



Australian Government



ចាត់វិធានការឥឡូវនេះ។
រក្សាសុវត្ថិភាព។

របៀបដែលអ្នកអាចរក្សាសុវត្ថិភាព តាមអនឡាញ

កំណែងាយស្រួលអាន



របៀបប្រើប្រាស់សៀវភៅមគ្គុទ្ទេសក៍នេះ



យើងជាអ្នករៀនសូត្រគ្នា។

យើងបានសរសេរសៀវភៅមគ្គុទ្ទេសក៍នេះ។



យើងបានសរសេរពាក្យមួយចំនួនជាអក្សរ **ដិតក្រាស់**។

យើងពន្យល់ថាពាក្យទាំងនេះមានន័យយ៉ាងម៉េច។

ក៏មានបញ្ជីនៃពាក្យទាំងនេះផងដែរនៅលើទំព័រ 28។



អ្នកអាចស្នើសុំនរណាម្នាក់ដែលអ្នកទុកចិត្តសម្រាប់ការគាំទ្រដើម្បី៖

- អានសៀវភៅមគ្គុទ្ទេសក៍នេះ
- ស្វែងរកព័ត៌មានបន្ថែម។



នេះជាសេចក្តីសង្ខេបងាយស្រួលអានមួយទៀត។

វារួមបញ្ចូលតែគំនិតសំខាន់បំផុតប៉ុណ្ណោះ។



អ្នកអាចស្វែងរកសៀវភៅមគ្គុទ្ទេសក៍មួយផ្សេងទៀតនៅលើគេហទំព័រ
របស់យើង។

www.actnowstaysecure.gov.au

តើមានអ្វីខ្លះនៅក្នុងសៀវភៅមគ្គុទ្ទេសក៍នេះ?

អំពីសៀវភៅមគ្គុទ្ទេសក៍នេះ	4
រក្សាគណនីរបស់អ្នកឱ្យមានសុវត្ថិភាព	6
ពិនិត្យការកំណត់របស់អ្នក ដើម្បីការពារព័ត៌មានរបស់អ្នក	10
ការពារឧបករណ៍របស់អ្នក	16
ការឆបោក	20
ហ៊ាននិយាយ	25
បញ្ជីពាក្យ	28
ទាក់ទងមកយើង	30

អំពីសៀវភៅមគ្គុទ្ទេសក៍នេះ



យើងទាំងអស់គ្នាត្រូវការគិតអំពីរបៀបដែលយើង
អាចរក្សាសុវត្ថិភាពតាមអនឡាញ។
យើងហៅវាថាសុវត្ថិភាពតាមអ៊ីនធឺណិត។



តាមអ៊ីនធឺណិត មានន័យថាអ្វីមួយដែលធ្វើជាមួយអ៊ីនធឺណិត។



សៀវភៅមគ្គុទ្ទេសក៍នេះពន្យល់ពីរឿងមួយចំនួនដែលអ្នកអាចធ្វើ
បាន ដើម្បីការពារខ្លួនអ្នកផ្ទាល់តាមអនឡាញ។
ឧទាហរណ៍ ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។



ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតគឺនៅពេលឧក្រិដ្ឋជនប្រើប្រាស់អ៊ីនធឺណិត
សម្រាប់បទឧក្រិដ្ឋ។

ឧទាហរណ៍ ពួកគេអាចប្រើប្រាស់អ៊ីនធឺណិតដើម្បី៖

- លួចព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នក
- កាន់កាប់គណនី ឬកម្រងព័ត៌មានតាមអនឡាញរបស់អ្នក។

ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតអាចកើតឡើងនៅលើឧបករណ៍ណាមួយ។



នេះរួមមាននៅលើឧបករណ៍នានារបស់អ្នកដូចជា៖

- កុំព្យូទ័រ
- ស្មាតហ្វូន
- នាឡិកាដៃវៃឆ្លាត។



មានរឿងមួយចំនួនដែលអ្នកអាចធ្វើបានដើម្បីរក្សាសុវត្ថិភាព
ពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត។



