Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC Australian Cyber Security Centre

निजी साइबर सुरक्षा

फर्स्ट सटैप्स

cyber.gov.au

निजी साइबर सुरक्षा श्रंखला

निजी साइबर सुरक्षा श्रंखला: फर्स्ट सटैप्स तीन दिशा-निर्देशिकाओं की श्रंखला की पहली दिशा-निर्देशिका है जिसकी रचना ऑस्ट्रेलिया के सामान्य जन को साइबर सुरक्षा के बारे में मूल बातों को समझने और आप सामान्य साइबर खतरों से खुद को को बचाने के लिए कैसे कार्यवाही कर सकते हैं उस बारे में सहायता करने के लिए की गई है।

फर्स्ट सटैप्स

नैक्स्ट सटैप्स

एडवांस्ड सटैप्स

विषय-वस्तु तालिका।

परिचय 1

ऑटोमैटिक अपडेट चालू करें 2

बहु-कारक प्रमाणीकरण (MFA) सक्रिय करें 4

नियमित रूप से अपने डिवाइसेज़ को बैकअप करें। 5

अपने महत्वपूर्ण खातों को सुरक्षित करने के लिए पासफ्रेज़ों का उपयोग करें 6

अपनी मोबाइल डिवाइस को सुरक्षित बनाएँ 7

अपनी साइबर सुरक्षा सोच विकसित करें 8

संक्षिप्त जाँच-सूची 11

शब्दावली 12

परिचय

निजी साइबर सुरक्षा क्या होती है?

दिन पर दिन तकनीक पर निर्भर होते विश्व में हम प्रतिदिन ऐसी डिवाइसों और खातों का उपयोग करते हैं जिन पर साइबर खतरा मंडाराता रहता है:

- आपकी डिवाइसों में कम्प्यूटरर्स, मोबाइल फोन्स, टेबलेट्स तथा इंटरनेट से जुड़ीं अन्य डिवाइसें शामिल हो सकती हैं।
- आप ईमेलों, बैंकिंग, खरीददारी, सोशल मीडिया, गेमिंग तथा अन्य कामों के लिए भी ऑनलाइन खातों का उपयोग करते होंगे।

निजी साइबर सुरक्षा निरंतर किए जा सकने वाले वो उपाय हैं जो आप अपने खातों और उपकरणों को साइबर खतरों से बचाने के लिए कर सकते हैं।

साइबर खतरे क्या होते हैं?

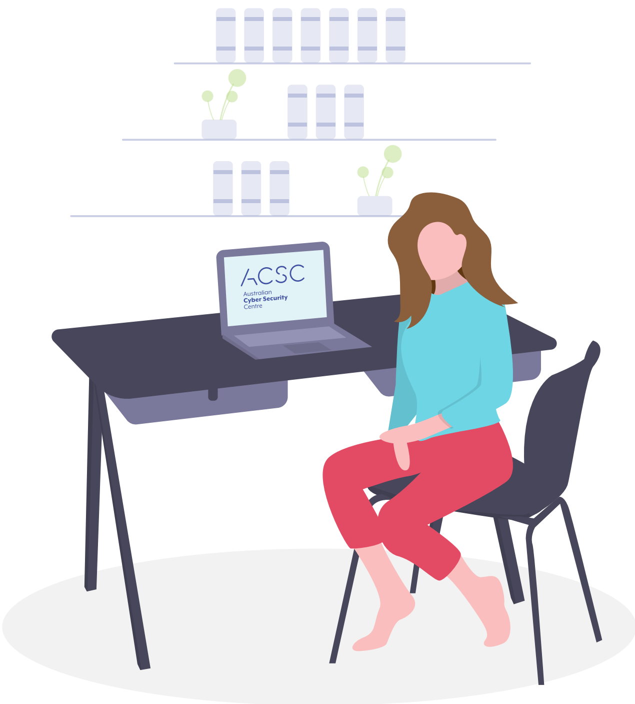
ऑस्ट्रेलिया के सामान्य निवासियों पर मंडराने वाले मुख्य साइबर खतरों में शामिल हैं **धोखाधड़ियाँ और मालवेयर।**

- **विभिन्न प्रकार के उन मलिशियस सॉफ्टवेयरों को मालवेयर कहा जाता है जिनकी** रचना हानि पहुँचाने के लिए की जाती है, इनमें शामिल हैं, वायरस, वर्म्स, स्पाइवेयर, ट्रोजन्स और रेंसमवेयर। साइबर अपराधियों द्वारा मालवेयर का प्रयोग आपकी जानकारी और पैसा चुराने के लिए, और अपकी डिवाइसों और खातों पर नियंत्रण पाने के लिए किया जाता है।
- **धोखाधड़ियाँ साइबर अपराधियों द्वारा भेजे जाने वाले ऐसे मैसेज होते हैं जिनकी** रचना, चालाकी से आपसे आपकी संवेदनशील जानकारी लेने और आपकी डिवाइस पर मालवेयर को सक्रिय करने के लिए की जाती है।

इन हमलों का प्रभावित लोगों पर निजी और आर्थिक रूप से बहुत ज़्यादा असर पड़ता है और इनकी जटिलता बढ़ रही है तथा ये बार-बार होने लगे हैं।

यह दिशा-निर्देशिका मुझे साइबर खतरों से बचाने में कैसे सहायता कर सकती है?

