Australian Government

तुरंत कार्रवाई करें। सुरक्षित रहें।

आप ऑनलाइन सुरक्षित कैसे रह सकते हैं

आसानी से पढ़ने योग्य संस्करण

इस गाइड का उपयोग कैसे करना है

हम ऑस्ट्रेलियाई सरकार हैं।

यह गाइड हमने लिखा है।

कुछ शब्दों को हमने **बोल्ड** में लिखा है।

हमने समझाया है कि इन शब्दों का क्या अर्थ है।

पृष्ठ 28 पर इन शब्दों की एक सूची भी दी गई है।

आप किसी ऐसे व्यक्ति से मदद मांग सकते हैं जिस पर आप भरोसा करते हैं कि वह:

- इस गाइड को पढ़ें
- अधिक जानकारी प्राप्त करें।

यह एक अन्य गाइड का सरल भाषा में सारांश है।

इसमें केवल सबसे महत्वपूर्ण विचारों को ही शामिल किया गया है।

उस अन्य गाइड को आप हमारी वेबसाइट पर देख सकते हैं।

www.actnowstaysecure.gov.au

इस गाइड में क्या है?

इस गाइड के बारे में	4
अपने खातों को सुरक्षित रखें	6
अपनी जानकारी की सुरक्षा के लिए अपनी सेटिंग्स की जाँच करें।	10
अपने उपकरणों की सुरक्षा करें	16
धोखा-धड़ी	20
अपनी आवाज़ उठाएँ	25
शब्द सूची	28
हमसे संपर्क करें:	30

इस गाइड के बारे में

हम सभी को इस बारे में सोचना चाहिए कि हम ऑनलाइन सुरक्षित कैसे रह सकते हैं।

इसे हम **साइबर** सुरक्षा कहते हैं।

साइबर का अर्थ है इंटरनेट से संबंधित कोई चीज़।

अपने आप को ऑनलाइन सुरक्षित रखने के लिए आप क्या-क्या कर सकते हैं यह गाइड इसके बारे में आपको कुछ चीज़ें बताता है।

उदाहरण के लिए, **साइबर अपराध** से।

साइबर अपराध उसे कहते हैं जब अपराधी अपराध करने के लिए इंटरनेट का उपयोग करते हैं।

उदाहरण के लिए, वे इंटरनेट का उपयोग निम्न के लिए कर सकते हैं:

- आपकी व्यक्तिगत जानकारी की चोरी
- आपके ऑनलाइन खातों या प्रोफाइल का नियंत्रण अपने हाथ में ले कर।

साइबर अपराध किसी भी डिवाइस पर हो सकता है।

इसमें शामिल हैं आपके:

- कंप्यूटर
- स्मार्टफ़ोन
- स्मार्टवाच।

साइबर अपराध से सुरक्षित रहने के लिए आप कुछ चीज़ें कर सकते हैं।

अगले पृष्ठों पर हमने बताया है कि आप क्या कर सकते हैं।

अपने खातों को सुरक्षित रखें

आपको इस बारे में सोचना चाहिए कि आप अपने ऑनलाइन खातों को कैसे सुरक्षित रख सकते हैं।

मज़बूत और अलग-अलग पासफ़्रेज़ उपयोग में लाएं

पासफ़्रेज़ एक अधिक मज़बूत प्रकार का पासवर्ड होता है।

दूसरों के लिए इसका अनुमान लगाना बहुत मुश्किल होता है।

मज़बूत और अलग-अलग पासफ़्रेज़ों का उपयोग करना अपने खातों की सुरक्षा करने के सर्वोत्तम तरीकों में से एक है।

आपको अपने प्रत्येक ऑनलाइन खाते के लिए एक अलग पासवर्ड का उपयोग करना चाहिए।

मज़बूत पासफ्रेज़ों में निम्नलिखित शामिल हैं:

