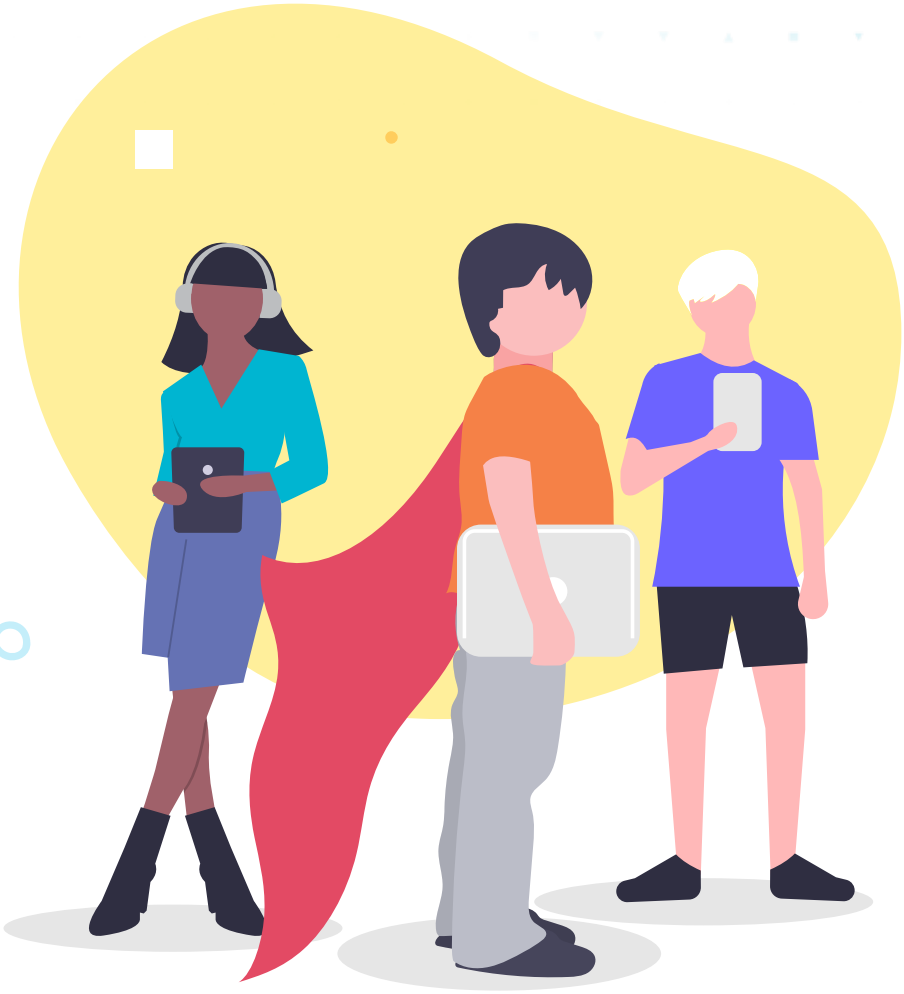
Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre



CYBER SECURITY

इंस्ट्रक्शन मैन्यूअल

इंटरनेट का सुरक्षित उपयोग करने के बारे में एक बाल दिशा-निर्देशिका

cyber.gov.au

परिचय

सीएटी मीम्स,असफल वीडियोज़, फेस फिल्टर्स इंटरनेट अद्भुत है! दुर्भाग्यवश, इंटरनेट के सभी उपयोगकर्ता उतने अच्छे नहीं होते हैं।

कुछ लोग ऑनलाइन सिर्फ परेशानी पैदा करने और दूसरों से चुराने के लिए जाते हैं।

इनको साइबर अपराधी कहा जाता है और ये लोग ही वो कारण है जिसकी वजह से हमें इंटरनेट का उपयोग करते समय सावधान रहना पड़ता है। आपकी सहायता करने के लिए, हमने यह मैन्यूअल तैयार किया है। यह ऐसे सुविधाजनक सुझावों से भरा हुआ है जिन्हे आप अपनी साइबर सुरक्षा बढ़ाने और ऑनलाइन सुरक्षित रहने के लिए काम में ले 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।

किरदार

साइबर सुरक्षा में शामिल खिलाड़ियों से मिलें।

नायक

अद्‌त, चतुर, अच्छा और मजेदार। साइबर सुरक्षा का नायक वह व्यक्ति होता है जो अभी इसे पढ़ रहा है। आप!