यदि आप साइबर सुरक्षा के बारे में पहली बार सीख रहे हैं, या खुद को नवीनतम जानकारी से अवगत करवा रहे हैं, यह दिशा-निर्देशिका इस काम को शुरु करने का सर्वश्रेष्ठ तरीका है। निजी साइबर सुरक्षा: फर्स्ट सटैप्स तीन दिशा-निर्देशिकाओं की श्रंखला की पहली दिशा-निर्देशिका है जिसकी रचना ऑस्ट्रेलिया के सामान्य जन को साइबर सुरक्षा के बारे में मूल बातों को समझने औरआप सामान्य साइबर खतरों से खुद को बचाने के लिए कैसे कार्यवाही कर सकते हैं उस बारे में सहायता करने के लिए की गई है।



ऑटोमैटिक अपडेट चालू करें

नवीनतम जानकारियाँ क्या हैं?

आपके द्वारा अपने कम्प्यूटर और मोबाइल डिवाइसों में सॉफ्टवेयर (प्रोग्राम्स, एप्प्स, और ऑपरेटिंग सिस्टम्स) का उन्नत प्रारूप इंस्टाल करना अपडेट कहलाता है।

सॉफ्टवेयर आपडेट्स, उन सॉफ्टवेयर बग्स (कोडिंग में गल्तियाँ या अरक्षितता) को ठीक करके आपकी डिवाइस को सुरक्षित रखने में सहायता करती हैं जिनका उपयोग साइबर अपराधियों और मालवेयर द्वारा आपकी डिवाइस में घुसने और आपके निजी डाटा, खातों, वित्तीय सूचनाओं और पहचान को चुराने के लिए किया जा सकता है।

सॉफ्टवेयर के नए बग्स लगातार मिलते रहते हैं और साइबर अपराधियों द्वारा उनका दुरुपयोग किया जाता है, इसलिए अपनी डिवाइसों में सॉफ्टवेयर को अपडेट करने से आपको साइबर हमलों से बचने में सहायता मिलती है।

मैं ऑटोमैटिक अपडेट्स की व्यवस्था कैसे कर सकता हूँ?

ऑटोमैटिक अपडेट एक डीफॉल्ट या'चालू करें और भूल जाएँ' प्रणाली होती है जो आपके सॉफ्टवेयर की अपडेट उपलब्ध होते ही उसे अपडेट कर देती है।

- **अपने सभी सॉफ्टवेयरों और डिवाइसों पर ऑटोमेटिक**अपडेट चालू करें।
- **आप अपनी सभी डिवाइस पर ऑटोमैटिक अपडेट कैसे चालू करते हैं, यह आपके सॉफ़्टवेयर और डिवाइस के आधार पर** अलग-अलग हो सकता है। ।
- **यदि संभव हो, तो ऑटोमैटिक अपडेट्स के लिए सुविधानुसार** समय तय कर दें, जैसे कि जब आपका सोने का समय हो, या जिस समय आप सामान्यतया आपनी डिवाइस काम में नहीं लेते हों।

आपकी डिवाइस का चालू होना, उसका प्लग बिजली के पोइंट में लगा हुआ होना और उसमें संग्रहण के लिए खाली जगह होना आवश्यक है।

सुझाव: यदि आपको अपने डिवाइस का सॉफ़्टवेयर अपडेट करने के लिए प्रॉम्प्ट मिलता है, तो आपको जल्द से जल्द ऐसा करना चाहिए।

वेबसाइट cyber.gov.au पर ‘Updates’ सर्च करके ऑटोमैटिक अपडेट्स ऑन करने के तरीके के बारे में और अधिक विस्तृत जानकारी पाई जा सकती है।

यदि ऑटोमैटिक अपडेट्स के लिए सेटिंग अनुपलब्ध हो तो क्या?

यदि ऑटोमैटिक अपडेट्स के लिए सेटिंग अनुपलब्ध हो, तो आपको उनके लिए नियमित रूप से पता लगाना चाहिए और अपने सॉफ्टवेयर या अपनी डिवाइस के सेटिंग्स मेन्यू के माध्यम से नई अपडेट्स को इंस्टाल करना चाहिए।

यदि मेरी पुरानी डिवाइसों और सॉफ्टवेयर को कोई भी अपडेट्स नहीं मिले तो क्या?

यदि आपकी डिवाइस, आपका ऑपरेटिंग सिस्टम या सॉफ्टवेयर बहुत पुराना है, तो हो सकता है कि, वो उसके निर्माता या डवेलपर द्वारा अब समर्थित न हों।

जब उत्पाद अपने 'समर्थन समाप्ति' चरण पर पहुँच जाते हैं तो उसके बाद उनको अपडेट्स नहीं मिलती हैं, जिससे आप जाने पहचाने सॉफ्टवेयर 'बग्स' के कारण साइबर हमलों की चपेट में आ सकते हैं। जो उत्पाद समर्थन समाप्ति चरण तक पहुँच चुके हैं उनके उदाहरणों में शामिल है Windows 7 ऑपरेटिंग सिस्टम और iPhone 6।

यदि आपकी डिवाइस, ऑपरेटिंग सिस्टम या सॉफ्टवेयर 'समर्थन समाप्ति' चरण पर पहुँच गए हैं, तो ACSC द्वारा सुझाव दिया जाता है कि आप सुरक्षित रहने के लिए जल्दी से जल्दी अपडेट करें।

और अधिक जानकारी प्राप्त करने के लिए वेबसाइट cyber.gov.au पर 'End of support' सर्च करें।

बहु-कारक प्रमाणीकरण (MFA) सक्रिय करें

MFA क्या होता है?

