Australian Government

तुरून्त कदम चाल्नुहोस्।
सुरक्षित रहनुहोस्।

अनलाइनमा कसरी सुरक्षित रहने

सरल पठन संस्करण

Easy Read

यो निर्देशिका कसरी प्रयोग गर्ने

हामी अष्ट्रेलियाली सरकार हौं।

यो निर्देशिका हामीले लेखेका हौं।

हामीले केही शब्दहरू **गाढा अक्षरमा** लेखेका छौं।

हामी यी शब्दहरूको अर्थ बुझाउँछौं।

यी शब्दहरूको सूची पृष्ठ 28 मा पनि छ।

तपाईंले सहयोगका लागि आफूले भरोसा गरेको व्यक्तिलाई निम्न कुराहरू गरिदिन भन्न सक्नुहुन्छ:

- यो निर्देशिका पढ्न
- थप जानकारी खोज्न।

यो अर्को निर्देशिकाको 'सरल पठन' (Easy Read) सारांश हो।

यसमा सबैभन्दा महत्त्वपूर्ण कुराहरू मात्र समावेश गरिएका छन्।

तपाईंले अर्को निर्देशिका हाम्रो वेबसाइटमा फेला पार्न सक्नुहुन्छ।

www.actnowstaysecure.gov.au

यो निर्देशिकामा के छ?

यो निर्देशिकाको बारेमा	4
आफ्ना खाताहरू सुरक्षित राख्नुहोस्	6
आफ्नो जानकारी सुरक्षित राख्न आफ्ना सेटिङहरू जाँच गर्नुहोस्	10
आफ्ना उपकरणहरू सुरक्षित राख्नुहोस्	16
ठगी	20
आवाज उठाउनुहोस्	25
शब्द सूची	28
हामीलाई सम्पर्क गर्नुहोस्	30

यो निर्देशिकाको बारेमा

हामी सबैले अनलाइनमा कसरी सुरक्षित रहने भन्ने बारे सोच्न आवश्यक छ।

हामी यसलाई **साइबर** सुरक्षा भन्छौं।

साइबर भन्नाले इन्टरनेटसँग सम्बन्धित कुरालाई बुझाउँछ।

यो निर्देशिकाले अनलाइनमा आफूलाई सुरक्षित राख्न तपाईंले गर्नसक्ने केही उपायहरूका बारेमा बताउँछ।

उदाहरणका लागि, **साइबर अपराध**बाट।

साइबर अपराध भनेको अपराधीहरूले अपराधका लागि इन्टरनेटको प्रयोग गर्नु हो।

उदाहरणका लागि, उनीहरूले निम्न कामका लागि इन्टरनेटको प्रयोग गर्न सक्छन्:

- तपाईंका व्यक्तिगत विवरणहरू चोर्न
- तपाईंका अनलाइन खाता वा प्रोफाइलहरू कब्जा गर्न।

साइबर अपराध जुनसुकै उपकरणमा हुनसक्छ।

यसमा तपाईंका निम्न उपकरणहरू पर्दछन्:

- कम्प्युटर
- स्मार्टफोन
- स्मार्ट घडी।

साइबर अपराधबाट सुरक्षित रहन तपाईंले गर्नसक्ने केही उपायहरू छन्।

के गर्न सकिन्छ भन्ने बारेमा हामीले निम्न पृष्ठहरूमा बताएका छौं।

आफ्ना खाताहरू सुरक्षित राख्नुहोस्

तपाईंले आफ्नो अनलाइन खाताहरू कसरी सुरक्षित राख्न सक्नुहुन्छ भन्ने बारेमा सोच्नुपर्छ।

बलियो र फरक पासफ्रेज प्रयोग गर्नुहोस्

पासफ्रेज एउटा बलियो प्रकारको पासवर्ड हो।

अरू मानिसहरूलाई यसको अनुमान लगाउन धेरै गाह्रो हुन्छ।

बलियो र फरक-फरक पासफ्रेजहरू (passphrases) प्रयोग गर्नु आफ्ना खाताहरू सुरक्षित राख्ने सबैभन्दा राम्रा उपायहरू मध्ये एक हो।

तपाईंले आफ्नो प्रत्येक अनलाइन खाताको लागि फरक पासफ्रेज प्रयोग गर्नुपर्छ।

बलिया पासफ्रेजहरूमा निम्न पर्दछन्:

- ४ वा सोभन्दा बढी असम्बन्धित शब्दहरू
- १५ वा सोभन्दा बढी अक्षर र अङ्कहरू।

तपाईंले केही ठूला (क्यापिटल) अक्षरहरू समावेश गर्न सक्नुहुन्छ।

तपाईं निम्न जस्ता चिह्नहरू पनि प्रयोग गर्न सक्नुहुन्छ:

- ड्यास
- डलर
- इमेल @ चिह्न।

तपाईंले आफ्ना पासफ्रेजहरूमा कुनै पनि व्यक्तिगत जानकारी प्रयोग गर्नु हुँदैन।

उदाहरण:

- तपाईंको जन्मदिन
- तपाईंको परिवारका सदस्यहरू वा घरपालुवा जनावरहरूका नाम।

आफ्नो खातामा लग इन (प्रवेश) गर्न अतिरिक्त चरणहरू थप्नुहोस्

तपाईंले आफ्ना अनलाइन खाताहरूलाई **बहु-कारक प्रमाणीकरण (MFA)** मार्फत सुरक्षित गर्न सक्नुहुन्छ।

MFA भनेको तपाईंले आफ्नो खातामा हरेक पटक लग इन गर्न २ वा बढी फरक तरिकाहरू प्रयोग गर्नु हो।

उदाहरणका लागि, तपाईंले पहिले आफ्नो पासफ्रेज लगाउनुपर्ने हुनसक्छ।

त्यसपछि तपाईंले आफ्नो फोनमा प्राप्त हुने कोड लाउनु हुन्छ।

तपाईंसँग निम्न विकल्प हुन सक्छन्:

- कोड प्राप्त गर्न आफ्नो फोनमा एउटा एप राख्ने

- कोड इमेलमा प्राप्त गर्ने

- कोड पाठ्य सन्देशमा प्राप्त गर्ने।

MFA ले अन्य मानिसहरूलाई तपाईंको अनलाइन खाताहरूमा पहुँच गर्न गाह्रो बनाउँछ।

तिनीहरूले तपाईंको पासफ्रेज पत्ता लगाए पनि।

आफ्नो जानकारी सुरक्षित राख्न आफ्ना सेटिङहरू जाँच गर्नुहोस्

तपाईं आफ्ना सेटिङहरूले तपाईंको जानकारी अनलाइनमा सुरक्षित राखिरहेका छन् कि छैनन् भनेर जाँच गर्न सक्नुहुन्छ।

यसमा तपाईंका निम्न सेटिङहरू पर्दछन्:

- अनलाइन खाताका
- उपकरणका
- एयापका।

तपाईंले:

- आफ्ना सेटिङहरू परिवर्तन गर्न सक्नुहुन्छ
- तपाईंको जानकारी कुन एपहरूलाई प्रयोग गर्न दिने भन्ने कुरा छनौट गर्न सक्नुहुन्छ।

तपाईंले आफ्नो उपकरणमा सेटिङहरू निम्न तरिकाले फेला पार्न सक्नुहुन्छ:

- गियर चित्र खोजेर

वा

- आफ्नो उपकरणको खोज पट्टीमा (सर्च बारमा) 'settings' टाइप गरेर।

तपाईंले मेनु खोलेर एप वा अनलाइन खातामा सेटिङहरू फेला पार्न सक्नुहुन्छ।

मेनु प्रायः ३ वटा सिधा रेखाहरू जस्तो देखिन्छ।

यी मध्ये केही सेटिङहरूले निम्न बारे जानकारी साझा गर्नसक्छन्:

- तपाईं को हुनुहुन्छ
- तपाईं कहाँ हुनुहुन्छ
- तपाईं कहाँ बस्नुहुन्छ।

यो जानकारी अनलाइन साझा गर्नाले तपाईंलाई साइबर अपराधको जोखिममा पार्नसक्छ।

साइबर अपराधीहरूले तपाईंको जानकारी प्रयोग गरेर उनीहरू तपाईं भएको नाटक गर्न सक्छन्।

उदाहरणका लागि, तिनीहरूले निम्न जानकारी प्रयोग गर्न सक्छन्:

- तपाईँ कहाँ बस्नुहुन्छ

- तपाईंको परिवारका सदस्यहरूको नाम

- तपाईंका घरपालुवा जनावरहरूको नाम।

तपाईंले आफ्ना खाताहरू तपाईंले चिन्ने व्यक्तिहरूले मात्र तपाईंको सामाजिक सञ्जाल प्रोफाइलहरू हेर्नसक्ने बनाउन सक्नुहुन्छ।

