្តិសុខក្នុងការប្រើប្រាស់ប្រព័ន្ធបណ្តាញសង្គម (ត)

ខ. ប្រើមុខងារ Passcode Lock

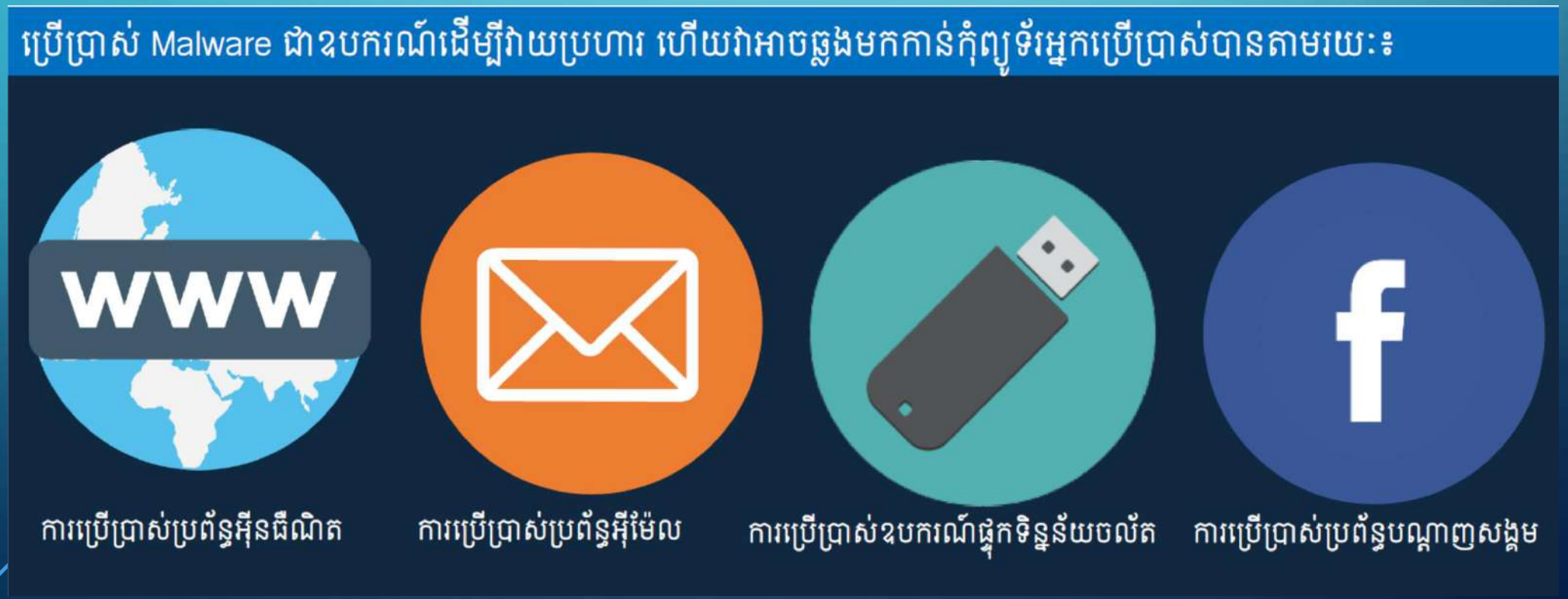
តេឡេក្រាម មានមុខងារដែលអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ចាក់សោកម្មវិធីដោយប្រើលេខកូដសម្ងាត់ ដើម្បីការពារនៅពេលដែលនរណាចូលប្រើប្រាស់តេឡេក្រាមនៅលើឧបករណ៍របស់ខ្លួន ដោយមុខងារនេះគឺតម្រូវឱ្យមានការបញ្ចូលលេខកូដសម្ងាត់ ដើម្បីអាចប្រើប្រាស់តេឡេក្រាមបាន។ ដើម្បីបង្កើតលេខកូដសម្ងាត់ សូមអនុវត្តតាមការណែនាំដូចខាងក្រោម÷