आप अपने सर्वाधिक महत्वपूर्ण खातों की सुरक्षा को बेहतर बनाने के लिए बहु-कारक प्रमाणीकरण (MFA) काम में ले सकते हैं। MFA में, किसी खाते में जाने की अनुमति देने से पहले आपको निम्नांकित में से दो या अधिक प्रकार के प्रमाणीकरण बनाने की आवश्यकता होती है:

- **कुछ चीजें जो आप जानते हैं** (जैसे कि पिन, पासवर्ड या पासफ्रेज़);
- **कुछ चीजें जो आपके पास होती हैं** (जैसे कि कोई स्मार्टकार्ड, फिज़िकल टोकन, प्रमाणक एप्प, SMS या ईमेल); तथा
- **कुछ चीजें जो आप हैं** (जैसे कि अंगुली की छाप, चेहरे से पहचान या आँख की पुतली का स्कैन)।

MFA आपके खाते के लिए प्रमाणीकरण की और अधिक परतें जोड़कर, साइबर अपराधियों के लिए खाते तक प्रारंभिक पहुंच मुश्किल बनाता है, इन परतों को जोड़ने से खाते को ब्रेक करने के लिए अधिक समय, प्रयास और संसाधनों की आवश्यकता पड़ती है।

मैं अपने सर्वाधिक महत्वपूर्ण खातों को सुरक्षित रखने के लिए 2FA को कैसे सक्रिय कर सकता हूँ?

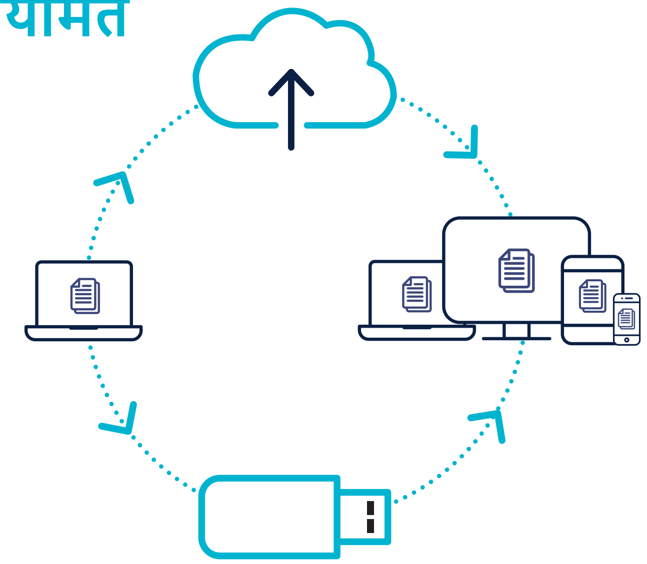
आपको 2FA को अभी सक्रिय कर देना चाहिए, अपने महत्वपूर्ण खातों में इसे शुरु करके:

- सारे ऑनलाइन बैंकिंग और वित्तीय खाते (जैसे कि आपका बैंक, पेपाल खाता)
- सारे ईमेल खाते (जैसे कि जीमेल, आउटलुक, हॉटमेल, याहू!)

यदि आपके बहुत सारे ईमेल खाते हैं, तो जो खाते आपकी ऑनलाइन बैंकिंग या अन्य महत्वपूर्ण सेवाओं से जुड़े हुए हैं उनको प्राथमिकता दें।

आप वेबसाइट cyber.gov.au पर 'Multi-factor authentication' या 'MFA' सर्च करके मल्टी-फैक्टर ऑथेंटिकेशन ऑन करने के तरीके के बारे में और अधिक पढ़ सकते/सकती हैं।

अपने डिवाइस का नियमित रूप से बैकअप लें



बैकअप क्या होता है?

बैकअप आपकी सबसे महत्वपूर्ण जानकारी (जैसे फ़ोटो, वित्तीय जानकारीया स्वास्थ्य रिकॉर्ड) की एक डिजिटल कॉपी होता है जिसे आप किसी बाहरी स्टोरेज डिवाइस या क्लाउड में सहेजते हैं।

- बैकअप लेना एक एहतियात के तौर पर किया गया उपाय होता है, ताकि आपकी जानकारी यदि कभी खो जाए, चोरी हो जाए या क्षतिग्रस्त हो जाए तो उसे वापस प्राप्त किया जा सके।

मैं अपनी डिवाइसों और फाइलों का बैकअप कैसे लूँ?

आपको नियमित रूप से अपनी फाइलों और डिवाइसेज़ का बैकअप करना चाहिए। यह कैसा दिखाई देता है, चाहे वह दैनिक, साप्ताहिक या मासिक हो, आखिर में आपके ऊपर निर्भर करता है। आप कितनी बार बैकअप करते/करती हैं, यह इनकी संख्या पर निर्भर करता है:

- आपके द्वारा अपने डिवाइस में लोड की गई नई फाइलें,
- आपके द्वारा फाइलों में किए गए परिवर्तन।

सुझाव: नियमित रूप से अपने बैकअप्स की जाँच करें, ताकि आपको रिकवरी प्रोसेस के बारे में जानकारी रहे। हमेशा सुनिश्चित करें कि आपके बैकअप्स ठीक से काम कर रहे हैं।

वेबसाइट cyber.gov.au पर 'Backups' सर्च करके अपनी जानकारी को बैकअप करने के तरीके के बारे में और अधिक विस्तृत जानकारी पाई जा सकती है।

अपने महत्वपूर्ण खातों को सुरक्षित करने के लिए पासफ्रेज़ों का उपयोग करें

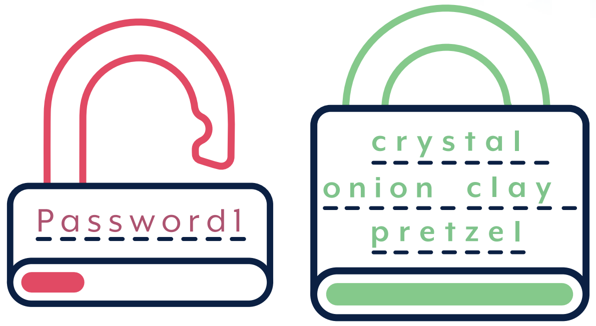
बहु चरणो वाला प्रमाणीकरण (MFA) (पृष्ठ 4 देखें) आपके खाते को साइबर अपराधियों से बचाने के सर्वाधिक प्रभावशाली तरीकों में से एक है। **यदि MFA उपलब्ध नहीं हो,** तो किसी सरल पासवर्ड की बजाय एक अनोखा सुदृढ़ पासफ्रेज़ आपके खाते की बेहतर सुरक्षा कर सकता है।

पासफ्रेज़ क्या होता है?