យើងពន្យល់ពីអ្វីដែលអ្នកអាចធ្វើបាននៅលើទំព័រដូចខាងក្រោម។

រក្សាគណនីរបស់អ្នកឱ្យមានសុវត្ថិភាព



អ្នកគួរគិតអំពីរបៀបដែលអ្នកអាចរក្សាគណនីតាម
អនឡាញរបស់អ្នកឱ្យមានសុវត្ថិភាព។

ប្រើឃ្លាសម្ងាត់រឹងមាំ និងខុសគ្នា



ឃ្លាសម្ងាត់ គឺជាប្រភេទនៃពាក្យសម្ងាត់ដែលរឹងមាំជាង។
វាពិបាកខ្លាំងណាស់សម្រាប់មនុស្សដទៃទៀតក្នុងការស្មាន។



ការប្រើឃ្លាសម្ងាត់រឹងមាំ និងខុសគ្នាគឺជាវិធីដ៏ល្អបំផុត
មួយ ដើម្បីការពារគណនីរបស់អ្នក។



អ្នកគួរប្រើឃ្លាសម្ងាត់ខុសគ្នាសម្រាប់គណនីតាម
អនឡាញនីមួយៗរបស់អ្នក។



ឃ្លាសម្ងាត់រឹងមាំ រួមមាន៖

- 4 ពាក្យដែលរើសព្រាវៗ ឬច្រើនជាងនេះ
- 15 តួអក្សរ និងលេខ ឬច្រើនជាងនេះ។



អ្នកអាចរួមបញ្ចូលអក្សរធំមួយចំនួន។



អ្នកក៏អាចរួមបញ្ចូលនិមិត្តរូបផងដែរ ដូចជា៖

- សហសញ្ញា
- សញ្ញាដុល្លារ
- សញ្ញាអ៊ីមែល @។



អ្នកមិនគួរប្រើព័ត៌មានផ្ទាល់ខ្លួនណាមួយនៅក្នុងឃ្លាសម្ងាត់របស់អ្នកទេ។



ឧទាហរណ៍៖

- ថ្ងៃខែឆ្នាំកំណើតរបស់អ្នក
- ឈ្មោះសមាជិកគ្រួសារ ឬសត្វចិញ្ចឹមរបស់អ្នក។

បន្ថែមជំហានមួយចំនួនថែមទៀតដើម្បីចុះឈ្មោះចូលគណនីរបស់អ្នក



អ្នកអាចការពារគណនីតាមអនឡាញរបស់អ្នកជាមួយ

ការផ្ទៀងផ្ទាត់ពហុកត្តា (MFA)។

MFA គឺនៅពេលអ្នកប្រើវិធីខុសគ្នា 2 ឬច្រើន ដើម្បីចុះឈ្មោះចូលទៅក្នុងគណនីរបស់អ្នករៀងរាល់ពេល។



ឧទាហរណ៍ អ្នកអាចត្រូវការវាយបញ្ចូលឃ្លាសម្ងាត់របស់អ្នកជាមុន។

បន្ទាប់មក វាយបញ្ចូលលេខកូដដែលអ្នកទទួលបាននៅលើ

ទូរសព្ទរបស់អ្នក។

អ្នកអាចមានជម្រើសដើម្បី៖



- ទទួលបានកម្មវិធី app នៅលើទូរសព្ទរបស់អ្នក ដើម្បីផ្តល់លេខកូដដល់អ្នក



- ទទួលបានលេខកូដនៅក្នុងអ៊ីមែល



- ទទួលបានលេខកូដនៅក្នុងសារជាអត្ថបទ។



MFA ធ្វើឱ្យវាកាន់តែពិបាកសម្រាប់មនុស្សដទៃទៀតដើម្បីចូលទៅក្នុងគណនីតាមអនឡាញរបស់អ្នក។

ទោះបីជាពួកគេស្វែងរកឃើញឃ្លាសម្ងាត់របស់អ្នកក៏ដោយ។

ពិនិត្យការកំណត់របស់អ្នក ដើម្បីការពារព័ត៌មានរបស់អ្នក



អ្នកអាចពិនិត្យថាការកំណត់របស់អ្នកកំពុងការពារ
ព័ត៌មានតាមអនឡាញរបស់អ្នក។



នេះរួមមានការកំណត់នានារបស់អ្នកនៅលើ៖

- គណនីតាមអនឡាញ
- ឧបករណ៍
- កម្មវិធី app។



អ្នកអាច៖

- ផ្លាស់ប្តូរការកំណត់របស់អ្នក
- ជ្រើសរើសកម្មវិធី app អ្វីខ្លះដែលអាចប្រើព័ត៌មានរបស់អ្នក។

