Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

# इंटरनेट का सुरक्षित रूप से उपयोग कैसे किया जाए

## वृद्धों (सीनियर्स) के लिए मार्गदर्शिका

cyber.gov.au

# परिचय

**ऑनलाइन जाने से आपको अपने मित्रों और परिवार वालों से संपर्क बनाए रखने में, विभिन्न विषयों के बारे में सीखने और यहाँ तक कि गेम्स खेलने में भी सहायता मिलती है।**

ड्राइव करने से पहले अपनी सीट बेल्ट बाँधने की तरह, और अधिक सुरक्षा के लिए आपको इंटरनेट का उपयोग शुरु करने से पहले कुछ कदम उठाने चाहिए।

ऑस्ट्रेलियन साइबर सिक्योरिटी सेन्टर (ACSC) यह सुनिश्चित करना चाहता है कि लोग जब ऑनलाइन हों तो सुरक्षित हों इस दस्तावेज़ में साइबर सिक्योरिटी के बारे में कुछ मूलभूत अभ्यासों के बारे में बताया गया है जिन्हें आप इंटरनेट का प्रयोग करते समय खुद को सुरक्षित करने के लिए अपना सकते हैं।


ऑस्ट्रेलियन साइबर सिक्योरिटी सेन्टर (ACSC), ऑस्ट्रेलियन सिग्नल्स डायरेक्ट्रेट (ASD) के भाग के तौर पर, ऑस्ट्रेलिया को साइबर खतरों को रोकने, पता लगाने और निराकरण करने के लिए साइबर सुरक्षा सलाह, सहायता और संचालनात्मक प्रतिक्रियाएँ देता है। ऑनलाइन कनेक्ट करने के लिए ऑस्ट्रेलिया को सबसे सुरक्षित स्थान बनाने में सहायता हेतु ACSC यहां मौजूद है।

**साइबर सिक्योरिटी के बारे में अधिक जानकारी, मार्गदर्शन और सलाह के लिए cyber.gov.au पर जाएँ।**





# वृद्धों (सीनियर्स) के लिए साइबर सिक्योरिटी।

## सलाह 1: अपनी डिवाइस को अपडेट करें

**अपने सॉफ्टवेयर को अपडेट करना अपनी कार की सर्विस कराने जैसा है। इससे आपकी डिवाइस के कार्य-संपादन (परफोर्मेंस) में सुधार होता है तथा वो और अधिक सुरक्षित बन जाती है।**

साइबर अपराधी हमेशा डिवाइसेज़ में हैक करने के नए-नए तरीकों का पता लगाते रहते हैं। अपनी डिवाइस में स्वतः (ऑटोमेटिक रूप से) अपडेट इंस्टाल करने की व्यवस्था कर देने से आपके सॉफ्टवेयर में यदि कोई दोष हो तो वो ठीक हो जाता है और हैकर्स भी दूर रहते हैं।

**और अधिक जानकारी प्राप्त करने के लिए वेबसाइट cyber.gov.au पर 'Updates' सर्च करें।**



**क्या आप जानते हैं:**

**अपडेट्स से आपके डिवाइस में नए फीचर्स भी आ सकते हैं और ये डिवाइस की स्पीड बढ़ा सकते हैं।**

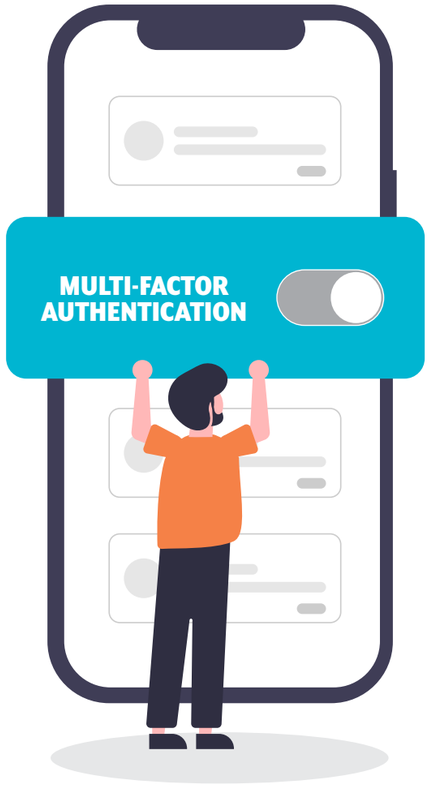
## सलाह 2: बहु चरणो वाला प्रमाणीकरण टर्न-ऑन करें

