National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

स्वयं को ऑनलाइन सुरक्षित रखना

साइबर (ऑनलाइन) सुरक्षा मेरे लिए क्यों महत्वपूर्ण है?

इंटरनेट और सोशल मीडिया अद्भुत प्लेटफॉर्म हैं जो हमें जानकारी साझा करने और मित्रों एवं परिवार के साथ संपर्क में रहने में मदद करते हैं।

हालाँकि, अपराधी और अन्य गैरकानूनी संगठन भी आपका पैसा, आपकी जानकारी प्राप्त करने या आपको डराने के लिए इनका उपयोग करते हैं।

वे दुनिया में कहीं से भी काम कर सकते हैं, अधिकांश भाषाओं को बहुत अच्छे से बोल सकते हैं और बहुत ही विश्वसनीय नकली वेबसाइट बना सकते हैं। वे ईमेल, सोशल मीडिया और टैक्स्ट मैसेज (संदेश) के जरिए आपसे संपर्क करेंगे और वे आपको डरा हुआ या चिंतित महसूस कराने की कोशिश करेंगे, ताकि आप स्पष्ट रूप से नहीं सोच पाएं।

इसका मतलब है कि आपको तैयार रहने और उनके द्वारा उपयोग की जाने वाली तरकीबों के बारे में हमेशा जागरूक रहने की आवश्यकता है।

मुझे ऑनलाइन किन सामान्य समस्याओं का सामना करना पड़ सकता है?

नीचे कुछ सबसे आम स्थितियाँ दी गई हैं जो हम देखते हैं।

- आपको एक संदिग्ध ईमेल या टैक्स्ट संदेश मिलता है जिसमें आपसे एक लिंक पर क्लिक करने के लिए कहा जाता है।
    - ये लिंक अक्सर आपको नकली वेबसाइटों पर ले जाते हैं जिन्हें आपके लॉगिन या आर्थिक ब्यौरा चुराने के लिए तैयार किया जाता है।
- आपको एक संदिग्ध फोन कॉल आती है जिसमें आपसे व्यक्तिगत जानकारी की मांग की जाती है।
    - जैसा कि ऊपर बताया गया है, फोन करने वाला आपके बैंक से होने का नाटक करेगा और आपसे जानकारी मांगेगा।
- आपको किसी ऐसे व्यक्ति से संदेश मिलता है जो प्राधिकरण का व्यक्ति होने का दिखावा करके आपसे कुछ करवाने की कोशिश करता है।
    - अक्सर यह व्यक्ति किसी प्रकार की धमकी देता है।
- कोई व्यक्ति आपके एक या अधिक ऑनलाइन खातों (उदाहरण के लिए: ईमेल या सोशल मीडिया) में प्रवेश कर जाता है।
    - यदि कोई व्यक्ति आपके ऑनलाइन खाते में प्रवेश कर जाता है, तो वे आपकी जानकारी चुरा सकते हैं, भुगतानों को रिडायरेक्ट कर (दूसरी जगह भेज) सकते हैं, और संभावित रूप से आपकी नकल करके आपके मित्रों या परिवार को निशाना बना सकते हैं।
- [इसमें] आपके क्रेडिट कार्ड के विवरण चुरा लिए जाते हैं, या फर्जी बिक्री या निवेश में आपसे पैसे ठग लिए जाते हैं।

- स्कैमर्स (घोटाला करने वाले या ठग) उम्मीद करते हैं कि आप एक अच्छा सौदा देखेंगे और बिना सोचे-समझे भुगतान करना चाहेंगे। या फिर शायद कोई वास्तविक वेबसाइट डेटा ब्रीच (उल्लंघन) में फंस गई हो और आपका डेटा (ब्यौरा) ऑनलाइन लीक हो गया हो।

यहाँ और भी सीनारियो (परिदृश्य) दिए गए हैं:
तुरंत सहायता प्राप्त करें - Own Your Online (ओन योर ऑनलाइन अर्थात अपना ऑनलाइन स्वामित्व बनाए रखें)

मैं ऑनलाइन सुरक्षित कैसे रह सकता/सकती हूँ?

- **लंबे और अनोखे पासवर्ड।**
  - पासवर्ड जितना लंबा होता है, वह उतना ही मजबूत होता है।
  - चार याद रखने योग्य शब्दों को एक साथ जोड़कर 16 से अधिक वर्णों का एक यादगार पासवर्ड बनाएं (उदाहरण के लिए: TriangleRhinoOperationShoes) और यदि आवश्यक हो तो संख्याएं, बड़े अक्षर और प्रतीकों को जोड़ें (उदाहरण के लिए: Triangle&"Rhino"Operation2Shoes)।
  - सबसे जरूरी बात, अपने पासवर्ड को दोहराएं नहीं। यदि किसी अपराधी को आपका पासवर्ड मिल जाता है तो वह उसका प्रयोग आपके अन्य खातों पर भी करेगा।
  - अपने पासवर्ड याद रखने और नये पासवर्ड बनाने के लिए एक पासवर्ड मैनेजर का उपयोग करें।
  - अच्छे पासवर्ड बनाएं - Own Your Online (ओन योर ऑनलाइन)
- **टू फैक्टर ऑथेंटिकेशन (दो-कारक प्रमाणीकरण) चालू रखें।**
  - यह एक अतिरिक्त जानकारी है - आमतौर पर आपके फोन पर एक कोड - जिसकी आपको किसी वेबसाइट पर लॉग इन करने के लिए आवश्यकता होती है।
  - यह तकनीक अतुलनीय रूप से शक्तिशाली है और आपके खातों में सेंध लगाने के अधिकांश प्रयासों को रोक सकती है।
  - जहाँ यह समर्थित हो, हम एक 'authenticator app (प्रमाणक ऐप)' का उपयोग करने की सलाह देते हैं।
  - टू फैक्टर ऑथेंटिकेशन (2FA) सेट करें - Own Your Online (अपना ऑनलाइन स्वामित्व बनाए रखें)
- **ऑनलाइन प्राइवेट (गोपनीय) बने रहें।**
  - सोशल मीडिया पर सुरक्षित रहने का सबसे अच्छा विकल्प यह है कि आप अपनी प्राइवेट सैटिंग्स (गोपनीयता सैटिंग) चालू रखें।
  - ऐसा करने से साइबर अपराधियों सहित अन्य अनजान लोग आपकी पोस्ट नहीं देख पाएंगे या आपको संदेश नहीं भेज पाएंगे।
  - फिर भी अपने, अपने परिवार या अपने मित्रों के बारे में व्यक्तिगत जानकारी पोस्ट करते समय सावधान रहें।
  - सुनिश्चित करें कि (आपके ऑनलाइन) संपर्क वही हैं जो वे होने का दावा करते हैं।
  - नकली मित्र अनुरोधों से सावधान रहें। ऐसे लोगों से सावधान रहें जो पत्रकार होने का दावा करते हैं या ऐसे अन्य लोग जिन्हें आप अच्छी तरह से नहीं जानते हैं।
  - ऑनलाइन अपनी गोपनीयता की रक्षा करें - Own Your Online (अपना ऑनलाइन स्वामित्व बनाए रखें)

- **सब कुछ अपडेटेड (नवीनतम) रखें।**
    - जब आप अपने फोन, कंप्यूटर या सॉफ्टवेयर को अपडेट करते हैं, तो यह सुरक्षा में किसी भी प्रकार की चूक को भी दूर कर देता है।
    - अपराधी हमेशा [आपके खातों में] घुसने के तरीकों की तलाश में रहते हैं और अपडेट कमजोरियों को ठीक कर देते हैं।
    - अपने डिवाइसों (उपकरणों) को नियमित रूप से रिस्टार्ट (बंद करके दोबारा चालू) करें।
    - अपने अपडेट्स को नवीनतम रखें - Own Your Online (अपना ऑनलाइन स्वामित्व बनाए रखें)
- **घोटालों से सावधान रहें।**
    - सबसे अच्छी सलाह यह है कि इन घोटालों के प्रति सचेत रहें और इनसे सावधान रहें।
    - यदि (आपको) कुछ भी गलत लगता है तो उस व्यक्ति से संपर्क न रखें जिसने आपसे संपर्क किया है। विशेष रूप से तब सावधान रहें जब वे पैसे मांगें, भले ही वे मित्रवत लगें।
    - अजीब लिंक और ईमेल पतों पर नजर रखें (उदाहरण के लिए: आपका बैंक आपको Gmail (जीमेल) खाते से ईमेल नहीं भेजेगा)।
    - टैक्स्ट मैसेज में दिए गए लिंक पर *कभी भी क्लिक न करें।*
    - अपनी डिवाइस पर केवल ऑफिशियल (आधिकारिक) ऐप स्टोर से ही ऐप डाउनलोड करें।
    - यदि कोई शक हो तो उस संगठन से सीधे संपर्क करें जिसने आपसे संपर्क किया है तथा आपको भेजे गए किसी भी लिंक या फोन नंबर का उपयोग न करें।
    - अपने लिए, अपने समुदाय के लिए तथा आप जिन समूहों का हिस्सा हैं उनके लिए ऑनलाइन सुरक्षा जोखिमों के प्रति जागरूक रहने का प्रयास करें।
- **अपनी जानकारी को सुरक्षित रखें।**
    - Signal (सिग्नल) जैसी एन्क्रिप्टेड मैसेजिंग ऐप का उपयोग करें। इससे कोई भी व्यक्ति आपके संदेशों को नहीं पढ़ सकेगा।
    - किसी भी वेबसाइट के साथ जानकारी केवल तभी साझा करें जब उसका पता HTTPS से शुरू हो। [HTTPS में] S (एस) का अर्थ है "सिक्योर - सुरक्षित" और इसका अर्थ है कि आपके और वेबसाइट के बीच भेजी गई कोई भी जानकारी एन्क्रिप्टेड है।
    - वर्चुअल प्राइवेट नेटवर्क (VPN-वीपीएन) का उपयोग करने के बारे में विचार करें जो आपके डेटा की सुरक्षा कर सकता है और आपकी लोकेशन (स्थान) को छिपा सकता है।
    - जाँच करें कि आपकी ऐप्स को कौन से डेटा तक पहुंच और अनुमतियां प्राप्त हैं। उदाहरण के लिए, किसी फिटनेस ऐप को आपके कॉन्टेक्ट्स (संपर्कों) तक पहुंचने की आवश्यकता नहीं होती।

यदि मेरे साथ धोखाधड़ी हो या इससे भी बुरा कुछ हो जाए तो मुझे क्या करना चाहिए?

ऐसी बहुत सी जगह हैं जहां आप मदद के लिए जा सकते हैं। ये संगठन आपकी जानकारी किसी अन्य के साथ तब तक साझा नहीं करेंगे, जब तक आप इसकी सहमति न दें।

- आप CERT NZ पोर्टल के माध्यम से NCSC को साइबर घटनाओं की रिपोर्ट कर सकते हैं और हम आपकी सहायता कर सकते हैं या आपका किसी अन्य एजेंसी से संपर्क करवा सकते हैं:
  घटना की रिपोर्ट करें | CERT NZ

- यदि आपको पैसों का नुक्सान हुआ है, तो आपको तुरंत अपने बैंक से संपर्क करना चाहिए।
- घोटाले से संबंधित टैक्स्ट संदेश, डिपार्टमेंट ऑफ इंटर्नल अफेयर्स (आंतरिक मामलों के विभाग) द्वारा संचालित सेवा 7726 पर निःशुल्क भेजे जा सकते हैं।