- ចូលទៅកាន់ “Settings” បន្ទាប់មកចុចលើ“ “Privacy and Security”
- ត្រង់ចំណុច “Security” ចុចលើពាក្យ “Turn on local passcode” ឬ “Passcode Lock” ឬ “Passcode & Touch ID”
- បន្ទាប់មកវាយបញ្ចូលលេខកូដសម្ងាត់ និងបញ្ចូលលេខកូដម្តងទៀតដើម្បីផ្ទៀតផ្ទាត់
- អ្នកប្រើប្រាស់ត្រូវតែចងចាំលេខកូដសម្ងាត់ដែលបានដាក់ ដើម្បីបញ្ចូលលេខកូដនេះរាល់ពេលចូលប្រើប្រាស់តេឡេក្រាម។

៣ ការទទួលខុសត្រូវទៅលើឯកជនភាពនៃការប្រើប្រាស់ និងគ្រប់គ្រងនិន្នន័យ

៩៥% នៃការរំលោភបំពានជោគជ័យលើសន្តិសុខបច្ចេកវិទ្យាព័ត៌មានបង្កឡើងចេញពីការធ្វេសប្រហែសរបស់អ្នកប្រើប្រាស់។ ដើម្បីការពារការវាយប្រហាសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន មន្ត្រីទាំងអស់ត្រូវមានការ ទទួលខុសត្រូវ និងឱ្យតម្លៃលើបញ្ហាសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន។

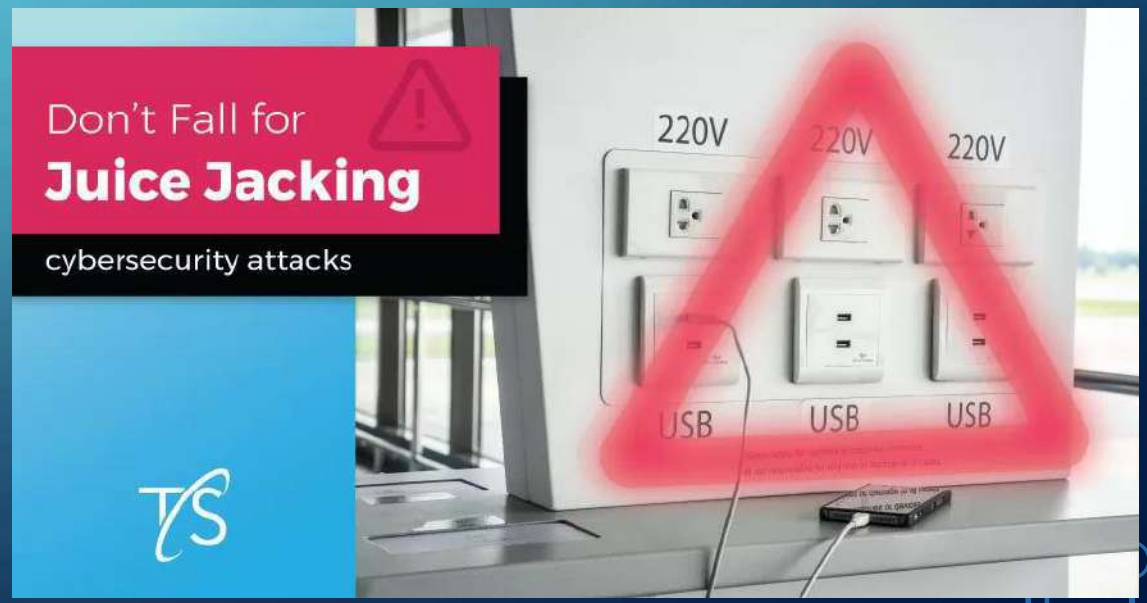
ការធ្វេសប្រហែលរបស់អ្នកប្រើប្រាស់ភាគច្រើនទៅលើការប្រើប្រាសឧបករណ៍បច្ចេកវិទ្យា ដែលនាំឱ្យមានការចម្លងមេរោគចូលក្នុងកុំព្យូទ័រ ដែលការវាយប្រហានោះ Hacker បានប្រើប្រាស់ Malware ជាឧបករណ៍ដើម្បីវាយប្រហា។