អ្នកអាចស្វែងរកការកំណត់នៅលើឧបករណ៍របស់អ្នកដោយ៖



- រកមើលរូបតំណាងស្តីចក្រ (gear)
- ឬ
- វាយបញ្ចូល 'ការកំណត់' ទៅក្នុងរបារស្វែងរករបស់ឧបករណ៍អ្នក។



អ្នកអាចរកឃើញការកំណត់នានានៅក្នុងកម្មវិធី app ឬគណនីតាមអនឡាញដោយបើកម៉ឺនុយ។

ជារឿយៗ ម៉ឺនុយមើលទៅដូចខ្សែបន្ទាត់ត្រង់ 3។



ការកំណត់មួយចំនួនទាំងនេះអាចចែករំលែកព័ត៌មានអំពី៖

- អ្នកជានរណា
- កន្លែងដែលអ្នកស្ថិតនៅ
- កន្លែងដែលអ្នករស់នៅ។



ការចែករំលែកព័ត៌មាននេះតាមអនឡាញ អាចធ្វើឱ្យ
អ្នកប្រឈមហានិភ័យនៃឧក្រិដ្ឋជនកម្មតាមអ៊ីនធឺណិត។



ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតអាចប្រើប្រាស់ព័ត៌មានរបស់អ្នក
ដើម្បីធ្វើពុតជាអ្នក។

ឧទាហរណ៍ ពួកគេអាចប្រើប្រាស់ព័ត៌មានដូចជា៖



- កន្លែងដែលអ្នករស់នៅ



- ឈ្មោះសមាជិកគ្រួសាររបស់អ្នក



- ឈ្មោះសត្វចិញ្ចឹមរបស់អ្នក។



អ្នកអាចកំណត់គណនីរបស់អ្នក ដើម្បីឱ្យតែមនុស្សដែលអ្នកស្គាល់
អាចមើលឃើញកម្រងព័ត៌មានប្រព័ន្ធផ្សព្វផ្សាយសង្គមរបស់អ្នក។

ឧទាហរណ៍ កម្រងព័ត៌មាន Facebook របស់អ្នក។



ជាធម្មតា ការកំណត់ទាំងនេះត្រូវបានគេហៅថា
ការកំណត់ឯកជនភាព។



អ្នកក៏អាចគ្រប់គ្រង ការកំណត់ទីតាំងរបស់អ្នក។
ការកំណត់ទីតាំងបង្ហាញកន្លែងដែលឧបករណ៍របស់អ្នកស្ថិតនៅ។



អ្នកក៏អាចបិទ ឬបើកការកំណត់ទីតាំងបាន។
អ្នកក៏អាចជ្រើសរើសកម្មវិធី app ណាមួយដែលអាចប្រើ
ការកំណត់ទីតាំងរបស់អ្នក។



អ្នកអាចធ្វើដូចនេះសម្រាប់៖

- គណនីតាមអនឡាញរបស់អ្នក
- ឧបករណ៍របស់អ្នក
- កម្មវិធី app របស់អ្នក។

កម្មវិធី app មួយចំនួនក៏អាចស្នើសុំអ្នកផងដែរ ប្រសិនបើវាអាច៖



- ប្រើកាមេរ៉ារបស់អ្នក



- មើលរូបថតរបស់អ្នក។



អ្នកគួរអនុញ្ញាតតែកម្មវិធី app ដែលអ្នកស្គាល់ប៉ុណ្ណោះឱ្យប្រើកាមេរ៉ា និងរូបថតរបស់អ្នក។

ការពារឧបករណ៍របស់អ្នក



អ្នកគួរគិតអំពីរបៀបដែលអ្នកអាចការពារឧបករណ៍របស់អ្នក
ដើម្បីជួយរក្សាអ្នកឱ្យមានសុវត្ថិភាពតាមអនឡាញ។
ឧទាហរណ៍ ទូរសព្ទ ឬនាឡិកាផៃឡាតរបស់អ្នក។