- 4 या अधिक अनियमित शब्द
- 15 या उससे अधिक अक्षर और संख्याएँ।

आप कुछ बड़े अक्षरों (capital letters) का उपयोग कर सकते हैं।

आप कुछ चिह्न भी शामिल कर सकते हैं जैसे कि:

- डैश
- डॉलर का चिह्न
- ईमेल का @ चिह्न।

आपको अपने पासफ्रेज़ों में किसी भी प्रकार की व्यक्तिगत जानकारी का उपयोग नहीं करना चाहिए।

उदाहरण के लिए:

- आपके जन्म की तारीख
- आपके परिवार के सदस्यों या पालतू जानवरों के नाम।

अपने खातों में लॉग इन करने के लिए अतिरिक्त चरण जोड़ें

आप अपने ऑनलाइन खातों को **मल्टी-फैक्टर ऑथेंटिकेशन (multifactor authentication/MFA)** से सुरक्षित रख सकते हैं।

मल्टी-फैक्टर ऑथेंटिकेशन (MFA) वह प्रक्रिया है जिसमें आप हर बार अपने खाते में लॉग इन करने के लिए 2 या 2 से अधिक, अलग-अलग तरीकों का उपयोग करते हैं।

उदाहरण के लिए, जैसे कि आपको पहले अपना पासफ़्रेज़ डालना होगा।

फिर आपको अपने फ़ोन पर प्राप्त कोड डालना होगा।

आपके पास ये विकल्प हो सकते हैं:

- अपने फ़ोन पर एक ऐप डाउनलोड करना जो आपको कोड प्रदान करेगी।

- आपको ईमेल में कोड मिल जाएगा।

- आपको टेक्स्ट मैसेज में कोड मिल जाएगा।

मल्टी-फैक्टर ऑथेंटिकेशन (MFA) अन्य लोगों के लिए आपके ऑनलाइन खातों में प्रवेश करना कठिन बना देता है।

भले ही उन्हें आपका पासफ़्रेज़ पता चल जाए।

अपनी जानकारी की सुरक्षा के लिए अपनी सेटिंग्स की जाँच करें।

आप यह जाँच सकते हैं कि आपकी सेटिंग्स आपकी ऑनलाइन जानकारी की सुरक्षा कर रही हैं या नहीं।

इसमें आपकी निम्नलिखित सेटिंग्स शामिल हैं:

- ऑनलाइन खाते
- डिवाइसें
- ऐप्स।

आप निम्न कर सकते हैं:

- अपनी सेटिंग्स बदलें
- यह चुनें कि कौन सी ऐप्स आपकी जानकारी का उपयोग कर सकती हैं।

आपके डिवाइस पर सेटिंग्स आप निम्न तरीकों से ढूँढ सकते हैं:

- गियर आइकन ढूंढें

  या

- अपने डिवाइस के सर्च बार में 'settings' टाइप करें।

आप मेन्यू खोलकर किसी ऐप या ऑनलाइन खाते में सेटिंग्स ढूँढ सकते हैं।

मेन्यू अक्सर तीन सीधी रेखाओं जैसा दिखता है।

इनमें से कुछ सेटिंग्स निम्न के बारे में जानकारी साझा कर सकती हैं:

- आप कौन हैं
- आप कहाँ हैं
- आप कहाँ रहते हैं।

इस जानकारी को ऑनलाइन साझा करने से आप साइबर अपराधों के खतरे में पड़ सकते हैं।

साइबर अपराधी आपकी जानकारी का उपयोग करके आपके होने का नाटक कर सकते हैं।

उदाहरण के लिए, वे निम्नलिखित जैसी जानकारी का उपयोग कर सकते हैं:

- आप कहाँ रहते हैं

- आपके परिवार के सदस्यों के नाम

- आपके पालतू जानवर(रों) के नाम।

आप अपने अकाउंट की सेटिंग इस तरह सेट कर सकते हैं कि केवल आपके जान-पहचान के लोग ही आपके सोशल मीडिया प्रोफाइल देख सकें।

