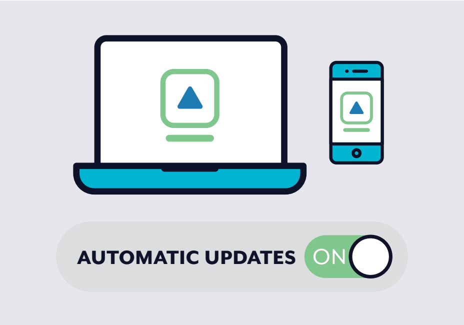
साइबर सुरक्षा के लिए सर्वश्रेष्ठ सुझाव

खुद को ऑनलाइन सुरक्षित रखने के व्यवहारिक तरीके

cyber.gov.au/learn



अपने डिवाइसेज़ को अपडेट करें

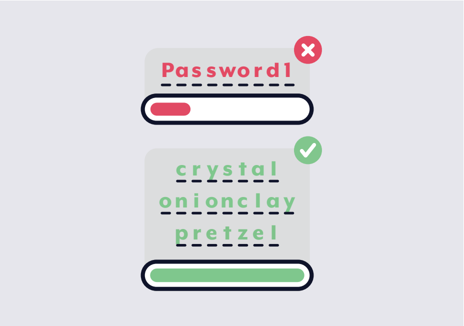
अपने डिवाइसेज़ को अपडेट करने से समस्याओं का समाधान हो सकता है तथा सुरक्षा संबंधी नई चिंताओं या उन कमियों पर ध्यान दिया जा सकता है जिनके माध्यम से हैकर्स आपकी डिवाइस में प्रवेश पा सकते हैं। वे आपकी एप्पों या डिवाइस में नए फीचर भी जोड़ सकते हैं।

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 घुस पाना अत्यधिक कठिन हो जाता है।

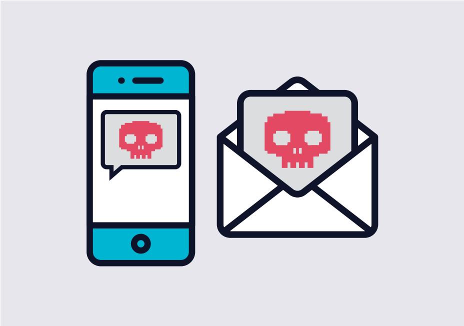
नियमित रूप से बैक-अप की व्यवस्था कर लें और बैक-अप लेते रहें।

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 हैं।



सुरक्षित पासफ्रेज़ सेट करें

यदि MFA उपलब्ध नहीं हो, तो अपना खाता सुरक्षित करने के लिए एक पासफ्रेज़ का उपयोग करें। पासफ्रेज़, पासवर्ड का और अधिक सुरक्षित स्वरूप होता है, जिसमें आपके पासवर्ड के रूप में चार या अधिक शब्दों का आकस्मिक उपयोग किया जाता है। इससे साइबर अपराधियों के लिए इनका अनुमान लगाना कठिन हो जाता है लेकिन आपके लिए इन्हें याद रखना आसान।



धोखाधड़ियों को पहचानें और उनकी रिपोर्ट करें

अपराधियों द्वारा लोगों से धोखाधड़ी करने के लिए अक्सर ऐसे ईमेल, एसएमएस, फोन कॉल्स और सोशल मीडिया का इस्तेमाल किया जाता है जिन्हें ऐसा दिखने के लिए बनाया जाता है मानों वो किसी ऐसे व्यक्ति या संगठन द्वारा भेजे गए हैं जो आपको अपनी जान-पहचान वाले लगते हैं, या आपको लगता है कि आपको उन पर भरोसा करना चाहिए।

किसी ईमेल में आए अटैचमैंटों या लिंकों 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 ख़तरों 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**पर उपलब्ध है।**

साइबर सुरक्षा से जुड़ी घटनाओं के बारे में
Cyber.gov.au | 1300 साइबर1 (1300 292 371) पर रिपोर्ट करें।

Australian Government
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।