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

साइन अप करें

हमारी मुफ़्त अलर्ट सेवा के लिए

cyber.gov.au

रिपोर्ट

REPORTCYBER के लिए साइबर अपराध:

cyber.gov.au/report

संपर्क

1300 CYBER1 पर कॉल करें या

cyber.gov.au पर जाएं

यह नंबर के वल ऑस्ट्रेलिया में उपयोग के लिए उपलब्ध है।

हमें फॉलो करें

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. स्कैमों से सावधान रहें

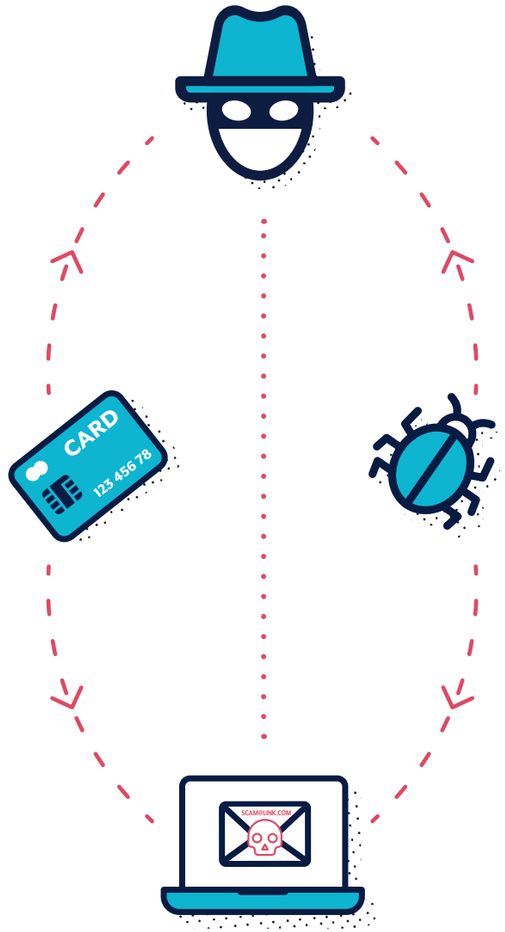
साइबर अपराधी ईमेल, एसएमएस, फोन कॉल और सोशल मीडिया का उपयोग आपको एक संलग्नक खोलने, वेबसाइट पर जाने, अकाउंट लॉगिन विवरण प्रकट करने, संवेदनशील जानकारी प्रकट करने या पैसे या उपहार कार्ड स्थानांतरित करने के लिए करते हैं। इन संदेशों को ऐसा प्रकट करने के लिए बनाया गया है जैसे कि वे उन व्यक्तियों या संगठनों से भेजे गए हैं जिन्हें आप जानते हैं, या आपको लगता है कि आपको भरोसा करना चाहिए।

स्कैम संदेशों का पता लगाने के लिए, रुकें और सोचें:

- **अथॉरिटी:** क्या यह संदेश किसी अधिकारी के होने का दावा कर रहा है?
- **अति-आवश्यकता:** क्या आप से कहा गया है कि प्रतिक्रिया देने के लिए आपके पास सीमित समय है?
- **भावना:** क्या यह संदेश आपको आकस्तिमक भय वाला, भयभीत, आशावान या जिज्ञासु बनाता है?
- **अभाव:** क्या संदेश न्यून आपूर्ति में कुछ दे रहा है?
- **वर्तमान घटनाएं:** क्या यह संदेश वर्तमान समाचारों, बड़ी घटनाओं या वर्ष के विशिष्ट समय (जैसे कर रिपोर्टिंग) से संबंधित है?

यह जांचने के लिए कि कोई संदेश वैध है:

- किसी ऐसी चीज़ पर वापस जाएं जिस पर आप भरोसा कर सकते हैं। आधिकारिक वेबसाइट पर जाएं, अपने खाते में लॉग इन करें, या उनके विज्ञापित फोन नंबर पर फोन करें। आपको भेजे गए या फोन पर दिए गए संदेश में लिंक या संपर्क विवरण का उपयोग न करें।
- यह देखने के लिए जांचें कि क्या आधिकारिक स्रोत ने आपको पहले ही बता दिया है कि वे आपसे कभी क्या नहीं पूछेंगे। उदाहरण के लिए, आपके बैंक ने आपसे कहा होगा कि वे आपका पासवर्ड कभी नहीं मांगेंगे।



स्कैम संदेशों का पता लगाने के बारे में अधिक जानकारी के लिए, ऑस्ट्रेलियाई साइबर सुरक्षा केंद्र (ACSC) का सामाजिक इंजीनियर संदेश प्रकाशन को देखें, और **cyber.gov.au** पर ACSC की अलर्ट सेवा को साइन अप करके सूचित रहें।

आसान चरण

अपने डिवाइस और खातों को सुरक्षित करने के लिए

इन चरणों का पालन करके साइबर अपराधियों द्वारा लक्षित होने के जोखिम को कम करें

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. अपने डिवाइसेस को अपडेट करें

साइबर अपराधी सिस्टम या ऐप्स में ज्ञात कमजोरियों का उपयोग करके डिवाइस को हैक करते हैं। इन कमजोरियों को ठीक करने के लिए अपडेट में सुरक्षा अपग्रेड होते हैं। स्वचालित अपडेट चालू करें ताकि यह आपके इनपुट के बिना हो।

अपने सभी डिवाइसेस पर ऑटोमेटिक अपडेट ऑन करें:

- मोबाइल फोन
- लैपटॉप
- डेस्कटॉप

अपने अपडेट को नियमित रूप से जांच करें:

- एप्स
- प्रोग्राम्स
- स्मार्ट डिवाइसेस

2. मल्टी-फैक्टर ऑथेंटिकेशन ऑन करें

MFA साइबर अपराधियों के लिए आपकी फाइलों या खाते तक पहुंच में बाधा को बढ़ाकर आपकी सुरक्षा में सुधार करता है।

अपने सबसे महत्वपूर्ण खातों से शुरू करते हुए, MFA सक्रिय करें:

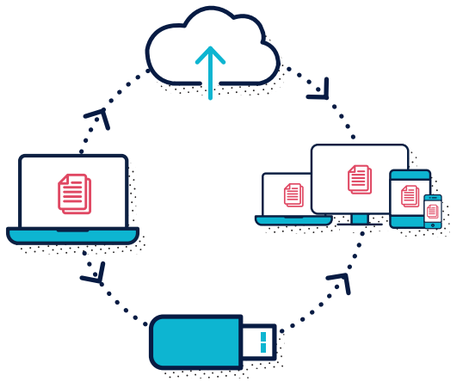
- ईमेल अकाउंटस
- ऑनलाइन बैंकिंग और संग्रहीत खाते भुगतान विवरण
- सोशल मीडिया

3. अपने डिवाइस का बैकअप लें

बैकअप आपके डिवाइस पर संग्रहीत जानकारी की एक डिजिटल प्रति है, जैसे कि फ़ोटो, दस्तावेज़, वीडियो और एप्लिकेशन का डेटा। इसे बाह्य संग्रहण डिवाइस या क्लाउड में सहेजा जा सकता है। बैकअप लेने का अर्थ है कि यदि आपका डिवाइस कभी खो जाता है, चोरी हो जाता है, या क्षतिग्रस्त हो जाता है तो आप अपनी फ़ाइलों को रिस्टोर कर सकते हैं।

अपने डिवाइस का नियमित रूप से बैकअप लें

- मोबाइल फोन
- लैपटॉप
- डेस्कटॉप
- टेबलेट



4. सुरक्षित पासफ़्रेज़ सेट करें

ऐसे मामलों में जहां MFA उपलब्ध नहीं है, एक सशक्त पासफ़्रेज़ अक्सर आपकी जानकारी और खातों को अपराधियों से सुरक्षित रखने वाली एकमात्र वस्तु है।

पासफ़्रेज़ आपके पासवर्ड की तरह ही चार या उससे अधिक अनियमित शब्दों का उपयोग करता है। अपने पासवर्ड को पासफ़्रेज़ में बदलें और यह जाँच कर लें कि वह:

- लंबे हों: आपका पासफ़्रेज़ जितना लंबा होगा, उतना ही बेहतर होगा। इसे कम से कम 14 अक्षरों की लंबाई तक रखें
- अप्रत्याशित हों: असंबंधित शब्दों को अनियमित रूप से घुला-मिलाकर इस्तेमाल करें
- यूनिक हों: एक से अधिक अकाउंट में पासफ़्रेज़ का दोबारा इस्तेमाल न करें