ईमेल सुरक्षा पद्धतियां

इंटरनेट उपयोगकर्ताओं को नीचे उल्लिखित बुनियादी ईमेल सुरक्षा पद्धतियों का पालन करने की सलाह दी जा सकती है:

1. एंटी-स्पाइवेयर सॉफ्टवेयर प्रदान करने का दावा करने वाले ईमेल लिंक (ऐसे मेल के मुख्य भाग में उल्लिखित हाइपरलिंक/वेब लिंक/ यूआरएल) को न खोलें/न उत्तर दें। लिंक विपरीत उद्देश्य को पूरा कर सकते हैं और वास्तव में उस स्पाइवेयर को स्थापित कर सकते हैं जिसे हटाने का दावा किया गया है।

2. डाउनलोड करने/खोलने से पहले मेल अटैचमेंट को स्कैन करें।

3. व्यक्तिगत और व्यावसायिक उद्देश्यों के लिए अलग-अलग ईमेल खातों का उपयोग करें।

4. किसी भी अनधिकृत पहुंच के लिए, समय-समय पर अंतिम लॉग-इन गतिविधि की जांच करें।

5. यदि विदेशी आईपी एड्रेसेज से ईमेल एक्सेस आदि जैसी कोई संदिग्ध गतिविधि देखी जाती है, तो किसी अन्य सुरक्षित कंप्यूटर से उनके सभी ऑनलाइन खातों (ईमेल और अन्य) के पासवर्ड बदल दें।

एनआईसी मेल उपयोग

1. अज्ञात ईमेल आईडी से आए ईमेल या अटैचमेंट को न खोलें।

2. एनआईसी मेल में प्राथमिकता विकल्प के तहत शेयर किए गए किसी भी फ़ोल्डर की जांच करें। यदि कोई शेयर्ड फ़ोल्डर मिलता है ,तो उसे तुरंत डिसेबल करें।

3. अकाउंट पहुंच विवरण के लिए लॉगिन हिस्ट्री की जांच करें।

4. ब्राउज़र में लॉगिन क्रेडेंशियल सेव न करें और सत्र समाप्त होने के बाद लॉगआउट न करें।

5. सभी एनआईसी ईमेल अकाउंट में कवच को इनेबल करें।