វគ្គបណ្តុះបណ្តាល

មូលដ្ឋានគ្រឹះនៃ សុវត្ថិភាពលើប្រព័ន្ធបច្ចេកវិទ្យា

គ្រូបណ្តុះបណ្តាល៖ ចាន់ ភារុណ

វគ្គបណ្តុះបណ្តាល

មូលដ្ឋានគ្រឹះនៃ សុវត្ថិភាពលើប្រព័ន្ធបច្ចេកវិទ្យា

“សុវត្ថិភាពកើតចេញពីខ្លួនយើង”

តើសុវត្ថិភាពលើប្រព័ន្ធបច្ចេកវិទ្យាជាអ្វី?

គឺជាការការពារ និងរក្សាព័ត៌មានឯកជន
ព័ត៌មានលម្អិតផ្ទាល់ខ្លួន អោយមានសុវត្ថិភាព
តាមរយៈឧបករណ៍ ឬប្រព័ន្ធបច្ចេកវិទ្យា។

ព័ត៌មាន

ឧបករណ៍

ការទំនាក់ទំនង

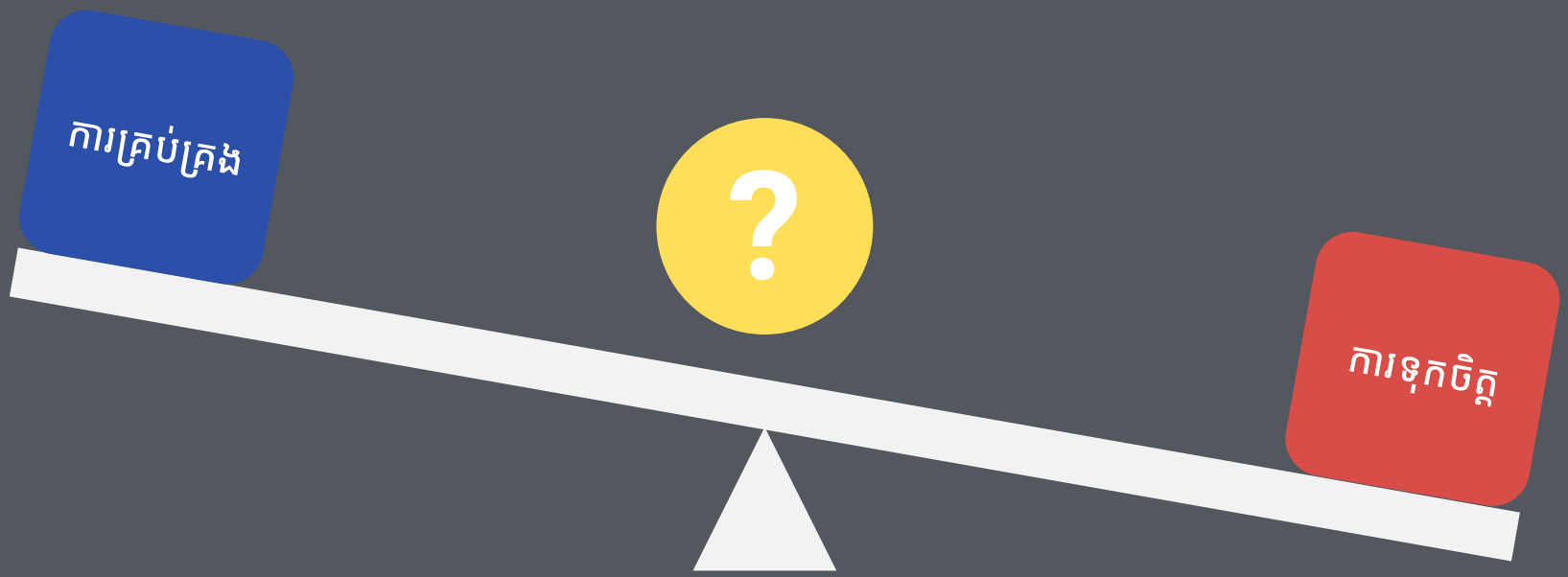
ព័ត៌មាន

ប្រភេទព័ត៌មាន៖

- ព័ត៌មានផ្ទាល់ខ្លួន
- របាយការណ៍ហិរញ្ញវត្ថុ
- របាយការណ៍ពេទ្យ
- ព័ត៌មានកន្លែងធ្វើការ
- ផ្សេងៗទៀត

តើអ្នកអាចគ្រប់គ្រងលើអ្វីបានខ្លះ?

តើអ្នកទុកចិត្តអ្នកណាខ្លះ?


ការគ្រប់គ្រង
?
ការទុកចិត្ត

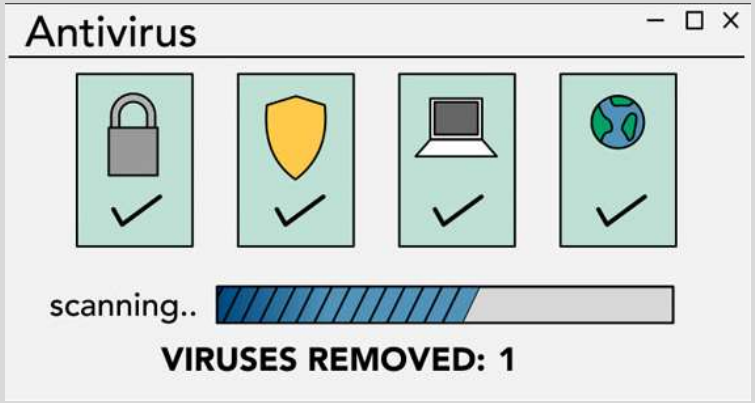
ឧបករណ៍

យើងចង់បានសុវត្ថិភាពឧបករណ៍៖

- កុំព្យូទ័ររបស់អ្នក
- ទូរស័ព្ទស្មាតហ្វូន និង ថេប្លេត
- ប្រព័ន្ធប្រតិបត្តិការ
- កម្មវិធីកុំព្យូទ័រនិងទូរស័ព្ទ
- ឧបករណ៍ផ្ទុកទិន្នន័យ
- ការផ្ទុកទិន្នន័យអនឡាញ

យុទ្ធសាស្ត្រការពារទិន្នន័យ ៖

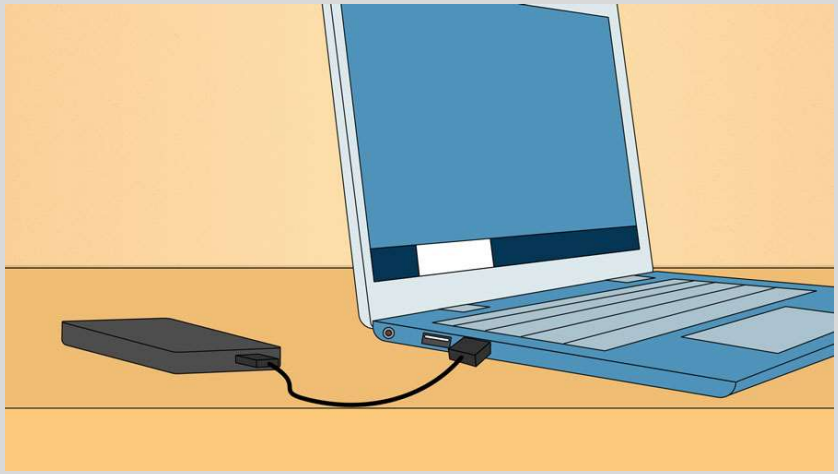
1. **សុវត្ថិភាពទិន្នន័យ (Data security)** - ការពារទិន្នន័យពីការខូចខាតដោយមេរោគ (Malware) ឬគ្រោះថ្នាក់ដោយចៃដន្យ (Antivirus)



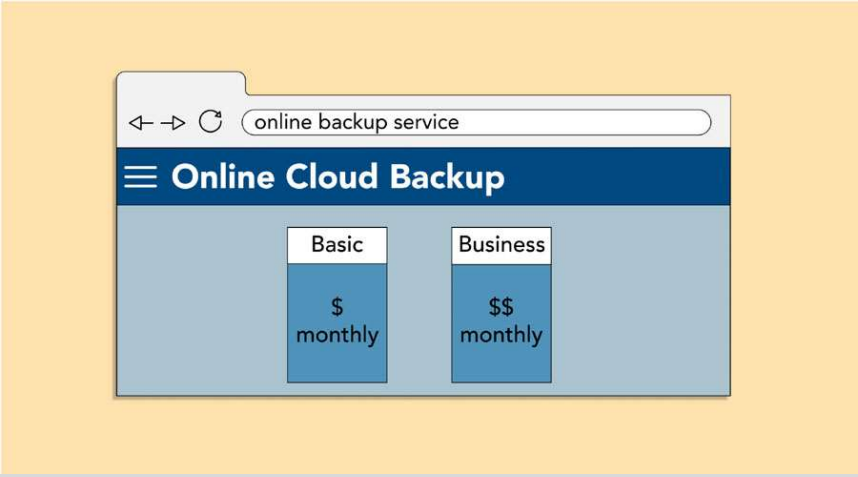
Malware គឺជាប្រភេទកម្មវិធីមួយដែលបង្កើតឡើងដើម្បីធ្វើឱ្យខូចកុំព្យូទ័ររបស់អ្នក ឬទទួលបានព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នកដោយគ្មានការអនុញ្ញាត។ វារួមបញ្ចូលមេរោគ ពពួក Worm, Trojan house និង spyware ។ មេរោគភាគច្រើនត្រូវបានចែកចាយតាមអ៊ីនធឺណិត ហើយជារឿយៗត្រូវបានរួមបញ្ចូលជាមួយកម្មវិធីផ្សេងទៀត។

