សុវត្ថិភាព និង ការពារទិន្នន័យ

Security & Data Protection

ជម្រាបសួរ និងសួស្តី

ខ្ញុំបាទឈ្មោះ **ស៊ឺន វិជ្ជ៉ា**

ជាមន្ត្រីផ្នែកអភិវឌ្ឍន៍គេហទំព័រ និងព័ត៌មានវិទ្យា

អង្គការទិន្នន័យអំពីការអភិវឌ្ឍ (ODC)

ហេតុអ្វីបានជាការពារទិន្នន័យមានសារៈសំខាន់?

- ការផ្លាស់ប្តូរទៅជាប្រព័ន្ធឌីជីថលកាន់តែច្រើនឡើង
- តម្លៃកើនឡើងនៃទិន្នន័យផ្ទាល់ខ្លួន ស្ថាប័ន និងក្រុមហ៊ុនរក្សាទុកក្នុងប្រព័ន្ធឌីជីថល
- ការលួចអត្តសញ្ញាណ ការលួចលក់ពត៌មាន ការខូចខាតកេរ្តិ៍ឈ្មោះ

អ្វីទៅជាការពារទិន្នន័យ ?

- ដើម្បីធានាថាទិន្នន័យមានសុវត្ថិភាព និងអាចចូលប្រើបានតែដោយបុគ្គលដែលមានសិទ្ធិ
- រួមមានការបំលែងកូដនីយកម្មសម្រាប់ទិន្នន័យ ការគ្រប់គ្រងការចូលប្រើ និងការផ្ទុកក្នុងប្រព័ន្ធសុវត្ថិភាព

ប្រភេទទិន្នន័យ

ទិន្នន័យផ្ទាល់ខ្លួន

- ឈ្មោះ អាសយដ្ឋាន លេខទូរស័ព្ទ អ៊ីមែល
- ទិន្នន័យរសើបៈ ព័ត៌មានសុខភាព ហិរញ្ញវត្ថុ ចំណង់ចំណូលចិត្ត

ទិន្នន័យស្ថាប័ន ឬក្រុមហ៊ុន

- កម្មសិទ្ធិបញ្ញា ព័ត៌មានសម្ងាត់ស្ថាប័ន និងទិន្នន័យអតិថិជន
- ព័ត៌មានហិរញ្ញវត្ថុ និងប្រតិបត្តិការ

គ្រោះថ្នាក់ដល់ទិន្នន័យ

ហានិភ័យ និងការប្រឈមទូទៅ៖

- ការវាយប្រហារបច្ចេកវិទ្យា (ឧ. Phishing, Ransomware)
- គ្រោះថ្នាក់ពីខាងក្នុង (ឧ. ការធ្វើឱ្យខូចដោយចេតនា ឬដោយអចេតនា)
- ការគ្រប់គ្រងការចូលដំណើរការខ្សោយ និងពាក្យសម្ងាត់ខ្សោយ
- ការខ្វះកូដនីយកម្ម និងវិធានការសុវត្ថិភាព

គោលការណ៍នៃការពារទិន្នន័យ

គោលការណ៍សំខាន់ៗ

- ការបង្រួមទិន្នន័យ៖ ប្រមូលតែអ្វីដែលចាំបាច់
- ការច្បាស់លាស់៖ ជម្រាបឱ្យអ្នកប្រើប្រាស់ដឹងអំពីការប្រមូល និងការប្រើប្រាស់ទិន្នន័យ
- សុវត្ថិភាព៖ ធ្វើឱ្យមានវិធានការការពារដ៏រឹងមាំ
- ការទទួលខុសត្រូវ៖ ការត្រួតពិនិត្យ និងសវនកម្មទៀងទាត់

របៀបធ្វើឱ្យទិន្នន័យមានសុវត្ថិភាព

សម្រាប់ស្ថាប័ន៖

- រៀបចំការវាយតម្លៃហានិភ័យជារឿយៗ
- បណ្តុះបណ្តាលបុគ្គលិកអំពីការពារទិន្នន័យ និងឯកជនភាព
- ប្រើប្រាស់ការផ្ទៀងផ្ទាត់អត្តសញ្ញាណ និងកូដនីយកម្មដ៏រឹងមាំ
- ដំណើរការទិន្នន័យ និងគោលនយោបាយការលុបចោលទិន្នន័យមិនចាំបាច់
- អនុវត្តតាមច្បាប់ និងបទប្បញ្ញត្តិពាក់ព័ន្ធ