उदाहरण के लिए, आपकी फेसबुक प्रोफाइल।

इन सेटिंग्स को आमतौर पर privacy settings (गोपनीयता सेटिंग्स) कहा जाता है।

आप अपनी **लोकेशन (स्थान) सेटिंग्स** को भी नियंत्रित कर सकते हैं।

लोकेशन सेटिंग से पता चलता है कि आपका डिवाइस कहाँ पर है।

आप लोकेशन सेटिंग को शुरू या बंद कर सकते हैं।

आप यह भी चुनाव कर सकते हैं कि कौन सी ऐप्स आपकी लोकेशन सेटिंग का उपयोग कर सकती हैं।

आप यह अपने निम्नलिखित के लिए कर सकते हैं:

- ऑनलाइन खाते
- डिवाइसें
- ऐप्स।

कुछ ऐप्स शायद आपसे पूछेंगी कि क्या वे निम्न कर सकती हैं:

- आपके कैमरे का उपयोग

- आपकी तस्वीरों को देखना।

आपको केवल उन्हीं ऐप्स को अपने कैमरे और तस्वीरों का उपयोग करने की अनुमति देनी चाहिए जिनसे आप परिचित हैं।

अपने उपकरणों की सुरक्षा करें

आपको यह सोचना चाहिए कि आप अपने उपकरणों को ऑनलाइन सुरक्षित रखने के लिए क्या कर सकते हैं।

उदाहरण के लिए, आपका फ़ोन या स्मार्ट वॉच।

यह उन उपकरणों के लिए महत्वपूर्ण है जो इंटरनेट से कनेक्ट होते हैं।

अपने उपकरणों को अपडेट करें

आप अपने उपकरणों को अपडेट करके उन्हें ऑनलाइन सुरक्षित रख सकते हैं।

उदाहरण के लिए, आपका फ़ोन और लैपटॉप।

आपका डिवाइस शायद इसे सॉफ़्टवेयर अपडेट कह सकता है।

अपडेट एक डिवाइस को साइबर अपराध से बचाने में मदद करते हैं।

आप किसी डिवाइस को स्वचालित रूप से अपडेट होने के लिए सेट कर सकते हैं।

आप हमारी वेबसाइट पर अपने उपकरणों को अपडेट करने के बारे में अधिक जानकारी प्राप्त कर सकते हैं।

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

सार्वजनिक वाई-फाई नेटवर्क

सार्वजनिक वाई-फाई का इस्तेमाल करते समय आपको सावधानी बरतनी चाहिए।

पब्लिक (सार्वजनिक) वाई-फाई एक मुफ्त वायरलेस इंटरनेट है जिसका उपयोग आप सार्वजनिक स्थानों पर कर सकते हैं।

उदाहरण के लिए, यह उपलब्ध होता है:

- कैफ़े में
- एयरपोर्ट पर
- होटल में।

सार्वजनिक वाई-फाई का उपयोग करके किसी वेबसाइट में क्या जानकारी दर्ज की जा रही है इसके बारे में आपको सावधान रहना चाहिए।

उदाहरण के लिए:

- आपके बैंक विवरण
- ईमेल खाते
- सोशल मीडिया प्रोफाइलें।

कुछ साइबर अपराधी सार्वजनिक वाई-फाई का उपयोग निम्न कार्यों के लिए कर सकते हैं:

- देखने के लिए कि आप ऑनलाइन क्या कर रहे हैं
- आपकी जानकारी की चोरी।

यह इसलिए क्योंकि:

- इसका इस्तेमाल कोई भी कर सकता है

- आपके उपकरणों की सुरक्षा करना अधिक कठिन होता है।

आप हमारी वेबसाइट पर सार्वजनिक वाई-फाई का उपयोग करते समय सुरक्षित रहने के तरीके सीख सकते हैं।