पासफ्रेज़ में आपके पासवर्ड के रूप में चार या उससे अधिक आकस्मिक (रैंडम) शब्दों का उपयोग होता है।

उदाहरण के लिए: 'क्रिस्टल अनिअन क्ले प्रिट्ज़ल'।

- **पासफ्रेज़, सरल पासवर्डों की तुलना में** अधिक सुरक्षित होते हैं।
- साइबर अपराधियों के लिए पासफ्रेज़ेस का अनुमान लगाना **कठिन होता है, लेकिन आपके लिए** इन्हें याद रखना आसान होता है।



मैं एक पासफ्रेज़ केसे बना सकता हूँ?

ऐसे पासफ्रेज़ेस बनाएँ जो:

- **लंबे हों:** कम से कम 14 अक्षर हों, जिनमें चार या अधिक असंबंधित शब्दों को का उपयोग किया गया हो। आपका पासफ्रेज़ जितना लंबा होगा, उतना ही सुरक्षित होगा।
- **जिनका अनुमान न लगाया जा सके:** चार या अधिक असंबंधित शब्दों को अनियमित रूप से घुला-मिलाकर इस्तेमाल करें। किसी भी प्रसिद्ध वाक्यांश, उद्धरण या बोलों का प्रयोग न करें।
- **अनोखे हों:** एक से अधिक खातों में पासफ्रेज़ का दोबारा इस्तेमाल न करें।

यदि किसी वेबसाइट या सेवा में सिम्बल्स, केपिटल लेटरों, या सँख्याओं सहित जटिल पासवर्ड की आवश्यकता हो, तो आप इन्हें अपने पासफ्रेज़ में शामिल कर सकते हैं। लेकिन तब भी उत्कृष्ट सुरक्षा के लिए आपके पासफ्रेज़ लंबे, अप्रत्याशित और अनोखे होने चाहिए।

मुझे कौनसा खाता पासफ्रेज़ द्वारा सुरक्षित करना चाहिए?

यदि आपके सबसे महत्वपूर्ण खाते MFA (पृष्ठ 4 देखें) द्वारा सुरक्षित नहीं हैं, तो अपने पासवर्डों को अनोखे सुदृढ़ पासफ्रेज़ों में बदल दें, जो शुरु होते हों:

- ऑनलाइन बैंकिंग और वित्तीय खाते
- ईमेल अकाउंटस

यदि आपके बहुत सारे ईमेल खाते हैं, तो जो खाते आपकी ऑनलाइन बैंकिंग या अन्य महत्वपूर्ण सेवाओं से जुड़े हुए हैं उनको प्राथमिकता दें।

आप अपने खाते के सेटिंग्स मेन्यू के माध्यम से अपने पासवर्ड को एक अनोखे सुदृढ़ पासफ्रेज़ में बदल सकते हैं।

यदि आपको अपने सभी पासफ्रेज़ेस याद रखने में मुश्किल होती है, तो पासवर्ड मैनेजर का उपयोग करने के बारे में सोचें। पासवर्ड मैनेजर से आपको केवल एक ही पासवर्ड याद रखने की आवश्यकता होती है, बाकी को पासवर्ड मैनेजर याद रखता है। और अधिक सलाह के लिए वेबसाइट cyber.gov.au पर 'password manager' सर्च करें।

वेबसाइट cyber.gov.au पर 'Passphrases' सर्च करके सुरक्षित पासफ्रेजेस बनाने के तरीके के बारे में और अधिक विस्तृत जानकारी पाई जा सकती है।

अपनी मोबाइल डिवाइस को सुरक्षित बनाएँ

आजकल किसी भी समय किसी भी स्थान से एक-दूसरे से जुड़ने, खरीददारी, नौकरी, बैंक, शोध, अपनी तंदुरुस्ती पर निगाह रखने और सैंकड़ों अन्य काम करने के लिए स्मार्टफोनों और टेबलेटों का उपयोग किया जाता है।

यदि मेरी मोबाइल डिवाइस खराब हो जाए, खो जाए या चोरी हो जाए तो क्या हो सकता है?

- साइबर अपराधियों द्वारा आपकी डिवाइस का उपयोग उसमें संग्रहित सोशल मीडिया और ईमेल खातों सहित आपकी अन्य जानकारी को काम में लेते हुए, आपका पैसा, आपकी पहचान चुराने के लिए लिया जा सकता है।
- आप फोटोज़, टिप्पणियों या मैसेजेस जैसे अनमोल डाटा को खो सकते हैं (यदि उसका बैकअप नहीं लिया गया है तो)।
- एक साइबर अपराधी द्वारा आपके फोन नंबर का इस्तेमाल दूसरे लोगों को ठगने के लिए किया जा सकता है।

मैं अपनी मोबाइल डिवाइस को कैसे सुरक्षित कर सकता हूँ?