इस मैन्यूअल के साथ, आपमें अपनी तरफ आने वाले किसी भी साइबर खतरे को समाप्त करने की शक्ति है। और आप अकेले नहीं हैं, ऑस्ट्रेलिया में आपको ऑनलाइन सुरक्षित करने के लिए बहुत सारे समूह काम कर रहे हैं।

ऑस्ट्रेलियन साइबर सिक्योरिटी सेन्टर

वो हम हैं! ACSC, आपको और आपके परिवार को सुरक्षित केसे रखा जा सकता है उस बारे में सलाह और जानकारी प्रदान करता है।

हम साइबर खतरों पर 24/7 निगाह रखते हैं।

स्कैमवॉच

स्कैमवॉच टीम लोगों को बताती है कि धोखों की पहचान, बचाव और रिपोर्ट कैसे की जाए।

धोखे वो कपटपूर्ण या गैर-कानूनी योजनाएँ होती हैं जिनके द्वारा साइबर अपराधी उन पीड़ितों पर हमला करते हैं जिन्हें सन्देह नहीं होता।

ईसुरक्षा आयुक्त

ईसुरक्षा ऑस्ट्रेलिया का ऑनलाइन सुरक्षा नियामक है। हानिकारक विषय-वस्तु (कन्टेन्ट) को हटाने के लिए ईसुरक्षा से शिकायत की जा सकती है।

ईसुरक्षा शोध भी करता है और ऑनलाइन सुरक्षा के लिए ज्ञान बढ़ाने हेतु प्रमाणआधारित सलाह, संसाधन तथा प्रोग्राम्स भी उपलब्ध करवाता है।

साइबरअपराधी

अपराध। धोखेबाज़। जालसाज। ये किसी-लायक-नहीं, ठग लोग अपने अपराधों को कार्यान्वित करने के लिए इंटरनेट का उपयोग करते हैं।

इनको लोगों की डिवाइसों को बिगाड़ने, गैरकानूनी फाइलें फैलाने और पैसे चुराना सबसे ज्यादा अच्छा लगता है!

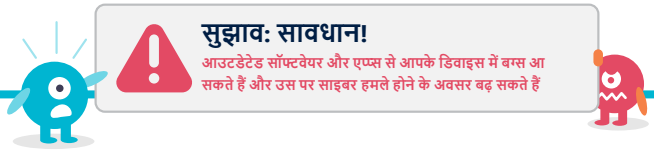
साइबर खतरों से कैसे बचा जा

चरण 1: अपनी डिवाइस को अपडेट करें

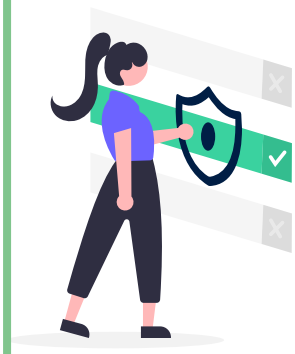
अपडेटों से आपकी डिवाइस की सुरक्षा शक्ति बढ़ जाती है!

अपडेटें सॉफ्टवेयर में उन त्रुटियों को ठीक करती हैं जिनका उपयोग साइबर अपराधी आपकी डिवाइस को हैक करने के लिए करते हैं। ये आपकी डिवाइस में नए फीचर भी जोड़ती हैं और इन के कारण आपकी डिवाइस अधिक तीव्रता से काम कर सकती है।

