Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

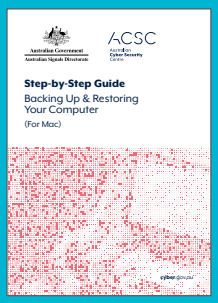
लघु व्यवसायों के लिए साइबर सुरक्षा दिशा-निर्देशिका

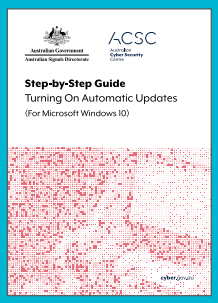
cyber.gov.au

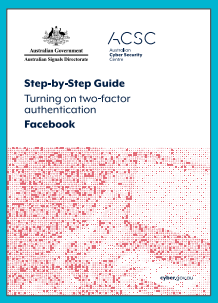
अनुपूरक दिशा-निर्देशिकाएँ

अपने व्यवसाय को सुरक्षित रखने के लिए साइबर सुरक्षा के अन्य उपायों के लिए, cyber.gov.au पर हमारा लघु व्यवसाय साइबर सुरक्षा स्यूट देखें।

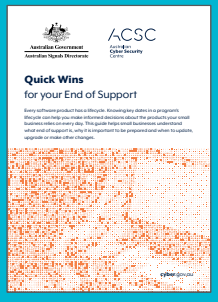
चरण दर चरण दिशा-निर्देशिकाएँ

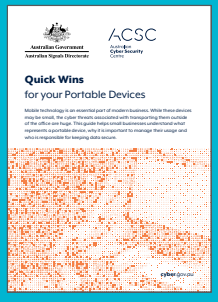


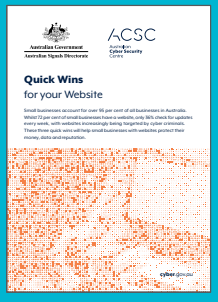




शीघ्र सफलता दिशा-निर्देशिकाएँ







विषयों की सूची

प्रस्तावना

इस दिशा-निर्देशिका की रचना छोटे व्यवसायों को सर्वाधिक सामान्य साइबर सुरक्षा घटनाओं से खुद को बचाने में सहायता के लिए की गई है।

साइबर सुरक्षा से जुड़ी किसी घटना का एल लघु व्यवसाय पर विनाशकारी प्रभाव पड़ सकता है।

दुर्भाग्यवश, ऑस्ट्रेलियन साइबर सिक्योरिटी सेन्टर (ACSC) में हम हर दिन और प्रतिदिन, लोगों, लघु व्यवसायों और बड़ी कंपनियों पर साइबर सुरक्षा घटनाओं के प्रभावों को देखते हैं।

हम यह मानते हैं कि लघु व्यवसायों के बहुत से मालिकों और संचालकों के पास साइबर सुरक्षा में लगाने के लिए समय या संसाधन नहीं होते हैं। लेकिन, कुछ सरल उपाय हैं जिन्हें, एक लघु व्यवसाय साइबर सुरक्षा से जुड़ी सामान्य घटनाओं को रोकने में सहायता के लिए अपना सकता है।

हमारी *लघु व्यवसायों के लिए साइबर सुरक्षा दिशा-निर्देशिका* को विशेष रूप से इसलिए तैयार किया गया है ताकि वे साइबर सुरक्षा के हमेशा बदलते रहने वाले खतरों के प्रति अपनी साइबर सुरक्षा के लचीलेपन के बारे में समझ सकें, कार्यवाही कर सकें, और उसे बढ़ा सकें। इसकी भाषा स्पष्ट है, सरल कार्यवाहियों के सुझाव दिए गए हैं, और दिया गया मार्गदर्शन लघु व्यवसायों को ध्यान में रखकर प्रस्तुत किया गया है।

साइबर सुरक्षा से जुड़ी मूल बातों के संक्षिप्त विवरण के लिए यह मार्ग-दर्शिका एक उत्कृष्ट शुरुआती साधन है। यदि आप अपनी साइबर सुरक्षा को आगे बढ़ाना चाहते हैं, तो आपको और अधिक जानकारी और सलाह ACSC की वेबसाइट **cyber.gov.au** पर मिल सकती है।

ऑनलाइन कनेक्ट करने के लिए ऑस्ट्रेलिया को सर्वाधिक सुरक्षित स्थान बनाने में सहायता हेतु ACSC यहां मौजूद है।

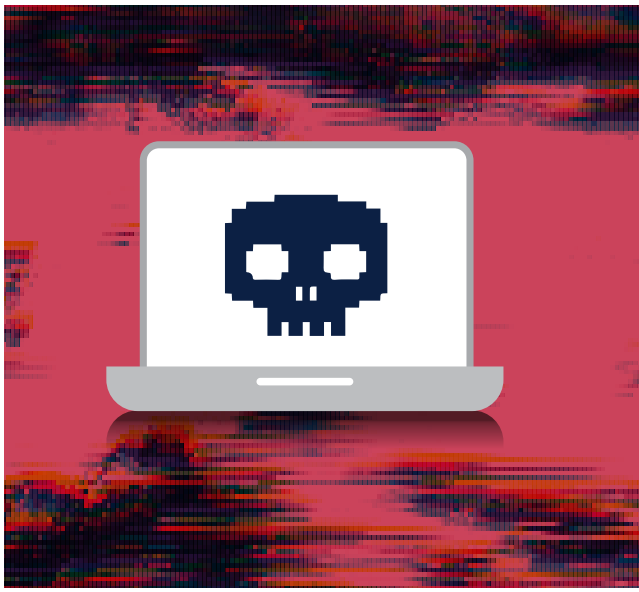
ऑस्ट्रेलियन साइबर सिक्योरिटी सेन्टर (ACSC), ऑस्ट्रेलियन सिग्नल्स डायरेक्ट्रेट (ASD) के भाग के तौर पर, ऑस्ट्रेलिया को साइबर खतरों को रोकने, पता लगाने और निराकरण करने के लिए साइबर सुरक्षा सलाह, सहायता और संचालनात्मक प्रतिक्रियाएँ देता है।

साइबर खतरेः मुख्य क्षेत्र

एक लघु व्यवसाय पर, साइबर सुरक्षा से जुड़ी किसी छोटी सी घटना का भी विनाशकारी प्रभाव पड़ सकता है।