**आपके खाते पर बहु चरणो वाला प्रमाणीकरण आपके घर के लिए सुरक्षा स्क्रीन जैसा है। ये उन अपराधियों से आपको बचाता है जो घुसने का प्रयास कर रहे हैं।**

बहु चरणो वाला प्रमाणीकरण सक्रिय होने से, आपको अपने खाते में जाने के लिए एकाधिक जानकारी देनी होगी। उदाहरण के लिए, आपको अपने सोशल मीडिया प्रोफाइल में लॉग इन करने के लिए अपना पासवर्ड और एक टैक्स्ट मैसेज से प्राप्त कोड डालना होगा।

इन एकाधिक परतों से साइबर अपराधियों के लिए हैक करके घुस पाना कठिन हो जाएगा। वे एक हिस्से को हल करने में सफल हो सकते हैं, जैसे कि आपका पासवर्ड, लेकिन उनको आपके खाते में जाने के लिए चक्रव्यूह के अन्य हिस्सों को भी हल करना पड़ेगा।

**और अधिक जानकारी के लिए वेबसाइट cyber.gov.au पर 'Multi-factor authentication' या 'MFA' सर्च करें।**


### याद रखें:

**यदि आपको एकाधिक फैक्टरों वाला प्रमाणीकरण चालू करने में सहायता की आवश्यकता है, तो किसी मित्र या अपने परिवार के किसी सदस्य से पूछें।**





## सलाह 3: अपने डिवाइस का बैकअप लें

**अपने महत्वपूर्ण दस्तावेज़ों की प्रति बनाना और उसे किसी सुरक्षित जगह पर डालना 'बैकअप' करना होता है। ये उसी तरह होता है जैसे अतिप्रिय फोटूओं की मूल प्रति के खो जाने की संभावना को देखते हुए उनकी फोटोकॉपी करके उसे किसी सुरक्षित जगह पर रखना।**

जब आप अपने कम्प्यूटर, फोन या टेबलेट का बैकअप लेते हैं, तो फाइलों की प्रतियों का सुरक्षित रूप से ऑनलाइन या किसी दूसरी डिवाइस में संग्रहण किया जाता है। अपनी महत्वपूर्ण फाइलों और अनमोल फोटूओं का बैकअप करने से आपके दिमाग में शांति रहेगी।

यदि आपकी डीवाइस में कुछ गड़बड़ हो जाती है या साइबर अपराधियों द्वारा उसे हैक कर लिया जाता है, तो आप बैकअप में से अपनी फाइलें आसानी से पुनः प्राप्त रीस्टोर कर सकते हैं।

**और अधिक जानकारी के लिए वेबसाइट cyber.gov.au पर 'Backups' सर्च करें।**



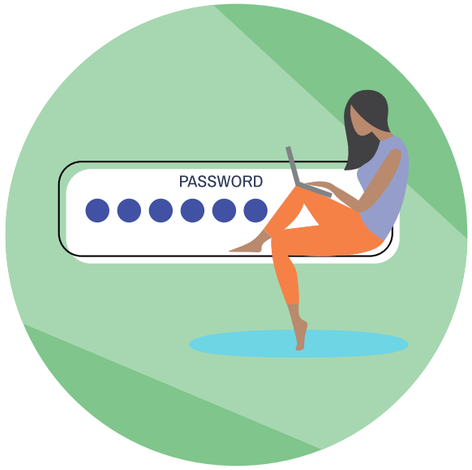
### क्या आप जानते हैं:

**अपनी डिवाइस का नियमित रूप से** बैकअप लेने का मतलब है कि आपकी सबसे नवीनतम फाइलें हमेशा आपके पास रहेंगी।

## सलाह 4: सुरक्षित पासफ़्रेज़ का प्रयोग करें

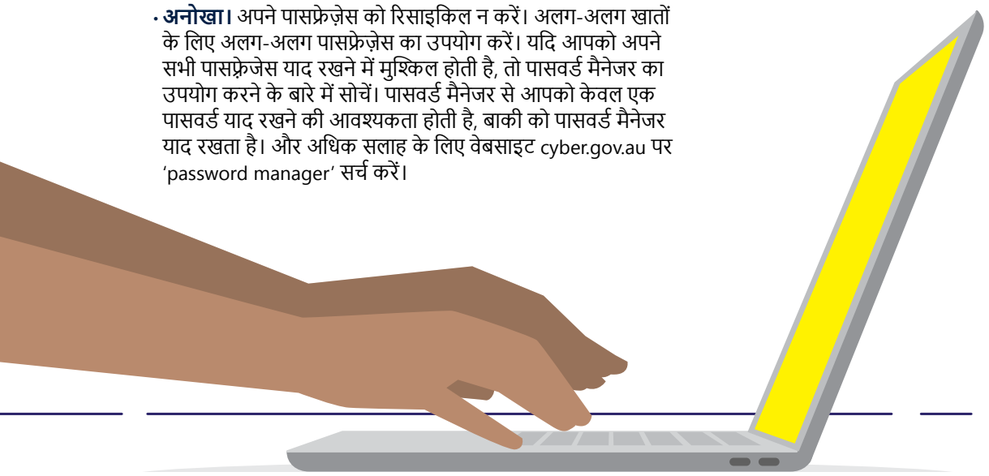
**यदि पासवर्ड आपके खाते पर चाबी वाला ताला लगाने के समान है, तो एक पासफ़्रेज़ उसे अपना खुद का सिक्योरिटी सिस्टम देने के समान होता है। वो पासवर्ड का ज़्यादा मजबूत और ज़्यादा सुरक्षित स्वरूप होता है।**