उदाहरणका लागि, तपाईंको फेसबुक प्रोफाइल।

यी सेटिङहरूलाई सामान्यतया गोपनीयता सेटिङस् भनिन्छ।

तपाईं आफ्नो **location settings (स्थान सेटिङहरू)** पनि नियन्त्रण गर्न सक्नुहुन्छ।

स्थान सेटिङहरूले तपाईंको उपकरण कहाँ छ भनेर देखाउँछ।

तपाईं स्थान सेटिङहरू सक्रिय वा निष्क्रिय राख्न सक्नुहुन्छ।

तपाईं कुन एपहरूलाई तपाईंको स्थान सेटिङहरू प्रयोग गर्न दिने भन्ने कुरा पनि छनौट गर्न सक्नुहुन्छ।

यो तपाईंले आफ्ना निम्न कुराका लागि गर्न सक्नुहुन्छ:

- अनलाइन खाताहरू
- उपकरणहरू
- एयापहरू।

केही एयापहरूले तपाईंलाई निम्न कुराहरूका लागि अनुमति पनि माग्न सक्छन्:

- तपाईंको क्यामेरा प्रयोग गर्न

- तपाईंका फोटोहरू हेर्न

तपाईंले आफूलाई राम्रोसँग थाहा भएका एपहरूलाई मात्र आफ्नो क्यामेरा र फोटोहरू प्रयोग गर्न दिनुपर्छ।

आफ्ना उपकरणहरू सुरक्षित राख्नुहोस्

अनलाइनमा सुरक्षित रहनका लागि तपाईंका उपकरणहरूलाई कसरी सुरक्षित राख्ने भन्ने बारे तपाईंले सोच्नुपर्छ।

उदाहरणका लागि, तपाईंको फोन वा स्मार्ट घडी।

इन्टरनेटमा जडान हुने उपकरणहरूका लागि यो महत्त्वपूर्ण छ।

आफ्ना उपकरणहरू अद्यावधिक गर्नुहोस्

तपाईं आफ्ना उपकरणहरू अनलाइनमा सुरक्षित राख्न अद्यावधिक गर्न सक्नुहुन्छ।

उदाहरणका लागि, तपाईंको फोन र ल्यापटप।

तपाईंको उपकरणले यसलाई सफ्टवेयर अपडेट भन्नसक्छ।

अपडेटहरूले उपकरणलाई साइबर अपराधबाट जोगाउन मद्दत गर्दछ।

तपाईंले आफ्नो उपकरण आफैं अपडेट हुने बनाउन सक्नुहुन्छ।

तपाईं हाम्रो वेबसाइटमा आफ्ना उपकरणहरू कसरी अपडेट गर्ने भन्ने बारे थप जान्न सक्नुहुन्छ।

www.actnowstaysecure.gov.au/cyber-safe-actions

सार्वाजनिक वाइ-फाइ नेटवर्कहरू

सार्वजनिक वाइफाइ प्रयोग गर्दा सावधानी अपनाउनुपर्छ।

सार्वजनिक वाइफाइ भनेको नि:शुल्क वायरलेस इन्टरनेट हो जुन तपाईंले सार्वजनिक स्थानहरूमा प्रयोग गर्न सक्नुहुन्छ।

उदाहरणका लागि निम्न स्थानमा:

- क्याफे
- विमानस्थल
- होटल।

सार्वजनिक वाइफाइ प्रयोग गरी वेबसाइटमा कस्ता जानकारी हाल्ने भन्नेमा तपाईंले सावधान रहनुपर्छ।

उदाहरणका लागि, तपाईंका:

- बैंक विवरणहरू
- इमेल खाताहरू
- सामाजिक सञ्जालका प्रोफाइलहरू।

केही साइबर अपराधीहरूले सार्वजनिक वाइफाइको प्रयोग निम्न कुराहरूका लागि गर्नसक्छन्:

- तपाईंले अनलाइनमा के गरिरहनुभएको छ भनेर हेर्न
- तपाईंका विवरणहरू चोर्न।

यो किनभने:

- यो कसैले पनि प्रयोग गर्नसक्छ

- तपाईंका उपकरणहरू सुरक्षित राख्न अझ गाह्रो हुन्छ

सार्वजनिक वाइफाइ प्रयोग गर्दा कसरी सुरक्षित रहने भन्ने बारे तपाईंले हाम्रो वेबसाइटमा सिक्न सक्नुहुन्छ।.