इस भाग की रचना लघु व्यवसायों को सतर्क और तैयार रहने में सहायता करने के लिए की गई है। इसमें बहुत ही सामान्य प्रकार के साइबर खतरों की पहचान और वर्णन है और यह भी बताया गया है कि आप अपने व्यवसाय को सुरक्षित करने के लिए क्या कर सकते हैं।

मलिशियस सॉफ्टवेयर (मालवेयर)



क्या? अनाधिकृत सॉफ्टवेयर को हानि पहुँचाने के लिए डिज़ाइन किया जाता है

मालवेयर एक वृहद रूप से इस्तेमाल किया जाने वाला शब्द है, जो रेंसमवेयर, वायरसेज़, स्पाईवेयर और ट्रोज़न्स सहित मिलिशियस सॉफ्टवेयर के लिए उपयोग किया जाता है।

क्यों? बाधित करना। क्षति पहुँचाना। धोखा देना।

मालवेयर अपराधियों को बैंक या क्रेडिट कार्ड नंबरों और पासवर्डों जैसी महत्वपूर्ण सूचनाओं तक पहुँचने का मार्ग उपलब्ध करवाता है।

यह उपयोगकर्ता के कम्प्यूटर पर **नियंत्रण या जासूसी भी** कर सकता है। डाटा तक इस पहुँच का अपराधी जो काम कर सकते हैं उनमें शामिल हैः

- **धोखाधड़ी**
- **पहचान की चोरी**
- **व्यवसाय को** बाधित करना
- **संवेदनशील** डाटा या बौद्धिक संपत्ति को चुराना
- **वृहद स्तरीय अपराधिक गतिविधि के लिए** कम्प्यूटर संसाधनों को बेईमानी से निकालना

कौन? कोई भी, कहीं भी

मालवेयर की रचना करने वाले विश्व में कहीं भी हो सकते हैं।

उनको बस एक कम्प्यूटर, तकनीकी योग्यताओं और दुर्भावनापूर्ण इरादों की जरूरत होती है। आपके विरुद्ध मालवेयर का उपयोग करने के लिए अपराधियों को सस्ते टूल्स आसानी से मिल जाते हैं।

अपराधी एक विशाल जाल फैला कर रखते हैं और सबसे ज्यादा असुरक्षितों को निशाना बनाते हैं। साइबर सुरक्षा के उपाय अपना कर और खतरों के प्रति सावधान रहकर, आप अपने व्यवसाय को एक सरल निशाना बनने से बचा सकते हैं।

मालवेयर से सुरक्षित करना

- अपने ऑपरेटिंग सिस्टम,सॉफ्टवेयर और एप्प्स के ऑटोमेटिक रूप से (अपने-आप) अपडेट होने की व्यवस्था चालू करें
- अपने महत्वपूर्ण डाटा का नियमित रूप से बैकअप करें
- अपने कर्मचारियों को संदिग्ध लिंक्स और अटैचमैंटों की पहचान करने के लिए प्रशिक्षित करें

स्कैम मेसेजेस (फिशिंग)

क्या? 'धूर्ततापूर्ण' ईमेलों, मैसेजों, या कॉल्स को, प्राप्तकर्ताओं से छल द्वारा पैसा और डाटा चुराने के लिए बनाया जाता है

अपराधियों द्वारा ईमेल, सोशल मीडिया, फोन कॉल्स, या टैक्स्ट मैसेजों द्वारा ऑस्ट्रेलियाई व्यवसायों को धोखा देने का प्रयास किया जाता है।

ये अपराधी कोई ऐसा व्यक्ति होने का ढोंग कर सकते हैं जिन्हें आप जानते हैं, या आपको लगता है कि आपको भरोसा करना चाहिए ।

उनके मैसेजों और कॉल्स से व्यवसायों को कोई विशेष कार्य करने के लिए बरगलाने का प्रयास करते हैं,जैसे कि:

- **ढोंगी इनवॉयसों का भुगतान करना या उचित इनवॉयसों का भुगतना विवरण बदलना**
- **बैंक खाते के विवरण, पासवर्ड, और क्रेडिट कार्ड नंबरो को बताना (अक्सर जिन्हें 'फिशिंग' धोखों के रूप में जाना जाता है, जिसमें अपराधी बैंको या वेबसाइटों के लोगोज़ प्रतीक चिन्हों की नकल कर सकते हैं जो देखने में असली लगते हैं)**
- **आपके**कम्प्यूटर या सर्वर का एक्सस देना
- **कोई ऐसा अटैचमेंट खोलना**, जिसमें मालवेयर हो सकता है
- **गिफ्ट कार्ड्स खरीदना** और उन्हें धोखा कर रहे व्यक्ति को भेजना

कहाँ? ईमेल, सोशल मीडिया, फोन कॉल्स, या टैक्स्ट मैसेजेस

फिशिंग धोखे ईमेलों तक ही सीमित नहीं होते। उनका पता लगाना अधिक जटिल और कठिन होता जाता है।

पैसों की अर्जेंट माँग, बैंक खातों में बदलाव, अनपेक्षित अटैचमेंटों, और लॉग इन विवरण की जाँच या पुष्टि करने वाले आग्रहों के प्रति सतर्कता बरतें।

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

कौन? ऑस्ट्रेलियाई व्यवसाय

धोखाधड़ी के मैसेज हज़ारों लोगों को भेजे जा सकते हैं, या इनसे किसी विशेष व्यक्ति को भी निशाना बनाया जा सकता है।

लेकिन, कुछ सामान्य तकनीकें ऐसी होती हैं जो अपराधियों द्वारा आपके कर्मचारियों से चालाकी करने के लिए काम में ली जाएँगी। उनके मैसेजों में शामिल हो सकता है:

- **अथॉरिटी:** क्या कोई मैसेज किसी अधिकारी से या व्यवसाय के किसी वरिष्ठ पदाधिकारी का होने का दावा करने वाला है?
- **तात्कालिकता:** क्या आप से कहा गया है कि कोई समस्या है, या ये कहा गया है कि जवाब देने या भुगतना करने के लिए आपके पास सीमित समय है?
- **भावना:** क्या किसी मैसेज से आपको घबराहट, आशावान या जिज्ञासु महसूस होता है?
- **अनोखापन:** क्या किसी मैसेज में किसी ऐसी चीज़ को उपलब्ध कराने का प्रस्ताव दिया जा रहा है जो आपके पास कम है, या आपके सामने कोई बहुत अच्छा प्रस्ताव रखा जा रहा है?
- **वर्तमान घटनाएं:** क्या कोई मैसेज किसी वर्तमान समाचार या बड़ी घटना के बारे में है?