अपडेटों को कैसे इन्सटॉल किया जाता है, यह सीखने के लिए cyber.gov.au पर जाएँ।



चरण 2: बहु चरणो वाला प्रमाणीकरण ऑन करें



बहु चरणों वाला प्रमाणीकरण (MFA) आपके खाते के लिए एक अतिरिक्त कवच का काम करता है।

MFA चालू होने से, आपको अपने खाते में जाने के लिए विभिन्न प्रकार की जानकारी डालनी होगी। उदाहरणार्थ, लॉग इन करने के लिए आपको एक टैक्स्ट मैसेज द्वारा कोड की और आपके पासवर्ड की आवश्यकता हो सकती है। इसका मतलब है कि अगर कभी साइबर अपराधी आपके लॉग इन विवरण के एक अंश का अनुमान लगाने या चुराने में सफल हो भी गए, तो भी आप एक अतिरिक्त कवच से सुरक्षित रहेंगे!

बहु चरणो वाला प्रमाणीकरण कैसे चालू किया जाता है, यह सीखने के लिए cyber.gov.au पर जाएँ।

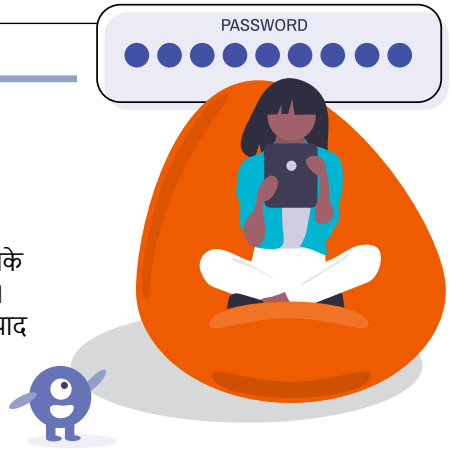
चरण 3: अपने डिवाइस का बैकअप करें

अपनी डिवाइस का बैक अप करना किसी खेल में आपकी प्रोग्रेस को सेव करने जैसा होता है।

यह उसी समय आपकी महत्वपूर्ण फाइलों की एक प्रति बनाता है और उन्हें किसी सुरक्षित स्थान पर रख देता है। बैक अप लेने का मतलब है कि यदि कुछ गड़बड़ हो जाए तो आप अपनी फाइलों को री-स्टोर कर सकते हैं।

अपनी डिवाइसों का बैक अप कैसे किया जाता है, यह सीखने के लिए cyber.gov.au पर जाएँ।

चरण 4: पासफ्रेज़ का प्रयोग करें।



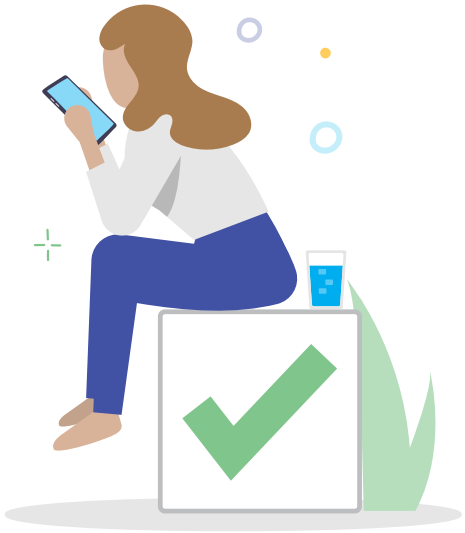
पासफ्रेज़ एक पासवर्ड के समान होता है, लेकिन विशेषज्ञ स्तर पर!

यदि आप MFA चालू नहीं कर सकते, तो 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 अनुमान लगाना कठिन हो जाता है और आपके लिए याद रखना आसान।

उदाहरण के लिए 'परपल डक बोट स्काई'।

एक सुदृढ़ पासवर्ड कैसे बनाया जाता है, यह सीखने के लिए cyber.gov.au **पर जाएँ।**

सुझाव: अपने पासफ्रेज़ में बड़े-बड़े शब्दों का उपयोग करने से वो और भी मुश्किल हो जाएगा!



