भारतीय बीमा विनियामक और विकास प्राधिकरण
INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA
Promoting insurance. Protecting insured.

साइबर सुरक्षा जागरूकता अभियान

अक्टूबर-2021

विशेष रूप से कोविड महामारी के दौरान सूचना और संचार प्रौद्योगिकी की पैठ के साथ-साथ डिजिटल गतिविधि में वृद्धि को ध्यान में रखते हुए, साइबर धोखाधड़ी को रोकने के लिए पॉलिसीधारकों और आम जनता के लिए साइबर सुरक्षा के बारे में जागरूकता समय की आवश्यकता है।

अपराध।

विभिन्न बीमा लेनदेन करते समय कुछ क्या करें और क्या न करें इस प्रकार हैं:

1. पॉलिसी ख़रीदना/नवीकरण करना

करने योग्य

विक्रेताओं की विश्वसनीयता की तलाश करें, अर्थात् एजेंट, मध्यस्थ जैसे दलाल या बीमा
कंपनी के कर्मचारी

केवल जानने की आवश्यकता के आधार पर व्यक्तिगत जानकारी प्रदान करें

आवश्यकता पड़ने पर केवाईसी जानकारी प्रदान करें

बीमा कंपनी की वेबसाइटों या वेब में खाता स्थापित करने के लिए एक मजबूत पासवर्ड का उपयोग करें
यदि आवश्यक हो तो एग्रीगेटर

क्या न करें

 बीमा से संबंधित वेबसाइटों से बचें जो https से शुरू न हों

संदिग्ध और नकली पहचान वाले विक्रेताओं / बिचौलियों से बचें

 संवेदनशील जानकारी मांगने वाले बीमा बिचौलियों से सावधान रहें

2. संचालन बीमा पॉलिसी और संचार

करने योग्य

बीमा खातों में मजबूत पासवर्ड का प्रयोग करें और बीमा कंपनी पोर्टल पर लॉगिन करें

अलग-अलग खातों के लिए अवैयक्तिक और अलग-अलग पासवर्ड का प्रयोग करें

वास्तविक ऑपरेटिंग सिस्टम का उपयोग करें (जिस पर इलेक्ट्रॉनिक बीमा खाते का उपयोग करके संचालन किया जाता है)

 अपने खाते का पासवर्ड गोपनीय रखें

संपर्क विवरण, पते में किसी भी प्रकार के परिवर्तन के बारे में बीमा कंपनी को समय-समय पर सूचित करें
समय

क्या न करें

डिफ़ॉल्ट पासवर्ड का प्रयोग न करें

कस्टमर केयर सर्विस से संपर्क करने पर कोई पिन/खाता पासवर्ड साझा न करें

किसी भी ओटीपी को तब तक साझा न करें जब तक कि उसके उपयोग के बारे में निश्चित न हो

3. दावा प्रक्रिया सुरक्षा

करने योग्य

आवश्यकतानुसार प्रामाणिक दावे संबंधी जानकारी और व्यक्तिगत/संवेदनशील जानकारी प्रदान करें

 वास्तविक पहचान और केवाईसी सत्यापन प्रदान करें

क्या न करें

संतुष्ट होने पर केवल बीमा कंपनी के कर्मचारियों/दावा टीम को खाते की जानकारी प्रदान करें

उनकी प्रामाणिकता के

किसी को अकाउंट पासवर्ड न दें

लेन-देन की महत्वपूर्ण जानकारी जैसे लेनदेन आईडी का रिकॉर्ड रखें

4. फ़िशिंग और संदिग्ध संचार से सुरक्षा

करने योग्य

 अपरिचित या नाजायज पते की जाँच करें

ईमेल में 'अत्यावश्यकता की भावना' से सावधान रहें। फ़िशिंग ई-मेल में लक्ष्य बनाने की प्रवृत्ति होती है

जल्दबाजी महसूस करें।

संदिग्ध ई-मेल में सामान्य अभिवादन/नमस्कार की जांच करें जैसे प्रिय मूल्यवान ग्राहक, प्रिय

नाम के बजाय उपयोगकर्ता

मेल सामग्री में वर्तनी और व्याकरण संबंधी गलतियों के माध्यम से फ़िशिंग ईमेल की पहचान करने का प्रयास करें

क्या न करें

व्यक्तिगत जानकारी के अनुरोधों का ईमेल के माध्यम से जवाब न दें

 कभी भी पॉप-अप स्क्रीन में व्यक्तिगत जानकारी दर्ज न करें

ई-मेल में सूचीबद्ध किसी भी लिंक पर क्लिक न करें। यदि लिंक को सत्यापित करना है, तो URL को कॉपी और पेस्ट करें

ब्राउज़र।

किसी भी संदिग्ध अटैचमेंट पर क्लिक न करें जैसे .exe फ़ाइल एक्सटेंशन वाले अटैचमेंट

5. साइबर नैतिकता - एक जिम्मेदार साइबर पॉलिसीधारक बनें

अनुचित साइबर आचरण में शामिल न हों, जैसे साइबर बुलिंग

किसी का प्रतिरूपण न करें, उदाहरण के लिए सोशल पेज, पोस्ट, साइट आदि बनाकर।

• बीमा या किसी अन्य जानकारी को डाउनलोड करते समय कॉपीराइट बाधाओं का पालन करें

इंटरनेट

दूसरों की जानकारी का उपयोग न करें जिससे उनकी पहचान हो सकती है

•सार्वजनिक वाई-फाई का उपयोग सावधानी और सावधानी से करें

6. साइबर अपराधों की रिपोर्ट करना

1. हेल्पलाइन 155260 - गृह मंत्रालय द्वारा राष्ट्रीय हेल्पलाइन और रिपोर्टिंग प्लेटफॉर्म

(एमएचए)

वित्तीय नुकसान को रोकने में मदद करता है

• संबंधित राज्य पुलिस द्वारा संचालित

रीयल-टाइम में डिजिटल धोखाधड़ी के खिलाफ कार्रवाई करने के लिए नए जमाने की तकनीकों का उपयोग करता है

कानून प्रवर्तन एजेंसियों और वित्तीय मध्यस्थों के साथ एकीकरण प्रतिक्रिया

• अधिक जानकारी: https://cybercrime.gov.in/Webform/Helpline.aspx

2. https://digitalpolice.gov.in/Default.aspx: यह पोर्टल नागरिकों के लिए अपराध दर्ज करने का एक मंच है

संबंधित शिकायतें ऑनलाइन करें और संभावित कर्मचारियों के पूर्ववृत्त सत्यापन की मांग करें

(घरेलू मदद, ड्राइवर आदि सहित), किरायेदार या किसी अन्य उद्देश्य के लिए। नागरिक भी कर सकते हैं

अपने स्वयं के पूर्ववृत्त के प्रमाणीकरण की मांग करें।