डिवाइस सुरक्षा:

- **ताला लगाकर** अपनी डिवाइस में पासफ्रेज़, पासवर्ड, पिन या पासकोड से ताला लगाएँ। अनुमान लगाना कठिन बनाएँ - साइबर अपराधियों के लिए आपकी जन्म तिथि और पैटर्न के तालों का अनुमान लगाना आसान होता है। सर्वोत्कृट सुरक्षा के लिए एक पासफ्रेज़ का प्रयोग करें (पृष्ठ 6 देखें)। आप अपनी डिवाइस का ताला खोलने के लिए चेहरे द्वारा पहचान या अंगुली के निशान का प्रयोग करने के बारे में विचार कर सकते हैं।
- **सुनिश्चित करें कि** आपकी डिवाइस में थोड़े समय तक निष्क्रियता के बाद अपने आप पर स्वतः ताला लगाने की व्यवस्था हो।
- **अपनी डिवाइस को किसी सार्वजनिक चार्जिंग स्टेशन पर चार्ज** नहीं करें और दूसरी कंपनियों के चार्जर्स का उपयोग करने से बचें।
- **अपने** फोन को अपने बटुए की तरह रखें। उसे सुरक्षित रखें और हमेशा अपने पास रखें।

सॉफ्टवेयर और एप्प की सुरक्षा:

- **नई एप्लीकेशनें** और ऑपरेटिंग सिस्टम अपडेटों के उपलब्ध होते ही सॉफ्टवेयर की अपडेट उपलब्ध होते ही उन्हें इंस्टाल करने के लिए अपनी डिवाइस के ऑटोमैटिक अपडेट फीचर का उपयोग करें (पृष्ठ 5 देखें)।
- **एप्लीकेशनों** को इंस्टाल करने से पहले डिवाइस को इस तरह से व्यवस्थित करें कि उसमें पासफ्रेज़/पासवर्ड की आवश्यकता हो। इस बारे में माता-पिता द्वारा नियंत्रण भी काम आ सकता है।
- **अपनी डिवाइस** पर नई एप्प्स को, विशेष रूप से मुफ्त में उपलब्ध एप्प्स को इंस्टाल करते समय, निजता की अनुमतियों को ध्यान से चैक कर लें। प्रतिष्ठित विक्रेताओं से उपलब्ध एप्प्स को ही इंस्टाल करें।

डाटा सुरक्षा:

- **दूर से लॉक करने और वाइप करने मिटाने के फंक्शनों को चालू** करें, यदि आपकी डिवाइस में ऐसा किया जा सकता हो तो।
- **सुनिश्चित करें कि** आपने अपनी डिवाइस को बेचने या फेंकने से पहले उसमें से अपना सारा निजी डाटा पूरी तरह से निकाल दिया है।

कनेक्टिविटी सुरक्षा:

- **जब आप** ब्लूटूथ और वाईफाई काम में नहीं ले रहे हों तो उन्हें बंद करदें।
- **सुनिश्चित करें** कि आपकी डिवाइस नए वाई-फाई नेटवर्कों से अपने आप नहीं जुड़े।

वेबसाइट cyber.gov.au पर 'Secure your mobile phone' सर्च करके अपने मोबाइल को सुरक्षित करने के तरीके के बारे में और अधिक विस्तृत जानकारी पाई जा सकती है।

अपनी साइबर सुरक्षा सोच विकसित करें

निजी साइबर सुरक्षा केवल सेटिंगे बदलना ही नहीं होता, यह अपनी सोच और व्यवहारों को बदलने के बारे में भी है।

साइबर धोखाधड़ियों से सावधान रहें

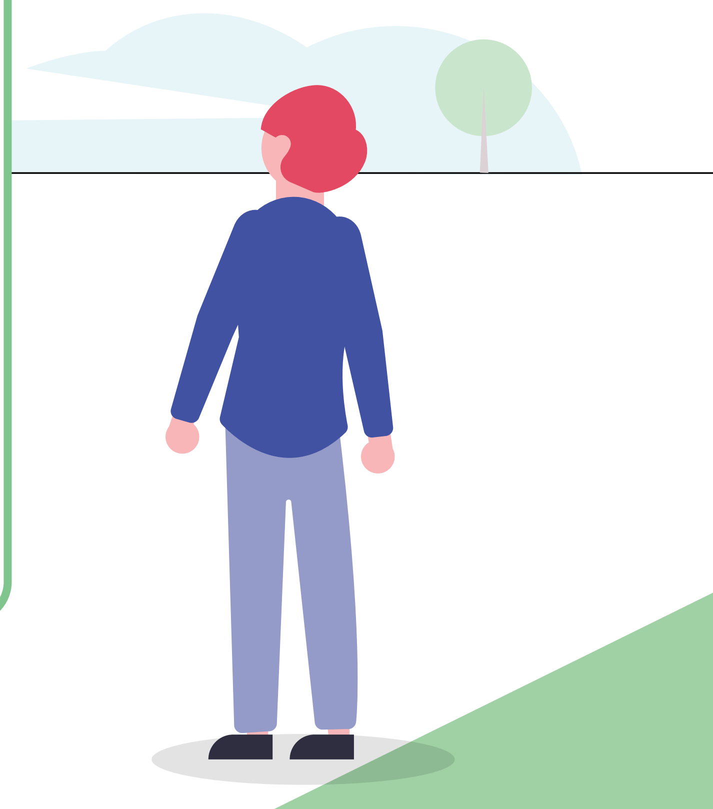
लोग जानते हैं कि साइबर अपराधी, ऑस्ट्रेलियावासियों को ईमेलों, मैसेजों, सोशल मीडिया या फोन कॉल्स के माध्यम से ठगने का प्रयास करते हैं। ये लोग कोई ऐसा व्यक्ति होने का ढोंग कर सकते हैं जिन्हें आप जानते हैं, या आपको लगता है कि आपको भरोसा करना चाहिए उनके मैसेज और कॉल्स आपको कोई विशेष कार्य करने के लिए बरगलाने का प्रयास करते हैं,जैसे कि:

- बैंक खाते के विवरण, पासवर्ड, और क्रेडिट कार्ड नंबरो को बताना
- आपके कम्प्यूटर या सर्वर को दूरवर्ती एक्सस देना
- कोई ऐसा अटैचमेंट खोलना, जिसमें मालवेयर हो सकता है
- पैसे या गिफ्ट कार्ड भेजना

मैं धोखाधड़ी के मैसेजों को कैसे पहचान सकता हूँ?