धोखाधड़ियों को पहचानें और उनकी रिपोर्ट करें

साइबर अपराधियों को हराने के लिए टीमवर्क की आवश्यकता होती है।

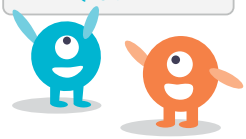
यदि आपको कोई संदिग्ध ईमेल या मैसेज मिले, तो तुरंत स्कैमवॉच को उसकी रिपोर्ट करें।

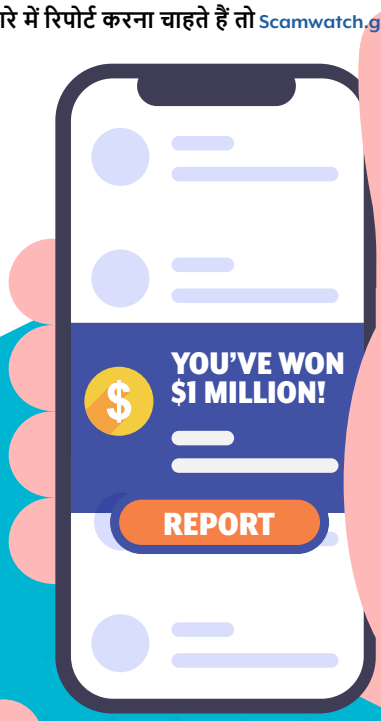
यदि किसी बात के सच होने में संदेह होता है, तो शायद वो सच नहीं होती।

साइबर अपराधी कुटिल होते हैं और आपकी जान पहचान का कोई नाम और ईमेल एडरस काम में ले सकते हैं, लेकिन अपनी अन्तः प्रेरणा के अनुसार काम करें। किसी धोखे के बारे में आप जितनी जल्दी सूचित करेंगे, उतनी ही जल्दी हम कार्यवाही कर पाएँगे।

यदि आप किसी संदिग्ध बात के बारे में रिपोर्ट करना चाहते हैं तो Scamwatch.gov.au **और** cyber.gov.au **पर जाएँ।**

सुझाव: आप जिनको नहीं जानते उनके भेजे लिंक्स या फाइलों को कभी नहीं खोलें।





अब जबकि आप साइबर सुरक्षा चतुर बन गए हैं, आप वापस लॉग ऑन करने और इंटरनेट का सुरक्षित तरीके से आनंद उठाने के लिए तैयार हैं।

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

अपनी साइबर सुरक्षा में सुधार करते रहने समय-समय परव्यवहारिक ज्ञान बढ़ाते रहने औरसुरक्षित रहने के नए तरीकों को सीखने में कभी कोई बुराई नहीं होती।