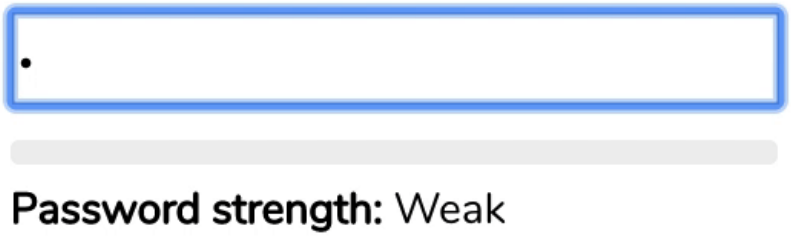
របៀបធ្វើឲ្យទិន្នន័យមានសុវត្ថិភាព (បន្ត)

សម្រាប់បុគ្គលៈ

- ប្រើពាក្យសម្ងាត់ខ្លាំង និងមានភាពប្លែក
- បើកប្រព័ន្ធផ្ទៀងផ្ទាត់ពីរកត្តា
- ប្រយ័ត្នចំពោះអ៊ីមែលក្លែងបន្លំ និងការបោកប្រាស់តាមប្រព័ន្ធផ្សេងៗ
- ពិនិត្យការកំណត់ឯកជនភាពលើកម្មវិធី និងឧបករណ៍ជានិច្ច

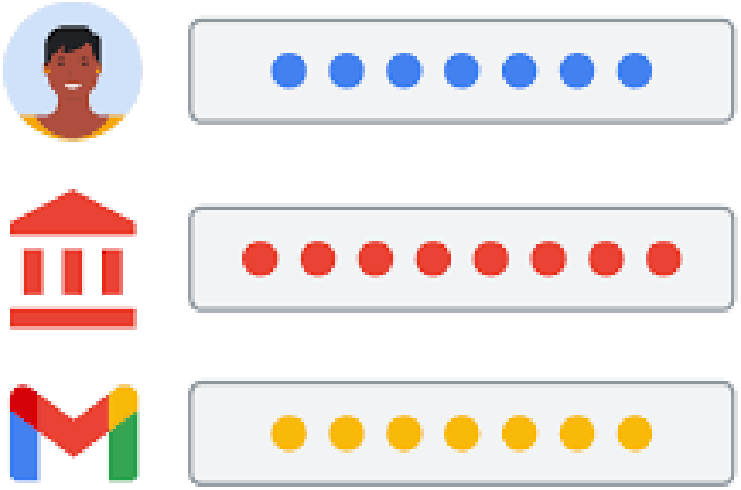
ពាក្យសម្ងាត់ មានសុវត្ថិភាព

- យ៉ាងហោចណាស់ 8-12 តួ
- បន្សំនៃ
  - “អក្សរធំ” A B C
  - “អក្សរតូច” a b c
  - “លេខ” 1 2 3
  - “សញ្ញា” ! @ # $

