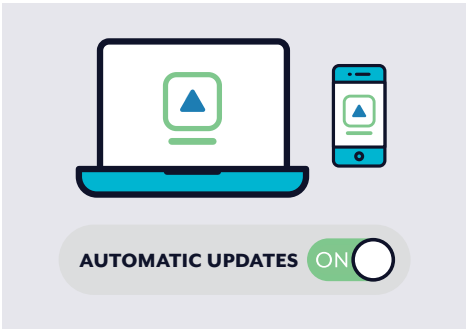
साइबर सुरक्षा के लिए सर्वश्रेष्ठ सुझाव

खुद को ऑनलाइन सुरक्षित रखने के व्यवहारिक तरीके

cyber.gov.au/learn



अपनी ऐप्स और डिवाइसेज़ को अपडेट करें

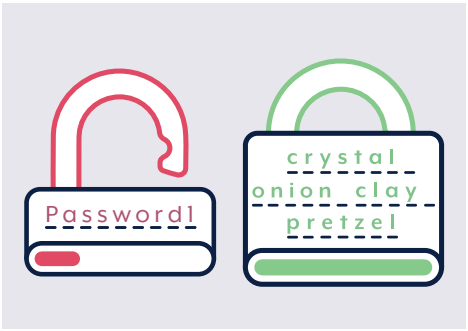
अपनी ऐप्स और डिवाइसेज़ को अपडेट करने से समस्याएँ ठीक की जा सकती हैं और सिक्योरिटी से संबंधित ऐसी चिंताओं या खामियों को संबोधित किया जा सकता है, जिनका उपयोग हैकर्स आपके डिवाइसेज़ या खातों की एक्सेस के लिए कर सकते हैं। इससे नए फीचर्स भी मिल सकते हैं।

बहु-चरणों वाला प्रमाणीकरण (MFA) ऑन करें

MFA का अर्थ होता है, किसी खाते के लिए आपकी पहचान प्रमाणित करने के लिए एक से अधिक परीक्षणों की व्यवस्था होना। उदाहरण के लिए, आपको एक टैक्स्ट मैसेज द्वारा कोड की और आपके पासफ्रेज़ की आवश्यकता हो सकती है। इससे साइबर अपराधियों के लिए आपके खातों में प्रवेश कर पाना अत्यधिक कठिन हो जाता है।

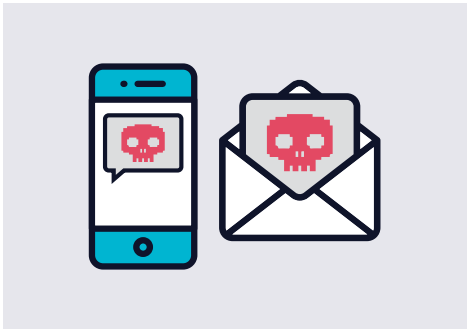
नियमित रूप से बैक-अप की व्यवस्था कर लें और बैक-अप लेते रहें

बैक-अप आपकी सबसे महत्वपूर्ण जानकारी की एक डिजिटल कॉपी होता है जिसे किसी बाहरी स्टोरेज डिवाइस या इंटरनेट पर क्लाउड जैसे किसी सर्वर में सहेजा जाता है। इससे यदि कुछ गड़बड़ हो जाए, तो आप अपनी फाइलों को री-स्टोर कर सकते/सकती हैं।



सुरक्षित पासफ्रेज़ सेट करें

जब MFA उपलब्ध न हो, तो अपने खाते को सुरक्षित रखने के लिए पासफ्रेज़ का उपयोग करें। पासफ्रेज़ एक कठिन तरह का पासवर्ड होता है, जिसमें चार या इससे अधिक रैंडम शब्दों का उपयोग किया जाता है। इससे साइबर अपराधियों के लिए अनुमान लगाना मुश्किल होता है, लेकिन यह आपके लिए याद रखना आसान है।



धोखाधड़ियों को पहचानें और उनकी रिपोर्ट करें

लोगों को ठगने के लिए अपराधी अक्सर ईमेल, एसएमएस, फोन कॉल और सोशल मीडिया का इस्तेमाल करते हैं। आमतौर पर वे आपसे संपर्क करते हैं और आपके किसी परिचित और भरोसेमंद व्यक्ति या संगठन होने का ढोंग करते हैं।

ईमेल या संदेशों में एटैचमेंट्स या लिंक्स पर क्लिक करते समय हमेशा सतर्क रहें।

निम्नांकित द्वारा अपनी साइबर सुरक्षा का स्तर बढ़ाएँ...

- इस बारे में सोचें कि आप ऑनलाइन क्या पोस्ट डालना चाहते हैं।
- नए खतरों के बारे में चेतावनियों का पता लगाते रहें। हमारी मुफ़्त अलर्ट सेवा के लिए साइनअप करें।
- साइबर सुरक्षा के बारे में अपने परिवार और मित्रों से बात करें।
- जब आप ऑनलाइन बैंकिंग या खरीददारी करें तो सार्वजनिक वाई-फाई का उपयोग करने से बचें।
- ऑस्ट्रेलिया को सुरक्षित रखने के लिए साइबर हमलों और घटनाओं की रिपोर्ट करें।

अधिक जानकारी **cyber.gov.au/learn** पर उपलब्ध है।

साइबर सुरक्षा से जुड़ी घटनाओं के बारे में
cyber.gov.au | 1300 साइबर1 (1300 292 371) पर रिपोर्ट करें।
यह नंबर केवल ऑस्ट्रेलिया में उपयोग के लिए उपलब्ध है।

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

क्या इस उत्पाद के बारे में आपके कोई सुझाव हैं? **cyber.gov.au** पर जाएँ और हमें बताएँ।