अगर आपको लगता है कि कोई मैसेज या कॉल सच में किसी ऐसे संस्थान से हो सकता है जिस पर आप विश्वास कर सकते हैं (जैसे कि आपका बैंक या सप्लायर) तो संपर्क का एक ऐसा तरीका ढूँढें जो आपके लिए विश्वसनीय हो।

उनकी आधिकारिक वेबसाइट पर जाएं या उनके द्वारा अपने विज्ञापन में दिए गए फोन नंबर पर फोन करें । आपको भेजे गए या फोन पर दिए गए संदेश में लिंक या संपर्क विवरण का उपयोग न करें क्योंकि ये छलपूर्ण हो सकते हैं।

रैंसमवेयर

क्या? एक प्रकार का मैलवेयर, आपके कम्प्यूटर या आपकी फ़ाइलों को तब तक लॉक कर देता है जब तक कि फिरौती का भुगतान नहीं कर दिया जाता

रेंसमवेयर का काम आपकी फ़ाइलों को लॉक या एन्क्रिप्ट करना होता है ताकि अब आप उन तक न पहुंच सकें। कभी-कभी यह आपकी डिवाइसों को काम करने से भी रोक सकता है। रेंसमवेयर आपकी डिवाइसों को उसी तरीके से खराब कर सकता है जैसे कि अन्य मालवेयर कर सकते हैं। उदाहरण के लिए:

- असुरक्षित या संदिग्ध वेबसाइटों पर जाना
- अनजान सोर्सेज़ से प्राप्त लिंकों, ईमेलों या फाइलों को खोलना
- आपके नैटवर्क या डिवाइसों (सर्वरों सहित) की कमज़ोर सुरक्षा

क्यों? पैसा

रेंसमवेयर साइबर अपराधियों को कम-जोखिम की उच्च-इनाम वाली आय उपलब्ध करवाता है। इसका विकास और वितरण आसान है। सामान्यतया फिरौतियों का भुगतान ऑनलाइन डिजिटल करेंसी या ब्रिटकोइन जैसी क्रिप्टोकरेंसी से किया जाता है, जिसे ट्रेस करना बहुत कठिन होता है। साइबर अपराधियों के पक्ष में एक बात ये भी है कि अधिकाँश लघु व्यवसाय रेंसमवेयर हमलों से बचने के लिए तैयार नहीं हैं।

कौन? लघु, मध्यम और बड़े व्यवसाय

लघु व्यवसाय विशेष रूप से असुरक्षित होते हैं, क्योंकि उनके द्वारा साइबर सुरक्षा के उन उपायों को कार्यान्वित करने की संभावना कम होती है जो रेंसमवेयर से बचाव और रीकवर करने में सहायता कर सकते हैं।

कभी भी फिरौती का भुगतान न करें

फिरौती का भुगतान,पीड़ित की फाइलें रीस्टोर करने की, चुराए गए किसी भी डाटा का प्रकाशन न होने या अन्य अपराधों में उपयोग के लिए बिक्री न होने की, गारंटी नहीं होता। इससे, पीड़ित के दोबारा निशाना बनने की संभावना भी बढ़ जाती है।

यदि आप किसी रेंसमवेयर घटना के शिकार हो जाएं और आपको सहायता की आवश्यकता हो, तो ACSC की हॉटलाइन को 1300 CYBER1 (1300 292 371) पर फोन करें।

फिरौती का भुगतान करने के निर्णय से पृथक, पीड़ितों को प्रोत्साहित किया जाता है कि वे रेंसमवेयर घटनाओं के बारे में ACSC को cyber.gov.au पर सूचित करें। घटनाओं के बारे में जानकारी साझा करने से अन्य ऑस्ट्रेलियाई व्यवसायों को सुरक्षित करने में सहायता मिलती है।

रेंसमवेयर से बचाव और रीकवर करना

- अपने महत्वपूर्ण डाटा का नियमित रूप से बैकअप करें
- अपने ऑपरेटिंग सिस्टमों,सॉफ्टवेयर और एप्प्स के ऑटोमेटिक रूप से (अपने-आप) अपडेट होने की व्यवस्था चालू करें
- जहाँ भी संभव हो, सेवाओं तक पहँचने के लिए बहु चरणो के प्रमाणीकरण को आवश्यक बनाएँ (पृष्ठ 12)
- अपनी डिवाइसों (यदि आपके पास सर्वर हों तो उनके सहित) और आपके नैटवर्क की इंटरनेट पर उजागर अन्य सेवाओं (रिमोट डेस्कटॉप, फाइल शेयर, वेबमेल) की ऑडिट करें और उनको सुरक्षित बनाएँ । यदि आपको कोई असमंजस हो तो अपने ऑडिटर से विचार-विमर्श करें।

सॉफ्टवेयर के बारे में ध्यान देने योग्य बातें: मुख्य क्षेत्र

अपने सॉफ्टवेयर, डाटा और ऑनलाइन खातों का प्रबंधन करने से आपके व्यवसाय की अत्यधिक सामान्य तरह के साइबर खतरों से सुरक्षा ज़बर्दस्त रूप से बढ़ जाती है।

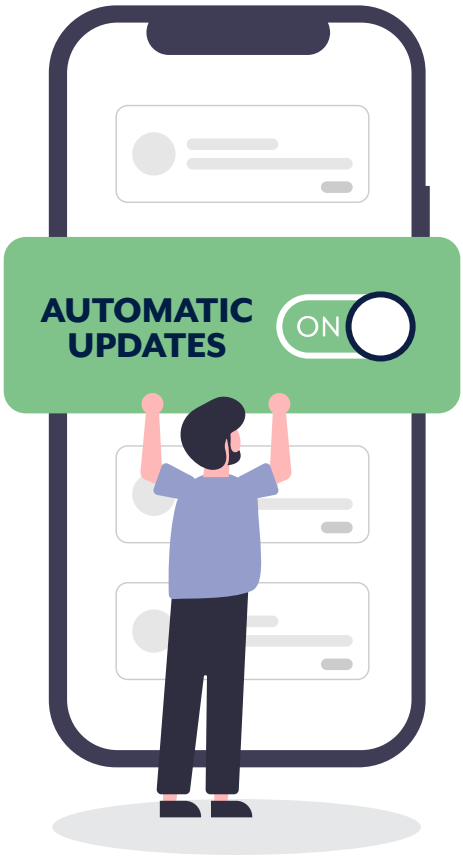
उदाहरण के लिए, आपका ऑपरेटिंग सिस्टम आपके कम्प्यूटर का सबसे महत्वपूर्ण हिस्सा होता है। यह आपके कम्प्यूटर के हार्डवेयर और उसके सभी प्रोग्रामों को मैनेज करता है, और इसलिए इसे लगातार अपडेट करने की ज़रूरत होती है ताकि यह सुनिश्चित हो सके कि आप हमेशा सर्वाधिक सुरक्षित प्रारूप काम में लेते हैं।