៣ ការធ្វេសខុសត្រូវទៅលើឯកជនភាពនៃការប្រើប្រាស់ និងគ្រប់គ្រងទិន្នន័យ

❖ ការប្រុងប្រយ័ត្នទៅលើការប្រើប្រាស់ Public Charging Station

Public Charging Station ជាបណ្តាស្ថានីយសាកថ្មទូរស័ព្ទសាធារណៈដែលមាន USB port និង ព្រ៊ីភ្លើងសម្រាប់ឱ្យអ្នកប្រើប្រាស់បញ្ចូលថ្មទូរស័ព្ទបាន។ ភាគច្រើនគឺមាននៅក្នុងប្រលានយន្តហោះ, សណ្ឋាគារ និង ទីកន្លែងទទួលភ្ញៀវ។ អ្នកប្រើប្រាស់អាចក្លាយទៅជាជនរងគ្រោះនៃ Juice Jacking Attack ដោយការប្រើប្រាស់ Public Charging Station។ ជនរងគ្រោះនឹងមានបញ្ហាដូចជា÷ រងការបំពានលើព័ត៌មានអាជីវកម្ម, ការកាន់កាប់គណនី Cloud, Spyware ត្រូវបានដាក់នៅលើទូរស័ព្ទ, លួចយកគណនីនៅក្នុងកុងធនាគា, លួយចយកទិន្នន័យនៅក្នុងទូរស័ព្ទ-ល-។



ការទទួលខុសត្រូវទៅលើឯកជនភាពនៃការប្រើប្រាស់ និងគ្រប់គ្រងទិន្នន័យ

- អ្នកប្រើប្រាស់ត្រូវមានទំនួលខុសត្រូវទៅលើសកម្មភាព និងប្រតិបត្តិការរបស់ខ្លួនដូចជា÷
  - ត្រូវពិនិត្យមើលអាសយដ្ឋានអ៊ីមែលដែលបានផ្ញើមកឱ្យបានច្បាស់លាស់។
  - ប្រុងប្រយ័ត្នជានិច្ចរាល់ពេលបើកឯកសារភ្ជាប់ ឬចុចលើតំណភ្ជាប់ដែលផ្ញើមកពីប្រភពមិនច្បាស់។
  - ប្រុងប្រយ័ត្នខ្ពស់ក្នុងការផ្តល់ព័ត៌មានសម្ងាត់ទៅកាន់បុគ្គលណាម្នាក់។
  - ផ្តាច់អ៊ីនធើណែតភ្លាម ប្រសិនបើសង្ស័យថាកុំព្យូទ័រត្រូវបានគេលួចចូលប្រើប្រាស់។
  - ប្រុងប្រយ័ត្នចំពោះ Pop-up ស្នើយប្រវត្តិឱ្យតំឡើង Software Update។
  - ប្រុងប្រយ័ត្នចំពោះការតំឡើង Plug-in ឬ Add-on នៅលើកម្មវិធីរុករក។
  - មិនគួរចុះឈ្មោះចូលលេងកម្មវិធីលើអ៊ីនធើណែតផ្តេសផ្តាស់។
  - មិនត្រូវប្រើប្រាស់ឧបករណ៍អេឡិចត្រូនិចដែលមិនដឹងប្រភពច្បាស់លាស់។

សូមអរគុណ

THANKS FOR YOUR ATTENTION

Facebook

Telegram

www.iauoffsa.gov.kh

អគារ ១៦៨F ជាន់ទី៩ ផ្លូវ៥៩៨ សង្កាត់ទ្រាំងចំរេះ១ ខណ្ឌឫស្សីកែវ រាជធានីភ្នំពេញ

សំណួរ & ចម្លើយ