



Australian Government
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

इंटरनेट का सुरक्षित रूप से उपयोग कैसे किया जाए

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 शुरू 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 डायरेक्ट (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 यहाँ 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।



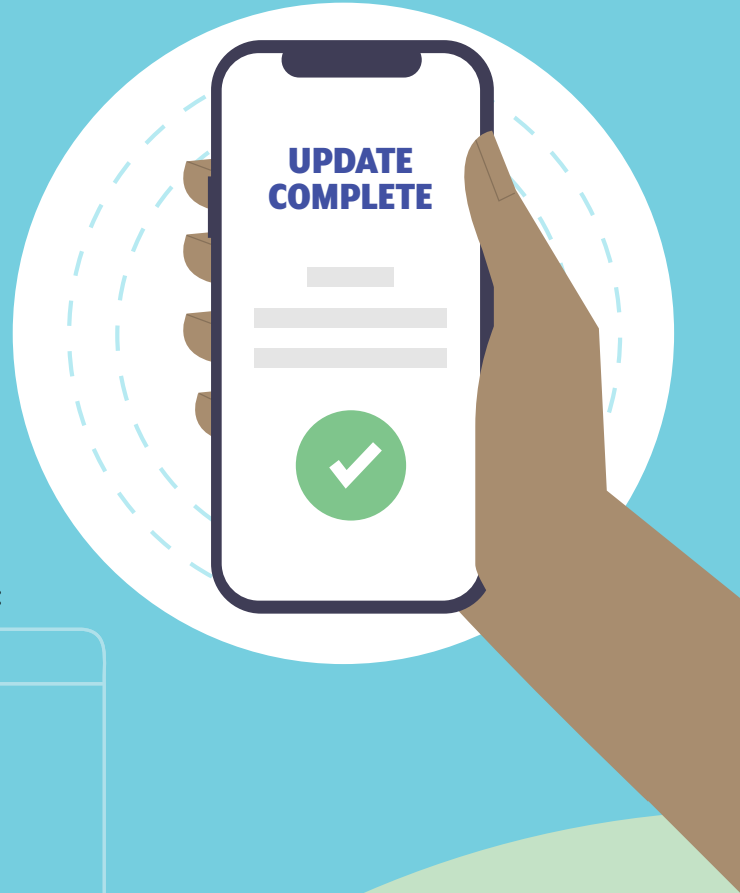
सलाह 1: अपनी डिवाइस को अपडेट करें

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 (ऑटोमैटिक 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।

स्वतः (ऑटोमैटिक) अपडेटों को चालू करने के बारे में हमारी चरण दर चरण दिशा-निर्देशिका को देखने के लिए:

1. देखें cyber.gov.au
2. क्लिक करें [व्यक्ति व परिवार](#)
3. क्लिक करें [चरण दर चरण दिशा-निर्देशिकाएँ।](#)
4. खोजें [ऑटोमैटिक अपडेट चालू करना](#)
5. एप्पल या विंडो डिवाइसेज़ में से चुनें।



क्या आप जानते हैं:
अपडेटों से आपकी डिवाइस में नए फीचर भी जुड़ जाएंगे और वो अधिक तीव्रता से काम करेगी।



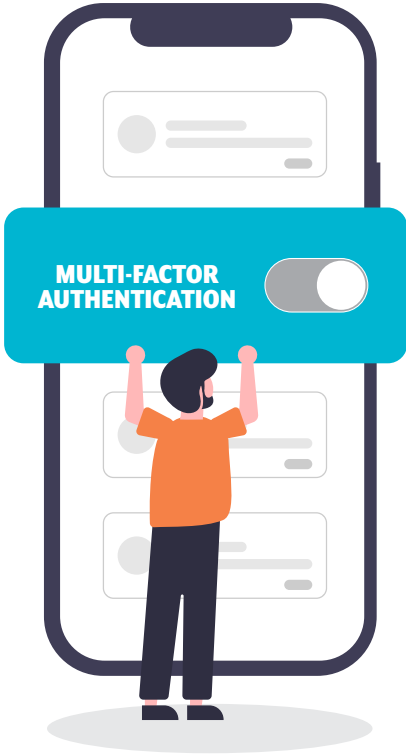
सलाह 2: बहु चरणो वाला प्रमाणीकरण टर्न-ऑन करें

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।

दो फैक्टरों वाले प्रमाणीकरण को चालू करने के बारे में हमारी चरण दर चरण दिशा-निर्देशिका को देखने के लिए:



1. देखें cyber.gov.au

2. क्लिक करें [व्यक्ति व परिवार](#)

3. क्लिक करें [चरण दर चरण दिशा-निर्देशिकाएँ](#)

4. खोजें [दो फैक्टरों वाला प्रमाणीकरण चालू करें](#)

5. आपका खाता जिस जिस प्रकार का है (जैसे कि फेसबुक, जीमेल या एप्पल आई डी) उस हिसाब से दिशा-निर्देशिका चुनें।

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।

इंटरनेट का सुरक्षित रूप से उपयोग कैसे किया जाए



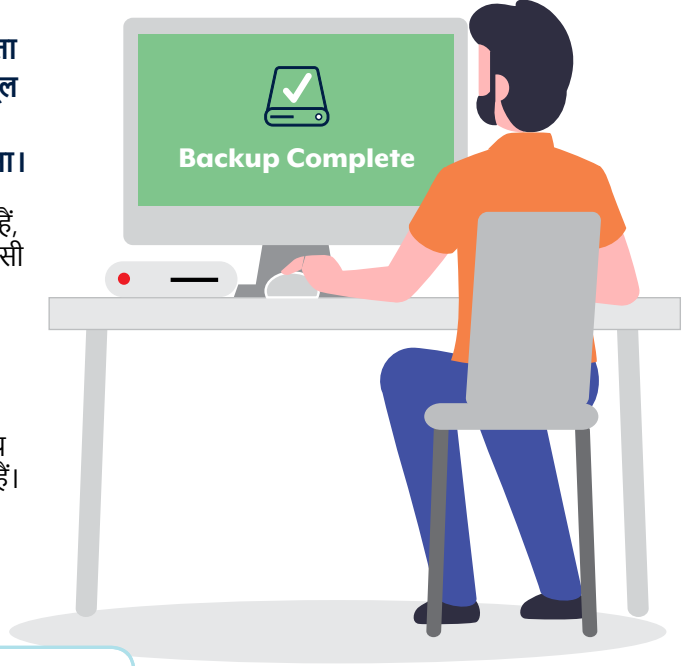
सलाह 3: अपने डिवाइस का बैकअप लें

अपने महत्वपूर्ण दस्तावेजों की प्रति बनाना और उसे किसी सुरक्षित जगह पर डालना 'बैकअप' करना होता है। ये उसी तरह होता है जैसे अतिप्रिय फोटों 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 फोटों का बैकअप करने से आपके दिमाग में शांति रहेगी।

यदि आपकी डिवाइस 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।


दो फैक्टरों वाले प्रमाणीकरण को चालू करने के बारे में हमारी चरण दर चरण दिशा-निर्देशिका को देखने के लिए:



1. देखें cyber.gov.au

2. क्लिक करें  व्यक्ति व परिवार

3. क्लिक करें  चरण दर चरण दिशा-निर्देशिकाएँ

4. खोजें  दो फैक्टरों वाले प्रमाणीकरण को चालू करने के बारे में हमारी चरण दर चरण दिशा-निर्देशिका को देखने के लिए:

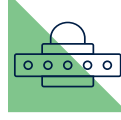
5. एप्पल या विंडो डिवाइसेज़ में से चुनें।

क्या आप जानते हैं:

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

इंटरनेट का सुरक्षित रूप से उपयोग कैसे किया जाए

सलाह 4: सुरक्षित पासफ्रेज़ का प्रयोग करें

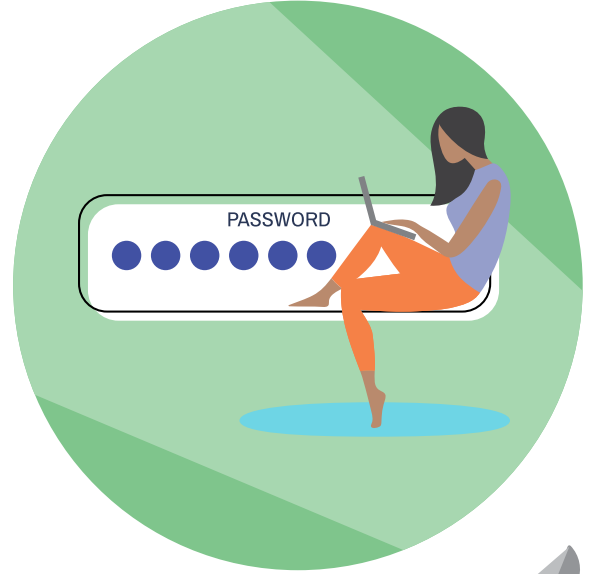


यदि पासवर्ड आपके खाते पर चाबी वाला ताला लगाने के समान है, तो एक पासफ्रेज़ उसे अपना खुद का सिक््योरिटी सिस्टम देने के समान होता है। वो पासवर्ड का ज़्यादा मजबूत और ज़्यादा सुरक्षित स्वरूप होता है।

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

अपना पासफ्रेज़ 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 पासफ्रेज़ अनुमान लगाने के लिए जितना कठिन होगा, उतना ही बेहतर होगा। वाक्यों से बहुत अच्छे पासफ्रेज़ बन सकते हैं, लेकिन उनका अनुमान लगाना आसान होता है। चार या उससे अधिक आकस्मिक (रैंडम) शब्दों से एक सुदृढ़ पासफ्रेज़ बन जाएगा।
- **अनोखा।** अपने पासफ्रेज़ों का पुनः प्रयोग न करें। अलग-अलग खातों के लिए अलग-अलग पासफ्रेज़ काम में लें।



सुरक्षित पासफ्रेज़ बनाने के बारे में

cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases पर और अधिक बातें सीखें।



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 मैसेज आपके लिए अनोखा नहीं है।

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

किसी धोखे की सूचना देने के लिए scamwatch.gov.au और cyber.gov.au पर जाएँ।



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।



इंटरनेट का सुरक्षित रूप से उपयोग कैसे किया 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 व्यावहारिक 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 मुफ्त 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 सुरक्षा 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।

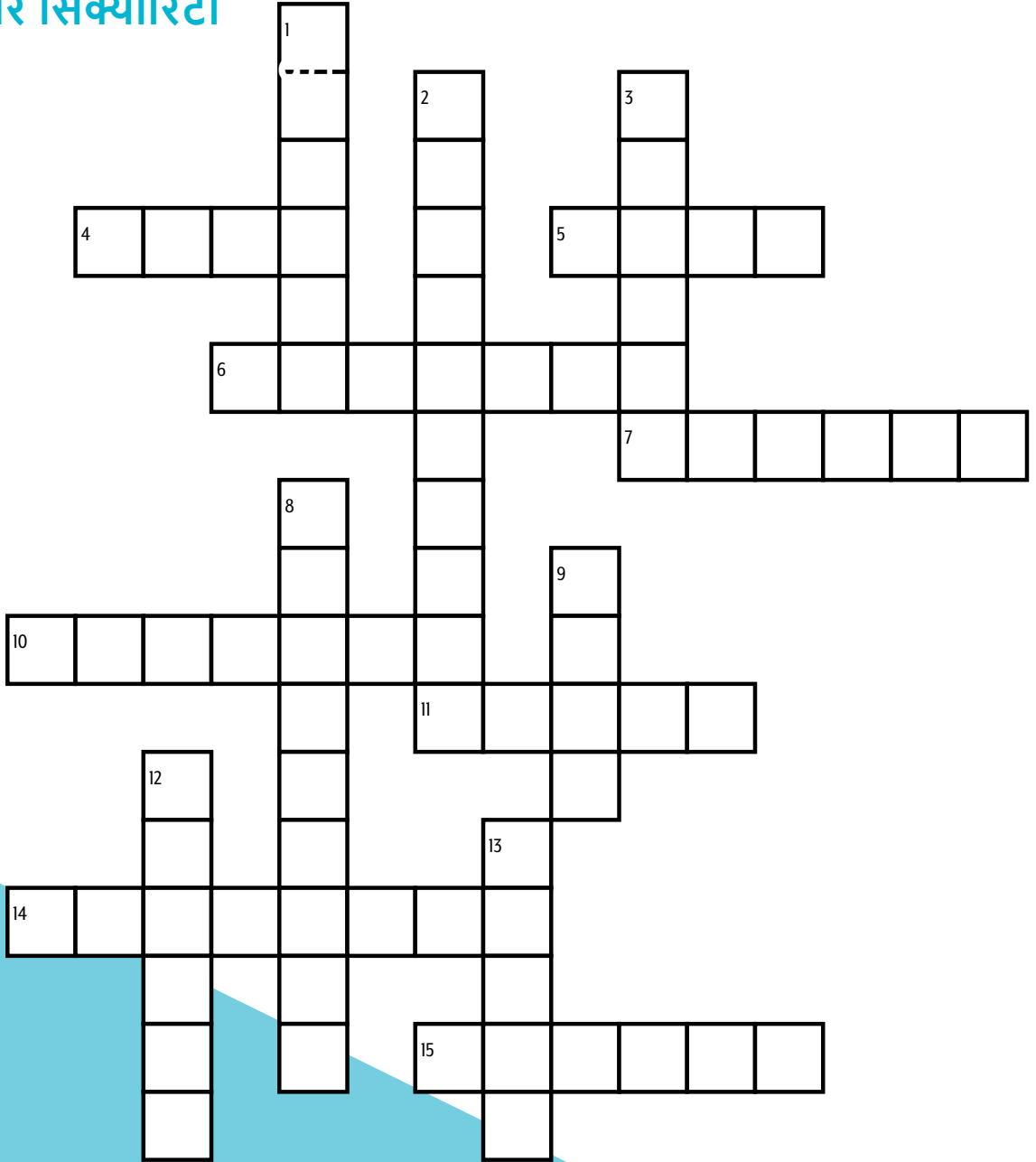
सार्वजनिक वाई-फाई, विडियोज़ देखने या वेबसाइटें पढ़ने के लिए अच्छा होता है लेकिन जो गतिविधि पैसे से जुड़ी हुई हो उसे अपने घर के इंटरनेट कनेक्शन से ही करें। सार्वजनिक वाई-फाई जोखिमयुक्त हो सकता है।

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।

इंटरनेट का सुरक्षित रूप से उपयोग कैसे किया जाए

साइबर सिक्योरिटी



नीचे

1. इंटरनेट से जुड़े
2. एक सुदृढ़ पासवर्ड
3. कम्प्यूटर से डाटा चुराने वाला व्यक्ति
8. सॉफ्टवेयर जो वायरसों को नष्ट कर देता है
9. एक भ्रामक योजना या चाल
12. आपके कम्प्यूटर की फाइलों की एक प्रति
13. कम्प्यूटरों से सम्बंधित, या जिसमें कम्प्यूटर शामिल हों

एक सिरे से दूसरे सिरे तक

4. वायरलैस नेटवर्किंग तकनीक
5. साइबर सुरक्षा के लिए ऑस्ट्रेलिया की मुख्य एजेंसी
6. वर्ल्ड वाइड वेब पर एक दस्तावेज़
7. किसी चीज़ के बारे में जानकारी देना
10. सॉफ्टवेयर के नए, बेहतर या और अधिक सुरक्षित प्रारूप
11. इलैक्ट्रॉनिक डाक (mail)
14. आपत्ति या से मुक्त होने की अवस्था
15. एक औजार जो इंटरनेट से जुड़ सकता है

इंटरनेट का सुरक्षित रूप से उपयोग कैसे किया जाए

अनुपूरक दिशा-निर्देशिका

आगे और अधिक जानकारी के लिए कृपया हमारी (Personal Cyber Security) श्रृंखला 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।

अधिक जानकारी के लिए, या साइबर सुरक्षा घटना की रिपोर्ट करने के लिए, हमसे संपर्क करें:
cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government
Australian Signals Directorate

ACSC Australian
Cyber Security
Centre