लघु व्यवसायों के लिए सॉफ्टवेयर के बारे में इन ध्यान देने योग्य बातों को कार्यान्वित करले लचीलापन बढ़ाएँ, नवीनतम जानकारी से अवगत रहें और सुरक्षित रहें।

ऑटोमैटिक अपडेट्स

क्या? सॉफ्टवेयर और अपडेट्स

आपके द्वारा अपने सर्वरों, कम्प्यूटरों और मोबाइल डिवाइसों में सॉफ्टवेयर (प्रोग्राम्स, एप्प्स, और ऑपरेटिंग सिस्टम्स) का उन्नत प्रारूप इंस्टाल करना **अपडेट** कहलाता है। **ऑटोमैटिक अपडेट** एक डीफॉल्ट या **'चालू करें और भूल जाएँ'** प्रणाली होती है जो आपके सॉफ्टवेयर की अपडेट उपलब्ध होते ही उसे अपडेट कर देती है।



क्यों? SECURITY

- अपने ऑपरेटिंग सिस्टम और एप्लीकेशनों को अप-टू-डेट रखना स्वयँ को साइबर सुरक्षा की घटना से सुरक्षित रखने के **सर्वश्रेष्ठ तरीकों में से एक है।**
- **अपने सॉफ्टवेयर को नियमित रूप से अपडेट करने से साइबर अपराधी की ओर से आपकी एक पहचानी गई कमजोरी का इस्तेमाल करके** मालवेयर चलाने या आपके कंप्यूटर को हैक करने की संभावना कम हो जाती है।
- ऑटोमैटिक अपडेट्स आपके समय और चिंता की बचत करती है, ये आपकी डिवाइसों और आपके डाटा को सुरक्षित रखने वाला एक महत्वपूर्ण अंश है।

कब? आज व प्रतिदिन

- **ऑटोमैटिक अपडेट्स को चालू कर दें**, विशेषकर ऑपरेटिंग सिस्टमों के लिए
- **यदि ऑटोमैटिक अपडेट्स** उपलब्ध नहीं हों तो नियमित रूप से अपडेट्स का पता लगाते रहें
- यदि आपको अपने ऑपरेटिंग सिस्टम या किसी दूसरे सॉफ्टवेयर को अपडेट करने के लिए प्रॉम्प्ट मिलता है, तो आपको **वो अपडेट जल्दी से जल्दी इंस्टाल करनी चाहिए**
- **व्यवसाय के सामान्य रूप से संचालन में बाधाओं से बचने के लिए** ऑटोमैटिक अपडेट्स हेतु सुविधानुसार समय तय कर दें
- यदि आप **वायरस निरोधी सॉफ्टवेयर का प्रयोग करते हैं, तो सुनिश्चित करें कि ऑटोमैटिक अपडेट्स की वावयस्था चालू है**

ध्यान दें:

यदि आपका हार्डवेयर या सॉफ्टवेयर बहुत पुराना है तो हो सकता है कि वो अपडेट नहीं कर पाए और आपका व्यवसाय सुरक्षा संबंधी मुद्दों के प्रति कमजोर पड़ जाए।

ACSC द्वारा सुझाव दिया जाता है कि आप अपनी डिवाइस या सॉफ्टवेयर को जल्दी से जल्दी अपडेट करें।

2020 से, विंडोज़ 7, माइक्रोसॉफ्ट ऑफिस 2010 और विंडोज़ सर्वर 2008 के लिए सपोर्ट का अंत हो गया है और अब वे सुरक्षित नहीं हैं।

अधिक जानकारी के लिए, ACSC की सपोर्ट के अंत के बारे में तुरंत सफलता दिशा-निर्देशिका पढ़ें जो cyber.gov.au पर उपलब्ध है

ऑटोमैटिक बैकअप्स

क्या? डाटा बैकअप्स

बैकअप आपके व्यवसाय की ग्राहक विवरणों और वित्तीय रिकॉर्डों जैसी सबसे महत्वपूर्ण जानकारी की एक डिजिटल कॉपी होता है। इसे बाह्य संग्रहण डिवाइस या क्लाउड में सहेजा जा सकता है।

ऑटोमैटिक बैकअप एक डीफॉल्ट या'चालू करें और भूल जाएँ' प्रणाली होती है जो मानव हस्तक्षेप के बगैर, आपके डाटा को ऑटोमैटिक रूप से (स्वतः) अपडेट कर देती है।

हर बार बैकअप के बाद अपनी बैकअप डिवाइस को सुरक्षित तरीके से डिस्कनेक्ट और अलग करने से यह सुनिश्चित हो सकेगा कि किसी साइबर घटना के दौरान वो सुरक्षित रहे।

क्यों? सहज रीकवरी

- **बैकअप लेना एक एहतियात के तौर पर किया गया उपाय होता है, ताकि यदि आपका डाटा कभी खो जाए,** चुरा लिया जाए या क्षतिग्रस्त हो जाए तो भी वो आपके लिए उपलब्ध रहे
- **इससे आपके व्यवसाय को किसी साइबर घटना जैसे कि रेंसमवेयर से उबारा जा सकता है और डाउनटाइम (जितने समय डिवाइस काम नहीं कर सकती) को कम से कम किया जा सकता है**
- **यह आपके व्यवसाय की विश्वसनीयता को बनाए रखता है** और कानूनी दायित्वों को पूरा करने सहायता करता है^