धोखाधड़ी के मैसेजों की पहचान करना एक कठिन काम हो सकता है। साइबर अपराधियों द्वारा कुछ आपसे छल करने के लिए अक्सर कुछ विशेष तरीके अपनाए जाते हैं उनके मैसेजों में शामिल हो सकता है:

- **अथॉरिटी** - क्या यह संदेश आपके बैंक जैसे अधिकृत से आने का दावा कर रहा है?
- **तकाजा** - क्या आप से कहा गया है कि कोई समस्या है, या ये कहा गया है कि जवाब देने या भुगतना करने के लिए आपके पास सीमित समय है?
- **भावना** - क्या यह संदेश आपको अचानक भयभीत, आशावान या जिज्ञासु बनाता है?
- **तंगी** - क्या किसी मैसेज में किसी ऐसी चीज़ को उपलब्ध कराने का प्रस्ताव दिया जा रहा है जो आपके पास कम है, या आपके सामने कोई बहुत अच्छा प्रस्ताव रखा जा रहा है?
- **वर्तमान घटनाएँ** - क्या कोई मैसेज किसी वर्तमान समाचार या बड़ी घटना के बारे में है?



वेबसाइट cyber.gov.au में 'Learn the basics' पर जाकर फ़िशिंग या स्कैम मैसेजस की पहचान करने का तरीका पता करें।

यदि मुझे धोखाधड़ी वाले मैसेज मिलें तो मुझे क्या करना चाहिए?

यदि आपको कोई संदिग्ध मैसेज या फोन आए, तो आपको उसे अनदेखा करना चाहिए, मिटा देना चाहिए या ACCC की स्कैमवॉच को scamwatch.gov.au पर उसकी रिपोर्ट करनी चाहिए।

यदि आप अपनी साइबर सुरक्षा के बारे में चिंतित हैं तो आप **1300 CYBER1** (1300 292 371) पर ACSC की साइबर सुरक्षा हॉटलाइन से भी संपर्क कर सकते हैं।

यदि आप किसी घोटाले में फंस गए/गई हैं और आपको लगता है कि आपके बैंक खाते, क्रेडिट या डेबिट कार्ड के लिए खतरा हो सकता है, तो तुरंत अपने वित्तीय संस्थान से संपर्क करें। वे आपके खाते को फ़्रीज़ करने या ट्राज़ेक्शन रोकने में सक्षम हो सकते हैं।

यदि मैं इस बारे में सुनिश्चित नहीं हूँ कि कोई मैसेज धोखा है या नहीं तो क्या?

अगर आपको लगता है कि कोई मैसेज या कॉल सच में किसी ऐसे संस्थान से हो सकता है जिस पर आप विश्वास कर सकते हैं (जैसे कि आपका बैंक) तो संपर्क का एक ऐसा तरीका ढूँढें जो आपके लिए विश्वसनीय हो। उनकी आधिकारिक वेबसाइट पर जाएं, उनके द्वारा अपने विज्ञापन में दिए गए फोन नंबर पर फोन करें, या किसी स्टोर या शाखा में जाएँ। आपको भेजे गए या फोन पर दिए गए संदेश में लिंक या संपर्क विवरण का उपयोग न करें क्योंकिये छलपूर्ण हो सकते हैं।

यदि आप सोचते हैं कि आप साइबर अपराध के शिकार हुए हैं ACSC तो के रिपोर्टसाइबर के माध्यम से cyber.gov.au पर जाकर या हमारी साइबर सुरक्षा हॉटलाइन को 1300 CYBER1 (1300 292 371) पर फोन करके आप इसकी रिपोर्ट दर्ज करवा सकते हैं।

आप एसीएससी की नि:शुल्क चेतावनी सेवा के सदस्य बनकर हाल के खतरों से अप-टु-डेट भी रह सकते/सकती हैं। वेबसाइट cyber.gov.au पर 'Subscribe to the ACSC alert service' सर्च करें। जब हमें किसी नए साइबर खतरे का पता चलेगा, तो हम आपको एक एलर्ट भेजेंगे।

आप सोशल मीडिया पर शेयर करें उससे पहले थोड़ा ठहर कर सोच लें

आपके द्वारा अपने सोशल मीडिया खाते/तों में सार्वजनिक रूप से पोस्ट की गई जानकारी का साइबर अपराधियों द्वारा अपने धोखों और साइबर-हमलों के लिए उपयोग किया जा सकता है।

याद रखें कि इंटरनेट स्थाई होता है और आप पोस्ट की जा चुकी चीजों को कभी भी पूर्णतया हटा नहीं सकते।

