Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

छोटे व्यवसाय साइबर सिक्योरिटी संदर्शिका

सामग्री जटिलता
सरल ●○○

cyber.gov.au

परिचय

किसी छोटे व्यवसाय के लिए एक मामूली-सी साइबर सिक्योरिटी दुर्घटना का भी विनाशकारी प्रभाव हो सकता है। इस संदर्शिका में साइबर सिक्योरिटी के सामान्य खतरों से आपके व्यवसाय के संरक्षण में सहायता के लिए बुनियादी सुरक्षा दिशानिर्देश शामिल हैं।
आरंभ करने के लिए हम निम्नलिखित तीन दिशानिर्देशों की सलाह देते हैं:

- मल्टी-फैक्टर ऑथेन्टिकेशन लागू करें
- अपने सॉफ्टवेयर को अपडेट करें
- अपनी जानकारी को बैकअप करें

इस मार्गदर्शिका में ऐसे दिशानिर्देश भी शामिल हो सकते हैं जो आपके व्यवसाय के लिए प्रासंगिक नहीं हैं, या आपके व्यवसाय की आवश्यकताएँ अधिक जटिल हो सकती हैं। हम छोटे व्यवसायों के लिए यह सलाह देते हैं कि इस संदर्शिका को पूरा करने के बाद वे एसेंशियल एट में से मैच्योरिटी लेवल एक लागू करें। यदि आपके पास इस सलाह या साइबर सिक्योरिटी के बारे में और अधिक व्यापक प्रश्न हैं, तो हम आपको किसी आईटी पेशेवर या विश्वसनीय सलाहकार से बात करने की सलाह देते हैं।

हमारी संपूर्ण मार्गदर्शिका पढ़ने के लिए वेबसाइट **cyber.gov.au** पर जाएँ, जिसमें प्रत्येक दिशानिर्देश के लिए कैसे-करें सलाह शामिल है।

सामग्री तालिका

छोटे व्यवसायों के लिए खतरे

स्कैम मैसेजेस

घोटाले एक सामान्य तरीका है, जिनके माध्यम से साइबर अपराधी छोटे व्यवसायों को लक्षित करते हैं। उनका लक्ष्य आपको या आपके कर्मचारियों को इन बातों के लिए धोखा देना है:

- पैसे या गिफ्ट कार्ड्स भेजना
- मैलिशियस लिंक्स या एटैचमेंट्स पर क्लिक करना
- संवेदनशील जानकारी, जैसे पासवर्ड्स देना।

साइबर अपराधी ईमेल, टेक्स्ट मैसेजेस, फोन कॉल्स और सोशल मीडिया के माध्यम से आपके व्यवसाय को धोखा देने की कोशिश कर सकते हैं। वे अक्सर आपके किसी भरोसेमंद व्यक्ति या संगठन होने का ढोंग करेंगे।

फ़िशिंग अटैक्स

छोटे व्यवसायों के लिए विशेष चिंता का विषय **फ़िशिंग अटैक्स** हैं। इन घोटालों में अक्सर नकली वेबसाइट का लिंक होता है, जिसमें आपको किसी खाते में लॉग इन करने या गोपनीय विवरण एंटर करने के लिए प्रोत्साहित किया जाता है।

आमतौर पर फ़िशिंग अटैक्स में आपके खाते के पासवर्ड्स लेने की कोशिश की जाती है। साइबर अपराधी इस तरीके का उपयोग अक्सर छोटे व्यवसायों के सोशल मीडिया खातों के "टेकओवर" और फिरौती के लिए करते हैं।

इसे कम करने के तरीके

यदि कोई मैसेज ज्ञात निकाय से आता है और संदिग्ध लगता है, तो सावधानी बरतें। मैसेज वैध है या नहीं, इसकी जांच करने के लिए अलग से उस व्यक्ति या व्यवसाय से संपर्क करें। वैध स्रोत के माध्यम से मिलने वाले संपर्क विवरण का उपयोग करें, उदाहरण के लिए व्यवसाय की आधिकारिक वेबसाइट पर जाकर, न कि संदिग्ध मैसेज में शामिल विवरण पर।

निम्नलिखित संसाधनों से घोटालों और फ़िशिंग अटैक्स की पहचान के बारे में और अधिक जानकारी प्राप्त करें:

- घोटालों की पहचान और रिपोर्ट करें
- फ़िशिंग स्कैम्स की पहचान करने का तरीका जानें
- सोशियली इंजीनियर्ड मैसेजेस की पहचान करना।

केस स्टडी:

कूरियर कंपनी के कर्मचारी को अपने एक कार्यकारी स्टाफ की ओर से एक ईमेल मिली, जिसमें उन्हें 6 x $500 मास्टरकार्ड प्रीपेड क्रेडिट कार्ड्स खरीदने के लिए कहा गया। कार्यकारी ने उन्हें इस बात को गोपनीय रखने के लिए कहा क्योंकि ये कार्ड्स स्टाफ सदस्यों के लिए गिफ्ट वाउचर्स होंगे। इन्हें खरीदने के बाद कर्मचारी को खरीद के प्रमाण के रूप में कार्ड्स के दोनों किनारों की तस्वीर खींचकर उस कार्यकारी को भेजने के लिए कहा गया था।

कर्मचारी निर्देश के अनुसार एक डाकघर में गई और उसने गिफ्ट कार्ड खरीदने के लिए अपने व्यक्तिगत क्रेडिट कार्ड का इस्तेमाल किया। उसने कार्यकारी की ईमेल का जवाब दिया और प्रमाण के रूप में गिफ्ट कार्ड्स की तस्वीरें भेजीं।