कब? आज व प्रतिदिन

- **एक ऐसी बैकअप प्रणाली चुनें जो आपके व्यवसाय के लिए सही हो।** आप अपने डाटा का कितने दिनों में बैकअप लेते हैं, इस तरह की आवश्यकताओं को पूरा करने में सहायता के लिए इस बारे में विचार करें कि बदतर स्थिति किस चीज के खोने से आपके ऊपर ज्यादा फर्क नहीं पड़ेगा
- **अपने डाटा को रीस्टोर करने का प्रयास करके** अपने बैकअप का नियमित रूप से परीक्षण करते रहें
- **कम से कम एक बैकअप को अपनी डिवाइस से हमेशा अलग रखें,** अगर कभी प्राकृतिक आपदाओं या चोरी की स्थिति हो जाए तो, उसे किसी ऑफसाइट स्थान पर रखना अच्छा रहेगा
- **अपने बैकअप को उन डिवाइसों से नहीं जोड़ें जो रेंसमवेयर या वायरसों के कारण** खराब हो गई हैं

^कुछ विशेष उद्योगों का निश्चित समयावधि के लिए रिकॉर्ड्स रखने का दायित्व होता है। सुनिश्चित करें कि आप अपनी डाटा रखने की आवश्यकताओं से अवगत हैं।

बहु चरणो वाला प्रमाणीकरण

क्या? एक सुरक्षा उपाय जिसमें आपको एक्सस की अनुमति दने के लिए पहचान के दो या प्रमाणों की आवश्यकता होती है

बहु चरणो वाले प्रमाणीकरण (MFA) में सामान्यतया निम्नांकित संयोजन की आवश्यकता होती है:

- **कुछ चीजें जो आप जानते हैं** (पासवर्ड/पासफ्रेज़, पिन (PIN), गुप्त प्रश्न)
- **कुछ चीजें जो आपके पास होती हैं** (स्मार्टकार्ड, फिज़िकल टोकन, प्रमाणक एप्प)
- **कुछ चीजें जो आप हैं** (अंगुली की छाप या अन्य बायोमेट्रिक)

क्यों? अत्यंत ज़्यादा शक्तिशाली सुरक्षा

MFA, आपकी मूल्यवान सूचना और खातों में अनाधिकृत प्रवेश से सुरक्षा के सबसे प्रभावी तरीकों में से एक है।

इन एकाधिक परतों से अपराधियों के लिए आपके व्यवसाय पर हमला करना बहुत ज़्यादा कठिन हो जाएगा। हो सकता है कि अपराधियों को आपकी पहचान का एक प्रमाण जैसे कि पासवर्ड चुराने में सफलता मिल जाए, लेकिन इसके बाद भी आपके खाते में घुसने के लिए उनको पहचान के अन्य प्रमाण प्राप्त करने की आवश्यकता होगी।

कहाँ? महत्वपूर्ण खातों में पहुँचने के लिए

लघु व्यवसायों को जहाँ भी संभव हो, महत्वपूर्ण खातों में MFA को कार्यान्वित करना चाहिए, वित्तीय और ईमेल खातों को प्राथमिकता देते हुए। MFA के कुछ विकल्पों में निम्नांकित शामिल है, लेकिन ये विकल्प इन तक ही सीमित नहीं है:

- फिज़िकल टोकन
- रैंडम पिन
- बायोमेट्रिक/अंगुली की छाप
- प्रमाणक एप्प
- ईमेल
- एसएमएस

व्यक्ति और प्रक्रियाएँ: मुख्य क्षेत्र

व्यवसायों को, चाहे वे कितने भी छोटे हों, हर स्तर पर साइबर सुरक्षा के उपायों से अवगत होना चाहिए और उन्हें जानबूझकर लागू करना चाहिए।

आपकी आंतरिक प्रक्रियाएँ और आपके कर्मचारी आपके व्यवसाय को साइबर सुरक्षा के खतरों से बचाने के लिए अंतिम, और अत्यंत महत्वपूर्ण रक्षा पंक्तियों में से एक होते हैं।

यह जानते हुए कि लघु व्यवसायों में समर्पित आईटी कर्मचारियों के लिए संसाधनों की कमी होती है, इस भाग में इस बारे में बताया गया है कि आप अपने व्यवसाय में सूचना में प्रवेश का प्रबंधन कैसे कर सकते हैं, अपने व्यवसाय के खातों को सुरक्षित कैसे रख सकते हैं, और अपने कर्मचारियों को कैसे प्रशिक्षित कर सकते हैं कि वे साइबर सुरक्षा से जुड़ी घटनाओं से बचाव, पहचान और रिपोर्ट कैसे कर सकते हैं।

एक्सस पर नियंत्रण

क्या? इस बात का प्रबंध करना कि आपके व्यवसाय के कम्प्यूटिंग परिवेश में कौन क्या एक्सस कर सकता है

एक्सस पर नियंत्रण, कम्प्यूटिंग सिस्टम में पहुँच को सीमित करने का एक तरीका होता है। यह निमंनांकित में एक्सस प्रतिबंधित करके आपके व्यवसाय को सुरक्षित करने में सहायता करता है:

- फाइलें और फोल्डर्स
- एप्लीकेशन्स
- डाटाबेस
- मेलबॉक्सेज़
- ऑनलाइन खाते
- नैटवर्क्स

क्यों? महत्वपूर्ण सूचनाओं में अनाधिकृत एक्सस का खतरा कम करने के लिए

सामान्यतया, किसी व्यवसाय में कर्मचारियों को अपनी भूमिका निभाने के लिए समस्त डाटा, खातों, और सिस्टमों में एक्सस की ज़रूरत नहीं होती है।

जहाँ भी संभव हो, यह एक्सस प्रतिबंधित होना चाहिए, ताकि कर्मचारी और बाहरी प्रदाता संयोग से या दुर्भावना से आपके व्यवसाय को खतरे में न डाल दें।

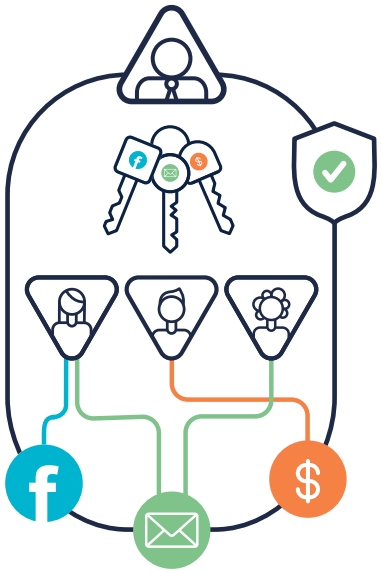
एक्सस नियंत्रण सिस्टमों और प्रक्रियाओं में व्यवसाय के मालिक या संचालक को निम्नांकित की अनुमति होती है:

- **यह निर्णय लेना कि** विशेष फाइलों, डाटाबेस, और मेलबॉक्सेज़ में कौन एक्सस कर सकता है
- **बाहरी प्रदाताओं** जैसे कि अकाउंटेंट्स, वेबासाइट होस्टिंग प्रदाता आदि को स्वीकृत किसी भी प्रकार के एक्सस पर नियंत्रण करना
- **यह प्रतिबंधित करना कि वितरक वेबसाइटों और सोशल मीडिया जैसे** खातों में कौन एक्सस कर सकता है
- **संभावित खतरे को कम करना यदि कोई खाता, डिवाइस, या सिस्टम क्षतिग्रस्त हो जाए तो**
- **जब कोई कर्मचारी अपना पद बदले या नौकरी छोड़ दे तो सिस्टम और डाटा में उसका एक्सस रद्द करना**

कौन? कम से कम विशेषाधिकार का सिद्धांत

आपके व्यवसाय के स्वरूप के आधार पर, अधिकतम लघु व्यवसायों के लिए कम से कम विशेषाधिकार का सिद्धांत सबसे सुरक्षित मार्ग होता है।

यह उपयोगकर्ताओं को को अपना काम करने के लिए जरूरत के अनुसार न्यूनतम एक्सस की अनुमति देता है। इससे किसी 'आंतरिक' व्यक्ति द्वारा संयोगवश या दुर्भावना से आपके व्यवसाय को खतरे में डालने का खतरा भी कम हो जाता है।



एक्सस नियंत्रण के सिद्धांत

- **व्यवसाय की डिवाइसों में अपने कर्मचारियों का एक्सस 'एडमिनिस्ट्रेटर' खातों से बदल कर सामान्य खातों में कर दें**
- **डिजीटल फाइलों और फोल्डरों में एक्सस की अनुमतियों पर पुनर्विचार करें**
- **कर्मचारियों के बीच खातों या पासफ्रेज़ों/ पासवर्डों को साझा न करें**
- **जब कोई कर्मचारी नौकरी छोड़कर जाए तो, एक्सस रद्द करना, खातों को मिटा देना और/या पासफ्रेज़ों/पासवर्डों को बदलना न भूलें।**

पासफ्रेज़ेस

क्या? पासवर्ड का और अधिक सुरक्षित प्रारूप

बहु चरणो वाला प्रमाणीकरण (MFA, पृष्ठ 12 देखें) आपके खाते को साइबर अपराधियों से बचाने के सर्वाधिक प्रभावशाली तरीकों में से एक है। लेकिन यदि MFA उपलब्ध नहीं हो, तो अपने खाते को सुरक्षित बनाने के लिए आपको एक पासफ्रेज़ का उपयोग करना चाहिए।

पासफ्रेज़ में आपके पासवर्ड के रूप में चार या उससे अधिक आकस्मिक (रैंडम) शब्दों का उपयोग होता है। उदाहरण के लिए 'क्रिस्टल अनिअन क्ले प्रिट्ज़ल'।

क्यों? सुरक्षित और याद रखने के लिए आसान

साइबर अपराधियों के लिए पासफ्रेज़ेस का अनुमान लगाना कठिन होता है, लेकिन आपके लिए इन्हें याद रखना आसान होता है।

पासफ्रेज़ बनाएं जो हैं:

- **लंबा** आपका पासफ्रेज़ जितना लंबा होगा, उतना ही बेहतर होगा। इसे कम से कम 14 अक्षरों की लंबाई तक रखें
- **जिसका अनुमान न लगाया जा सके:** असंबंधित शब्दों को अनियमित रूप से घुला-मिलाकर इस्तेमाल करें किसी भी प्रसिद्ध वाक्यांश, उद्धरण या बोलों का प्रयोग न करें।
- **अनोखा:** एक से अधिक अकाउंट में पासफ्रेज़ का दोबारा इस्तेमाल न करें

यदि किसी वेबसाइट या सेवा में सिम्बल्स, केपिटल लेटरों, या सँख्याओं सहित जटिल पासवर्ड की आवश्यकता हो, तो आप इन्हें अपने पासफ्रेज़ में शामिल कर सकते हैं। लेकिन तब भी उत्कृष्ट सुरक्षा के लिए आपके पासफ्रेज़ लंबे, अप्रत्याशित और अनोखे होने चाहिए।

कहाँ? आपके खातों और डिवाइसों में

यदि आप किसी खाते या डीवाइस में MFA का उपयोग नहीं कर सकते, तो सुरक्षित रहने के लिए एक पासफ्रेज़ का उपयोग करना आवश्यक है। ऐसी स्थितियों में, एक सशक्त पासफ्रेज़ ही विरोधियों और आपकी कीमती जानकारी के बीच एकमात्र अड़चन बन सकता है।

अपने पासफ्रेज़ों को अनोखा बनाना न भूलें, क्योंकि किसी पासवर्ड को एक से अधिक जगह काम में लेने से साइबर अपराधियों के लिए एकाधिक खातों को हैक करना आसान हो जाता है।

पासफ्रेज़ेस बनाने के बारे में और अधिक जानकारी के लिए, **cyber.gov.au** पर उपलब्ध ACSC की सुदृढ़ पासफ्रेज़ों की रचना करना दिशा-निर्देशिका देखें।

एक पासवर्ड मैनेजर का उपयोग करने के बारे में विचार करें

पासवर्ड मैनेजर्स (जिन्हें पासफ्रेज़ेस रखने के लिए भी काम में लिया जा सकता है) साइबर सुरक्षा से जुड़ी अच्छी आदतें डालते हैं। **प्रत्येक मूल्यवान खाते के लिए एक अनोखा पासफ्रेज़ रखना अभिभूत कर देने वाला लग सकता है लेकिन, आपके पासफ्रेज़ेस सेव करने के लिए पासवर्ड मैनेजर का प्रयोग करने से आपके सर से यह बोझ हट जाएगा कि कौनसा पासवर्ड कहाँ के लिए है।** सुनिश्चित करें कि आप जो पासवर्ड मैनेजर काम में ले रहे हैं वो किसी विश्वसनीय और सम्माननीय स्त्रोत से प्राप्त हुआ है **और वो अपने खुद के सुदृढ़ और याद रखने योग्य पासफ्रेज़ से सुरक्षित है।**