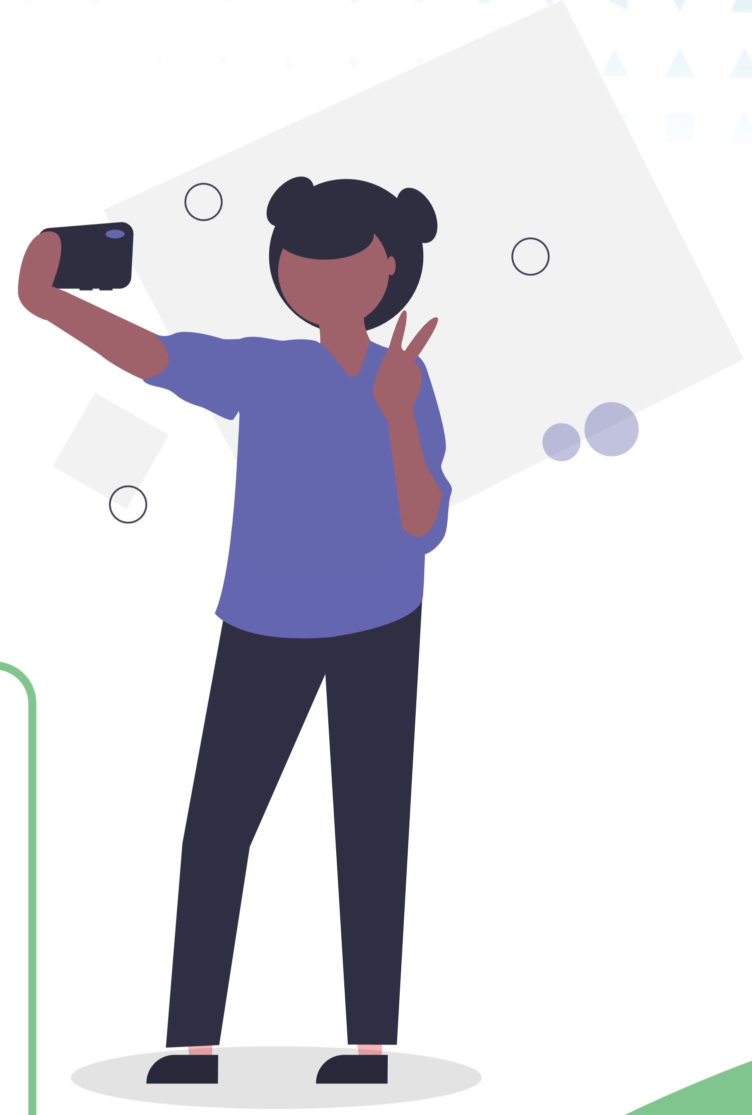
मैं पोस्ट करने से पहले कैसे ठहर और सोच सकता हूँ?

- **सोचें:** कोई साइबर अपराधी मुझे या मेरे खातों को निशाना बनाने के लिए इस जानकारी का उपयोग कैसे कर सकता है?
- **सोचें:** क्या मैं इस बात से सहज रहूँगा कि इस सूचना या चित्र को पूरी तरह से अनजान कोई व्यक्ति ऑफलाइन देखें?

मुझे कौनसी जानकारी साझा करने से बचना चाहिए?

उस जानकारी फोटोज़ सहित को ऑनलाइन साझा करने से बचें जिसका उपयोग साइबर अपराधी काम में ले सकते हैं: आपकी पहचाने करने, धोखे से आपसे चालाकी करने या आपके खाते के रिकवरी प्रश्नों का अनुमान लगाने के लिए। इसमें शामिल हो सकता है:

- आपका जन्म स्थान और जन्म ति
- आपका पता और फोन नंब
- आपका नियोक्ता और नौकरी का इतिहा
- आप कहाँ पर स्कूल गए
- कोई अन्य निजी जानकारीजिसका उपयोग आपको निशाना बनाने के लिए किया जा सकता



संक्षिप्त जाँच-सूची

क्या आपने इस दिशा-निर्देशिका को पूरा कर लिया है?

अपनी प्रोग्रेस का पता लगाने के लिए इस सुविधाजनक जाँच-सूची को काम में लें:

मैंने अपनी सभी डिवाइसों में ऑटोमैटिक अपडेट्स चालू कर दी हैं:

- कम्प्यूटर (डेस्कटॉप और लैपटॉप)
- मोबाइल फोन
- टेबलेट

मैंने अपने सर्वाधिक महत्वपूर्ण खातों में बहु चरणो वाला प्रमाणीकरण चालू कर दिया है:

- मेरे सारे ऑनलाइन बैंकिंग और वित्तीय खाते(जैसे कि अपना बैंक, पेपाल खाता)
- मेरे सारे ईमेल खाते (जैसे कि जीमेल, आउटलुक, हॉटमेल, याहू!)

मैं अपनी डिवाइसों का नियमित रूप से बैकअप लेता हूँ:

- कम्प्यूटर (डेस्कटॉप और लैपटॉप)
- मोबाइल फोन
- टेबलेट

मेरे जो सर्वाधिक महत्वपूर्ण खाते द्वारा सुरक्षित नहीं हैं उनके लिए मैं अनोखे सुदृढ़ पासफ्रेज़ेस काम में लेता हूँ:

- ऑनलाइन बैंकिंग और वित्तीय खाते
- ईमेल अकाउंटस

मैंने अपनी मोबाइल डिवाइसों को सुरक्षित कर दिया है:

- लैपटॉप
- मोबाइल फोन
- टेबलेट

अपने साइबर सुरक्षा विचारों का उपयोग प्रतिदिन करें:

- मैं धोखाधड़ी के मैसेजों को पहचान सकता हूँ
- मुझे पता है कि अगर मुझे धोखाधड़ी का कोई मैसेज मिले तो मुजे क्या करना चाहिए
- मुझे पता है कि यदि मैं इस बारे में सुनिश्चित नहीं हूँ कि कोई मैसेज धोखा है या नहीं तो मुझे क्या करना है
- मैं लिंकों और अटैचमेंटों पर क्लिक करने से पहले सोचता हूँ
- मैं सोशल मीडिया पर कुछ भी साझा करने से पहले सोचता हूँ

मुझे पता है कि यदि मुझ पर किसी साइबर अपराध या किसी धोखे का प्रभाव पड़े तो मुझे कहाँ से सहायता मिलेगी

शब्दावली

अकाउंट रीकवरी
एक प्रक्रिया जिसमें किसी खाते में पुनः एक्सस पाने या किसी खाते का पासफ्रेज़/पासवर्ड बदलने के लिए प्रश्नों या प्रमाणीकरण के अन्य तरीकों का उपयोग किया जाता है।

