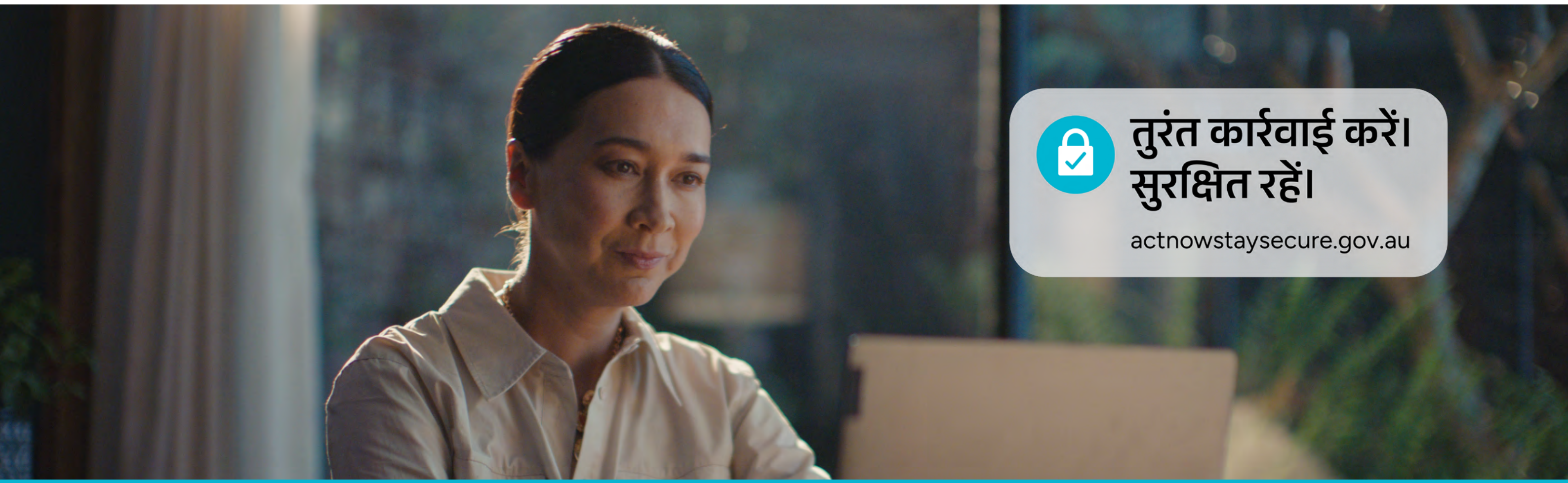
Australian Government

actnowstaysecure.gov.au



आपको ऑनलाइन क्या ख़तरे हो सकते हैं?

जैसे-जैसे प्रौद्योगिकी तेज़ी से आगे बढ़ रही है और हम ऑनलाइन अधिक समय बिता रहे हैं, तो इससे ऑस्ट्रेलियाई लोगों की साइबर हमलों का शिकार होने की संभावना लगातार बनी रहती है।

तुरंत कार्रवाई करें। सुरक्षित रहें। (Act Now. Stay Secure.) अभियान ऑस्ट्रेलियाई लोगों को साइबर सुरक्षित रहने के लिए उन सरल उपायों के बारे में शिक्षित कर रहा है जिन्हें अपना कर हर कोई स्वयं को ऑनलाइन सुरक्षित रख सकता है।

तुरंत कार्रवाई करें। सुरक्षित रहें।

ऑनलाइन सुरक्षित कैसे रहें

प्रत्येक अकाउंट के लिए एक अद्वितीय और मज़बूत पासफ़्रेज़ का उपयोग करें।

अपने प्रत्येक ऑनलाइन अकाउंटों के लिए अलग-अलग, अद्वितीय और मज़बूत पासफ़्रेजों का उपयोग करना ऑनलाइन सुरक्षित रहने के सबसे प्रभावी तरीकों में से एक है।

पासफ़्रेज एक अधिक सुरक्षित पासवर्ड होता है। इसमें कुछ अव्यवस्थित (random) शब्दों का एक अनुक्रम होता है। ये आपके लिए याद रखने में आसान होते हैं लेकिन साइबर अपराधियों के लिए उनका अनुमान लगाना कठिन होता है।

मज़बूत और अद्वितीय पासफ़्रेज बनाते समय सुनिश्चित करें कि:

- ✓ इसमें चार या अधिक अव्यवस्थित शब्द हों।
- ✓ 15 या अधिक अक्षर हों।
- ✓ यह हर अकाउंट के लिए अलग हो।
- ✓ इसमें पारिवारिक सदस्यों के नाम, जन्म तिथि या पता जैसी पहचान बताने वाली जानकारी शामिल न हों।
- ✓ यदि वेबसाइट या सेवा की आवश्यकता हो, तो इसमें प्रतीक (symbols), बड़े अक्षर (capital letters) या संख्याएँ शामिल हों।

अपनी अद्वितीय पासफ़्रेजें बनाने और स्टोर करने के लिए एक पासवर्ड मैनेजर का उपयोग करने के बारे में विचार करें।

सॉफ़्टवेअर की सभी अपडेटों को इंस्टॉल करें जिससे आपकी सभी डिवाइसें सुरक्षित रहें।

इंटरनेट से जुड़ी अपनी सभी डिवाइसों (जैसे आपके फ़ोन, लैपटॉप या स्मार्टवॉच) के लिए सॉफ़्टवेयर अपडेट को तुरंत इंस्टॉल करना ऑनलाइन सुरक्षित रहने के लिए अत्यधिक महत्वपूर्ण है।