कर्मचारियों को प्रशिक्षण

क्या? अपने कर्मचारियों और व्यवसाय को साइबर खतरों से बचाने के लिए ज्ञान

खुद को और अपने कर्मचारियों को सिखायें कि साइबर अपराध को रोका केसे जा सकता है, उसकी पहचान और रिपोर्ट कैसे की जा सकती है।

अपने कर्मचारियों को, अपनी डिवाइसों को अपडेट करने, अपने खातों को सुरक्षित करने, और छलयुक्त मैसेजों की पहचाने करने सहित, साइबर सुरक्षा की मूल बातों के बारे में प्रशिक्षित करें।

साइबर घटना घटित होने पर अपने व्यवसाय और अपने कर्मचारियों का मार्गदर्शन करने के लिए आपको **साइबर सुरक्षा घटना पर कार्यवाही की** योजना कार्यान्वित करने पर भी विचार करना चाहिए।

इससे आपको मुख्य डिवाइसों और प्रक्रियाओं को समझने में सहायता मिलेगी, और साथ ही वे मुख्य संपर्क भी प्राप्त होंगे जिन्हें आप प्रत्युत्तर देने और रीकवर करने के लिए काम में ले सकते हैं।

क्यों? कर्मचारी, साइबर सुरक्षा के खतरों के विरूद्ध प्रथम और अंतिम सुरक्षा पंक्ति होते हैं

प्रशिक्षण से कर्मचारियों की आदतें और बर्ताव बदल सकते है और आपके व्यवसाय को सुरक्षित रखने के लिए साझा ज़िम्मेदारी भी उत्पन्न होती है।

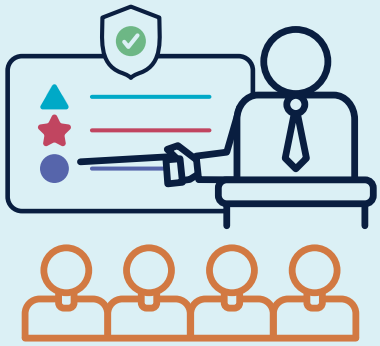
साइबर सुरक्षा सभी का उत्तरदायित्व होता है।

कब? साइबर सुरक्षा के बारे में नियमित जागरूकता और प्रशिक्षण

साइबर सुरक्षा निरंतर विकसित होती है।

साइबर सुरक्षा के खतरों के बारे में सब को नवीनतम जानकारी से अवगत रखना, अपराधियों को आपके पैसे, खातों और डाटा में एक्सस मिलने और न मिलने के बीच का अंतर हो सकता है।

"खुद को और अपने कर्मचारियों को सिखायें कि साइबर अपराध को रोका केसे जा सकता है, उसकी पहचान और रिपोर्ट कैसे की जा सकती है।"



साइबर सिक्योरिटी जागरूकता सुझाव

- अपने कर्मचारियों को संदिग्ध लिंक्स और अटैचमैंटों की पहचान करने के लिए प्रशिक्षित करें
- साइबर सिक्योरिटी के बारे में नवीनतम प्रशिक्षण नियमित रूप से उपलब्ध करवाएँ
- साइबर सुरक्षा घटना प्रत्युत्तर योजना बनाएँ
- सशक्त साइबर सुरक्षा सँस्कृति को बढ़ावा दें
- कर्मचारियों को साइबर सुरक्षा खतरों की पहचान में सहायता करने के लिए छलयुक्त मैसेजों के उदाहरण साझा करें

संक्षिप्त जाँच-सूची

सॉफ्टवेयर के बारे में ध्यान देने योग्य बातें

अपने ऑपरेटिंग सिस्टमों,सॉफ्टवेयर और एप्प्स के ऑटोमेटिक रूप से (अपने-आप) अपडेट होने की व्यवस्था चालू करें

- यदि आपको अपने ऑपरेटिंग सिस्टम या किसी दूसरे सॉफ्टवेयर को अपडेट करने के लिए प्रॉम्प्ट मिलता है, तो आपको वो अपडेट जल्दी से जल्दी इंस्टाल करनी चाहिए
- व्यवसाय के सामान्य रूप से संचालन में बाधाओं से बचने के लिए ऑटोमैटिक अपडेट्स हेतु सुविधानुसार समय तय कर दें

व्यक्ति और प्रक्रियाएँ

इस बात का प्रबंध करें कि आपके व्यवसाय में कौन क्या एक्सस कर सकता है

- कम से कम विशेषाधिकार के सिद्धांत का उपयोग करें
- जब कोई कर्मचारी नौकरी छोड़कर जाए तो, खातों को मिटाना और/या पासफ्रेज़ों/पासवर्डों को बदलना न भूलें।

जहाँ MFA संभव न हो, वहाँ खातों और डिवाइसों को सुरक्षित करने के लिए पासफ्रेज़ों का उपयोग करें

- पासफ्रेज़ में आपके पासवर्ड के रूप में चार या उससे अधिक आकस्मिक (रैंडम) शब्दों का उपयोग होता है।
- पासफ्रेज़ सबसे अधिक असरदार तब होते हैं जब वे लंबे, पूर्वानुमान न लगाने योग्य और बिलकुल अलग होते हैं।

अपने महत्वपूर्ण डाटा का नियमित रूप से बैकअप करें

- अपने डाटा को रीस्टोर करने का प्रयास करके अपने बैकअप का नियमित रूप से परीक्षण करते रहें
- कम से कम एक बैकअप को अपनी डिवाइस से हमेशा अलग रखें

जहाँ भी संभव हो महत्वपूर्ण खातों में MFA को कार्यान्वित करें

- MFA, आपकी मूल्यवान सूचना और खातों की सुरक्षा के सबसे प्रभावी तरीकों में से एक है
- अधिकतम प्रभाव के लिए वित्तीय तथा ईमेल खातों को प्राथमिकता दें

अपने कर्मचारियों को सुरक्षा की मूल बातों का प्रशिक्षण दें

- इसमें शामिल हो सकता है उनकी डिवाइसों को अपडेट करना, उनके खातों को सुरक्षित करना, और छलयुक्त मैसेजों की पहचाने करना
- साइबर सिक्योरिटी के बारे में नवीनतम प्रशिक्षण नियमित रूप से उपलब्ध करवाएँ