www.actnowstaysecure.gov.au/cyber-safe-actions

ठगी

जब कसैले निम्न कुराहरू गर्ने प्रयास गर्छ, हामी त्यसलाई **ठगी** भन्छौं:

- तपाईंलाई झुक्याउन
- तपाईंको पैसा लिन।

ठगी गर्ने व्यक्तिलाई **स्क्यामर (ठग)** भनिन्छ।

ठगहरूले तपाईंलाई निम्न माध्यमबाट झुक्याउने प्रयास गर्न सक्छन्:

- पाठ्य सन्देश वा फोन सम्पर्क
- इमेल
- सामाजिक सञ्जाल
- वेबसाइट।

उनीहरू मिलनसार जस्तो देखिन सक्छन्।

तर उनीहरूले तपाईंलाई झुक्याएर तपाईंका विवरणहरू लिनसक्छन्।

उनीहरूले यसलाई निम्न कुराका लागि प्रयोग गर्न सक्छन्:

- तपाईंका अनलाइन खाताहरूमा पहुँच पाउन

- तपाईं बनेर झुक्याउन

- तपाईंको पैसा चोर्न।

ठगहरूले निम्न कुराहरू पनि गर्नसक्छन् :

- तपाईंलाई झुक्याउन नक्कली खाताहरू बनाउन

- तपाईंलाई क्लिक गर्न (थिच्न) लगाउनका लागि लिङ्क र विज्ञापनहरू पठाउन।

ठगी कसरी चिन्ने

यो ठगी हुनसक्छ यदि यसले:

- तपाईंलाई कुनै काम छिटो गर्न भन्छ भने

- तपाईंलाई धेरै पैसा दिने प्रस्ताव गर्छ भने

- तपाईंसँग पैसा माग्छ भने

- तपाईंलाई कुनै लिङ्क मा क्लिक गर्न भन्छ भने।

ठगहरूले तपाईंले चिनेको र भरोसा गरेको संस्थाको नाममा झुक्याउन पनि सक्छन्।

उदाहरणका लागि, तपाईंको बैंक।

ठगहरूले यसो गर्छन् ताकि तपाईंले आफ्ना व्यक्तिगत विवरणहरू उनीहरूलाई दिनुहोस्।

यदि तपाईंलाई कोही ठग हो भन्ने लागे त्यो व्यक्तिसँग कुरा गर्न छोड्नुपर्छ।

तपाईंले त्यो व्यक्ति वास्तवमा उसलेले भनेकै व्यक्ति हो कि होइन भनेर जाँच गर्नुपर्छ।

तपाईंले आफूलाई विश्वास लागेको र आफैंले फेला पारेको विवरणहरू प्रयोग गरेर सम्बन्धित व्यक्ति वा संस्थासँग सम्पर्क गर्न सक्नुहुन्छ।

केही कुरा गलत भएको महसुस भएमा आफ्नो सुरक्षाका लागि तुरुन्तै कदम चाल्नुहोस्।

ठगीको बारेमा जानकारी (रिपोर्ट) दिने

Scamwatch (स्क्यामवाच) ले अष्ट्रेलियालीहरूलाई निम्न कुराहरूमा मद्दत गर्दछ:

- ठगी बुझ्न
- ठगीको रोपोर्ट गर्न।

Scamwatch (स्क्यामवाच) ले ठगीमा परेका अष्ट्रेलियालीहरूलाई पनि सहयोग गर्दछ।

तपाईंले Scamwatch को वेबसाइटमा ठगीको बारेमा रिपोर्ट गर्न सक्नुहुन्छ।

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

आवाज उठाउनुहोस्

अरूले अनलाइनमा कसरी आफ्नो सुरक्षा गर्नसक्छन् भन्ने बारेमा तपाईंले आवाज उठाउनुपर्छ (वा अरूलाई जानकारी दिनुपर्छ)।

यसमा निम्न पर्दछन्:

- साइबर अपराधको बारेमा रिपोर्ट गरेर

- तपाईंले थाहा पाउनुभएका कुरा परिवार तथा साथीभाइसँग गरेर।

हामीले निम्न पानाहरूमा तपाईंले कसरी आफ्ना कुराहरू राख्न (वा आवाज उठाउन) सक्नुहुन्छ भन्ने बारेमा बताएका छौं।

साइबर अपराधको रिपोर्ट गर्नुहोस्

साइबर अपराधको रिपोर्ट गर्नाले सरकारलाई निम्न कुराहरूमा मद्दत पुग्छ:

- साइबर अपराधीहरूले कसरी मानिसहरूमाथि आक्रमण गर्ने प्रयास गर्छन् भन्ने कुरा सिक्न

- अझ धेरै मानिसहरूलाई सुरक्षित राख्न।

तपाईंले ReportCyber को वेबसाइटमा साइबर अपराधको बारेमा रिपोर्ट गर्न सक्नुहुन्छ।

www.cyber.gov.au/report

अनलाइनमा सुरक्षित रहने बारे परिवार र साथीभाइसँग कुरा गर्नुहोस्

तपाईंले अनलाइनमा सुरक्षित रहने बारे आफ्ना उपायहरू परिवार तथा साथीभाइसँग साझा गर्नुपर्छ।

तपाईंले उनीहरूबाट पनि सिक्न सक्नुहुन्छ।

तपाईंले अनलाइनमा सुरक्षित रहने बारे आफूलाई थाहा भएका कुराहरू साझा गरेर आफू र आफ्नो वरपरका मानिसहरूलाई सुरक्षित राख्न सक्नुहुन्छ।

विभिन्न व्यक्तिहरूले उही उपकरणहरू चलाउनुहुन्छ भने पनि यो महत्त्वपूर्ण छ।

शब्द सूची

यो सूचीले यस निर्देशिकामा **गाढा अक्षरमा** लेखिएका शब्दहरूको अर्थ बुझाउँछ।

साइबर

साइबर (Cyber) भन्नाले इन्टरनेटसँग सम्बन्धित कुरालाई बुझाउँछ।

साइबर अपराध

साइबर अपराध भनेको अपराधीहरूले अपराधका लागि इन्टरनेटको प्रयोग गर्नु हो।

उदाहरणका लागि, उनीहरूले निम्न कामका लागि इन्टरनेटको प्रयोग गर्न सक्छन्:

- तपाईंका व्यक्तिगत विवरणहरू चोर्न
- तपाईंका अनलाइन खाताहरू कब्जा गर्न।

लोकेसन सेटिङ्स् (Location settings)

लोकेसन सेटिङ्स्ले तपाईंको उपकरण कहाँ छ भनेर देखाउँछ।

मल्टि-फ्याक्टर अथेन्टिकेसन (MFA)

MFA भनेको प्रत्येक पटक आफ्नो खाता लग-इन गर्दा २ वा सोभन्दा बढी फरक तरिकाहरू प्रयोग गर्नु हो।

पासफ्रेज (Passphrase)

पासफ्रेज पासवर्डभन्दा बलियो प्रकारको गोप्य शब्द वा वाक्यांश हो।

अरू मानिसहरूलाई यसको अनुमान लगाउन निकै गाह्रो हुन्छ।

सार्वजनिक वाइफाइ

सार्वजनिक वाइफाइ भनेको नि:शुल्क वायरलेस इन्टरनेट हो जुन तपाईंले सार्वजनिक ठाउँहरूमा प्रयोग गर्न सक्नुहुन्छ।

ठगी

जब कसैले निम्न कुराहरू गर्ने प्रयास गर्छ, हामी त्यसलाई ठगी भन्छौं:

- तपाईंलाई झुक्याउन
- तपाईंको पैसा लिन।

ठग

ठग भनेको ठगी गर्ने व्यक्ति हो।

हामीलाई सम्पर्क गर्नुहोस्

तपाईंले अष्ट्रेलियाली साइबर सुरक्षा हटलाइन (Australian Cyber Security Hotline) लाई फोन गर्न सक्नुहुन्छ।

1300 292 371

तपाईं हाम्रो वेबसाइटमा जान सक्नुहुन्छ।

www.actnowstaysecure.gov.au

तपाईंले ReportCyber को वेबसाइटमा साइबर अपराधको बारेमा रिपोर्ट गर्न सक्नुहुन्छ।

www.cyber.gov.au/report

इन्फरमेसन एक्सेस ग्रुप (The Information Access Group) ले स्टक फोटोग्राफी र विशेष रूपमा तयार पारिएका चित्रहरू प्रयोग गरी यो सरल पठन (Easy Read) कागजात तयार पारेको हो। अनुमति बिना यी चित्रहरू पुनः प्रयोग गर्न पाइने छैन। चित्रहरू सम्बन्धी कुनै पनि सोधपुछका लागि, कृपया www.informationaccessgroup.com मा जानुहोस्। सोधपुछ गर्दा कोट नम्बर ६३४२ उल्लेख गर्नुहोस्।