រឿងនេះសំខាន់សម្រាប់ឧបករណ៍នានាដែលភ្ជាប់ទៅអ៊ីនធឺណិត។

ធ្វើបច្ចុប្បន្នភាពឧបករណ៍របស់អ្នក



អ្នកអាចធ្វើបច្ចុប្បន្នភាពឧបករណ៍របស់អ្នក ដើម្បីរក្សាវាឱ្យមានសុវត្ថិ
ភាពតាមអនឡាញ។
ឧទាហរណ៍ ទូរសព្ទ និងកុំព្យូទ័រយួរដៃ ឬនាឡិកាផៃឡាតរបស់អ្នក។



ឧបករណ៍របស់អ្នករបស់អ្នកអាចហៅវាថា
ការធ្វើបច្ចុប្បន្នភាពសុហ្វវែរ។



ការធ្វើបច្ចុប្បន្នភាពជួយការពារឧបករណ៍ខ្លួនពី
ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត។



អ្នកអាចកំណត់ឧបករណ៍ឱ្យបើកការធ្វើបច្ចុប្បន្នភាពដោយខ្លួនវា
ផ្ទាល់បាន។



អ្នកអាចស្វែងយល់បន្ថែមអំពីរបៀបធ្វើបច្ចុប្បន្នភាពឧបករណ៍របស់
អ្នកនៅលើគេហទំព័ររបស់យើង។

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

បណ្តាញ Wi-Fi សាធារណៈ



អ្នកគួរប្រុងប្រយ័ត្ននៅពេលអ្នកប្រើ **Wi-Fi សាធារណៈ**។



Wi-Fi សាធារណៈ គឺជាអ៊ីនធឺណិតឥតខ្សែមិនគិតថ្លៃ
ដែលអ្នកអាចប្រើនៅទីកន្លែងសាធារណៈ។



ឧទាហរណ៍ នៅ៖

- ហាងកាហ្វេ
- ព្រលានយន្តហោះ
- សណ្ឋាគារ។



អ្នកគួរប្រុងប្រយ័ត្នអំពីព័ត៌មានអ្វីខ្លះដែលអ្នកបញ្ចូលទៅក្នុង គេហទំព័រមួយ ដោយប្រើ Wi-Fi សាធារណៈ។



ឧទាហរណ៍ ដូចជា៖

- ព័ត៌មានលម្អិតធនាគារ
- គណនីអ៊ីមែល
- កម្រងព័ត៌មានប្រព័ន្ធផ្សព្វផ្សាយសង្គមរបស់អ្នក។



ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតខ្លះអាចប្រើ Wi-Fi សាធារណៈដើម្បី៖

- មើលអ្វីដែលអ្នកកំពុងធ្វើនៅតាមអនឡាញ
- លួចព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នក។

នេះដោយសារតែ៖



- អ្នកណាក៏អាចប្រើវាបាន



- វាកាន់តែពិបាកក្នុងការការពារឧបករណ៍របស់អ្នក។



អ្នកអាចស្វែងយល់ពីរបៀបរក្សាសុវត្ថិភាព នៅពេលប្រើ Wi-Fi
សាធារណៈ នៅលើគេហទំព័ររបស់យើង។