यदि MFA चालू नहीं कर सकते, तो अपना खाता सुरक्षित करने के लिए एक पासफ़्रेज़ का उपयोग करें। पासफ़्रेज़ में आपके पासवर्ड के रूप में चार या उससे अधिक आकस्मिक (रैंडम) शब्दों का उपयोग होता है। इससे साइबर अपराधियों के लिए इनकाअनुमान लगाना कठिन हो जाता है लेकिन आपके लिए इन्हें याद रखना आसान।




अपना पासफ़्रेज़ बनाते समय आप उसे बना सकते हैं:

- **लंबा।** जितना लंबा, उतना ही बेहतर होगा। इसे कम से कम 14 अक्षरों तक लंबा रखें। इसमें यदि आप ऐसे चार या अधिक आकस्मिक रैंडम शब्द चुनें जो आपको याद रह सकें तो बहुत अच्छा रहेगा। उदाहरण के लिए, 'परपल डक पोटेटो बोट'।
- **जिसका अनुमान न लगाया जा सके।** आपका पासफ़्रेज़ अनुमान लगाने के लिए जितना कठिन होगा, उतना ही बेहतर होगा। वाक्यों से बहुत अच्छे पासफ़्रेज़ बन सकते हैं, लेकिन उनका अनुमान लगाना आसान होता है। चार या उससे अधिक आकस्मिक (रैंडम) शब्दों से एक सुदृढ़ पासफ़्रेज़ बन जाएगा।
- **अनोखा।** अपने पासफ़्रेज़ेस को रिसाइकिल न करें। अलग-अलग खातों के लिए अलग-अलग पासफ़्रेज़ेस का उपयोग करें। यदि आपको अपने सभी पासफ़्रेजेस याद रखने में मुश्किल होती है, तो पासवर्ड मैनेजर का उपयोग करने के बारे में सोचें। पासवर्ड मैनेजर से आपको केवल एक 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 पासफ़्रेजेस बनाने के बारे में और अधिक पता करें।**



इंटरनेट का सुरक्षित रूप से उपयोग कैसे किया जाए

## सलाह 5: धोखाधड़ियों को पहचानें और उनकी रिपोर्ट करें

**किसी धोखे के बारे में आप जितनी जल्दी सूचित करेंगे, उतनी ही जल्दी हम कार्यवाही कर पाएँगे।**

यदि आपको विश्वास है कि कोई व्यक्ति आपको धोखा देने के लिए इंटरनेट का प्रयोग करना का प्रयास कर रहा है, तो पहले से सक्रिय होना और सतर्क रहना अच्छा रहेगा बजाय यह खतरा मोल लेने के कि कोई आपका लाभ उठा ले।

यदि किसी बात के सच होने में संदेह होता है, तो शायद वो सच नहीं होती। यदि किसी मैसेज में आपसे कहा गया है कि आपके कम्प्यूटर में वायरस है, तो वह मेसेज आपके लिए अनोखा नहीं है।

वह किसी धोखेबाज का भेजा हुआ मैसेज हो सकता है और हो सकता है कि वे आपका लाभ उठाना चाहते हों।