एप्प
एप्प को मोबाइल एप्लीकेशन भी कहा जाता है, यह सॉफ्टवेयर का वो पारिभाषिक शब्द है जिसका उपयोग सामान्यतया स्मार्टफोन या टेबलेट के लिए होता है।

अटैचमेंट
किसी ईमेल मेसेज के साथ भेजी गई एक फाइल।

प्रमाणक एप्प
किसी कम्प्यूटर उपयोगकर्ता की पहचान करने लिए काम में ली जाने वाली एक एप्प जो बहु चरणो वाले प्रमाणीकरण (MFA) के द्वारा एक्सस की अनुमति देती है।

क्लाउड
सुदूरवर्ती सर्वरों का एक नेटवर्क जो विशाल, वितरित संग्रहण और प्रोसेसिंग क्षमता उपलब्ध कराता है।

साइबरअपराधी
वह व्यक्ति जो गैर-कानूनी रूप से किसी कम्प्यूटर सिस्टम या खाते में एक्सस करता है, सूचना को क्षतिग्रस्त करने या चुराने के लिए।

वडिाइस
एक कम्प्यूटिंग या कम्यूनिकेशन्स डिवाइस। उदाहरण के लिए, एक कम्प्यूटर, लैपटॉप, मोबाइल फोन या टेबलेट।

समर्थन समाप्ति
समर्थन समाप्ति उस स्थिति का संकेत देता है जिसमें कोई कंपनी किसी उत्पाद या सेवा के लिए सहायता प्रदान करना बंद कर देती है। यह विशेष तौर पर हार्डवेयर और सॉफ्टवेयर उत्पादों पर लागू होता है जब कोई कंपनी कोई नया प्रारूप प्रस्तुत करती है और पूर्ववर्ती प्रारूपों के लिए समर्थन समाप्त कर देती है।

मालवेयर
किसी उपयोगकर्ता के कम्प्यूटर में अनाधिकृत एक्सस पाने, जानकारी चुराने और नैटवर्कों को बाधित या अक्षम करने के लिए मलिशियस सॉफ्टवेयर का प्रयोग किया जाता है।

ऑपरेटिंग सिस्टम
किसी कम्प्यूटर की हार्ड ड्राइव में इंस्टॉल किया गया सॉफ्टवेयर जिसके कारण कम्प्यूटर का हार्डवेयर कम्प्यूटर प्रोग्रामों के साथ संचारण करता है और उन्हें चलाता है। उदाहरण: माइक्रोसॉफ्ट विंडोज़, एप्पल macOS,iOS, एन्ड्रॉयड।

फिज़िकल टोकन
सामान्यतया किसी चाबी के छल्ले में फिट होने वाली एक फिज़िकल डिवाइस, जो MFA का उपयोग करने वाले कम्प्यूटर उपयोगकर्ता की पहचान की पुष्टि करने के लिए एक सुरक्षा कोड उत्पन्न करती है।

दूरवर्ती (रिमोट) एक्सस
जिस स्थल पर डिवाइसें या नैटवर्क हो उससे दूर किसी अन्य जगह से उनमें एक्सस और नियंत्रण पाना।

सॉफ्टवेयर
सामान्यतया जिसे प्रोग्रामों के नाम से जाना जाता है, यह निर्देशों का एक संकलन होता है जिससे उपयोगकर्ता किसी कम्प्यूटर, उसके हार्डवेयर से बातचीत कर सकता है, या दिए गए कार्य कर सकता है।

अस्वीकरण
इस गाइड की विषय-वस्तु एक आम प्रकृति की है और इसे कानूनी सलाह के तौर पर नहीं लिया जाना चाहिए या किसी ख़ास हालात या आपातकालीन स्थिति में मदद हेतु इस पर निर्भर नहीं होना चाहिए। किसी भी तरह के जरूरी मामले में, आपको अपने हालातों को लेकर उचित स्वतंत्र पेशेवर से सुझाव लेना चाहिए।

इस गाइड में दी गई जानकारी पर निर्भरता से होने वाली किसी भी क्षति, नुकसान या खर्च के लिए राष्ट्रमंडल कोई जिम्मेदारी या दायित्व स्वीकार नहीं करता है।

कॉपीराइट
© Commonwealth of Australia 2023.
Coat of Armsके अपवाद समेत और जहां और भी कहा गया है, इस प्रकाशन में दी गई सारी विषय-वस्तु क्रिएटिव कॉमन्स एट्रिब्यूशन 4.0 इंटरनेशनल लाइसेंस (www.creativecommons.org/licenses) के तहत प्रदान की जाती है।

भ्रम को टालने के लिए, इसका मतलब है कि यह लाइसेंस सिर्फ विषय-वस्तु पर लागू होता है जैसा कि इस दस्तावेज़ में तय किया गया है।

प्रासंगिक लाइसेंस शर्तों का विवरण क्रिएटिवकॉमन्स वेबसाइट पर उपलब्ध है जैसा कि CC BY 4.0 लाइसेंस के लिए पूर्ण कानूनी कोड है (www.creativecommons.org/licenses)।

Coat of Arms का प्रयोग।
जिन शर्तों के तहत Coat of Arms का इस्तेमाल किया जा सकता है, वे उनका वर्णन प्रधानमंत्री के विभाग और कैबिनेट की वेबसाइट पर (www.pmc.gov.au/government/commonwealth-coat-arms)पर है।

अधिक जानकारी के लिए, या साइबर सुरक्षा घटना की रिपोर्ट करने के लिए, हमसे संपर्क करें:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

यह नंबर केवल ऑस्ट्रेलिया में उपयोग के लिए उपलब्ध है।

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre