National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

अपने संगठन को ऑनलाइन सुरक्षित रखना

सामुदायिक समूहों और संगठनों के लिए साइबर (ऑनलाइन) सुरक्षा क्यों महत्वपूर्ण है?

इस पृष्ठ पर कुछ सलाह और कुछ कदम दिए गए हैं जिन्हें आप अपने सामुदायिक समूह या संगठन को साइबर सुरक्षा के खतरों से बचाने के लिए अपना सकते हैं। व्यक्तिगत रूप से स्वयं को ऑनलाइन सुरक्षित रखने के लिए एक अलग गाइड भी उपलब्ध है।

यह सलाह सबसे आम और गंभीर खतरों पर आधारित है।

- अपडेट (अद्यतन) - सुरक्षा में किसी भी कमी या ढील को दूर करने के लिए अपनी डिवाइस (उपकरणों) पर सॉफ़्टवेयर को अपडेट रखें।
    - अपने सामुदायिक समूह या संगठन की डिवाइस को अपडेट करके रखें। इसमें फोन, कंप्यूटर, वाईफाई राउटर और इंटरनेट से जुड़ने वाली अन्य सभी चीजें शामिल हैं - इनमें स्मार्ट डिवाइस भी शामिल है।
    - जहां तक संभव हो ऑटोमैटिक (स्वचालित) अपडेट का उपयोग करें।
- टू फैक्टर ऑथेंटिकेशन - (दो-कारक प्रमाणीकरण 2FA) - एक पासवर्ड तथा एक अतिरिक्त कदम (जैसे कि आपके फोन पर किसी ऐप से एक कोड की जरूरत) के जरिए आपके खातों को अतिरिक्त सुरक्षा प्रदान करता है।
    - नोट: इसे मल्टी-फैक्टर ऑथेंटिकेशन (बहु-कारक प्रमाणीकरण - MFA), टू-स्टेप वेरिफिकेशन (दो-चरणीय सत्यापन - 2SV) तथा कई अन्य नामों से भी जाना जाता है।
    - अपने सभी सामुदायिक समूह या संगठन के खातों पर 2FA (दो-कारक प्रमाणीकरण) को चालू करें।
    - यदि संभव हो तो 2FA के ऐसे रूप का प्रयोग करने की कोशिश करें जो फ़िशिंग प्रतिरोधी हो, जिसका अर्थ है कि इसे धोखे से आप से ना लिया जा सके। यह एक फिजिकल सिक्योरिटी की (भौतिक सुरक्षा कुंजी) या फिंगरप्रिंट (ऊँगली की छाप) अथवा फेस आईडी (चेहरे की पहचान) जैसा तरीका हो सकता है।
- अपने ऑनलाइन खातों पर नज़र रखें - सुनिश्चित करें कि समुदाय समूह या संगठन छोड़ने के बाद भूतपूर्व सदस्य उन खातों का प्रयोग न कर सकें।
    - यदि आपके एक ही खाते का प्रयोग करने वाले एक से अधिक व्यक्ति हैं, तो सुनिश्चित करें कि उन सभी के पास अलग-अलग लॉगिन हैं, और सभी ने 2FA चालू किया हुआ है।
    - खातों का उपयोग करने वाले सभी लोगों की एक सूची अपने पास रखें और जिनकी आवश्यकता न हो उन्हें निष्क्रिय कर दें, जैसे कि कर्मचारियों के काम छोड़ कर चले जाने पर।

- अपने सदस्यों को दिए गए किसी भी उपकरण का रजिस्टर (रिकॉर्ड) रखें तथा यदि वह व्यक्ति संगठन छोड़ देता है तो उसे वापस लेना तथा फैक्टरी रीसेट करना याद रखें। आपको बिल्डिंग में पहुँच के लिए भौतिक कोड भी बदलने की आवश्यकता हो सकती है।

- इस बात की जाँच करें कि आपके ऑनलाइन खातों तक किसकी पहुँच है - आपके सामुदायिक समूह या संगठन के लोगों की एक्सेस (पहुँच) केवल उन्हीं चीज़ों तक होनी चाहिए जिनकी उन्हें जरूरत है।
    - यदि किसी एक व्यक्ति का अकाउंट हैक हो जाता है तो इन कदमों से हमलावर द्वारा पहुंचाई जाने वाली हानि को सीमित किया जा सकता है।
    - नियमित रूप से जाँचते रहें और अनावश्यक अनुमतियों को हटा दें।
    - यदि आपके पास एक ही "एडमिन (व्यवस्थापक)" खाता है जिसका उपयोग एक से अधिक लोग करते हैं, तो किसी भी असामान्य गतिविधि के लिए उस खाते पर नज़र रखें। अगर हो सके तो इस प्रकार के खातों को सीमित रखें, खासकर रोज़मर्रा के कामों के लिए।
    - ये नियम राउटर जैसी डिवाइसों (उपकरणों) तक एडमिनिस्ट्रेटर यानि व्यवस्थापक की पहुँच पर भी लागू होते हैं।

- यदि आपने आईटी सेवाएं चलाने के लिए किसी को नियुक्त किया है- तो सेवा प्रदाताओं के साथ अपने अनुबंधों की समीक्षा करें।
    - सुनिश्चित करें कि आपके सामुदायिक समूह या संगठन की आवश्यकताओं को पूरा करने के लिए उन्होंने साइबर सुरक्षा उपाय लागू किए हुए हैं।

- इस बात की जानकारी रखें कि आपके सभी खाते और सिस्टम एक साथ कैसे काम करते हैं - उनके बीच के संपर्क को समझने से आपको यह जानने में मदद मिलती है कि कोई हमलावर (उन सिस्टम/ खातों में) कहाँ से प्रवेश कर सकता है।
    - अपने सारे सिस्टम, उदाहरण के लिए, ईमेल, क्लाउड स्टोरेज और अकाउंटिंग प्लेटफ़ॉर्म के बीच के कनेक्शन (संपर्क) की समीक्षा करें।
    - अतिरिक्त ऑनलाइन सुरक्षा के लिए वर्चुअल प्राइवेट नेटवर्क (VPN-वीपीएन) का उपयोग करने के बारे में विचार करें। VPN (वीपीएन) का उपयोग करने से आपकी ऑनलाइन गतिविधि ऐसे किसी भी व्यक्ति से भी छिप जाती है जो आपको ट्रैक करने (नज़र रखने या ढूंढने) का प्रयास कर सकता है। यह विशेष रूप से अच्छा है यदि आपके सामुदायिक समूह या संगठन का कोई भी सदस्य रिमोटली (दूरस्थ रूप से) कनेक्ट करते हैं।

- अपने लोगों को 'साइबर स्मार्ट' बनाए रखें - आपके सिस्टम की तुलना में आपके सामुदायिक समूह या संगठन के लोगों को निशाना बनाए जाने की संभावना अधिक होती है।

- सभी कर्मचारियों को बुनियादी साइबर सुरक्षा में प्रशिक्षित करें। Own Your Online (ओन योर ऑनलाइन) वेबसाइट Own Your Online | NCSC पर ऑनलाइन सुरक्षित रहने और धोखाधड़ी को पहचानने में मदद करने के लिए विस्तृत सलाह और सुझाव हैं।
- उन्हें याद दिलाएं कि यह उनके व्यक्तिगत खातों के साथ-साथ उनके द्वारा उपयोग किए जाने वाले आपके संगठन के खातों के लिए भी महत्वपूर्ण है।
- हमारे पास व्यक्तिगत रूप से स्वयं को ऑनलाइन सुरक्षित रहने के लिए एक गाइड (मार्गदर्शिका) भी है।

- घटना के लिए योजना बनाएं - किसी घटना के घटित होने पर लोगों को घबराहट होने से बचाने के लिए रिसपॉन्स प्लॉन (प्रतिक्रिया योजना) का होना जरूरी है।
  - एक घटना प्रतिक्रिया योजना यह रेखांकित करती है कि घटना के दौरान कौन क्या करता है। टेम्पलेट्स (खाके) Incident Management | NCSC पर उपलब्ध हैं।
  - फोन, कंप्यूटर या अन्य सिस्टम खराब होने पर क्या करना है, इसकी योजना बनाना भी इसमें शामिल करें। इस योजना को अपडेट करके (नवीनतम) रखें।
  - सभी आवश्यक व्यक्तियों के संपर्क विवरण रखें तथा यदि उनसे संपर्क करने का मुख्य तरीका खराब हो जाए (जैसे कि ईमेल) तो ऐसी स्थिति के लिए उनके अन्य विवरण भी रखें।
  - यदि आप उस तक नहीं पहुंच पाते तो [उस तक पहुंच के लिए] योजना को अपने सिस्टम (कम्प्यूटर आदि) से बाहर भी कहीं रखें।