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

धोखा-धड़ी

एक घटना को हम **धोखा-धड़ी** कहते हैं जब कोई व्यक्ति कोशिश करता है:

- आपको चकमा देने की
- आपके पैसे लेने की।

scammer/स्कैमर एक ऐसा व्यक्ति होता है जो धोखाधड़ी करता है।

धोखाधड़ी करने वाले आपको निम्न तरीकों से चकमा देने कोशिश कर सकते हैं:

- टेक्स्ट मैसेज या फ़ोन कॉल से
- ई-मेल से
- सोशल मीडिया से
- किसी वेबसाइट से।

व्यवहार से वे दोस्ताना प्रतीत हो सकते हैं।

लेकिन वे आपको बहला-फुसलाकर आपकी जानकारी हासिल कर सकते हैं।

वे इसका उपयोग निम्न कार्यों के लिए कर सकते हैं:

- आपके ऑनलाइन खातों में लॉग इन करना

- आपके होने का नाटक करना

- आपके पैसे को चुरा लेना।

धोखाधड़ी करने वाले लोग निम्न भी कर सकते हैं:

- आपको धोखा देने के लिए नकली खाते बनाना

- ऐसे लिंक और विज्ञापन साझा करना जिनपर आप क्लिक करें।

धोखाधड़ी की पहचान कैसे करनी है

वह एक धोखा-धड़ी का मामला हो सकता है यदि वह:

- आपसे जल्दी से कुछ करने के लिए कह रहा है

- आपको बहुत सारा पैसा देने की पेशकश करता है

- आपसे पैसे की मांग करता है

- आपसे एक लिंक पर क्लिक करने के लिए कहा जाता है।

धोखाधड़ी करने वाले लोग किसी ऐसे संगठन का रूप धारण करने का भी दिखावा कर सकते हैं जिसे आप जानते हैं और जिस पर आप भरोसा करते हैं।

उदाहरण के लिए, आपका बैंक।

धोखेबाज़ (scammer) ऐसा इसलिए करते हैं ताकि आप अपनी व्यक्तिगत जानकारी उनके साथ साझा कर लें।

अगर आपको लगता है कि वह व्यक्ति धोखेबाज़ है, तो आपको उससे बात करना बंद कर देना चाहिए।

आपको यह सुनिश्चित करना चाहिए कि वह व्यक्ति वही है जो वह होने का दावा करता है।

आप उन विवरणों का उपयोग करते हुए अपने भरोसेमंद व्यक्ति या संस्था को संपर्क कर सकते हैं जिन पर आप भरोसा रखते हैं या जो आपने स्वयं ढूँढी हैं।

अगर आपको कुछ ग़लत लगे तो तुरंत अपनी सुरक्षा के लिए कदम उठाएँ।

धोखाधड़ी की रिपोर्ट करना

स्कैमवॉच ऑस्ट्रेलियावासियों की मदद करता है:

- घोटालों को समझने में
- घोटालों की रिपोर्ट करने में।

स्कैमवॉच उन ऑस्ट्रेलियाई लोगों की भी मदद करता है जो धोखाधड़ी का शिकार हुए हैं।

आप स्कैमवॉच वेबसाइट पर धोखाधड़ी की रिपोर्ट कर सकते हैं।

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

अपनी आवाज़ उठाएँ

आपको इस बारे में खुलकर बोलना चाहिए कि दूसरे लोग ऑनलाइन खुद को कैसे सुरक्षित रख सकते हैं।

इसमें शामिल है:

- साइबर अपराध की रिपोर्ट करना

- जो कुछ आप जानते-समझते हैं उसे अपने परिवार और दोस्तों के साथ साझा करना।

अगले पृष्ठों पर हम बताएंगे कि आप अपनी बात कैसे रख सकते हैं।

साइबर अपराध की रिपोर्ट करना

साइबर अपराध की रिपोर्ट करने से सरकार को निम्न में मदद मिलती है:

- यह सीखने में कि साइबर अपराधी लोगों पर हमला करने की कोशिश कैसे करते हैं

- और अधिक लोगों की रक्षा करने में।

आप ReportCyber वेबसाइट पर साइबर अपराध की रिपोर्ट कर सकते हैं।

www.cyber.gov.au/report

ऑनलाइन सुरक्षित रहने के बारे में परिवार और दोस्तों से बात करें

आपको ऑनलाइन सुरक्षित रहने के बारे में अपने सुझाव अपने परिवार और दोस्तों के साथ साझा करने चाहिए।

आप उनसे सीख भी सकते हैं।

ऑनलाइन सुरक्षित रहने के बारे में आप जो कुछ भी जानते हैं उसे साझा करके आप स्वयं को और अपने आसपास के लोगों को सुरक्षित रख सकते हैं।

यह तब भी महत्वपूर्ण होता है जब आप दूसरों के साथ डिवाइस साझा करते हैं।

शब्द सूची

यह सूची बताती है कि इस गाइड में दिए गए **बोल्ड** शब्दों का क्या अर्थ है।

साइबर

साइबर का अर्थ है इंटरनेट से संबंधित कोई चीज़।

साइबर अपराध

साइबर अपराध उसे कहते हैं जब अपराधी अपराध करने के लिए इंटरनेट का उपयोग करते हैं।

उदाहरण के लिए, वे इंटरनेट का उपयोग निम्न के लिए कर सकते हैं:

- आपकी व्यक्तिगत जानकारी की चोरी
- आपके ऑनलाइन खातों का नियंत्रण अपने हाथ में लेना।

स्थान सेटिंग्स

लोकेशन सेटिंग से पता चलता है कि आपका डिवाइस कहाँ पर है।

मल्टी-फैक्टर ऑथेंटिकेशन (MFA)

मल्टी-फैक्टर ऑथेंटिकेशन (MFA) वह प्रक्रिया है जिसमें आप हर बार अपने खाते में लॉग इन करने के लिए 2 या 2 से अधिक, अलग-अलग तरीकों का उपयोग करते हैं।

पासफ्रेज़

पासफ्रेज़ एक अधिक मज़बूत प्रकार का पासवर्ड होता है।

दूसरों के लिए इसका अनुमान लगाना बहुत मुश्किल होता है।

सार्वजनिक वाई-फाई

पब्लिक (सार्वजनिक) वाई-फाई एक मुफ्त वायरलेस इंटरनेट है जिसका उपयोग आप सार्वजनिक स्थानों पर कर सकते हैं।

धोखा-धड़ी

जब कोई व्यक्ति निम्न करने का प्रयास करता है तो हम उसे धोखा-धड़ी (scam) कहते हैं:

- आपको चकमा देना
- आपके पैसे ले लेना।

धोखाधड़ी करने वाले

धोखाधड़ी करने वाला व्यक्ति स्कैमर कहलाता है।

हमसे संपर्क करें:

आप ऑस्ट्रेलियाई साइबर सुरक्षा हॉटलाइन पर फ़ोन कर सकते हैं।

1300 292 371

आप हमारी वेबसाइट पर जा सकते हैं।

www.actnowstaysecure.gov.au

आप ReportCyber वेबसाइट पर साइबर अपराध की रिपोर्ट कर सकते हैं।

www.cyber.gov.au/report

इंफॉर्मेशन एक्सेस ग्रुप ने स्टॉक फोटोग्राफी और कस्टम छवियों का उपयोग करके यह आसानी से पढ़े जाने योग्य दस्तावेज़ तैयार किया है। इन छवियों का पुन: उपयोग अनुमति के बिना नहीं किया जा सकता है। तस्वीरों के बारे में किसी भी पूछताछ के लिए, कृपया यहाँ जाएँ।

www.informationaccessgroup.com।

जॉब नंबर 6342 का उल्लेख करें।