डाकघर से लौटने के बाद कर्मचारी ने कार्यकारी को वास्तविक कार्ड्स दिए – जिन्हें कार्ड्स के बारे में कोई जानकारी नहीं थी। समीक्षा करने पर पता चला कि **गिफ्ट कार्ड्स के बारे में सभी ईमेलें एक रैंडम ईमेल पते से आई थीं और वे कार्यकारी के वैध ईमेल खाते से नहीं थीं। यह एक घोटाला था।**

ईमेल अटैक्स

फ़िशिंग जैसे घोटालों के अलावा छोटे व्यवसायों के प्रति एक सामान्य ईमेल अटैक **बिज़नेस ईमेल कॉम्प्रोमाइज़** (बीईसी) होता है। कॉम्प्रोमाइज़ किए गए ईमेल खातों के उपयोग या अन्य माध्यमों से अपराधी बिज़नेस प्रतिनिधि होने का ढोंग कर सकते हैं – उदाहरण के लिए, वास्तविक व्यवसाय के जैसे लगने वाले डोमेन नेम का उपयोग करना। आमतौर पर इन अटैक्स का लक्ष्य जानकारी की चोरी के अलावा पीड़ितों को स्कैमर द्वारा संचालित बैंक खाते में पैसे भेजने के लिए धोखा देना होता है।

इसे कम करने के तरीके

ईमेल अटैक्स से सबसे अच्छा बचाव आपके कर्मचारियों के लिए प्रशिक्षण और जागरुकता है। यह सुनिश्चित करें कि आपके कर्मचारी ऐसी ईमेलों के प्रति हमेशा सावधानी बरतें, जिनमें निम्नलिखित शामिल होता है:

- भुगतान के निवेदन, खासकर जो तुरंत या ओवरड्यू होते हैं
- बैंक विवरणों में परिवर्तन
- ऐसा ईमेल पता जो बिल्कुल सही नहीं लगता है, जैसे सप्लायर कंपनी के नाम के साथ डोमेन नेम बिल्कुल सही तरीके से मेल नहीं खाता है।

ये अटैक्स विनाशकारी हो सकते हैं, किंतु इनसे बचाव के दिशानिर्देश आसान होते हैं और इनके लिए लगभग कुछ भी खर्चा नहीं आता है। **कर्मचारी को इस तरह की ईमेल मिलने पर इससे सबसे प्रभावी बचाव ईमेल भेजने वाले को कॉल करना होता है, ताकि इस बात की पुष्टि की जा सके कि ये वैध हैं।** आपको जो संपर्क विवरण भेजे गए हैं, उनका उपयोग न करें क्योंकि ये धोखाधड़ी हो सकती है। कर्मचारियों के लिए एक औपचारिक प्रक्रिया शुरू करें, जिसका पालन उन्हें भुगतान के निवेदन मिलने पर या बैंक विवरणों के बदलने पर करना होगा।

बीईसी घोटालों और ईमेल कॉम्प्रोमाइज़ के प्रति निम्नलिखित संसाधनों के माध्यम से अपने व्यवसाय की सुरक्षा करना सीखें:

- बिज़नेस ईमेल कॉम्प्रोमाइज़
- ईमेल धोखाधड़ी और कॉम्प्रोमाइज़ से अपने व्यवसाय का संरक्षण करें
- यदि आपके व्यवसाय को ईमेल धोखाधड़ी या कॉम्प्रोमाइज़ द्वारा लक्षित किया गया है, तो क्या करें।

केस स्टडी:

एक छोटे निर्माण व्यवसाय को अपने आपूर्तिकर्ता से एक ईमेल मिली जिसमें बताया गया था कि उन्होंने बैंक बदल दिया है। आपूर्तिकर्ता ने इन्वॉइस के भुगतानों के लिए नए खाते के विवरण दिए। ईमेल जायज़ लग रही थी, **इसलिए निर्माण व्यवसाय ने बैंक खाते के विवरण में परिवर्तन की पुष्टि करने के लिए आपूर्तिकर्ता को कॉल नहीं किया।**

व्यवसाय ने आपूर्तिकर्ता से प्राप्त हुई इन्वॉइस के लिए $70,000 से भी अधिक धनराशि का भुगतान किया। अगले दिन एक अन्य कर्मचारी ने उसी इन्वॉइस के लिए गलती से $70,000 से अधिक अतिरिक्त धनराशि का भुगतान कर दिया। कुल मिलाकर नए बैंक खाते में $150,000 से भी अधिक धनराशि का भुगतान कर दिया गया।

जब व्यवसाय ने अपने आपूर्तिकर्ता को यह पूछने के लिए फोन किया कि क्या वे दोहरा भुगतान वापस कर सकते हैं, तो आपूर्तिकर्ता ने बताया कि वे बैंकिंग विवरण गलत थे। तुरंत एक जांच शुरू की गई, और आपूर्तिकर्ता को पता चला कि उनके ईमेल खातों में से एक खाते की हैकिंग कर ली गई थी और धोखाधड़ी वाले बैंक खाते के विवरण भेजे जा रहे थे। **किसी भी धनराशि की वसूली नहीं हो पाई।**

मैलिशियस सॉफ्टवेयर

मैलवेयर नुकसान पहुंचाने के लिए डिज़ाइन किए गए मैलिशियस सॉफ्टवेयर के लिए एक व्यापक शब्द है, जैसे रैंसमवेयर, वायरस, स्पाइवेयर और ट्रोजन। मैलवेयर यह कर सकता है:

- आपके उपकरण में से फाइलों की चोरी करना या उसे लॉक करना
- आपके बैंक या क्रेडिट कार्ड नंबर की चोरी करना
- आपके यूज़रनेम और पासवर्ड की चोरी करना
- आपके कंप्यूटर पर नियंत्रण रखना या जासूसी करना।