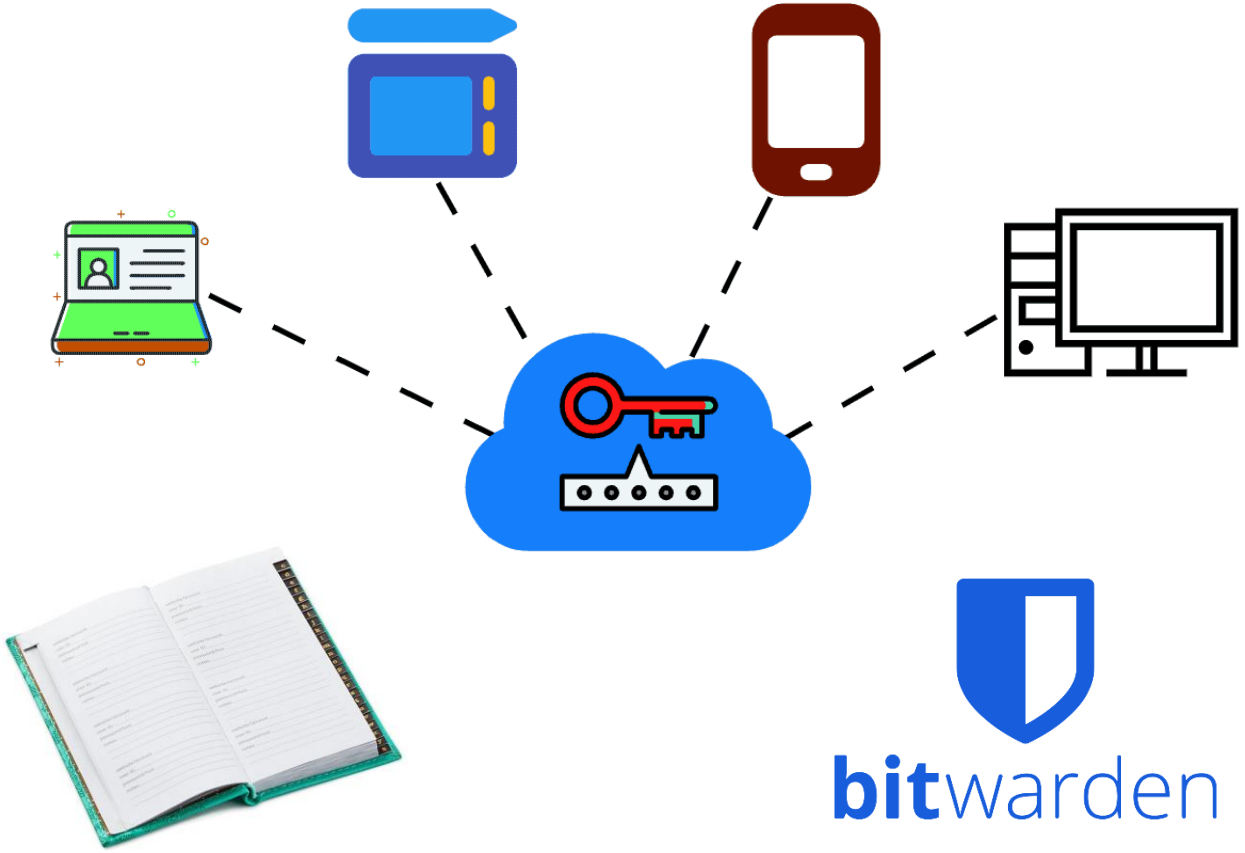


ពាក្យសម្ងាត់ មានសុវត្ថិភាព (បន្ត)

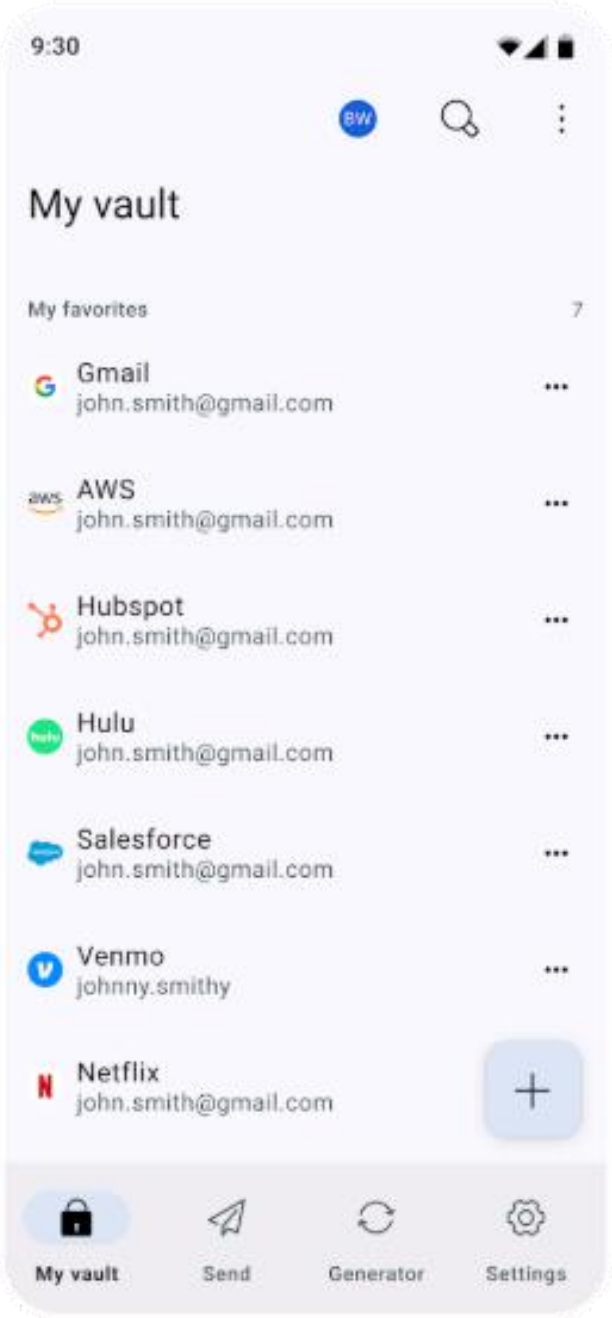
- មិនប្រើប្រាស់ពាក្យសម្ងាត់តែមួយ សម្រាប់គណនីអនឡាញច្រើន
- មិនប្រើព័ត៌មានដែលអាចទាយបាន៖
  - ឈ្មោះ
  - ថ្ងៃខែឆ្នាំកំណើត
  - អាសយដ្ឋាន លេខទូរស័ព្ទ
  - ពាក្យសាមញ្ញ ឧទាៈ football, pizza...



