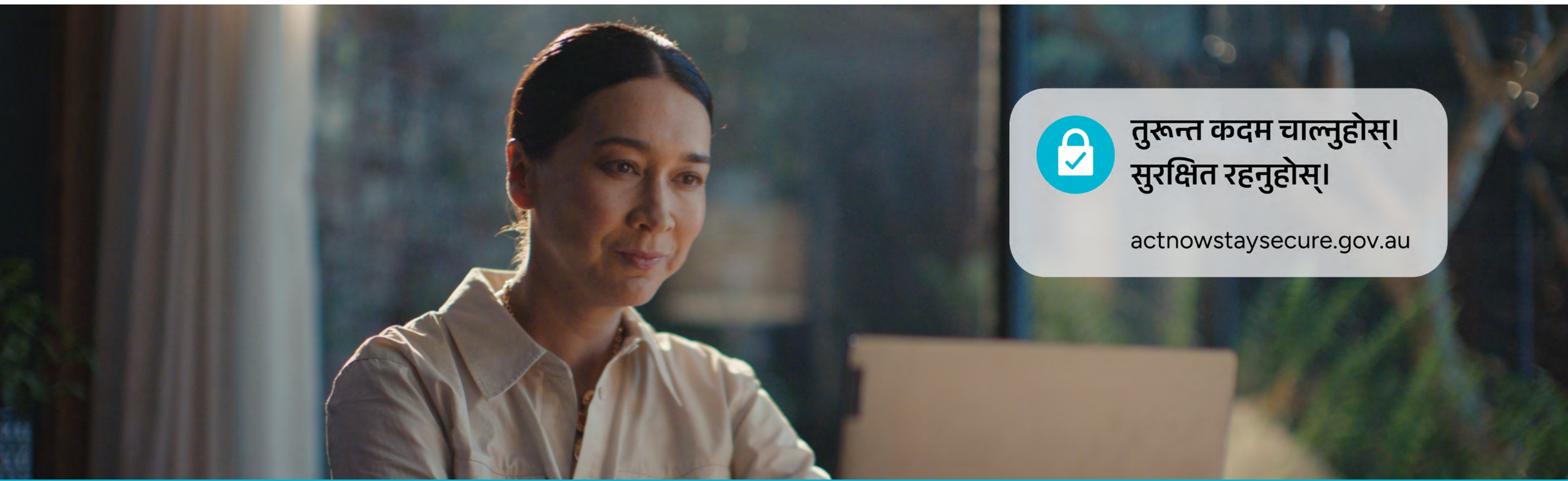
Australian Government

actnowstaysecure.gov.au



अनलाइन हुँदा तपाईंले के के जोखिममा पारिरहनुभएको छ?

प्रविधिको तीव्र विकास हुँदै जाँदा र हामीले अनलाइनमा बढी समय बिताउँदा, अष्ट्रेलियालीहरू साइबर आक्रमणको जोखिममा रहिरहने छन्।

"तुरून्त कदम चाल्नुहोस्। सुरक्षित रहनुहोस्।" अभियानले अष्ट्रेलियालीहरूलाई अनलाइन हुँदा आफूलाई सुरक्षित राख्न सबैजनाले चाल्न सकिने सरल साइबर सुरक्षा कदमहरूको बारेमा शिक्षित गरिरहेको छ।

तुरून्त कदम चाल्नुहोस्। सुरक्षित रहनुहोस्।

अनलाइन हुँदा कसरी सुरक्षित हुने?

प्रत्येक खातामा पृथक र कठिन पासफ्रेज प्रयोग गर्नुहोस्।

तपाईंको प्रत्येक अनलाइन खाताहरूको लागि एक पृथक र कठिन पासफ्रेज प्रयोग गर्नु तपाईंले अनलाइन सुरक्षित रहन गर्नसक्ने सबैभन्दा प्रभावकारी कार्यहरू मध्ये एक हो।

पासफ्रेज अझ बढि सुरक्षित पासवर्ड हो। यसमा अनियमित शब्दहरू (random words) हुन्छन्। यो तपाईंको लागि सम्झन सजिलो हुन्छ तर साइबर अपराधीहरूको लागि अनुमान गर्न कठिन हुन्छ।

कठिन र पृथक हुनको लागि, तपाईंको पासफ्रेजहरू निम्नानुसार हुने सुनिश्चित गर्नुहोस्:

- ✔ चार वा बढी अनियमित शब्दहरू भएको
- ✔ १५ वा सो भन्दा बढी क्यारेक्टर (character) हरू भएको
- ✔ प्रत्येक खाताका लागि फरक
- ✔ परिवारको नामथर, जन्ममिति वा ठेगाना जस्ता पहिचान गर्ने जानकारी समावेश नभएको
- ✔ यदि वेबसाइट वा सेवाद्वारा आवश्यक भएमा प्रतीकहरू, ठूला अक्षरहरू, वा नम्बरहरू समावेश गर्नुहोस्।

तपाईंको अद्वितीय पासफ्रेज सिर्जना गर्न र भण्डारण गर्न पासवर्ड प्रबन्धक प्रयोग गर्न विचार गर्नुहोस्।

आफ्नो उपकरणहरू सुरक्षित राख्न सबै सफ्टवेयर अपडेटहरू इन्सटल गर्नुहोस्।

तपाईंको सबै इन्टरनेट-जडान उपकरणहरू (जस्तै तपाईंको फोन, ल्यापटप वा स्मार्ट वाच) को लागि सफ्टवेयर अपडेटहरू सँधै इन्सटल गर्नु आफैलाई अनलाइन सुरक्षित राख्नको लागि महत्त्वपूर्ण छ।

सफ्टवेयर अपडेटहरूले तपाईंको उपकरणहरूको सुरक्षामा कमजोरी हरू वा ग्यापहरू ठीक गर्दछ। नियमित अपडेटहरू स्थापना गर्नाले तपाईंको उपकरणहरू सुरक्षित राख्छ र साइबर अपराधीहरूलाई तिनीहरूलाई पहुँच गर्न गाह्रो बनाउँछ।

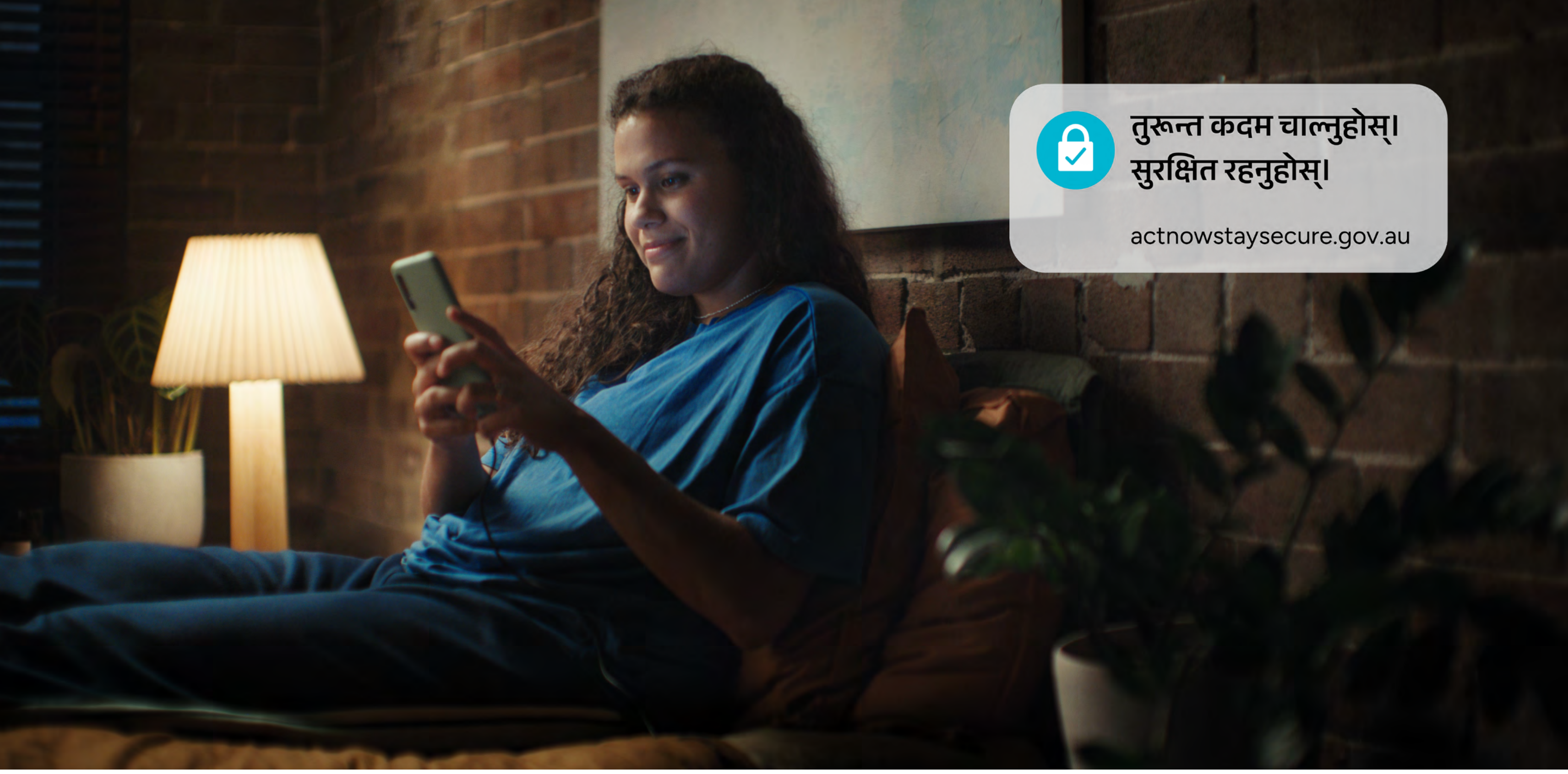
स्वचालित अपडेटहरू चालू गर्नुहोस् र सोधिएमा गर्दा तिनीहरूलाई इन्सटल गर्न नबिर्सनुहोस्।

सदैव मल्टि-फ्याक्टर प्रमाणीकरण सेट अप गर्नुहोस्।

तपाईंको सबै अनलाइन खाताहरूमा सुरक्षाको अतिरिक्त तह थप्न उपलब्ध मल्टि-फ्याक्टर प्रमाणीकरण चालू गर्नुहोस्।

मल्टि-फ्याक्टर प्रमाणीकरणलाई तपाईंको खातामा लग इन गर्न दुई वा बढी प्रमाणीकरण विधिहरू आवश्यक पर्दछ। उदाहरणका लागि, तपाईंको पासवर्ड वा पासफ्रेज प्रविष्ट गरेपछि, तपाईंलाई दोस्रो प्रमाणीकरण प्रदान गर्न संकेत गरिनेछ जस्तै प्रमाणीकरणकर्ता एप्स, इमेल वा संदेशमार्फत तपाईंलाई पठाइएको कोड प्रविष्ट गर्नुहोस्।

मल्टि-फ्याक्टर प्रमाणिकरणले अन्य प्रमाणिकरण विधिहरू (जस्तै पासफ्रेज) चोरिए पनि तपाईंको खातालाई सुरक्षित राख्छ।



अनलाइन सुरक्षित रहने थप तरिकाहरू थाहापाउन चाहनुहुन्छ?

के तपाईं साइबर सुरक्षित रहनका लागि थप तरिकाहरू खोज्दै हुनुहुन्छ? अनलाइन हुँदा आफूलाई सुरक्षित राख्न तपाईंले चाल्न सक्ने अन्य केही कदमहरू यहाँ दिइएका छन्।

सार्वजनिक वाई-फाई (Wi-Fi) प्रयोग गर्दा सतर्क हुनुहोस्।

सार्वजनिक वाई-फाई प्रयोग गर्दा, कुनै पनि संवेदनशील वा निजी जानकारी नहेर्नुहोस् किनकि त्यस्तो कनेक्सन सुरक्षित हुँदैन। यसमा तपाईंको सामाजिक सञ्जाल, इमेल वा अनलाइन बैंकिङ्ग पर्दछन्। तपाईंले प्रविष्ट गर्नुभएको कुनै पनि जानकारी साइबर अपराधीहरूले हेर्न सक्छन्।

तपाईंको गोपनीयता र स्थान सेटिङ नियमित रूपमा जाँच गर्नुहोस् र अद्यावधिक गर्नुहोस्।

तपाईंले आफ्नो गोपनीयता र स्थान सेटिङहरू अक्सर जाँच गर्न महत्त्वपूर्ण छ ता कि तपाईंले दुर्घटनावश सार्वजनिक रूपमा व्यक्तिगत वा आफ्नो पहिचान जानकारी उपलब्ध गर्नुहुनेछैन।

जाँच गर्नुपर्ने सेटिङ्गहरूमा तपाईंको सामाजिक मिडिया खाताहरूको गोपनीयता सेटिङ्गहरू र तपाईंको एप्स र उपकरणहरूमा जियोलोकेशन ट्र्याकिंग पर्दछन्।

साथी तथा परिवारजनसँग कसरी साइबर सुरक्षित रहने भन्ने बारेमा कुरा गर्नुहोस्।

आफूलाई, आफ्नो परिवारजन तथा साथीहरूलाई अनलाइन हुँदा सुरक्षित राख्न शिक्षा र जागरूकता निकै महत्त्वपूर्ण हुन्छ - विशेषगरी यदि तपाई इन्टरनेट-जडित उपकरणहरू साझा प्रयोग गर्नुहुन्छ भने। तपाईंको संजालका व्यक्तिहरूसँग यसको बारेमा कुरा गर्दा साइबर सुरक्षालाई प्राथमिकतामा राख्छ र सुनिश्चित गर्दछ कि उनीहरूले आफूलाई अनलाइन कसरी सुरक्षित गर्ने भन्ने बारेमा सबैभन्दा नयाँ जानकारी प्राप्त गरिरहेका छन्।

कुनै पनि scam (स्क्याम वा अनलाइन हुने ठगी) पहिचान गर्न सिक्नुहोस्।

स्क्यामर (स्क्याम गर्ने) हरूले मानिसहरूलाई झुक्याएर उनीहरूलाई पैसा तिर्न वा व्यक्तिगत जानकारी उपलब्ध गर्न लगाउँछन्।

यदि तपाईं कोसँग कुरा गर्दै हुनुहुन्छ भनेर निश्चित हुनुहुन्न भने कसैलाई पनि पैसा वा व्यक्तिगत जानकारी नदिनुहोस्। आधिकारिक वेबसाइट वा एप्स मार्फत तपाईंले आफैं प्राप्त गर्नसक्ने विवरणहरू प्रयोग गरेर उक्त व्यक्ति वा संगठनलाई सम्पर्क गरेर यसको पुष्टि गर्नुहोस्।

साइबर आक्रमण र घटनाहरू रिपोर्ट गर्नुहोस्।

स्क्याम वा साइबर घटनाहरूको रिपोर्टिंग गर्नु सरकारलाई नयाँ ट्रेन्डहरूको पहिचान गर्न, समुदायलाई सचेत गर्न र साइबर घटनाबाट वसूल गर्न मद्दत गर्न महत्त्वपूर्ण हुन्छ।

आफूलाई सुरक्षित राख्न तपाईंले लिन सक्ने सरल कदमहरूका बारे सिक्न निम्न लिंकमा जानुहोस्
actnowstaysecure.gov.au

तुरून्त कदम चाल्नुहोस्।
सुरक्षित रहनुहोस्।
actnowstaysecure.gov.au