मैलवेयर आपके उपकरण को ठीक से काम करने से रोक सकता है, आपकी फाइलों को डिलीट या करप्ट कर सकता है, या दूसरों को आपकी व्यक्तिगत या व्यवसाय-संबंधी जानकारी को एक्सेस करने की अनुमति दे सकता है। यदि आपका उपकरण मैलवेयर से संक्रमित है, तो आप अन्य अटैक्स की चपेट में आ सकते/ती हैं। मैलवेयर आपके नेटवर्क में शामिल अन्य उपकरणों में भी फैल सकता है।

आपका उपकरण कई तरीकों से मैलवेयर सेसंक्रमित हो सकता है, जिसमें शामिल हैं:

- मैलवेयर से संक्रमित वेबसाइटों पर जाना
- इंटरनेट से संक्रमित फाइलें या सॉफ्टवेयर डाउनलोड करना
- संक्रमित ईमेल अटैचमेंट्स खोलना।

रैंसमवेयर

रैंसमवेयर एक सामान्य और खतरनाक प्रकार का मैलवेयर होता है। यह आपकी फाइलों को लॉक या एन्क्रिप्ट कर देता है, ताकि आप उन्हें एक्सेस न कर सकें। फाइलों तक फिर से एक्सेस बहाल करने के लिए फिरौती मांगी जाती है, आमतौर पर क्रिप्टोकरेंसी के रूप में। जब तक फिरौती का भुगतान नहीं किया जाता है, तब तक साइबर अपराधी डेटा को ऑनलाइन प्रकाशित करने या बेचने की धमकी भी दे सकते हैं।

इसे कम करने के तरीके

एँटी-वायरस या सिक्योरिटी सॉफ्टवेयर आपको मैलवेयर से सुरक्षित रखने में सहायता कर सकते हैं, लेकिन कोई भी सॉफ्टवेयर 100% प्रभावी नहीं होता है। कर्मचारियों को ईमेलों, वेबसाइटों और फाइलों के डाउनलोड में सतर्क रहना चाहिए, और सुरक्षित रहने के लिए नियमित रूप से अपने उपकरणों को अपडेट करना चाहिए।

अपने व्यवसाय को रैंसमवेयर से सुरक्षित रखने के बारे में और अधिक जानकारी के लिए निम्नलिखित संसाधन देखें:

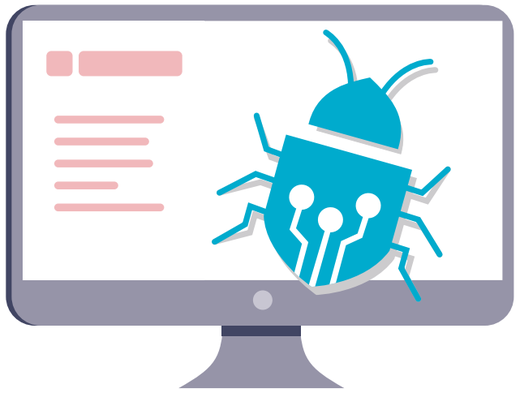
- रैंसमवेयर
- खुद को रैंसमवेयर अटैक्स से सुरक्षित रखें
- यदि आपसे फिरौती मांगी जाए, तो क्या करें।

केस स्टडी:

एक ऑटो पार्ट्स स्टोर के कर्मचारी सुबह काम पर आए और वे अपने सर्वर कंप्यूटर को बूट नहीं कर पाए। जब उनके आईटी प्रदाता को सर्वर की एक्सेस मिली, तो उन्हें एक खुली विंडो मिली जिसमें दिखाया गया था कि सभी कंप्यूटरों का डेटा एन्क्रिप्ट कर लिया गया है। नोट में उनसे फाइलों को अनलॉक करने के लिए बिटकॉइन में फिरौती का भुगतान करने की मांग की गई थी।

कंप्यूटर में एक बैकअप ड्राइव प्लगइन की गई थी, और उसे भी एन्क्रिप्ट कर लिया गया था। उन्होंने अन्य बैकअप ड्राइव्स कनेक्ट करने की कोशिश की, लेकिन कुछ ही सेकंडों में फाइलें स्वतः एन्क्रिप्ट हो गईं। **वे अपने डेटा को फिर से हासिल करने की कोशिश करने से पहले रैंसमवेयर को हटाने में असफल रहे थे और उनके पास पहले मौजूद हर एक बैकअप फाइल गुम हो गई।**

एकमात्र विकल्प बस यही था कि सर्वर को फैक्टरी रीसेट किया जाए और एक नए सिस्टम के साथ नए सिरे से शुरू किया जाए। उनके व्यवसाय का कई वर्षों का डेटा गुम हो गया और उन्हें नए सिरे से शुरू करना पड़ा।



अपने खातों को सुरक्षित रखें

मल्टी-फैक्टर ऑथेन्टिकेशन लागू करें

मल्टी-फैक्टर ऑथेन्टिकेशन (एमएफए) साइबर अपराधियों के लिए आपके खातों को एक्सेस करना कठिन बनाता है।

एमएफए आपके खाते में सुरक्षा की एक और पर्त जोड़ता है। यह आपके खातों को किसी व्यक्ति द्वारा एक्सेस किए जाने से संरक्षित रखने के सबसे प्रभावी तरीकों में से एक तरीका है, इसलिए जितना भी संभव हो सके आपको इसका उपयोग करना चाहिए। जो कोई भी आपके खाते में लॉग इन करता है, उसे आपके यूज़रनेम और पासवर्ड के अलावा कुछ और भी उपलब्ध कराना होगा। यह एक टेक्स्ट मैसेज या ऑथन्टिकेटर ऐप से एक यूनीक कोड हो सकता है। एमएफए के बारे में और अधिक जानकारी के लिए हमारी सलाह पढ़ें, जो वेबसाइट **cyber.gov.au/mfa** पर उपलब्ध है।

