connect SMART
Protect yourself online

newzealand.govt.nz

Connect Smart साईबर सुरक्षा के प्रति जागरूकता बढ़ाने तथा स्वयं को ऑनलाईन सुरक्षित रहने के तरीकों को प्रोत्साहित करने से संबंधित है। न्यू ज़ीलैंड के सभी निवासियों को इसका लाभ मिलेगा, यदि हम एक सुरक्षित व विश्वसनीय ढंग से इन्टरनैट की संपूर्ण सामर्थ्य का उपयोग कर सकें। अन्य शब्दों में, Connect Smart सीखें।

Connect Smart - स्वयं को ऑनलाईन सुरक्षित रखें

1. प्रतीक्षा न करें, कहीं देरी न हो जाए - अग्रसक्रिय बनें; शिकार बनने से पूर्व ही अपनी डिजीटल सुरक्षा को सुधार लें।
2. आपकी डिजिटल सुरक्षा में सुधार लाना आसान है - स्वयं को तथा अपनी निजी जानकारी को सुरक्षित रखने हेतु मूलभूत कदम उठाना कोई पेचीदा अथवा महंगा कार्य नहीं है।
3. अपने सभी उपकरणों का उपयोग करते समय स्वयं को सुरक्षित रखें-अपने स्मार्टफ़ोन व टैबलेट पर सुरक्षित रहना उतना ही महत्त्वपूर्ण है, जितना आपको अपने पी सी या लैपटॉप पर सुरक्षित रहना महत्त्वपूर्ण है।
4. स्वयं की सुरक्षा से आपके मित्रगण, परिवार एवं कार्य सभी सुरक्षित रहते हैं - आपकी कोई निजी जानकारी किसी अन्य व्यक्ति के पास चले जाना आपके लिये एक असुविधा से अधिक है तथा आपको व आपके सभी जानकारों को बड़े नतीजे भी भुगतने पड़ सकते हैं।

मैं ऑनलाईन अपनी स्वयं की सुरक्षा कैसे करूँ ?

पासवर्ड्स (Passwords)

- यह सुनिश्चित करें कि इन्टरनैट से जुड़ने वाले आपके सभी उपकरण जैसे कि डैस्क टॉप कंप्यूटर्स, लैपटॉप्स, टैबलैट्स एवं मोबाईल फ़ोन सभी विभिन्न पासवर्डस द्वारा सुरक्षित हों।
- मज़बूत व जटिल पासवर्ड्स का प्रयोग करें (सामान्य अक्षरों के साथ-साथ शिफ़्ट दबा कर पड़ने वाले अक्षरों, अंकों एवं विराम चिन्हों को सम्मिलित करें), विशेषतया अपनी ई-मेल व ऑनलाईन बैंकिंग हेतु।
- पासवर्ड्स को नियमित रूप से बदलते रहें।

Wifi

- Wifi: अपने वायरलैस क्नैक्शन्स को सुनिश्चित बनाएं – उन्हें किसी मज़बूत पासवर्ड एवं कूटबद्धता (एनक्रिप्शिन) से सुरक्षित रखें।
- यदि आप किसी असुरक्षित Wifi पर संचालन कर रहे हैं, तो इस संबंधी सचेत रहें कि आप क्या करते हैं। असुरक्षित Wifi का प्रयोग बैंकिंग व अन्य वित्तीय लेन-देन संबंधी न करें।

ई-मेल्स एवं सोशल मीडिया

- अजनबियों की ओर से आने वाले या असामान्य दिखाई देने वाले ई-मेल संदेशों के प्रति संदिग्ध रहें। यह स्पैम ई-मेल हो सकती है, जिसमें कोई दुर्भावनापूर्ण सॉफ़्टवेयर संलग्न हो सकता है।
- अज्ञात वैबसाईट्स के लिंक्स के प्रति भी संदिग्ध ही रहें। यदि आप विश्वस्त नहीं हैं, तो उन पर क्लिक न करें। केवल विश्वसनीय अथवा प्रतिष्ठित साईट्स पर ही जाएं।
- स्वयं, मित्रगणों अथवा परिवार की पहचान संबंधी व अन्य ऐसी कोई जानकारी को किसी के साथ ई-मेल द्वारा या ऑनलाईन कम से कम ही साझी करें।
- सोशल मीडिया साईट्स पर अपनी गोपनीयता (प्राईवेसी) सैटिंग्स को चैक करें।

कंप्यूटर सुरक्षा

- कंप्यूटर सुरक्षाः उचित फायरवाल्स को अधिष्ठापित (इनस्टाल) करें।
- अपना एन्टी-वायरस सॉफ़्टवेयर अप-टू-डेट रखें।
- सुनिश्चित करें आपका ऑपरेटिंग सॉफ़्टवेयर अप-टू-डेट है।
- सुनिचित करें कि यदि कुछ भी घटित हो जाए तो आपके पास सारी जानकारी का बैक-अप सुरक्षित पड़ा हो। यदि कंप्यूटर को बेच रहे हैं या उसका निपटान कर रहे हैं, तो यह सुनश्चित करें कि आपने अपने सभी निजी आंकडे व जानकारी उसमें से हटा दिए हैं तथा हार्ड ड्राईव को पूर्णतया साफ़ करने हेत् कदम उठाए हैं।

मोबाईल उपकरण

- किसी पासवर्ड द्वारा इसे सुरक्षित रखें।
- अपने अन्य इन्टरनैट उपकरणों की तरह, एन्टी-सॉफ़्टवेयर का उपयोग करें तथा सॉफ़्टवेयर सदैव अप-टू-डेट रखें।
- केवल प्रतिष्ठित एप्लीकेशन्स को ही डाऊनलोड करें।

ऑनलाईन ख़रीददारी

- ऑनलाईन ख़रीददारी करते समय किसी सुरक्षित भुगतान विधि जैसे PayPal अथवा अपने क्रैडिट कार्ड का प्रयोग करें।
- घोटालों, ऑनलाईन धोखाधड़ियों एवं झूठे सप्लायरों से चौकस रहें।
- यह सुनिश्चित करें कि पहचान अथवा वित्तीय जानकारी हेतु कंपनियों अथवा व्यक्तियों के निवेदन प्रामाणिक भी हैं या नहीं।