

# साइबर सुरक्षा के लिए सर्वश्रेष्ठ सुझाव

## खुद को ऑनलाइन सुरक्षित रखने के व्यावहारिक तरीके

[cyber.gov.au/learn](https://cyber.gov.au/learn)



AUTOMATIC UPDATES

### 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 नई चिंताओं या खामियों को संबोधित किया जा सकता है।



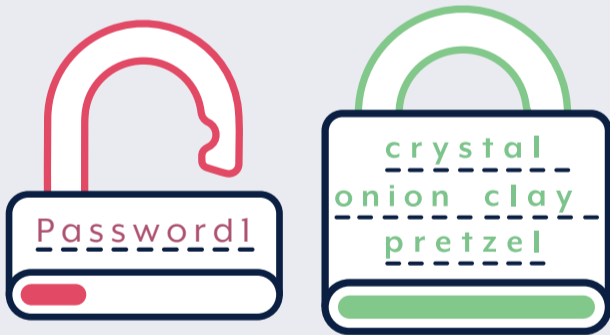
### बहु-चरणों वाला प्रमाणीकरण (MFA) ऑन करें।

MFA का अर्थ होता है, किसी खाते के लिए आपकी पहचान प्रमाणित करने के लिए एक से अधिक परीक्षणों की व्यवस्था होना।



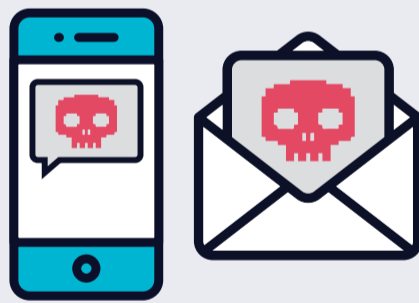
### नियमित रूप से बैक-अप की व्यवस्था कर लें और बैक-अप लेते रहें।

बैक-अप आपकी जानकारी की एक डिजिटल कॉपी होता है जिसे बाहरी स्टोरेज डिवाइस या क्लाउड जैसे किसी सर्वर में सहेजा जाता है।



### सुरक्षित पासफ्रेज़ सेट करें

जब MFA उपलब्ध न हो, तो अपने खाते को सुरक्षित रखने के लिए एक पासफ्रेज़ का उपयोग करें। पासफ्रेज़ कठिन तरह का पासवर्ड होता है, जिसमें चार या इससे अधिक रैंडम शब्दों का उपयोग किया जाता है।



### धोखाधड़ियों को पहचानें और उनकी रिपोर्ट करें

आप जो बातें पढ़ते हैं उन सभी पर विश्वास नहीं करें। किसी ईमेल या मैसेज में आए अटैचमेंटों या लिंकों पर क्लिक करते समय हमेशा सतर्क रहें।



### [cyber.gov.au](https://cyber.gov.au) पर जाकर अपनी साइबर सुरक्षा का स्तर बढ़ाएँ।

अधिक जानकारी [cyber.gov.au/learn](https://cyber.gov.au/learn) पर उपलब्ध है।

साइबर सुरक्षा से जुड़ी घटनाओं के बारे में [cyber.gov.au](https://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](https://cyber.gov.au) पर जाएँ और हमें बताएँ।