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

ការឆបោក



យើងហៅវាថា **ការឆបោក** នៅពេលនរណាម្នាក់ព្យាយាម៖

- បញ្ឆោតអ្នក
- យកប្រាក់របស់អ្នក។



អ្នកឆបោក គឺជានរណាម្នាក់ដែលធ្វើការឆបោក។

អ្នកឆបោកអាចព្យាយាមបញ្ឆោតអ្នកតាមរយៈ៖



- សារជាអត្ថបទ ឬការហៅទូរសព្ទ
- អ៊ីមែល
- ប្រព័ន្ធផ្សព្វផ្សាយសង្គម
- គេហទំព័រ។



ពួកគេអាចមើលទៅដូចជារាក់ទាក់។

ប៉ុន្តែពួកគេអាចបញ្ឆោតអ្នកឱ្យផ្តល់ឱ្យពួកគេនូវព័ត៌មានរបស់អ្នក។

ពួកគេអាចប្រើប្រាស់វាដើម្បី៖



- ចូលទៅក្នុងគណនីតាមអនឡាញរបស់អ្នក



- ធ្វើពុតថាជាអ្នក



- លួចប្រាក់របស់អ្នក។

អ្នកឆបោកក៏អាច៖



- បង្កើតគណនីក្លែងក្លាយដើម្បីបញ្ឆោតអ្នកផងដែរ



- ចែករំលែកតំណ និងការផ្សាយពាណិជ្ជកម្មដើម្បីឱ្យអ្នកចុចលើវា។

របៀបសម្គាល់មើលការឆបោក

វាអាចជាការឆបោក ប្រសិនបើវា៖



- ស្នើសុំឱ្យអ្នកធ្វើអ្វីមួយឱ្យលឿន



- ផ្តល់ឱ្យអ្នកនូវប្រាក់ជាច្រើន



- សុំប្រាក់អ្នក



- ស្នើសុំអ្នកឱ្យចុចលើតំណមួយ។



អ្នកបោកក៏អាចធ្វើពុតជាអង្គការមួយដែលអ្នកស្គាល់ និងទុកចិត្ត។
ឧទាហរណ៍ ធនាគាររបស់អ្នក។



អ្នកបោកធ្វើដូចនេះដើម្បីឱ្យអ្នកចែករំលែក
ព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នកជាមួយពួកគេ។



អ្នកគួរតែឈប់និយាយជាមួយបុគ្គលនោះ
ប្រសិនបើអ្នកគិតថាពួកគេជាអ្នកបោក។



អ្នកគួរតែពិនិត្យមើលថាបុគ្គលនោះជានរណា
ដែលពួកគេនិយាយថាពួកគេជាអ្នកណានោះ។
អ្នកអាចទាក់ទងបុគ្គល ឬអង្គការនោះដោយប្រើព័ត៌មានលម្អិត
ដែលអ្នកទុកចិត្ត និងបានរកឃើញដោយខ្លួនអ្នកផ្ទាល់។



ចាត់វិធានការឱ្យបានលឿនដើម្បីការពារខ្លួនអ្នកផ្ទាល់
ប្រសិនបើអ្វីមួយមានអារម្មណ៍ថាមិនត្រឹមត្រូវទេ។

ការរាយការណ៍អំពីការឆបោក



Scamwatch (ការឃ្លាំមើលការឆបោក) ជួយពលរដ្ឋអូស្ត្រាលី៖

- យល់ដឹងអំពីការឆបោក
- រាយការណ៍អំពីការឆបោក។



Scamwatch (ការឃ្លាំមើលការឆបោក) ក៏ជួយពលរដ្ឋ
អូស្ត្រាលីដែលបានជួបប្រទះការឆបោកផងដែរ។



អ្នកអាចរាយការណ៍អំពីការឆបោកនៅលើគេហទំព័រ

Scamwatch (ការឃ្លាំមើលការឆបោក)។

www.scamwatch.gov.au/report-a-scam

ហ៊ាននិយាយ



អ្នកគួរហ៊ាននិយាយអំពីរបៀបដែលអ្នកដទៃទៀតអាចការពារខ្លួនពួកគេបានតាមអនឡាញ។

នេះរួមមាន៖



- ការរាយការណ៍អំពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត



- ការចែករំលែកអ្វីដែលអ្នកដឹងជាមួយគ្រួសារ និងមិត្តភក្តិ។



យើងពន្យល់ពីរបៀបដែលអ្នកអាចហ៊ាននិយាយនៅលើទំព័រខាងក្រោម។

របាយការណ៍អំពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត

ការរបាយការណ៍អំពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត ជួយរដ្ឋាភិបាល៖



- ស្វែងយល់ពីរបៀបដែលឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតព្យាយាមវាយប្រហារមនុស្ស



- ការការពារមនុស្សបានកាន់តែច្រើន។



អ្នកអាចរបាយការណ៍អំពីឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតនៅលើគេហទំព័រ
ReportCyber (របាយការណ៍តាមអ៊ីនធឺណិត)។

www.cyber.gov.au/report

និយាយជាមួយជាមួយក្រុមគ្រួសារ និងមិត្តភក្តិអំពីការរក្សាសុវត្ថិភាពតាមអនឡាញ



អ្នកគួរចែករំលែកគន្លឹះអំពីការបន្តនៅមានសុវត្ថិភាព តាមអនឡាញ
ជាមួយជាមួយគ្រួសារ និងមិត្តភក្តិរបស់អ្នក។