शब्द खोज

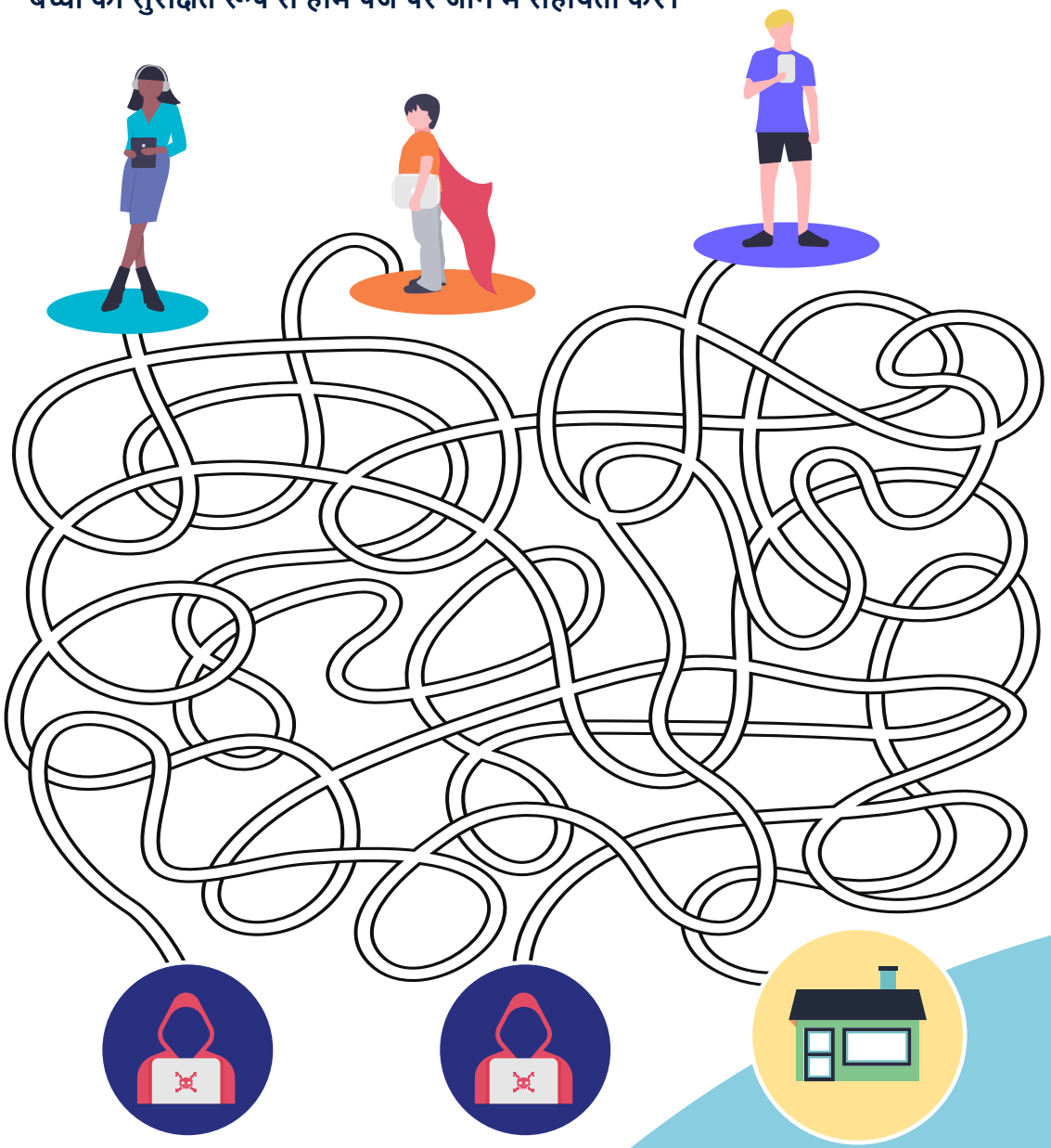
देखें आप साइबर सुरक्षा के सभी शब्द खोज पाते हैं या नहीं!

T C W V T D T M M J R F R E D
W F Y H A H B U O J X C B N H
C S P A S S P H R A S E P U X
Z C R C B A C K U P S K F W Z
Y A Z K L W G S E C U R I T Y
K M D E V I C E D E F J V X W
Z J X R Q V H L W P K V P V D
V V S W R E P O R T M E S B O
X S I A C S C W O X O M S C C
F G W F Y U H E L M B A A H S
O N L I N E F B Z T A I F N U
M A V V U O I S E E Y L E Q C
W I F I M A L I Q C Y B E R L
E W E M I M E T E G R R T G P
W H D Z G H S E I H S L L C S

ACSC
BACKUPS
CYBER
DEVICE
EMAIL
FILES
HACKER
ONLINE
PASSPHRASE
REPORT
SCAM
SECURITY
WEBSITE
WIFI

साइबर चक्र-व्यूह

बच्चों को सुरक्षित रूप से होम पेज पर जाने में सहायता करें।



BONUS TIPS

साइबर सिक्योरिटी में दक्ष होने के लिए जो जानना चाहिए वो सब मालूम है?

1. आप ऑनलाइन क्या पोस्ट डाल रहे हैं उस बारे में सोचें।
2. **ACSC** से प्राप्त चेतावनियों से नवीनतम जानकारी रखें।
3. साइबर सुरक्षा के बारे में अपने परिवार और मित्रों से बात करें।
4. जब आप ऑनलाइन खरीददारी करें तो सार्वजनिक वाई-फाई का उपयोग करने से बचें।

सुरक्षित रहते हुए सर्फ करें!

अनुपूरक दिशा-निर्देशिकाएँ

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।

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