याद रखें, घोटालेबाज अक्सर वह व्यक्ति या संगठन होने का दिखावा करेंगे, जिसपर आप विश्वास करते/करती हैं। यदि आपको ऐसा कोई मैसेज मिलता है जो आपके किसी विश्वसनीय व्यक्ति द्वारा भेजा गया दिखता है, लेकिन वे कोई नया फोन नंबर, ईमेल पता या सोशल मीडिया प्रोफ़ाइल का उपयोग कर रहे हैं, तो सतर्क रहें। जवाब देने से पहले अपने किसी भरोसेमंद माध्यम से यह सत्यापित कर लें कि आपको मैसेज भेजने वाला व्यक्ति या संगठन वास्तव में वही है, जो वह होने का दावा करता है। उदाहरण के लिए, यदि आपको टेक्स्ट मैसेज मिलता है जो आपके बेटे/बेटी की ओर से भेजा गया दिखता है, लेकिन यह किसी नए नंबर से आया है, तो जवाब न दें। इस बात की जांच करने के लिए पहले उन्हें सोशल मीडिया पर मैसेज भेजें कि उन्होंने वास्तव में अपना फोन नंबर बदल लिया है।

### क्या आप जानते हैं:

**साइबर अपराधी कुटिल होते हैं और कोई परिचित नाम और ईमेल एडरस काम में ले सकते हैं। सतर्क रहें यदि:**

- **आपसे तुरंत किसी बिल का भुगतान करने के लिए कहा जाए**
- **आपसे आपका विवरण या पासवर्ड बदलने के लिए कहा जाए**
- **आपसे किसी लिंक पर क्लिक करने या कोई अटैचमेंट खोलने के लिए कहा जाए।**

## निष्क

**अब जबकि आपको इंटरनेट को और अधिक सुरक्षित तरीके से काम में लेने की जानकारी मिल गई है, आप भरोसे के साथ ब्राउज़ कर सकते हैं और ऑनलाइन अपने समय का आनंद उठाना जारी रख सकते हैं।**

यह बात याद रखें कि, साइबर अपराधी लोगों को निशाना बनाने के लिए हमेशा नए तरीके अपनाते रहते हैं।

अपनी साइबर सुरक्षा में सुधार करते रहने समय-समय पर व्यवहारिक ज्ञान बढ़ाते रहने और सुरक्षित रहने के नए तरीकों को सीखने में कभी कोई बुराई नहीं होती।

# बोनस सुझाव।

## ऑनलाइन सुरक्षित रहने के और अधिक तरीके सीखना चाहते हैं? निम्नांकित सुझावों को देखें।

**आप क्या पोस्ट डालते हैं उस बारे में सोचें।**

आप जिन बातों को ऑनलाइन साझा करते हैं उनके बारे में और कौन-कौन उन्हें देखेगा उस बारे में विचार करें। केवल उन्हीं लोगों का मित्रता का आग्रह स्वीकार करें जिन्हें आप अपने जीवन में वास्तविक रूप से जानते हैं।

**नए खतरों के बारे में चेतावनियों का पता लगाते रहें।**

हमारी मुफ़्त अलर्ट सेवा के लिए साइनअप करें। इससे, जब भी हमें किसी नई साइबर खतरे का पता लगेगा तो आपको भी उसके बारे में ज्ञात हो जाएगा।

इससे आपको यह सलाह भी मिलेगी कि यदि कोई हमला होता है तो क्या करना चाहिए।

**साइबर सुरक्षा के बारे में अपने परिवार और मित्रों से बात करें।**

अब जबकि आपने साइबर ससुरक्षा के बारे में अपना कौशल बढ़ा लिया है, आपने जो सीखा है उसे अपने परिवार और मित्रों के साथ साझा करें। आपके ज्ञान से आगे कभी उनको किसी कठिन परिस्थिति में सहायता मिल सकती है!

**जब आप ऑनलाइन बैंकिंग या खरीददारी करें तो सार्वजनिक वाई-फाई का उपयोग करने से बचें।**

सार्वजनिक वाई-फाई, विडियोज़ देखने या वेबसाइटें पढ़ने के लिए अच्छा होता है लेकिन जो गतिविधि पैसे से जुड़ी हुई हो उसे अपने घर के इंटरनेट कनेक्शन से ही करें। सार्वजनिक वाई-फाई जोखिमयुक्त हो सकता है।

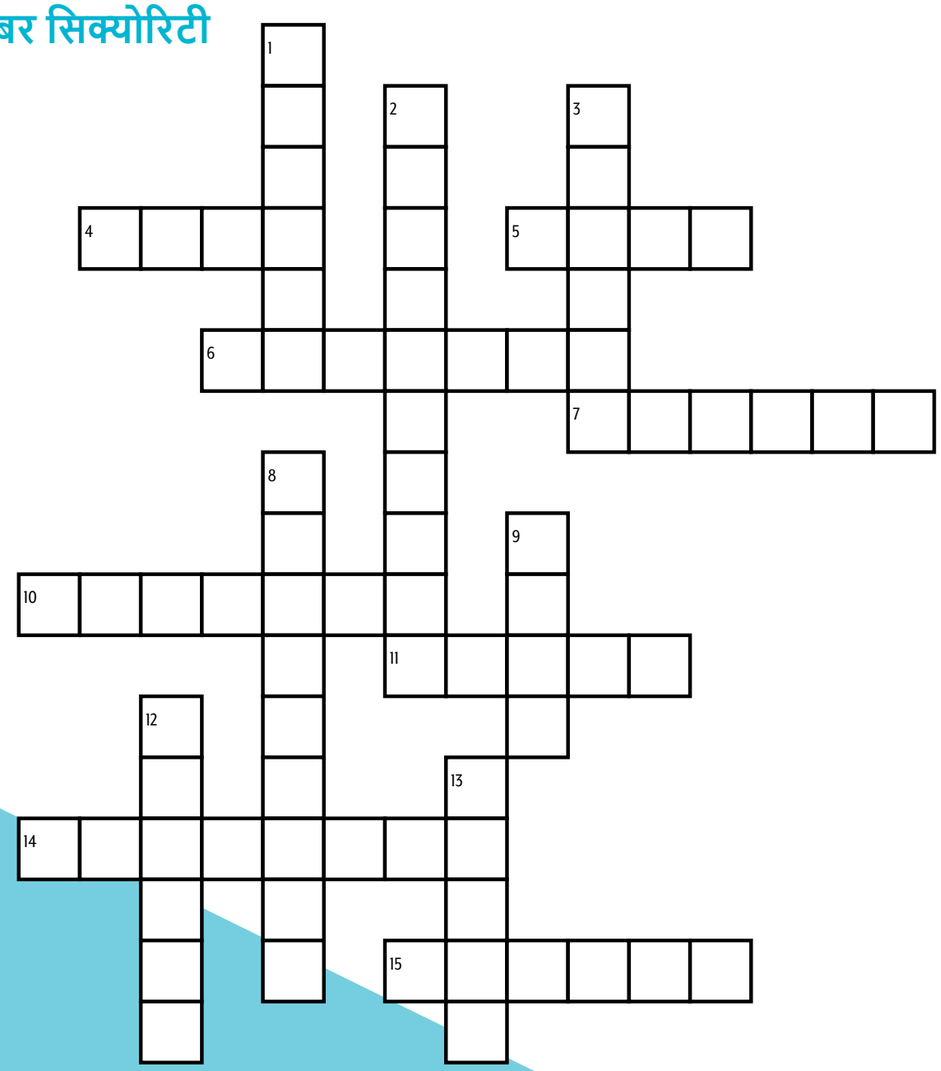
**ऑस्ट्रेलिया को सुरक्षित रखने के लिए साइबर अपराधों और घटनाओं की रिपोर्ट करें।**

अगर आप सोचते हैं कि आप साइबर अपराध के पीड़ित हैं, तो तुरंत कार्यवाही करें। और अधिक सलाह cyber.gov.au पर उपलब्ध है





## साइबर सिक्योरिटी



### नीचे

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

### एक सिरे से दूसरे सिरे तक

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

## अनुपूरक दिशा-निर्देशिका

आगे और अधिक जानकारी के लिए कृपया हमारी *(Personal Cyber Security)* श्रंखला देखें:
तीनों दिशा-निर्देशिकाओं की 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।


आप इन तीनों दिशा-निर्देशिकाओं को **cyber.gov.au** पर देख सकते हैं।

## पहेली के उत्तर

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device





# ध्यान देने योग्य बातें

**पहेली के उत्तर**

इस मार्गदर्शिका में निहित सामग्री सामान्य प्रकृति की है और इसे कानूनी सलाह के रूप में नहीं माना जाना चाहिए अथवा किसी विशेष परिस्थिति या आपातकालीन स्थिति में इसपर सहायता के लिए निर्भर नहीं होना चाहिए। किसी भी महत्वपूर्ण मामले में आपको अपनी परिस्थितियों के संबंध में उचित स्वतंत्र पेशेवर सलाह लेनी चाहिए।

इस मार्गदर्शिका में निहित जानकारी पर निर्भरता के परिणामस्वरूप होने वाली किसी भी क्षति, हानि या व्यय के लिए राष्ट्रमंडल कोई जिम्मेदारी या उत्तरदायित्व स्वीकार नहीं करता है।



**कोट ऑफ आर्म्स का उपयोग**

जिन शर्तों के तहत कोट ऑफ आर्म्स का उपयोग किया जा सकता है, वे प्रधानमंत्री एवं कैबिनेट विभाग की वेबसाइट
(www.pmc.gov.au/government/commonwealth-coat-arms) पर उपलब्ध हैं।

**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