सोशल इंजीनियरिंग

1. 'सोशल इंजीनियरिंग गलत चित्रण के माध्यम से जानकारी तक पहुंच प्राप्त करने का एक तरीका है। यह लोगों से जानकारी प्राप्त करने के लिए उन्हें सचेत रूप से मैनिपुलेट करता है जिसमें उन्हें यह एहसास भी नहीं होता कि दरअसल सुरक्षा का उल्लंघन हो रहा है। यह टेलीफोन के माध्यम से या व्यक्तिगत रूप से और ईमेल के माध्यम से प्रतिरूपण का रूप ले सकता है।

2. कुछ ईमेल प्राप्तकर्ता को एक अटैचमेंट खोलने के लिए लुभाते हैं जो आपके कंप्यूटर में वायरस या दुर्भावनापूर्ण प्रोग्राम को सक्रिय कर देता है।

3. कर्मचारियों या अन्य आंतरिक जानकारी के बारे में पूछने वाले व्यक्तियों के अनचाहे फोन कॉल, मुलाक़ात या ईमेल संदेशों पर संदेह करें। यदि कोई अज्ञात व्यक्ति किसी वैध संगठन से होने का दावा करता है, तो सीधे कंपनी के साथ उसकी पहचान सत्यापित करने का प्रयास करें।

4. अपने संगठन के बारे में, उसकी संरचना या नेटवर्क के बारे में और साथ ही व्यक्तिगत जानकारी तब तक प्रदान न करें, जब तक कि आप जानकारी प्राप्त करने वाले व्यक्ति के प्राधिकार के बारे में आश्वस्त न हों।

5. ईमेल में व्यक्तिगत या वित्तीय जानकारी प्रकट न करें और इस जानकारी के लिए ईमेल सॉलिसिटेशन का जवाब न दें। इसमें ईमेल में भेजे गए फॉलो किए जाने वाले लिंक भी शामिल हैं।

6. वेबसाइट की सुरक्षा जांचने से पहले इंटरनेट पर संवेदनशील जानकारी न भेजें। किसी वेबसाइट के यूआरएल पर ध्यान दें। दुर्भावनापूर्ण वेबसाइटें किसी वैध साइट के समान दिख सकती हैं, लेकिन यूआरएल की वर्तनी में भिन्नता या भिन्न डोमेन (उदाहरण के लिए, .com बनाम -net) दिख सकता है।

7. इस ट्रैफ़िक को कम करने के लिए एंटी-वायरस सॉफ़्टवेयर, फ़ायरवॉल और ईमेल फ़िल्टर इंस्टॉल करें और उन्हें लगातार अपडेट करें।

8. अपने ईमेल क्लाइंट और वेब ब्राउज़र द्वारा दी जाने वाली किसी भी एंटी-फ़िशिंग सुविधा का लाभ उठाएं।

9. आपके द्वारा बताए गए किसी भी पासवर्ड को तुरंत बदल दें। यदि आपने कई संसाधनों के लिए एक ही पासवर्ड का उपयोग किया है, तो इसे प्रत्येक अकाउंट के लिए बदलना सुनिश्चित करें।