2. ភាពអាចរកបានមកវិញនៃទិន្នន័យ (Data availability) -

ការស្តារទិន្នន័យឡើងវិញយ៉ាងឆាប់រហ័សក្នុងករណីមានការខូចខាត ឬបាត់បង់ (Backup)



External Drive



Online Cloud Backup

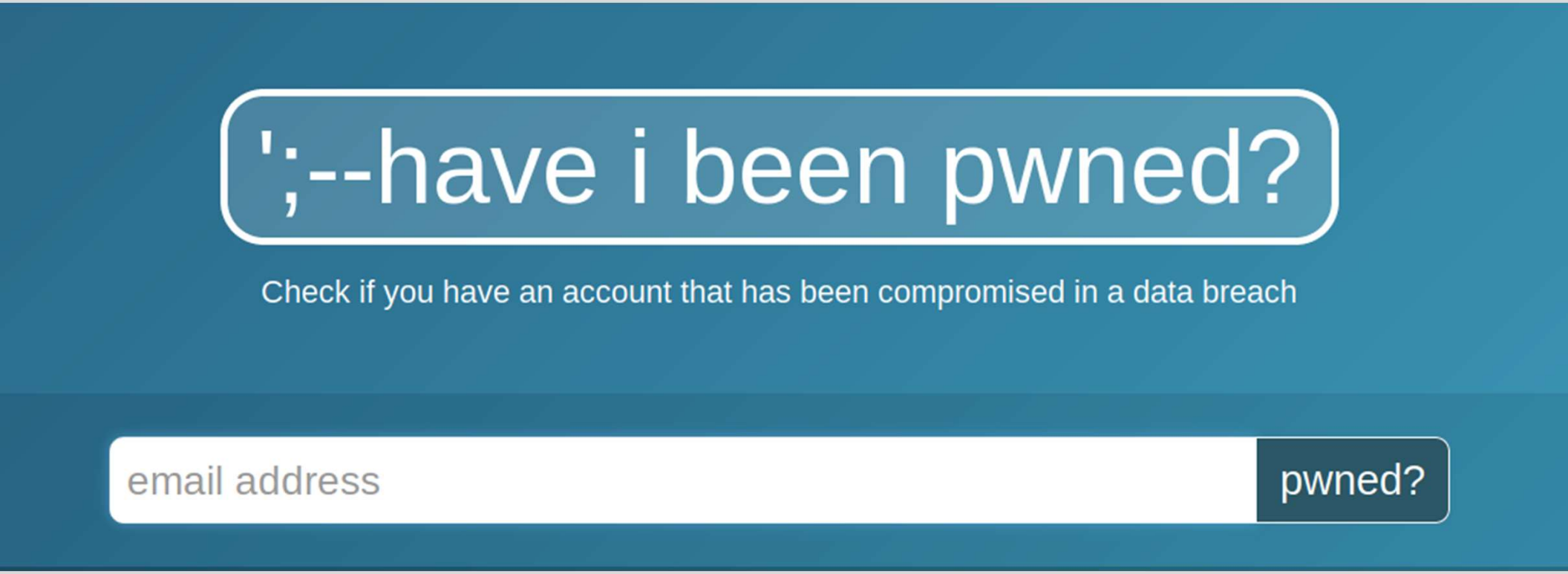
3. ការគ្រប់គ្រងការចូលប្រើ (Access Control)

ធានាថាទិន្នន័យអាចចូលប្រើបាន
សម្រាប់អ្នកដែលត្រូវការវា មិនមែន
សម្រាប់នរណាម្នាក់ផ្សេងទៀតទេ។

(Password & Encryption)

ការការពារឧបករណ៍របស់អ្នកពីពួក Hacker៖

1. មេរោគតាមរយៈអ៊ីមែល ឬ សារបណ្តាញសង្គម
2. តំណរភ្ជាប់ក្លែងក្លាយ
3. USB មានមេរោគ
4. កុំប្រើកម្មវិធី Crack



https://haveibeenpwned.com/

ពាក្យសម្ងាត់ Password (*****)

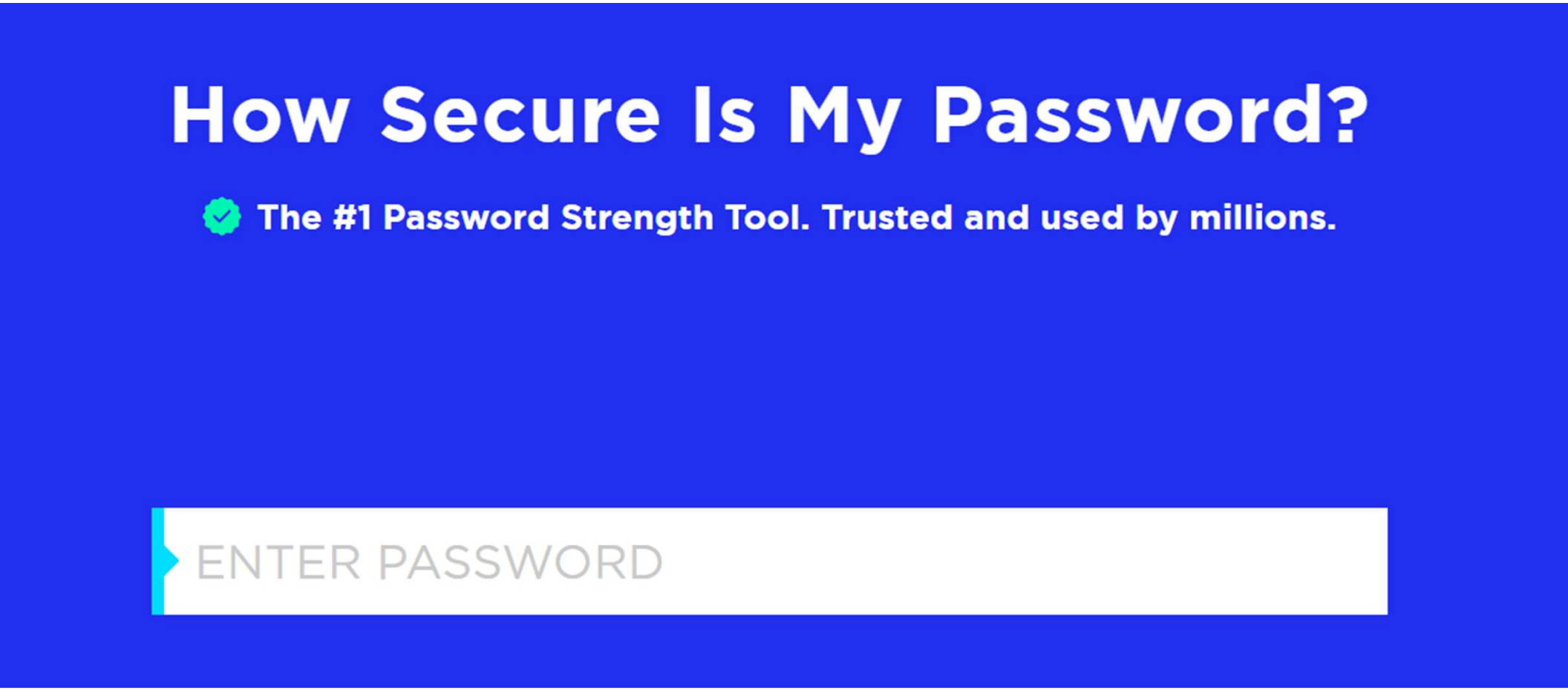
យើងត្រូវការពាក្យសម្ងាត់ ដើម្បីមានសិទ្ធិធ្វើអ្វីគ្រប់យ៉ាងបាននៅលើឧបករណ៍ និងគេហទំព័រ រួមមាន ៖ ការពិនិត្យអ៊ីមែល រហូតដល់សេវាធនាគារតាមអនឡាញ។ ហើយខណៈពេលដែលពាក្យសម្ងាត់កាន់តែខ្លី ហើយសាមញ្ញក្នុងការប្រើ និងងាយស្រួលចងចាំ វាក៏អាចបង្ក**ហានិភ័យយ៉ាងធ្ងន់ធ្ងរ**ដល់សុវត្ថិភាពអនឡាញរបស់អ្នកផងដែរ។

ដើម្បីការពារខ្លួនអ្នក និងព័ត៌មានរបស់អ្នក អ្នកត្រូវតែប្រើពាក្យសម្ងាត់ដែល**វែង ហើយរឹងមាំ** សម្រាប់អ្នកផ្សេងក្នុងការទស្សន៍ទាយ ខណៈពេលដែលអ្នកនៅតែរក្សាវាទុកយ៉ាងងាយស្រួលសម្រាប់អ្នកក្នុងការចងចាំ។

ខាងក្រោមនេះគឺជាពាក្យសម្ងាត់ពេញនិយមបំផុតសម្រាប់ឆ្នាំ 2021 ដែលធ្វើឱ្យគណនីដែលពួកគេ ងាយស្រួលក្នុងការលួចចូល ៖

1. 123456
2. 123456789
3. 12345
4. Qwerty
5. Password
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567

Published by NordPass

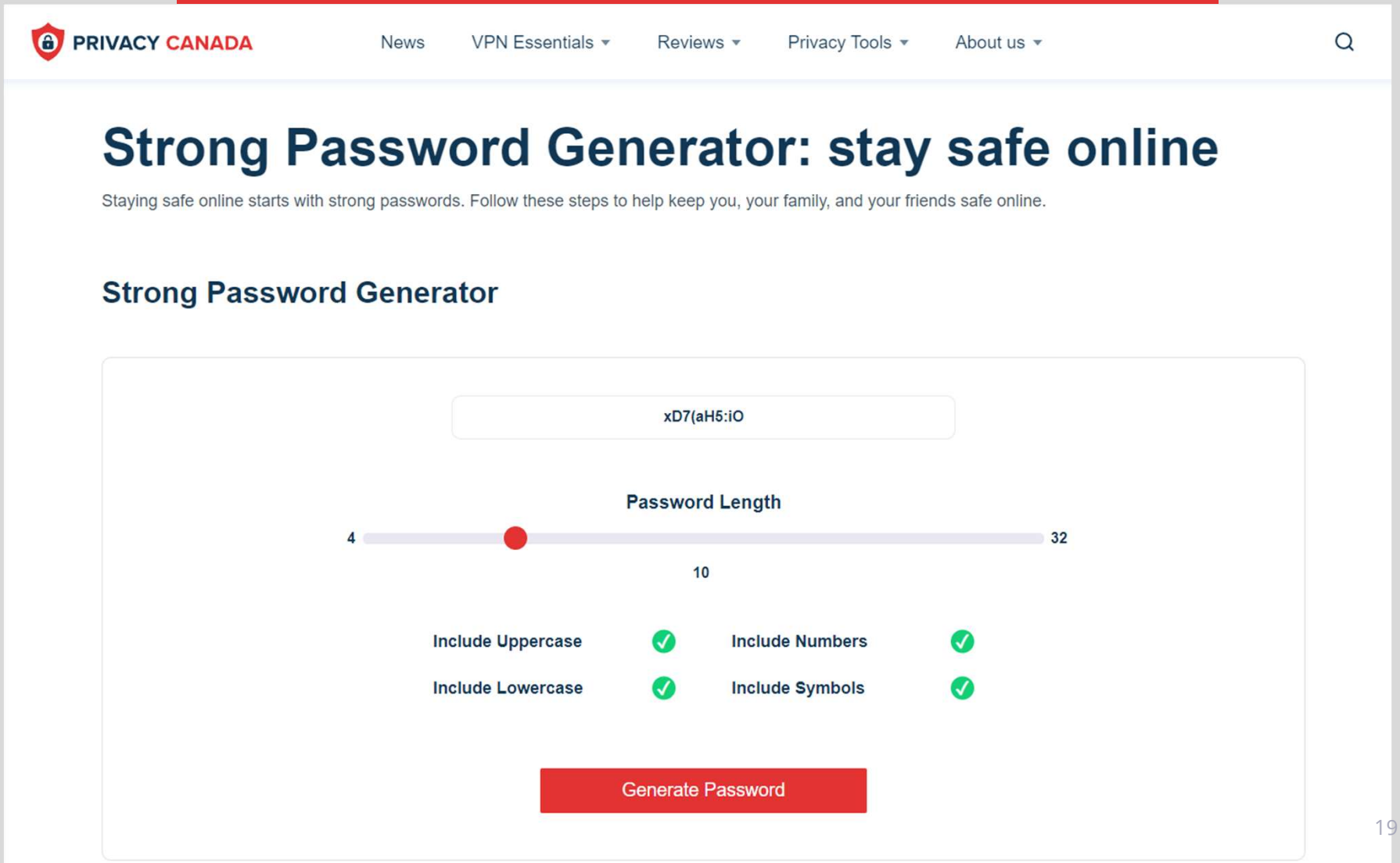


https://www.security.org/how-secure-is-my-password/

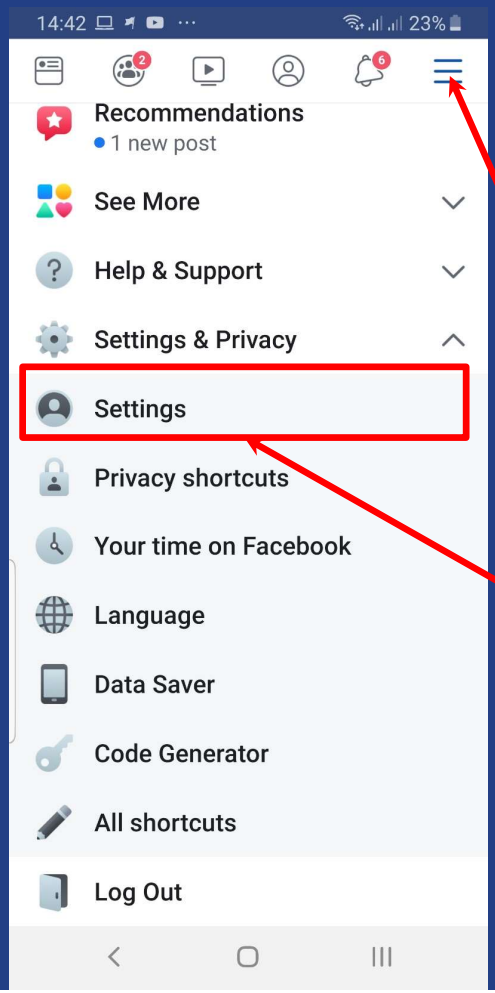
គន្លឹះបង្កើតពាក្យសម្ងាត់រឹងមាំ

- កុំប្រើព័ត៌មានផ្ទាល់ខ្លួន
- កុំប្រើពាក្យសម្ងាត់ដូចគ្នា
- ពាក្យសម្ងាត់គួរតែមានយ៉ាងតិច ១០ តួរអក្សរ, ប្រើលេខ និងសញ្ញា, អក្សរធំ តូច, កុំប្រើឡើងវិញ។ **ឧទាហរណ៍៖** m#P52s@ap$V
- ប្រសិនអ្នកពិបាកក្នុងការគិតរកដាក់ សូមប្រើកម្មវិធីជំនួយ **Password Generator**

https://privacycanada.net/strong-password-generator/



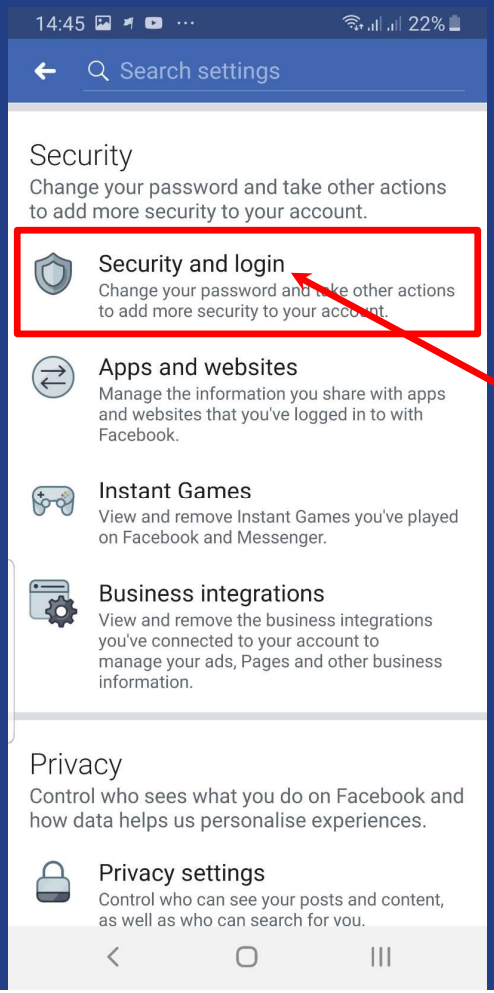
អនុវត្តន៍លើបណ្តាញសង្គម Facebook



1 ចុចរូបសញ្ញាត្រែបី

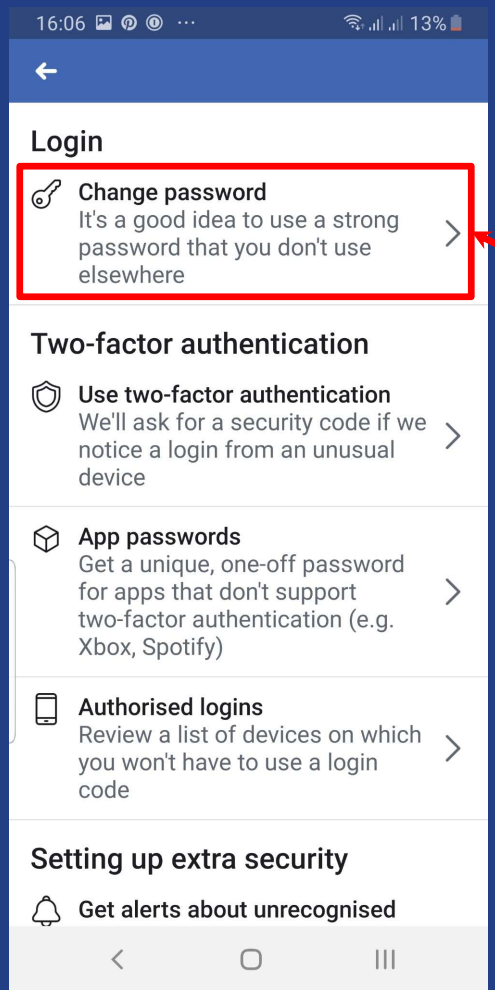
Settings & Privacy

2 Settings



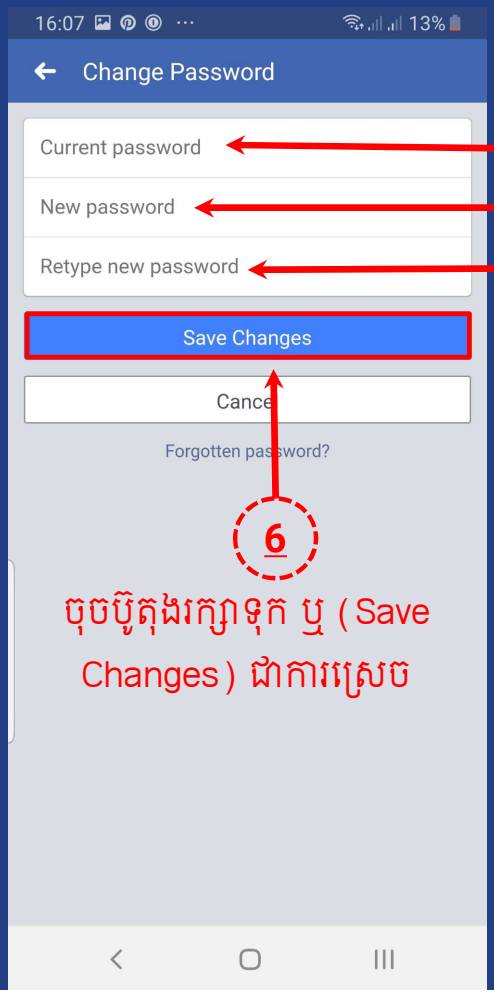
3 Security and login

អនុវត្តន៍លើបណ្តាញសង្គម Facebook



4

ចុចយក Change password ដើម្បីធ្វើការផ្លាស់ប្តូរ



5

ត្រូវដាក់លេខសម្ងាត់ចាស់

ដាក់លេខសម្ងាត់ថ្មី

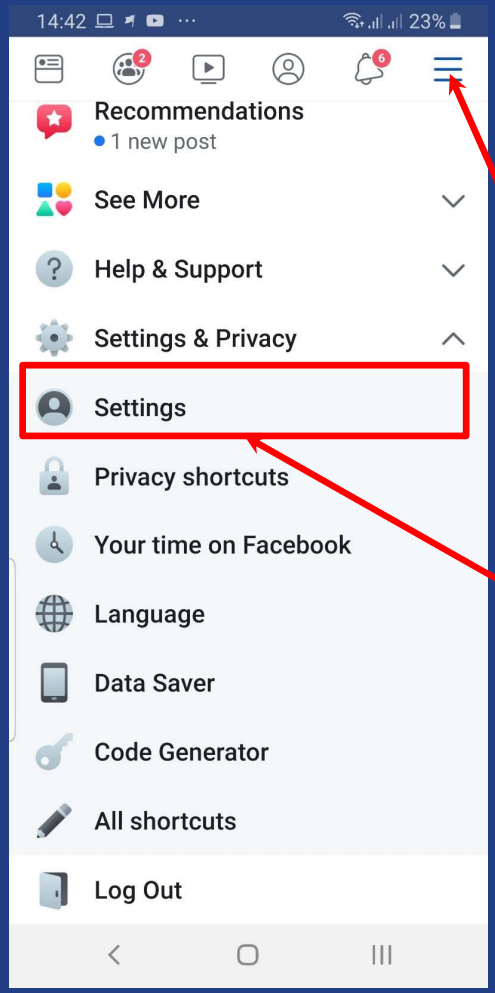
ដាក់បញ្ជាក់លេខសម្ងាត់ថ្មីម្តងទៀត

6

ចុចប៊ូតុងរក្សាទុក ឬ (Save Changes) ជាការស្រេច

មុខងារចាក់សោរពីរជាន់ ឬផ្ទៀងផ្ទាត់២កត្តា

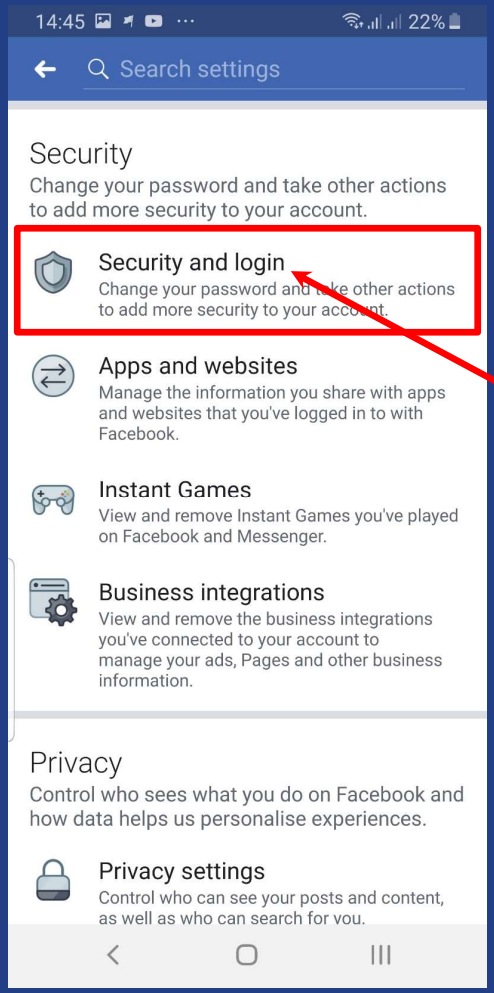
- ការផ្ទៀងផ្ទាត់២កត្តា គឺជាវិធីដែលអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់កំណត់អត្តសញ្ញាណខ្លួនទៅអ្នកផ្តល់សេវាកម្មដោយតំរូវអោយមានការបញ្ចូលលេខសំងាត់ ដើម្បីផ្ទៀងផ្ទាត់។
- https://2fa.directory/int/
- អនុវត្តន៍លើបណ្តាញសង្គម **Facebook**



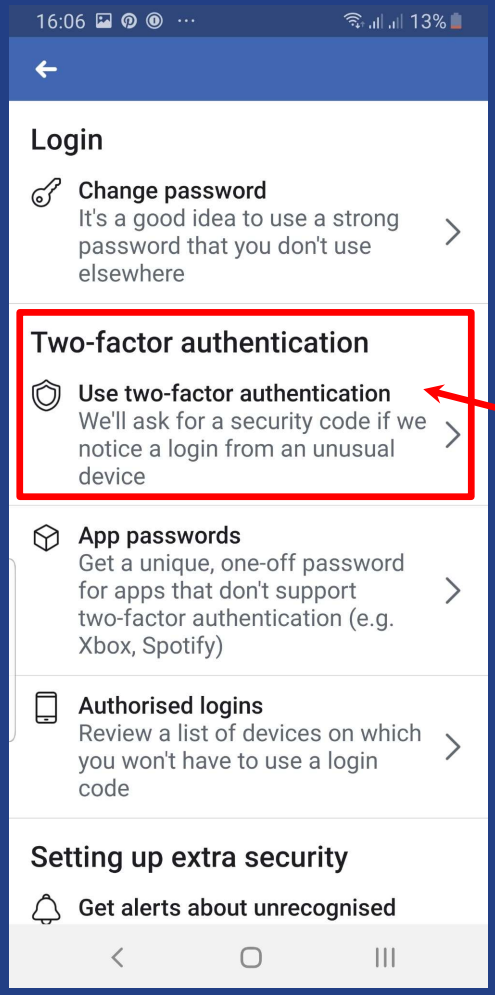
1 ចុចរូបសញ្ញាត្រែបី

Settings & Privacy

2 Settings

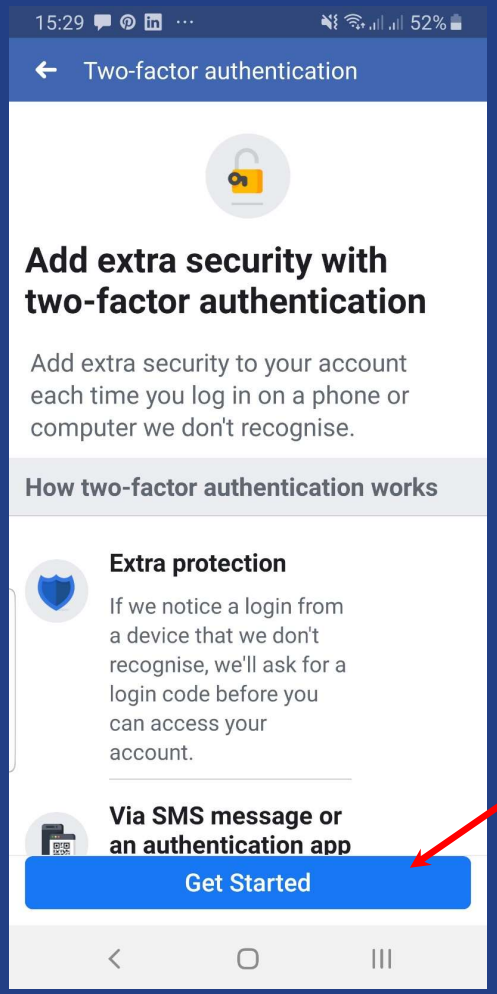


3 Security and login

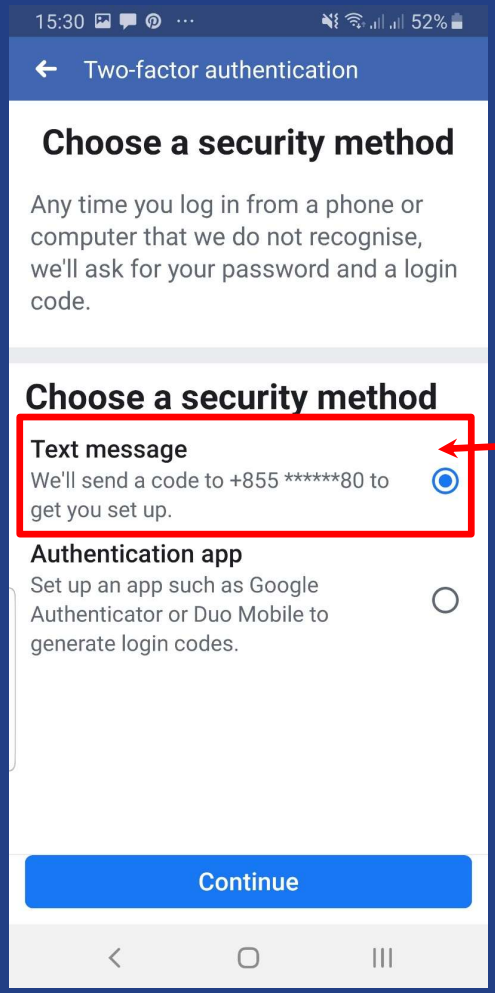


ចុចពាក្យ

Use two-factor authentication



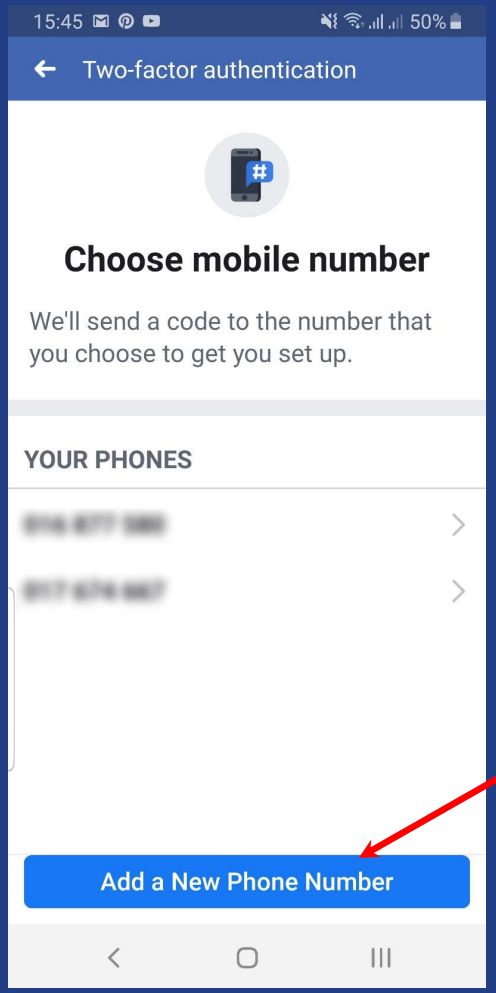
ចុចប៊ូតុង **Get Started**



6

សូមរើសយក

Text message

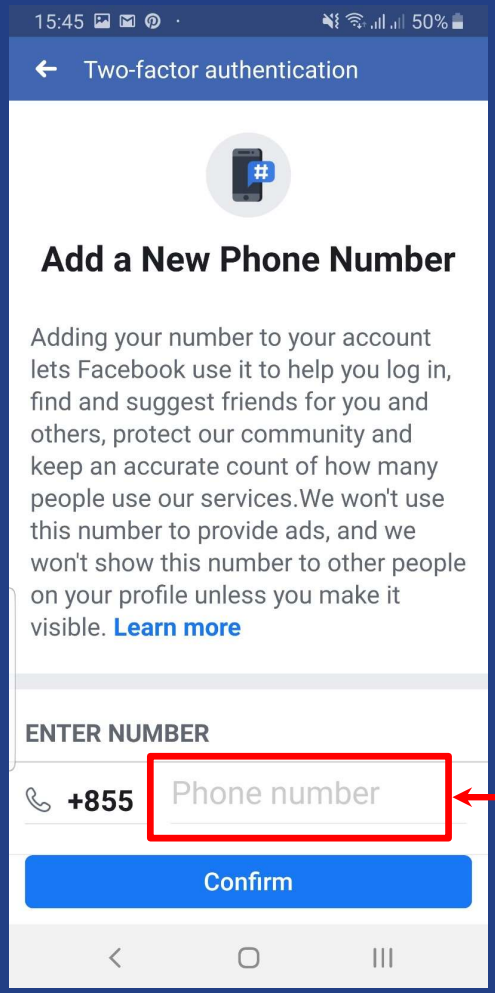


7

ចុចប៊ូតុង

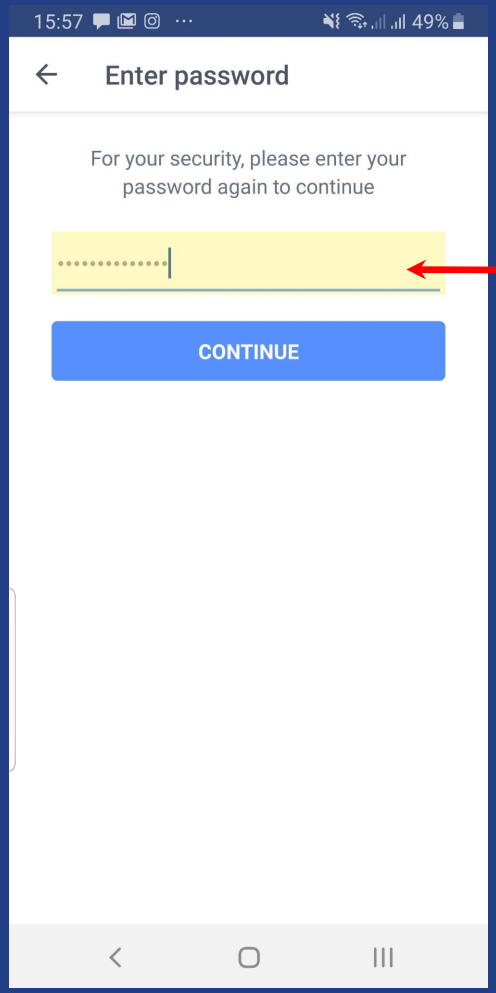
Add a New Phone Number

ដើម្បីបញ្ចូលលេខទូរស័ព្ទ



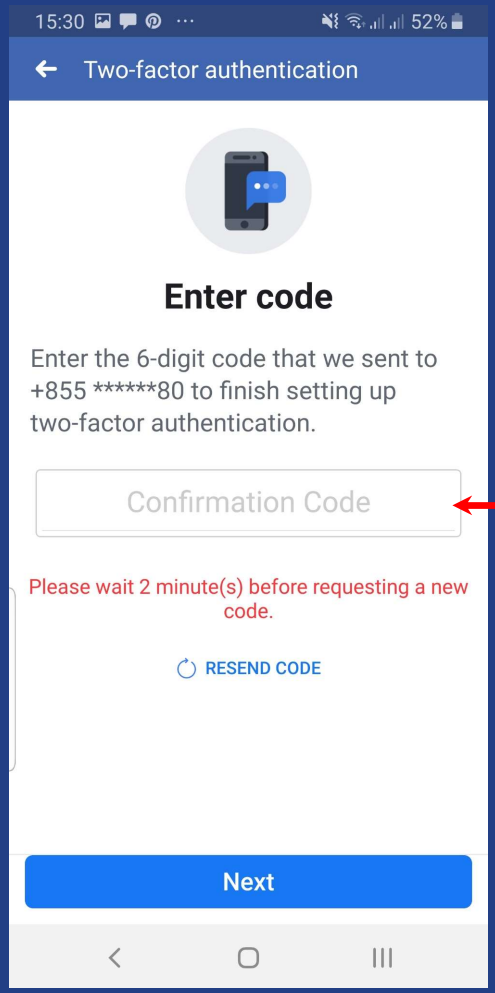
8

បញ្ចូលលេខទូរស័ព្ទ
រួចចុចប៊ូតុង Confirm



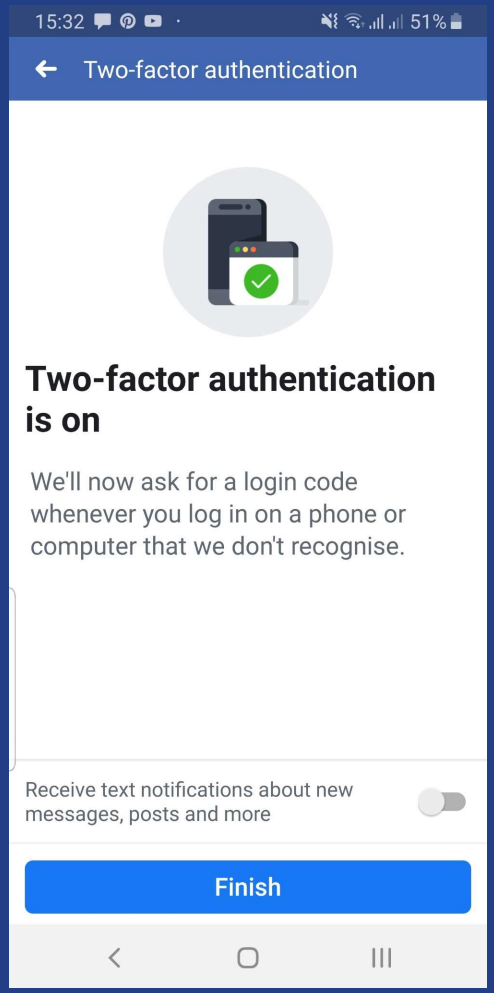
9

បញ្ចូល Password អ្នក
រួចចុច CONTINUE
រួចលេខកូដនឹងផ្ញើចូល
ទូរស័ព្ទដៃរបស់អ្នក



10

បញ្ចូលលេខកូដ
រួចចុចប៊ូតុង Next



11 ចុច **Finish**

តើកម្មវិធីរុករក (Browser) ជាអ្វី?

Browser ជាកម្មវិធីសំរាប់ធ្វើការរុករក និងស្រាវជ្រាវព័ត៌មានតាមរយៈអ៊ីនធើណេត។

Microsoft Edge

Apple Safari

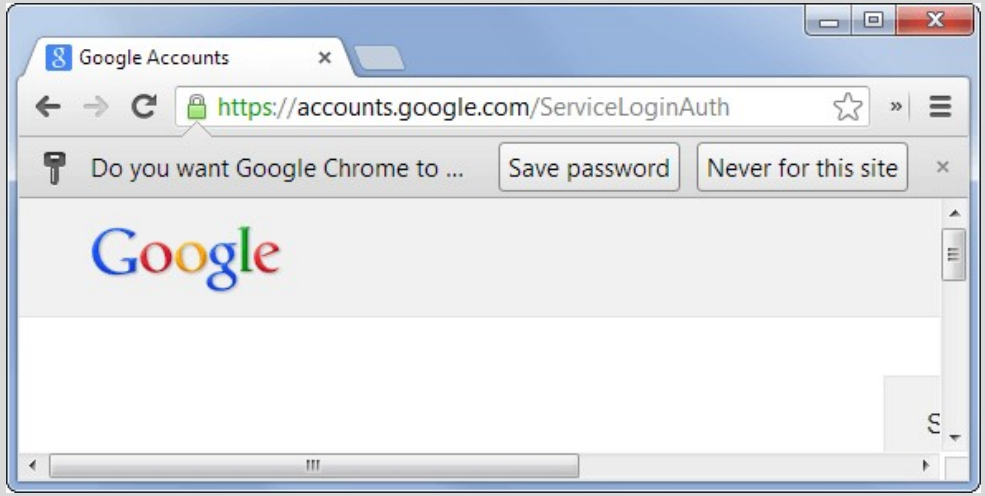
Google Chrome

Brave Browser

Mozilla Firefox

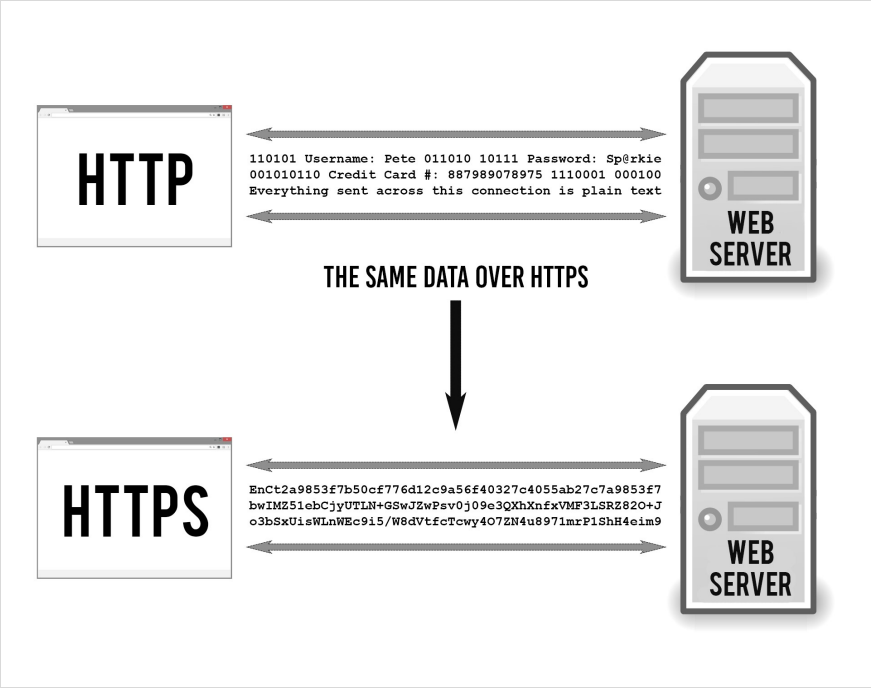
TOR Browser

តើការរក្សាទុក Password ក្នុង Browser ល្អដែរឬទេ?



https > http

Encryption


HTTP
110101 Username: Pete 011010 10111 Password: Sp@rkie
001010110 Credit Card #: 887989078975 1110001 000100
Everything sent across this connection is plain text
WEB SERVER
THE SAME DATA OVER HTTPS
HTTPS
EnCt2a9853f7b50cf776d12c9a56f40327c4055ab27c7a9853f7
bwIMZ51ebCjyUTLN+GSwJZwPsv0j09e3QXhXnfxVMF3LSRZ82O+J
o3bSxUisWLnWEc9i5/W8dVtfcTcwy4O7ZN4u8971mrP1ShH4eim9
WEB SERVER

ការទំនាក់ទំនង

យើងចង់ធានាឯកជនភាពនិងសន្តិសុខពីអ្នកណា?

- រដ្ឋាភិបាល
- ក្រុមហ៊ុនទូរគមនាគមន៍
- ក្រុមហ៊ុនផ្តល់សេវាអ៊ីនធើណេត
- ក្រុមហ៊ុនផ្តល់សេវាផ្សេងៗទៀត
- ។ល។

តើកូដនីយកម្មជាអ្វី Encryption?

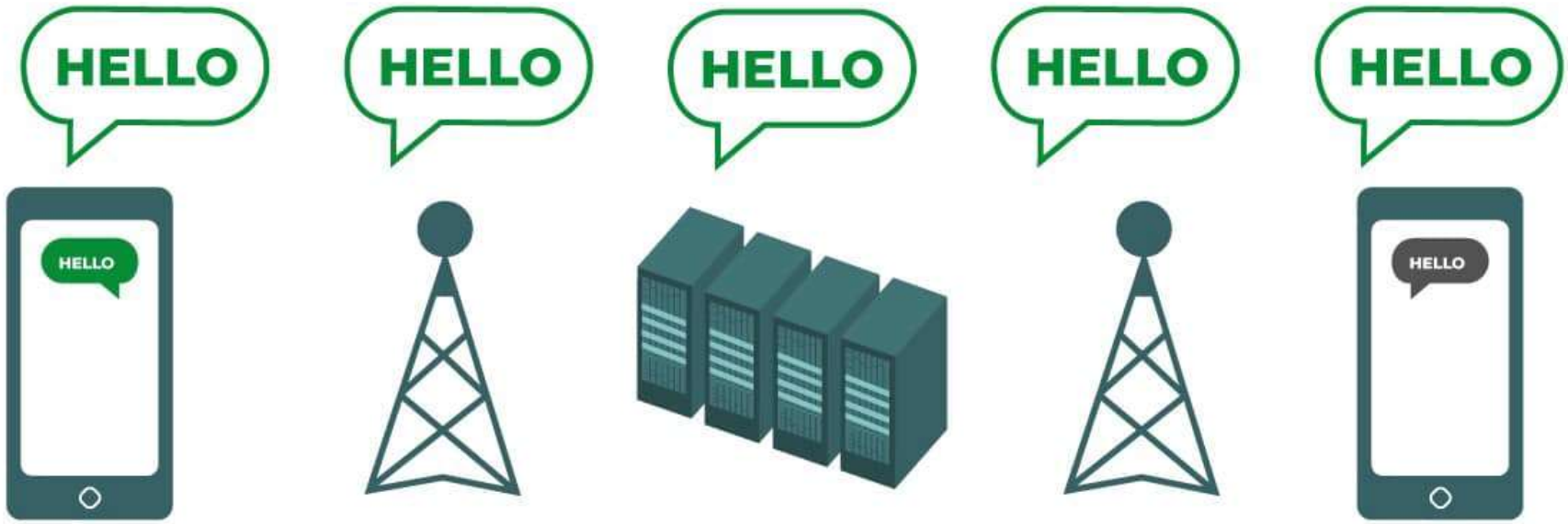
ដំណើរការនៃការបំលែងសារ (ព័ត៌មាន ឬទិន្នន័យ) ទៅជាកូដ ដើម្បីកុំអោយ(ភាគីទី៣)ចូលមើលបាន ដោយគ្មានការអនុញ្ញាត។

Signal

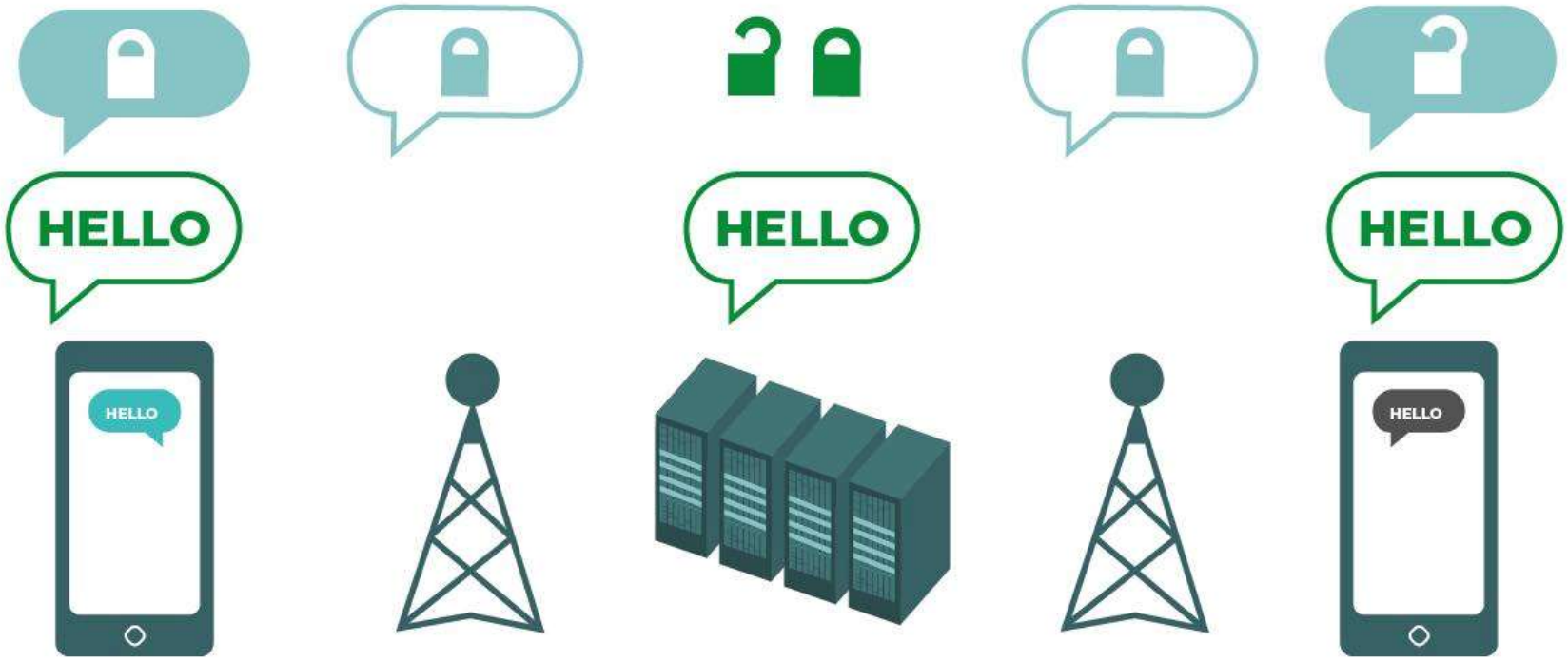
Telegram

WhatsApp

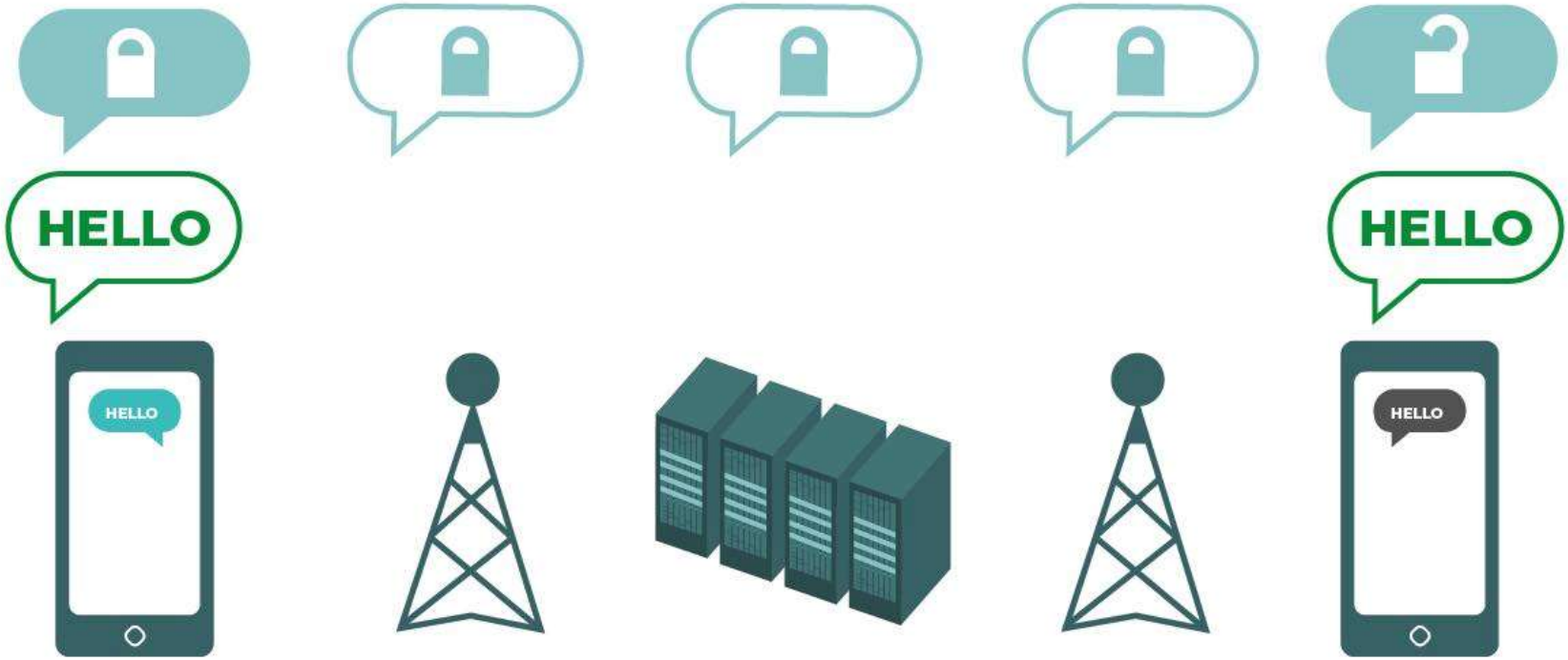
ការទំនាក់ទំនងដោយស្ទុះវត្ថុភាព និងឯកជនភាព



ការទំនាក់ទំនងដោយសុវត្ថិភាព និងឯកជនភាព



ការទំនាក់ទំនងដោយសុវត្ថិភាព និងឯកជនភាព



ការទំនាក់ទំនងដោយសុវត្ថិភាព និងឯកជនភាព

Signal គឺជាកម្មវិធីផ្ញើសារ ដែលត្រូវបានណែនាំជាចម្បង ដោយមានកូដនីយកម្មសារ End-2-End Encryption ហើយក៏ជាកម្មវិធី...

- កម្មវិធីបើកទូលាយ
- មិនមានការផ្សាយពាណិជ្ជកម្ម
- សវនកម្មឯករាជ្យ

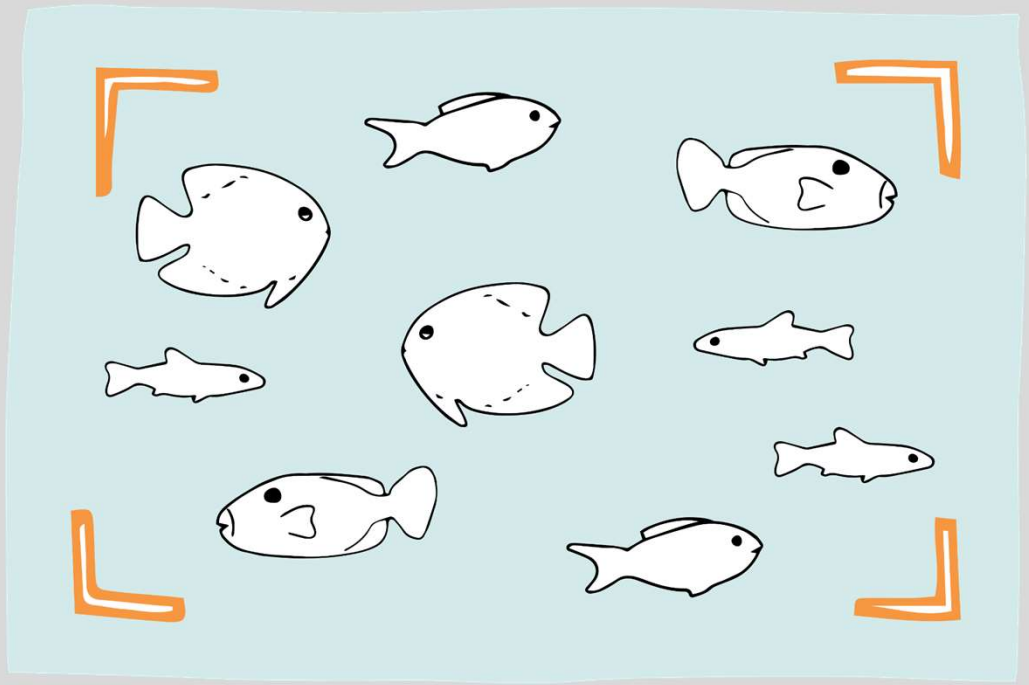
តន្ត្រីសុវត្ថិភាព

- មានការប្រុងប្រយ័ត្ន លើកាំមេរ៉ាសុវត្ថិភាព និងការប្រើ **WiFi** សាធារណៈ
- ប្រើប្រាស់ **VPN** ដើម្បីផ្លាស់ប្តូរ **IP Address** ទីតាំងតំបន់និង **Encrypts** ការសន្ទនារបស់អ្នក។ **(ProtonVPN, RiseupVPN, TunnelBear)**

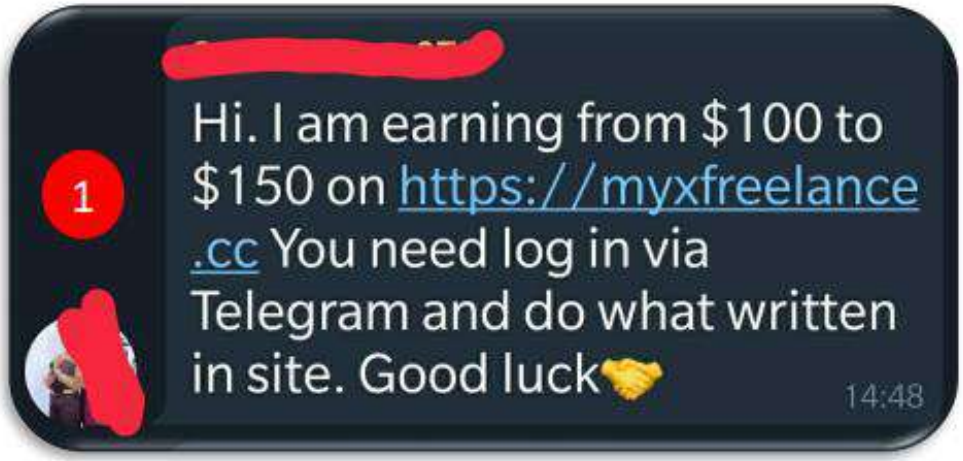
Phishing

ការឆបោកតាមអ៊ីនធឺណិត

“phishing” មកពីពាក្យថា “fishing”



Phishing គឺជាការឆបោកតាមអ៊ីនធឺណិត។ វាចាប់ផ្តើមជាមួយនឹងការប្រាស្រ័យទាក់ទងតាមរយៈ៖ អីមែល សារ ឬបណ្តាញសង្គម ដែលត្រូវបានរចនាឡើងដើម្បីមើលទៅដូចជាវាមកពីប្រភពដែលអាចទុកចិត្តបាន។

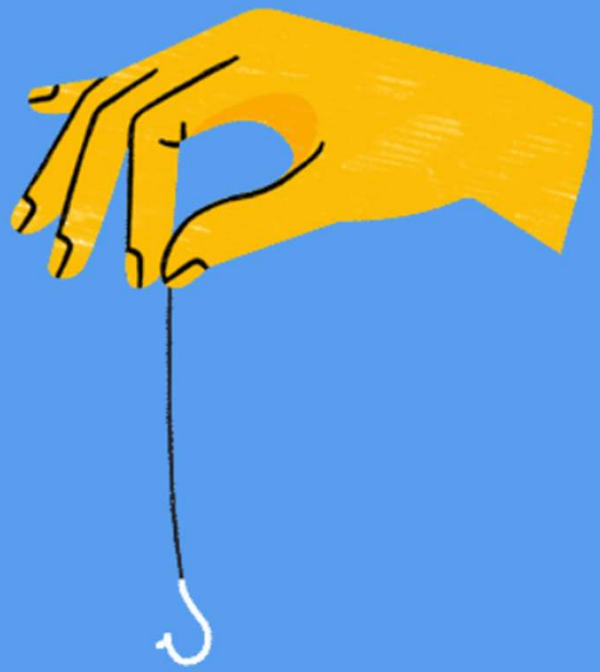


សារបោកប្រាស់ / បោកបញ្ឆោត

Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

TAKE THE QUIZ



https://phishingquiz.withgoogle.com/

សំនួរ និង ចម្លើយ

“អ្វីដែលមានសន្តិសុខថ្ងៃនេះ
ប្រហែលជាមិនមានសន្តិសុខទេនៅថ្ងៃស្អែក”

សូមបន្តសិក្សារៀនសូត្របន្ថែម

ស្វែងយល់បន្ថែម

- https://getcybersafe.ca
- **Totem project** – https://totem-project.org/
- **Digital first aid** – https://digitalfirstaid.org/en/topics/account-access-issues/
- **Journalist Tool Kits** – https://gcatoolkit.org/journalists/beyond-simple-passwords/?_tk=tools-for-2fa
- **Surveillance Self-Defense** – https://ssd.eff.org/
- **The Canadian organization Citizen Lab** – https://citizenlab.ca/

ស្វែងយល់បន្ថែម

- https://www.security.org/how-secure-is-my-password/
- https://haveibeenpwned.com/
- https://phishingquiz.withgoogle.com/
- https://2fa.directory/
- https://bit.ly/3vasc8k

ស្វែងយល់បន្ថែម

- 1Password – https://1password.com
- KeePass – https://keepassxc.org
- LastPass – https://lastpass.com
- VeraCrypt – https://www.veracrypt.fr/en/Downloads.html
- ProtonVPN – https://protonvpn.com/
- TunnelBear – https://www.tunnelbear.com