शब्दावली

एंटीवायरस सॉफ्टवेयर

आपके कम्प्यूटर या नेटवर्क को कम्प्यूटर वायरसों से सुरक्षित रखने के लिए बनाया गया एक सॉफ्टवेयर।

एप्प

एप्प को मोबाइल एप्लीकेशन भी कहा जाता है, यह सॉफ्टवेयर का वो पारिभाषिक शब्द है जिसका उपयोग सामान्यतया स्मार्टफोन या टेबलेट के लिए होता है।

अटैचमेंट

किसी ईमेल मेसेज के साथ भेजी गई एक फाइल

प्रमाणक एप्प

किसी कम्प्यूटर उपयोगकर्ता की पहचान करने लिए काम में ली जाने वाली एक एप्प जो बहु चरणो वाले प्रमाणीकरण (MFA) के द्वारा एक्सस की अनुमति देती है।

बायोमैट्रिक्स

किसी व्यक्ति की वो पहचान जो उनके शारीरिक फीचरों, जेसे कि अंगुली की छाप या आवाज़ को माप कर की जाती है

बिट्कोइन

एक डिजिटल करेंसी (क्रिप्टोकरेंसी), जो इंटरनेट पर विभिन्न सेवाओं के लिए काम में ली जाती है।

ब्रूट फोर्स अटैक

एक तरह का हमला जिसमें प्रति सैकण्ड लाखों अक्षरों का संयोजन बनता है। वे छोटे या शब्द वाले पासवर्डों के विरुद्ध प्रभावशाली होते हैं।

क्लाउड

सुदूरवर्ती सर्वरों का एक नेटवर्क जो विशाल, वितरित संग्रहण और प्रोसेसिंग क्षमता उपलब्ध कराता है।

साइबरअपराधी

वह व्यक्ति जो गैर-कानूनी रूप से किसी कम्प्यूटर सिस्टम को हैक करता है, सूचना को क्षतिग्रस्त करने या चुराने के लिए।

डाटा

डाटा, सूचना होती है, इसमें फाइलें, टैक्स्ट, सँख्याएँ, पिक्चरें, ध्वनी या वीडियो शामिल होते हैं।

डीफाल्ट सेटिंग्स

किसी कम्प्यूटर, ऑपरेटिंग सिस्टम या प्रोग्राम में उपयोगकर्ता के लिए पहले से निर्धारित चीज।

डिक्शनरी अटैक्स

एक तरह का हमला जिसमें प्रति सैकण्ड लाखों संभावित प्रयत्न होते हैं, नियमों और डाटाबेस के आधार पर। ये हमले कम जटिल और सामान्यतया काम में लिए जाने वाले पासफ्रेज़ों के विरुद्ध प्रभावशाली होते हैं।

एन्क्रिप्शन

दूसरों द्वारा डाटा को अपठनशील बनाने की प्रक्रिया जिसका उद्देश्य अन्य लोगों को इसकी विषय-वस्तु तक पहुँचने से रोकना होता है।

नैटवर्क

कम्प्यूटरों, सर्वरों, मुख्यफ्रेमों, नेटवर्क डिवाइसों, पेरिफेरलों, या अन्य डिवाइसों का संग्रह जो आपसे में जुड़े होते हैं ताकि डाटा को साझा किया जा सके।

ऑपरेटिंग सिस्टम

किसी कम्प्यूटर की हार्ड ड्राइव में इंस्टॉल किया गया सॉफ्टवेयर जिसके कारण कम्प्यूटर का हार्डवेयर कम्प्यूटर प्रोग्रामों के साथ संचारण करता हे और उन्हें चलाता है। उदाहरण: माइक्रोसॉफ्ट विंडोज़, एप्पल macOS, iOS, एन्ड्रॉयड।

सॉफ्टवेयर

सामान्यतया जिसे प्रोग्रामों के नाम से जाना जाता है, यह निर्देशों का एक संकलन होता है जिससे उपयोगकर्ता किसी कम्प्यूटर, उसके हार्डवेयर से बातचीत कर सकता है, या दिए गए कार्य कर सकता है।

स्पाईवेयर

एक प्रोग्राम जिसे, किसी उपयोगकर्ता की अपनी डिवाइस पर की जाने वाली गतिविधियों की सूचना चोरी-चोरी इकट्ठा करने के लिए डिज़ाइन किया जाता है।

टोकन

किसी फिज़िकल डिवाइस या प्रमाणन एप्लीकेशन द्वारा बु चरणो वाले प्रमाणीकरण के दौरान उपयोग के लिए जेनरेट किया गया एक सिक्योर कोड। टोकन शब्द का मतलब किसी फिज़िकल डिवाइस से भी हो सकता है जो ऐसे कोड जेनरेट करती है जो इतने छोटे होते हैं कि वे किसी कीचैन में फिट हो सकते हैं या जिनका आकार एक क्रेडुट कार्ड के समान होता है।

ट्रोजन्स

एक प्रकार का मालवेयर जो छद्म होते हुए भी असली सॉफ्टवेयर लगता है, लेकिन यह साइबर अपराधियों द्वारा उपयोगकर्ता के सिस्टमों में एक्सस पाने के लिए हानिकारक कोड से युक्त होता है।

वायरस

एक प्रोग्राम जिसकी रचना क्षति पहुँचाने, निजी जानकारी चुराने, डाटा में बदलाव करने, ईमेल भेजने, मैसेजों का प्रदर्शन करने के लिए की जाती है या इसमें उपरोक्त में से किन्हीं कार्यवाहियों का कॉम्बिनेशना भी हो सकता है।

अस्वीकरण।
इस गाइड की विषय-वस्तु एक आम प्रकृति की है और इसे कानूनी सलाह के तौर पर नहीं लिया जाना चाहिए या किसी ख़ास हालात या आपातकालीन स्थिति में मदद हेतु इस पर निर्भर नहीं होना चाहिए। किसी भी तरह के जरूरी मामले में, आपको अपने हालातों को लेकर उचित स्वतंत्र पेशेवर से सुझाव लेना चाहिए।

इस गाइड में दी गई जानकारी पर निर्भरता से होने वाली किसी भी क्षति, नुकसान या खर्च के लिए राष्ट्रमंडल कोई जिम्मेदारी या दायित्व स्वीकार नहीं करता है।

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