អ្នកអាចស្វែងយល់ពីពួកគេផងដែរ។



អ្នកអាចការពារខ្លួនអ្នកផ្ទាល់ និងមនុស្សនៅជុំវិញអ្នក ដោយចែក
រំលែកនូវអ្វីដែលអ្នកដឹងអំពីការរក្សាសុវត្ថិភាពតាមអនឡាញ។



រឿងនេះក៏សំខាន់ផងដែរ ប្រសិនបើអ្នកចែករំលែក
ឧបករណ៍នានាជាមួយអ្នកដទៃ។

បញ្ជីពាក្យ

បញ្ជីនេះពន្យល់ពីអត្ថន័យនៃអក្សរ**ជិតក្រាស់** នៅក្នុងសៀវភៅមគ្គុទ្ទេសក៍នេះ។



តាមអ៊ីនធឺណិត

តាមអ៊ីនធឺណិត មានន័យថាអ្វីមួយទាក់ទងជាមួយអ៊ីនធឺណិត។



ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត

ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិតគឺនៅពេលឧក្រិដ្ឋជន

ប្រើប្រាស់អ៊ីនធឺណិតសម្រាប់បទឧក្រិដ្ឋ។

ឧទាហរណ៍ ពួកគេអាចប្រើប្រាស់អ៊ីនធឺណិតដើម្បី៖

- លួចព័ត៌មានផ្ទាល់ខ្លួនរបស់អ្នក
- កាន់កាប់គណនីតាមអនឡាញរបស់អ្នក។



ការកំណត់ទីតាំង

ការកំណត់ទីតាំងបង្ហាញកន្លែងដែលឧបករណ៍របស់អ្នកស្ថិតនៅ។



ការផ្ទៀងផ្ទាត់ពហុកត្តា (MFA)

MFA គឺនៅពេលអ្នកប្រើវិធីខុសគ្នា 2 ឬច្រើន ដើម្បីចុះឈ្មោះចូលទៅក្នុងគណនីរបស់អ្នករៀងរាល់ពេល។



ឃ្លាសម្ងាត់

ឃ្លាសម្ងាត់ គឺជាប្រភេទនៃពាក្យសម្ងាត់ដែលរឹងមាំជាង។

វាពិបាកខ្លាំងណាស់សម្រាប់មនុស្សដទៃទៀតក្នុងការស្មាន។



Wi-Fi សាធារណៈ

Wi-Fi សាធារណៈ គឺជាអ៊ីនធឺណិតឥតខ្សែមិនគិតថ្លៃដែលអ្នកអាចប្រើនៅទីកន្លែងសាធារណៈ។



ការទូទាត់

យើងហៅវាថាការទូទាត់ នៅពេលនរណាម្នាក់ព្យាយាម៖

- បញ្ឆោតអ្នក
- យកប្រាក់របស់អ្នក។



អ្នកទូទាត់

អ្នកទូទាត់ គឺជានរណាម្នាក់ដែលធ្វើការទូទាត់។

ទាក់ទងមកយើង



អ្នកអាចហៅទូរសព្ទទៅបណ្តាញទូរសព្ទទាន់ហេតុការណ៍ស្តីពីសន្តិសុខតាមអ៊ីនធឺណិតអូស្ត្រាលី (Australian Cyber Security Hotline)។

1300 292 371



អ្នកអាចចូលមើលគេហទំព័ររបស់យើង។

www.actnowstaysecure.gov.au



អ្នកអាចរាយការណ៍ឧក្រិដ្ឋកម្មតាមអ៊ីនធឺណិត នៅលើគេហទំព័រ ReportCyber (រាយការណ៍តាមអ៊ីនធឺណិត)។

www.cyber.gov.au/report



ក្រុមចូលប្រើប្រាស់ព័ត៌មាន បានបង្កើតឯកសារងាយស្រួលអាននេះ

ដោយប្រើរូបថតដែលបានផ្តល់ មានអាជ្ញាប័ណ្ណ និងរូបភាពតម្រូវតាមបុគ្គល។

រូបភាពនានាអាចមិនត្រូវបានប្រើឡើងវិញ ដោយគ្មានការអនុញ្ញាតឡើយ។

សម្រាប់ការសាកសួរណាមួយអំពីរូបភាព សូមចូលមើលគេហទំព័រ

www.informationaccessgroup.com។ លេខសម្រង់ការងារ 6342។