सॉफ़्टवेयर अपडेट आपकी डिवाइसों की सुरक्षा की कमज़ोरियों या कमियों को ठीक करते हैं। नियमित अपडेटों को इंस्टॉल करने से आपकी डिवाइसें सुरक्षित रहती हैं और साइबर अपराधियों के लिए उन तक पहुँच पाना कठिन हो जाता है।

आटोमैटिक अपडेट का विकल्प ऑन करें और जब भी 'अपडेट करें' के बारे में संदेश मिले, उन अपडेटों को इंस्टॉल करें।

हमेशा मल्टी-फ़ैक्टर ऑथेंटिकेशन (प्रमाणीकरण) सेट करें

जिन अकाउंटों में मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) का विकल्प उपलब्ध हो, अपने उन अकाउंटों की सुरक्षा बढ़ाने के लिए उसका उपयोग करें।

मल्टी-फ़ैक्टर ऑथेंटिकेशन में आपके अकाउंट में लॉग इन करने के लिए दो या अधिक सत्यापन विधियों की आवश्यकता होती है। उदाहरण के लिए, अपना पासवर्ड या पासफ़्रेज़ लिखने के बाद, आपको एक दूसरी विधि से सत्यापन के लिए कोड लिखने के लिए कहा जाएगा, जैसे कि किसी प्रमाणक ऐप (authenticator app), ईमेल या टेक्स्ट मैसेज के माध्यम से आपके पास भेजा गया कोड।

मल्टी-फ़ैक्टर ऑथेंटिकेशन आपके अकाउंट की सुरक्षा करता है, भले ही आपकी प्रमाणीकरण विधियों में से एक (जैसे पासफ़्रेज़) का किसी ने पता लगा लिया हो।

ऑनलाइन सुरक्षित रहने के लिए और अधिक तरीके जानना चाहते हैं?

क्या आप साइबर सुरक्षा बनाए रखने के अधिक तरीकों के बारे में जानना चाहते हैं? यहाँ कुछ अन्य तरीके बताए गए हैं जिनसे आप स्वयं को ऑनलाइन सुरक्षित रख सकते हैं:

सार्वजनिक वाई-फ़ाई का उपयोग करते समय सतर्क रहें

सार्वजनिक वाई-फ़ाई कनेक्शन सुरक्षित नहीं होता। उसका उपयोग करते समय कोई भी संवेदनशील या निजी जानकारी न देखें। संवेदनशील या निजी जानकारी में सोशल मीडिया, ईमेल या ऑनलाइन बैंकिंग जैसी आपकी सेवाएँ शामिल हैं। आप द्वारा लिखी गई किसी भी जानकारी को साइबर अपराधी देख सकते हैं।

अपनी गोपनीयता और स्थान संबंधी सेटिंग्स को नियमित रूप से जाँचते और अपडेट करते रहें

यह सुनिश्चित करना महत्वपूर्ण है कि आप अनजाने में अपनी निजी या आपकी पहचान कर लिए जाने संबंधी जानकारी सार्वजनिक रूप से साझा तो नहीं कर रहे हैं।

जिन सेटिंग्स की जाँच करनी चाहिए उनमें शामिल हैं आपके सोशल मीडिया अकाउंटों की गोपनीयता सेटिंग्स, और आपकी ऐप्स और डिवाइसों पर जियोलोकेशन ट्रैकिंग।

अपने परिवार और मित्रों के साथ साइबर सुरक्षा के बारे में चर्चा करें

आपको, आपके परिवार और मित्रों को ऑनलाइन सुरक्षित रखने के लिए शिक्षा और जागरूकता महत्वपूर्ण हैं – विशेष रूप से यदि आप इंटरनेट से जुड़ी डिवाइसें साझा करते हैं। अपने जानकार लोगों के साथ इस विषय पर चर्चा करने से साइबर सुरक्षा आप सभी के विचारों में प्राथमिकता पर रहती है और यह भी सुनिश्चित होता है कि वे स्वयं को ऑनलाइन सुरक्षित रखने के बारे में नवीनतम जानकारी प्राप्त कर रहे हैं।

स्कैम को पहचानना सीखें

स्कैमर (घोटाला/धोखाधड़ी करने वाले), लोगों से पैसे ऐंठने या उनकी व्यक्तिगत जानकारी प्राप्त करने के लिए धोखाधड़ी करते हैं।

यदि आप निश्चित रूप से नहीं जानते हैं कि आप किसके साथ बात कर रहे हैं, तो कभी भी किसी को पैसे या व्यक्तिगत जानकारी न दें। आधिकारिक वेबसाइट या ऐप पर दिए गए विवरण का उपयोग करके स्वयं ही किसी व्यक्ति या संगठन से संपर्क करें और उनका सत्यापन करें।

साइबर हमलों और घटनाओं की रिपोर्ट करें

घोटालों या स्कैम की साइबर घटनाओं की रिपोर्ट करना सरकार को नए तरीकों की पहचान करने, समुदाय को सचेत करने और आपको साइबर घटना से उबरने में सहायता करने के लिए अत्यधिक महत्वपूर्ण है।

स्वयं को सुरक्षित रखने के आसान क़दमों के बारे में जानें:
actnowstaysecure.gov.au

तुरंत कार्रवाई करें।
सुरक्षित रहें।
actnowstaysecure.gov.au