កម្មវិធីគ្រប់គ្រងពាក្យសម្ងាត់



bitwarden

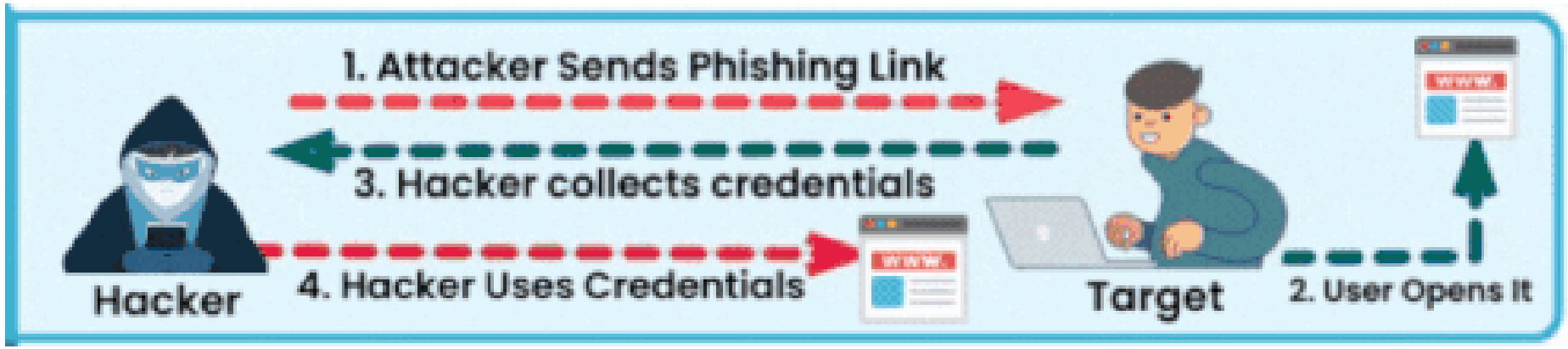


Phishing Attack មានទម្រង់បែបណាខ្លះ?

- សារជាអក្សរ (SMS)
- សារជាសម្លេង
- ការហៅទូរស័ព្ទ (Voice Call)
- អ៊ីម៉ែល
- QR Code

ការវាយប្រហារដោយបំភ័ន្ត (Phishing Attack)

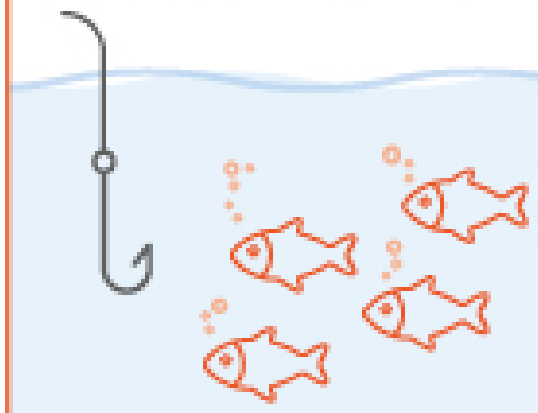
- ការបំភ័ន្តដោយប្រើប្រាស់ អ៊ីម៉ែល សារ ឬតំណរវេបសាយ ដើម្បីបន្លំយកព័ត៌មានសម្ងាត់ផ្ទាល់ខ្លួន
  - ពាក្យសម្ងាត់ លេខអត្តសញ្ញាណប័ណ្ណ លេខចូលគណនីធនាគារ



គោលដៅនៃការវាយប្រហារ

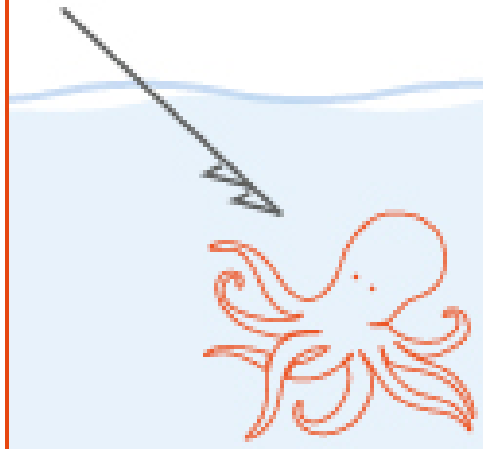
Phishing

មិនរើសមុខ



Spear phishing

មានគោលដៅ
ជាក់លាក់



Whaling

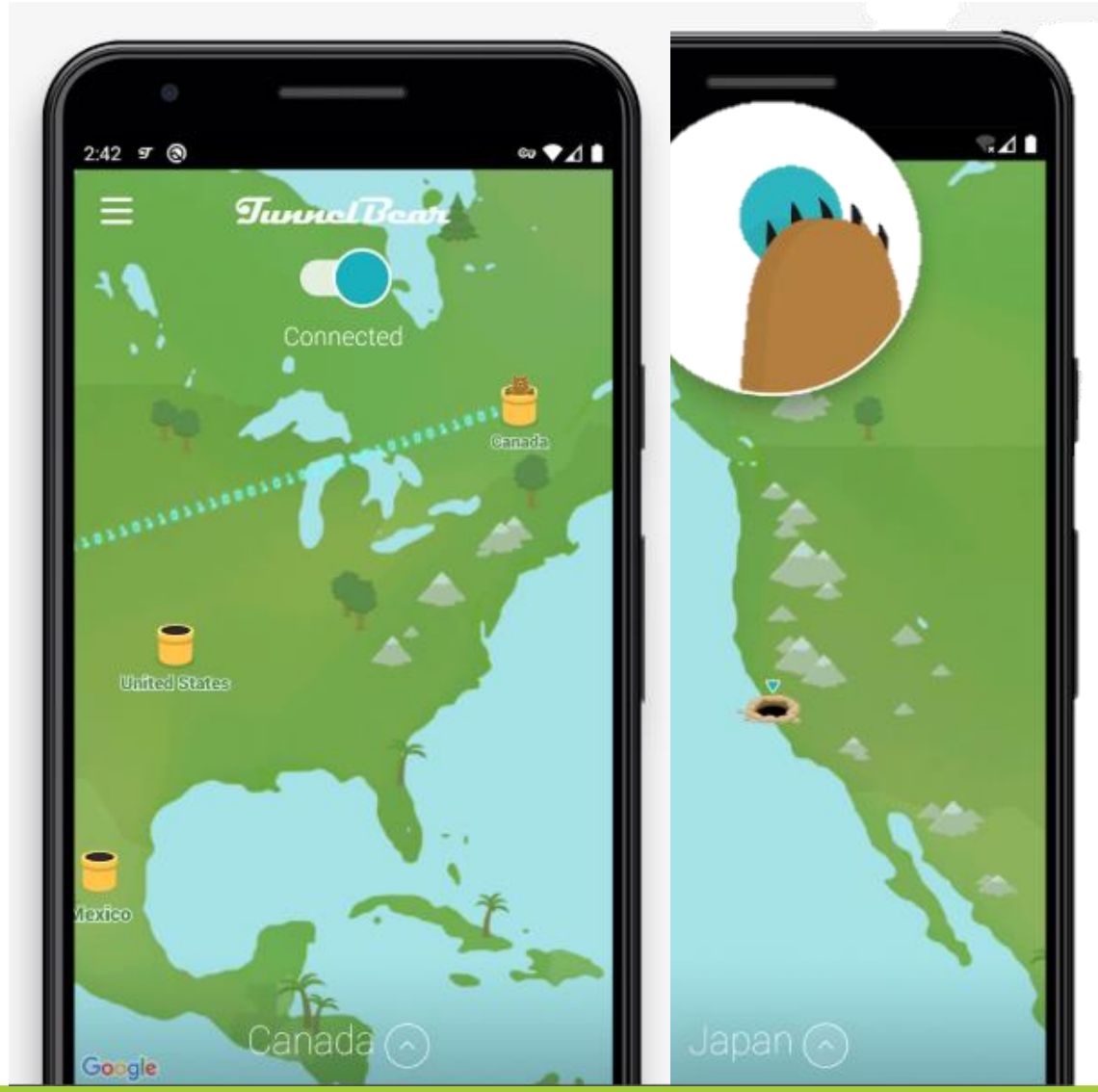
សំដៅអ្នកមានឋានៈ ឬ
តួនាទីខ្ពស់

សូមប្រើ VPN ពេលចាំបាច់

- បណ្តាញឯកជនសិប្បនិម្មិត

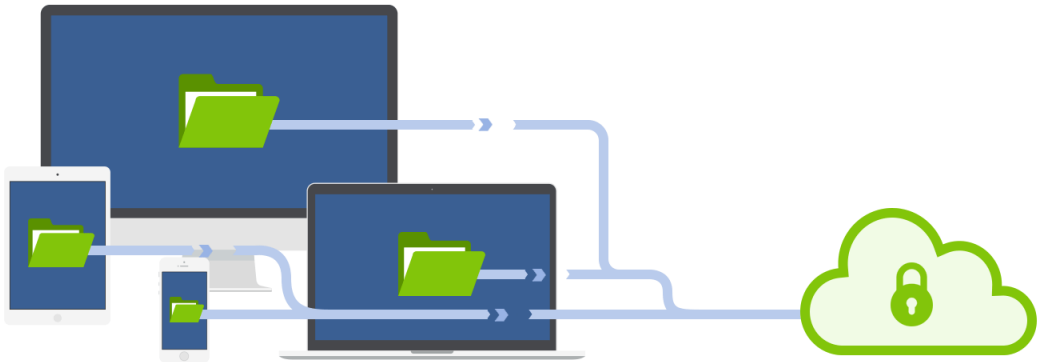
  Virtual Private Network

- ប្តូរទីតាំងបណ្តាញទៅប្រទេសផ្សេងៗ
- ការពារការតាមដានពីភាគីដទៃ



បែកអាប់ (Backup)

- Backup ឯកសារសំខាន់ៗទៅទីតាំងដែលមានសុវត្ថិភាព
  - បង្ការការបាត់បង់ទិន្នន័យ បើឧបករណ៍របស់អ្នកខូច បាត់ ឬត្រូវបានវាយប្រហារ
  - វិធីសាស្ត្រ 3-2-1 Backup គឺធ្វើការ Backup ទិន្នន័យរបស់អ្នកនៅ ៣ កន្លែងផ្សេងគ្នា
  - Physical Backup & Cloud Backup



Google Drive

OneDrive

ការប្រើប្រាស់ USB Flash Drives

- កុំជឿជាក់លើ USB ដែលមិនស្គាល់ប្រភព
- ស្កេន USB មុនពេលបើកប្រាស់
- បិទមុខងារ Autorun ឬ Autoplay
- ការពារ USB របស់អ្នកដោយប្រើកូដនីយកម្ម (encryption)
- ជៀសវាងការប្រើកុំព្យូទ័រជាសាធារណៈដែលគ្មានសុវត្ថិភាព

ដានជើងឌីជីថល

- រាល់សកម្មភាពនៅលើអនឡាញ តែងបន្សល់ “ដាន”
  - ចុច (Click)
  - ស្វែងរក (Search)
  - ទាញយក (Download)

កំណាកំហុសមនុស្ស

Human Error


តើទ្វារនេះអាច
ការពារបានល្អ
ដោយសារអ្វី?

- មនុស្សគឺជាខ្សែ**ការពារដំបូង**។
- ប្រុងប្រយ័ត្នជានិច្ច ទោះបីជាសំណើហាក់ដូចជាបានមកពីនរណាម្នាក់ដែលអ្នកទុកចិត្តក៏ដោយ។
- **ការយល់ដឹង** = ការការពារ។

- https://myshadow.org/
- https://www.security.org/
- https://duckduckgo.com/

សំណួរ ចម្លើយ