✓ **अपने सबसे महत्वपूर्ण खातों से शुरू करके जहाँ भी संभव हो, एमएफए लागू करें।**

एक्सेस कंट्रोल्स लागू करें

उपयोगकर्ता की एक्सेस को प्रतिबंधित करने से साइबर सिक्योरिटी घटना से होने वाले नुकसान को सीमित किया जा सकता है।

एक्सेस कंट्रोल कुछ फाइलों और सिस्टम्स की एक्सेस को सीमित करने का एक तरीका है। आमतौर पर किसी व्यवसाय में कर्मचारियों को सभी डेटा, खातों और सिस्टम्स की संपूर्ण एक्सेस की आवश्यकता नहीं होती है। उन्हें केवल वही एक्सेस मिलने की अनुमति दी जानी चाहिए, जिसकी आवश्यकता उन्हें अपने कर्तव्यों का पालन करने के लिए होती है।

एक्सेस को प्रतिबंधित करने से साइबर सिक्योरिटी घटना से होने वाले नुकसान को सीमित करने में सहायता मिलेगी। उदाहरण के लिए, यदि किसी स्टाफ सदस्य का कंप्यूटर रैंसमवेयर से संक्रमित है, तो उचित एक्सेस नियंत्रण के माध्यम से पूरे व्यवसाय के बजाय केवल कुछ ही फाइलें प्रभावित हो सकती हैं।

✓ **यह सुनिश्चित करें कि हर एक उपयोगकर्ता केवल अपनी भूमिका के लिए आवश्यक जानकारी ही एक्सेस कर पाए।**

मजबूत पासवर्ड्स या पासफ्रेज़ेस का उपयोग करें

सुरक्षित पासवर्ड या पासफ्रेज़ के माध्यम से साइबर अपराधियों से अपने खातों का संरक्षण करें।

कई छोटे व्यवसायों को बुरे पासवर्ड व्यवहार के परिणामस्वरूप साइबर अटैक्स का सामना करना पड़ता है। उदाहरण के लिए, एक से अधिक खातों के लिए एक ही पासवर्ड का दोबारा उपयोग करना। आप मजबूत पासवर्ड बनाने के लिए पासवर्ड मैनेजर और पासफ्रेज़, इन दोनों का उपयोग कर सकते/ती हैं।

पासवर्ड मैनेजर आपके पासवर्ड के लिए वर्चुअल सेफ की तरह कार्य करता है। आप अपने हर एक खाते के लिए मजबूत, **यूनीक** पासवर्ड बनाने और सेव करने के लिए इसका इस्तेमाल कर सकते/ती हैं। यदि आपके पास बहुत सारे खाते हैं, तो इससे यूनीक पासवर्ड्स याद रखने का बोझ दूर हो जाता है। आपको पासवर्ड्स या उनसे संबंधित खातों को याद रखने की आवश्यकता नहीं होती है, क्योंकि ये सभी आपके पासवर्ड मैनेजर में रिकॉर्ड किए गए रहते हैं।

आप जिन खातों में नियमित रूप से साइन इन करते/ती हैं, या आप जिन्हें अन्यथा पासवर्ड मैनेजर में सेव नहीं करना चाहते/ती हैं, उन खातों के लिए अपने पासवर्ड के रूप में एक पासफ्रेज़ का उपयोग करने पर विचार करें। पासफ्रेज़ेस रैंडम शब्दों का संयोजन होते हैं, उदाहरण के लिए 'क्रिस्टल ऑनियन क्ले प्रेट्ज़ेल'। जब आप याद रखने में आसान सुरक्षित पासवर्ड चाहते/ती हैं, तो ये उपयोगी रहते हैं। चार या इससे अधिक शब्दों के रैंडम संयोजन का उपयोग करें और इसे यूनीक रखें - **एक से अधिक खातों में पासफ्रेज़** का दोबारा उपयोग न करें। और अधिक जानकारी के लिए हमारी पासफ्रेज़ेस और पासवर्ड मैनेजरों के बारे में सलाह पढ़ें, जो वेबसाइट **cyber.gov.au/passphrases** पर उपलब्ध है।

✓ **अपने प्रत्येक महत्वपूर्ण खाते के लिए यूनीक पासवर्ड बनाने और सेव करने के लिए पासवर्ड मैनेजर का उपयोग करें।**

साझा खातों का प्रबंधन करें

खातों को साझा करने से सुरक्षा में कॉम्प्रोमाइज़ हो सकता है और मैलिशियस गतिविधि को ट्रैक करना कठिन हो जाता है।

किसी छोटे व्यवसाय में कर्मचारियों के लिए खातों को साझा करने के वैध कारण हो सकते हैं, लेकिन इससे यथासंभव बचना चाहिए। जब कई कर्मचारी एक ही खाते का उपयोग करते हैं, तो गतिविधि को किसी विशिष्ट कर्मचारी तक वापस ट्रैक करना कठिन हो सकता है और साइबर अपराधियों को ट्रैक करना भी कठिन हो सकता है। यदि आप पासवर्ड नहीं बदलते/ती हैं, तो कर्मचारी व्यवसाय छोड़ने के बाद भी खातों को एक्सेस करना जारी रख सकते हैं।

✓ **साझा किए जाने वाले खातों के उपयोग को सीमित करें और अपने व्यवसाय में उपयोग किए जाने वाले सभी खातों को सुरक्षित रखें।**

अपने उपकरणों और जानकारी को सुरक्षित रखें

अपने सॉफ्टवेयर को अपडेट करें

अपने व्यवसाय को साइबर अटैक्स से बचाने के बेहतरीन तरीकों में से एक तरीका अपने सॉफ्टवेयर को अप-टु-डेट रखना है।

आपके ऑपरेटिंग सिस्टम और अन्य सॉफ्टवेयर में सुरक्षा खामियाँ अपडेट्स से ठीक हो सकती हैं, ताकि साइबर अपराधी के लिए सेंध लगाना कठिन हो जाए। हर समय नई खामियाँ सामने आती रहती हैं, इसलिए अपडेट के प्रॉम्प्ट्स को अनदेखा न करें। नियमित रूप से अपने सॉफ्टवेयर को अपडेट करने से इस बात की संभावना कम हो जाएगी कि साइबर अपराधी किसी ज्ञात खामी का उपयोग करके मैलवेयर को रन कर सके या आपके उपकरण को हैक कर सके। यदि आपको सहायता की आवश्यकता है, तो एसीएससी ने अपडेट्स के बारे में दिशानिर्देश प्रकाशित किए हैं।

यदि आपका उपकरण या सॉफ्टवेयर बहुत पुराना है, तो हो सकता है कि अपडेट्स उपलब्ध न हों। यदि निर्माता ने उत्पाद के लिए अपडेट्स का सपोर्ट बंद कर दिया है, तो आपको सुरक्षित रहने के लिए नए उत्पाद में अपग्रेड करने पर विचार करना चाहिए। जिन सिस्टम्स के लिए अब मेजर अपडेट्स प्राप्त नहीं होते हैं, उनके उदाहरण हैं - **आईफोन 7** और **माइक्रोसॉफ्ट विंडोज़ 7**।

और अधिक जानकारी के लिए वेबसाइट **cyber.gov.au/updates** पर उपलब्ध अपडेट्स के बारे में हमारा मार्गदर्शन पढ़ें।

✓ **अपने उपकरण और सॉफ्टवेयर के लिए स्वचालित अपडेट लागू करें।**

सिक्योरिटी सॉफ्टवेयर का उपयोग करें

एँटीवायरस और रैंसमवेयर प्रोटेक्शन जैसे सिक्योरिटी सॉफ्टवेयर आपके उपकरणों की सुरक्षा में सहायता कर सकते हैं।

अपने उपकरणों में मैलवेयर का पता लगाने और इन्हें डिलीट करने के लिए सिक्योरिटी सॉफ्टवेयर का उपयोग करें। संदिग्ध फाइलों और प्रोग्रामों के लिए नियमित रूप से स्कैन करने के उद्देश्य से एँटीवायरस सॉफ्टवेयर की सेटिंग की जा सकती है। जब कोई खतरा पाया जाता है, तो आपको एक एलर्ट प्राप्त होगा और संदिग्ध फाइल को क्वारंटीन कर दिया जाएगा या हटा दिया जाएगा।

छोटे आकार के व्यवसाय खुद को वायरस और मैलवेयर से बचाने के लिए **विंडोज़ सिक्योरिटी का उपयोग** कर सकते हैं। विंडोज़ 10 और विंडोज़ 11 उपकरणों में विंडोज़ सिक्योरिटी अंतर्निहित है और इसमें वायरस व खतरों से नि:शुल्क सुरक्षा शामिल है। आप अपने उपकरण पर रैंसमवेयर सुरक्षा फीचर्स को लागू करने के लिए भी इसका उपयोग कर सकते/ती हैं।

वैकल्पिक उत्पादों और विकल्पों के लिए वेबसाइट cyber.gov.au पर एँटीवायरस सर्च करके एँटीवायरस सॉफ्टवेयर के बारे में हमारी सलाह पढ़ें।

✓ **नियमित रूप से अपने उपकरणों में स्कैन पूरा करने के लिए सिक्योरिटी सॉफ्टवेयर को सेट करें।**

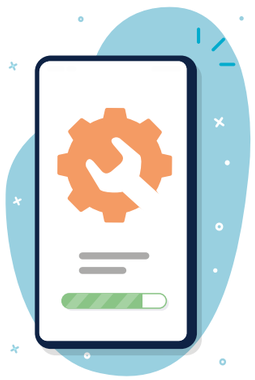
अपनी जानकारी को बैकअप करें

यदि आपकी जानकारी गुम हो जाती है या उसे कॉम्प्रोमाइज़ कर लिया जाता है, तो नियमित रूप से बैकअप करने से आपको जानकारी दोबारा प्राप्त करने में सहायता मिल सकती है।

महत्वपूर्ण जानकारी का बैकअप लेना आपके व्यवसाय में एक नियमित या स्वचालित अभ्यास होना चाहिए। नियमित बैकअप के बिना साइबर अटैक्स के बाद अपनी जानकारी को दोबारा प्राप्त कर पाना आपके लिए असंभव हो सकता है।

ऐसे कई तरीके और उत्पाद उपलब्ध हैं, जिन्हें आप अपनी जानकारी के बैकअप के लिए इस्तेमाल कर सकते/ती हैं। अपने व्यवसाय का बैकअप लेने के बारे में विस्तृत सलाह के लिए वेबसाइट **cyber.gov.au/backups** पर उपलब्ध बैकअप्स के लिए हमारी सलाह पढ़ें। हर एक व्यवसाय के लिए सबसे अच्छा विकल्प अलग-अलग होगा, इसलिए यदि आप अनिश्चित हैं तो किसी आईटी पेशेवर से बात करें।

✓ **अपनी जानकारी को नियमित रूप से बैकअप करने की एक योजना बनाएँ और इसे लागू करें।**



अपने नेटवर्क और बाहरी सेवाओं को संरक्षित करें

अपने नेटवर्क में संभावित खामियों को संबोधित करके अपने व्यवसाय को साइबर अटैक्स से सुरक्षित रखें।

साइबर अपराधियों के लिए आपके नेटवर्क में उपकरण और सेवाएँ मुख्य लक्ष्य हो सकती हैं। इनमें से कई सिस्टम्स का संरक्षण करना जटिल हो सकता है, इसलिए निम्नलिखित सिफारिशों के बारे में किसी आईटी पेशेवर के साथ चर्चा करें।

- **अपने सर्वर को संरक्षित करें**: यदि आप अपने घर या व्यवसाय में एनएएस या किसी अन्य सर्वर का उपयोग करते/ती हैं, तो इन्हें संरक्षित करने के लिए अतिरिक्त सावधानी बरतें। ये उपकरण साइबर अपराधियों के लिए आम लक्ष्य होते हैं, क्योंकि अक्सर इनमें महत्वपूर्ण फाइलें स्टोर की गई होती हैं या ये महत्वपूर्ण कार्य करते हैं। इन उपकरणों के संरक्षण के लिए अटैक्स को कम करने की कई कार्यनीतियों की आवश्यकता होती है। उदाहरण के लिए, यह सुनिश्चित करना महत्वपूर्ण होता है कि किसी भी सर्वर या एनएएस उपकरण को नियमित रूप से अपडेट किया जाए। एडमिनिस्ट्रेटिव खातों को मजबूत पासफ्रेज़ या मल्टी-फैक्टर ऑथेन्टिकेशन के माध्यम से संरक्षित किया जाना चाहिए।
- **बाहरी-फेसिंग फुटप्रिंट को कम से कम करें**: अपने नेटवर्क में इंटरनेट पर प्रकट होने वाली किसी भी सेवा का ऑडिट और संरक्षण करें। इसमें रिमोट डेस्कटॉप, फाइल शेयर्स, वेबमेल और रिमोट एडमिनिस्ट्रेशन सेवाएँ शामिल हो सकती हैं।
- **क्लाउड सेवाओं में माइग्रेट करें:** ऑनलाइन या क्लाउड सेवाओं का उपयोग करने पर विचार करें, जिनमें खुद सिक्योरिटी का प्रबंधन करने के बजाय अंतर्निहित संरक्षण उपलब्ध होता है। उदाहरण के लिए, इन सेवाओं को खुद से रन और संरक्षित करने के बजाय ईमेल या वेबसाइट होस्टिंग जैसी चीजों के लिए ऑनलाइन सेवाओं का उपयोग करें।
- **अपने राउटर की सिक्योरिटी बढ़ाएँ:** अपने राउटर को संरक्षित करने के तरीकों पर हमारे मार्गदर्शन का पालन करें, जिसमें डिफ़ॉल्ट पासवर्ड्स को अपडेट करना, सेवार्थियों या विज़िटर्स के लिए "गेस्ट" वाई-फाई लागू करना और सबसे मजबूत एन्क्रिप्शन प्रोटोकॉलों का उपयोग करना शामिल है। और अधिक जानकारी के लिए वेबसाइट **cyber.gov.au** पर राउटर के लिए सर्च करें।
- **अपनी साइबर सप्लाई चेन को समझें:** आधुनिक व्यवसाय अक्सर कई सेवाओं की आउटसोर्सिंग करते हैं। उदाहरण के लिए, अपने आईटी के रख-रखाव के लिए मैनेज्ड सर्विस प्रोवाइडर का उपयोग करना। इन सेवाओं या प्रोवाइडर्स के साथ सुरक्षा-संबंधी समस्याएँ आपके व्यवसाय पर गंभीर प्रभाव डाल सकती हैं। साइबर सप्लाई चेन खतरा प्रबंधन के बारे में विस्तृत सलाह के लिए वेबसाइट **cyber.gov.au** पर हमारा साइबर सप्लाई चेन मार्गदर्शन पढ़ें।

✓ **अपने नेटवर्क को संरक्षित करने के तरीकों के बारे में किसी आईटी पेशेवर से बात करें।**

अपनी वेबसाइट को मजबूत बनाएँ

वेबसाइटें साइबर अटैक्स के लिए मुख्य लक्ष्य होती हैं।

कुछ बुनियादी सिक्योरिटी दिशानिर्देशों का पालन करके अपनी वेबसाइट को हाइजैक किए जाने से बचाएँ:

- अपने वेबसाइट लॉगिन को मल्टी-फैक्टर ऑथेन्टिकेशन या मजबूत पासवर्ड के साथ संरक्षित करें
- अपनी वेबसाइट के कंटेन्ट मैनेजमेंट सिस्टम्स और प्लगइन्स को नियमित रूप से अपडेट करें
- अपनी वेबसाइट को नियमित रूप से बैकअप करें, ताकि साइबर अटैक्स के बाद आप इसे रिस्टोर कर सकें।

एसीएससी के पास वेबसाइट मालकों के लिए अतिरिक्त संसाधन उपलब्ध हैं। वेबसाइट **cyber.gov.au** पर इन संसाधनों के लिए सर्च करें:

- Quick Wins for your Website
- Implementing Certificates, TLS, HTTPS and Opportunistic TLS
- Domain Name System Security for Domain Owners
- Preparing for and Responding to Denial-of-Service Attacks

✓ **वेबसाइट सिक्योरिटी के बारे में एसीएससी के संसाधन पढ़ें।**

अपने उपकरणों की बिक्री या निपटान करने से पहले उन्हें रीसेट करें

आपके पुराने उपकरणों पर डेटा को अजनबियों द्वारा एक्सेस किया जा सकता है।

यदि आप अपने उपकरणों का निपटान सुरक्षित रूप से नहीं करते/ती हैं, तो साइबर अपराधी उपकरण में मौजूद जानकारी को एक्सेस सकते हैं। इसमें इमेलें, फाइलें और अन्य व्यवसाय-संबंधी डेटा शामिल हो सकता है। अपने व्यवसाय-संबंधी उपकरणों को बेचने, अदला-बदली करने या फेंकने से पहले उनमें से सभी जानकारी को हटा दें। उदाहरण के लिए, फैक्टरी रीसेट करके। इससे सभी जानकारी को हटाने और उपकरण को उसकी मूल सेटिंग्स में रिस्टोर करने में सहायता मिलेगी।

अपने उपकरण को रीसेट करने के बारे में सलाह के लिए हमारा मार्गदर्शन पढ़ें: अपने उपकरण का सुरक्षित रूप से निपटान कैसे करें। वेबसाइट **cyber.gov.au** पर डिस्पोज़ की सर्च करें।

✓ **व्यवसाय-संबंधी उपकरणों की बिक्री या निपटान करने से पहले उन्हें फैक्टरी रीसेट करें।**

अपने उपकरणों को लॉक करके सुरक्षित रखें

अपने व्यवसाय-संबंधी उपकरणों तक भौतिक एक्सेस को बाधित करने से मैलिशियस गतिविधि के अवसर कम हो जाएँगे।

डेटा की चोरी या अन्य मैलिशियस गतिविधि को रोकने का एक आसान तरीका यह है कि अपने व्यवसाय-संबंधी उपकरणों तक भौतिक एक्सेस को सीमित किया जाए। व्यवसाय-संबंधी उपकरणों को वहाँ नहीं रखा जाना चाहिए, जहाँ अनधिकृत कर्मचारी या आम लोग उन्हें एक्सेस कर सकें।

अपने व्यवसाय-संबंधी उपकरणों को और भी अधिक सुरक्षित बनाने के लिए सिक्योरिटी कंट्रोल्स का उपयोग करें। न्यूनतम रूप से उन्हें पासफ्रेज़, पिन या बायोमेट्रिक्स के साथ लॉक किया जाना चाहिए। इस्तेमाल न करने की छोटी अवधि के बाद इन्हें स्वत: लॉक हो जाने के लिए सेट करना सुनिश्चित करें।

✓ **उपकरणों को इस्तेमाल न करने की छोटी अवधि के बाद स्वत: लॉक हो जाने के लिए कॉन्फिगर करें।**

अपने व्यवसाय-संबंधी डेटा को सुरक्षित रखें

साइबर अपराधियों के लिए आपके व्यवसाय के पास मौजूद डेटा आकर्षक लक्ष्य होता है।

डेटा ब्रीचेज़ बढ़ रहे हैं - अपने व्यवसाय को इनका शिकार न बनने दें। यह समझना महत्वपूर्ण है कि आपके व्यवसाय में कौन सा डेटा किन स्थानों पर मौजूद है। एक बार जागरुक हो जाने के बाद अपने डेटा को साइबर अपराधियों द्वारा एक्सेस किए जाने से सुरक्षित रखने में सहायता के लिए इस संदर्शिका में दी गई सलाह का उपयोग करें। कुछ छोटे व्यवसायों के लिए कानून के तहत अतिरिक्त दायित्व भी हो सकते हैं।

- **अपने व्यवसाय-संबंधी डेटा को समेकित करें।** आपके पास कई उपकरणों या सेवाओं में डेटा संग्रहीत हो सकता है। डेटा के विकेंद्रित होने पर उन सिस्टम्स की संख्या बढ़ जाती है, जिनका आपको संरक्षण और बैकअप करना होता है। बहुत सारे सिस्टम्स होने से साइबर अपराधी के अटैक्स के लिए अधिक अवसर भी पैदा हो सकते हैं। जहाँ तक संभव हो, अपने व्यवसाय के डेटा को ऐसे केंद्रीय स्थान पर संग्रहीत करें, जो सुरक्षित है और जिसका नियमित रूप से बैकअप लिया जाता है। आपके डेटा के केंद्रित होने से आपके सिस्टम्स के कॉम्प्रोमाइज़ होने की स्थिति में काफी बड़ा ब्रीच पैदा हो सकता है, इसलिए यह सुनिश्चित करें कि यह केंद्रीय स्थान सुरक्षित कॉन्फिगरेशन और प्रतिबंधित एक्सेस के साथ पर्याप्त रूप से संरक्षित है। सलाह के लिए किसी आईटी या साइबर सिक्योरिटी पेशेवर से बात करें।
- **डेटा की सुरक्षा के लिए अपने दायित्वों से अवगत रहें।** कुछ छोटे व्यवसायों के लिए उनके द्वारा एकत्र की जाने वाली व्यक्तिगत जानकारी के साथ व्यवहार करने के संबंध में कानूनी दायित्व हो सकते हैं। और अधिक जानकारी के लिए ऑस्ट्रेलियाई सूचना आयुक्त कार्यालय (Office of the Australian Information Commissioner) की छोटे व्यवसायों के लिए मार्गदर्शिका पढ़ें, जो वेबसाइट **oaic.gov.au** पर उपलब्ध है। यदि आप अनिश्चित हैं, तो किसी कानूनी पेशेवर से परामर्श करें।

✓ **अपने व्यवसाय के डेटा और इसके संरक्षण के संबंध में अपनी जिम्मेदारियों को समझें।**

अपने कर्मचारियों को तैयार करें

कर्मचारियों को शिक्षित करें

साइबर अटैक्स के प्रति आपकी पहली सुरक्षा रेखा अच्छी साइबर सिक्योरिटी कार्यप्रथाओं का पालन करने वाले कर्मचारी होते हैं।

आपके कर्मचारियों को साइबर सिक्योरिटी के बारे में जागरुक होना चाहिए, जिसमें निम्नलिखित विषय शामिल हैं:

- साइबर सिक्योरिटी के लिए सामान्य खतरे, जैसे बिज़नेस ईमेल कॉम्प्रोमाइज़ और रैंसमवेयर
- संरक्षणात्मक कदम, जिसमें मज़बूत पासवर्ड्स या पासफ्रेज़ेस, एमएफए और सॉफ्टवेयर अपडेट्स शामिल हैं
- घोटालों और फ़िशिंग अटैक्स की पहचान कैसे करें
- व्यवसाय विशिष्ट नीतियाँ (उदाहरण के लिए, संदिग्ध ईमेलों की रिपोर्ट करने या भुगतान करने से पहले इन्वॉइसों का सत्यापन करने की प्रक्रियाएँ)
- आपातकाल में क्या करना है?

एसीएससी वेबसाइट cyber.gov.au/learn पर इनमें से अधिकांश विषयों के बारे में संसाधन उपलब्ध हैं। आप अपने कर्मचारियों को शिक्षित करने के लिए अन्य तरीकों पर विचार कर सकते/ती हैं, उदाहरण के लिए औपचारिक कोर्स या आंतरिक प्रशिक्षण के माध्यम से। आप जो भी निर्णय लें, यह याद रखें कि साइबर सिक्योरिटी प्रशिक्षण एकबारगी आवश्यकता नहीं होती है और इसे समय-समय पर रिफ्रेश किया जाना चाहिए।

✓ **यह तय करें कि आपके व्यवसाय में साइबर सिक्योरिटी जागरुकता को कैसे सिखाया जाएगा।**

एक आपात योजना बनाएँ

आपात योजना आपके व्यवसाय पर साइबर अटैक्स के प्रभाव को कम कर सकती है।

साइबर सिक्योरिटी घटना का जवाब देते समय हर एक मिनट महत्वपूर्ण होता है। आपात योजना होने का अर्थ है कि आपके स्टाफ को यह पता लगाने में कम समय लग सकता है कि क्या करना है, और वे कार्यवाही करने में अधिक समय बिता सकते हैं।

अपनी आपात योजना बनाते समय निम्नलिखित प्रश्नों पर विचार करें:

- आपके कर्मचारियों के लिए संभावित साइबर सिक्योरिटी घटनाओं की रिपोर्ट करने की प्रक्रिया क्या है?
- आपको सहायता के लिए किससे संपर्क करना चाहिए? उदाहरण के लिए, आईटी पेशेवर और आपका बैंक।
- आपके कर्मचारियों, हितधारकों या सेवार्थियों को घटना के बारे में कैसे सूचित किया जाएगा?
- यदि कोई महत्वपूर्ण सिस्टम्स ऑफलाइन हैं, तो आप सामान्य रूप से व्यवसाय का प्रबंधन कैसे करेंगे/गी?

यह सुनिश्चित करें कि आपके कर्मचारी आपात योजना से परिचित हैं, जिसमें उनकी कोई भी संभावित भूमिकाएँ या जिम्मेदारियाँ शामिल होनी चाहिए। योजना की एक हार्ड कॉपी बनाकर रखें, ताकि आवश्यकता पड़ने पर यदि आपके सिस्टम्स ऑफलाइन हों तो यह उपलब्ध रहे।

✓ **साइबर सिक्योरिटी घटनाओं के लिए एक आपात योजना बनाएँ।**

जानकारी से अवगत रहें

एसीएससी से नवीनतम जानकारी प्राप्त करने के लिए एसीएससी पार्टनर बनें।

एसीएससी पार्टनर बनकर सबसे हाल के साइबर खतरों और खामियों के बारे में अवगत रहें। किसी नए साइबर खतरे की पहचान होने पर यह सेवा आपको मासिक न्यूज़लेटर्स और एलर्ट्स भेजेगी।

साइबर सिक्योरिटी तेजी से विकसित होने वाला क्षेत्र है। साइबर अपराधी खामियों की पहचान होने के कुछ मिनटों के अंदर ही सक्रियात्मक रूप से इनका फायदा उठाते हैं। साइबर सिक्योरिटी परिदृश्य के बारे में अवगत रहने से आपके व्यवसाय को संभावित रूप से सामने आने वाले खतरों, और उनसे सुरक्षा कैसे की जाए, इस बारे में समझने में सहायता मिलेगी।

✓ **अपने व्यवसाय को एसीएससी पार्टनरशिप प्रोग्राम (ACSC Partnership Program) के साथ रजिस्टर करें।**

अस्वीकरण

इस संदर्शिका में दी गई सामग्री सामान्य प्रकृति की है और इसे कानूनी सलाह के रूप में नहीं लिया जाना जाना चाहिए अथवा किसी विशेष परिस्थिति या आपात स्थिति में इसपर सहायता के लिए भरोसा नहीं किया जाना चाहिए। किसी भी महत्वपूर्ण मामले में आपको अपनी परिस्थितियों के संबंध में उपयुक्त स्वतंत्र पेशेवर सलाह लेनी चाहिए।

इस संदर्शिका में निहित जानकारी पर निर्भरता के परिणामस्वरूप किसी भी क्षति, हानि या खर्चे के लिए राष्ट्रमंडल कोई भी जिम्मेदारी या दायित्व को स्वीकार नहीं करता है।

और अधिक जानकारी या किसी साइबर सिक्योरिटी 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