सीआईएसओ- स्तरीय गाइड: अपने ग्राहकों की रक्षा करना

खातों का प्रशासन करना

- आपकी सेवाओं में लॉग करने के लिए आवश्यक है कि ग्राहक मजबूत यूजर आईडी और पासवर्ड का उपयोग करें। उन्हें सलाह दें कि वे उसी पासवर्ड का उपयोग न करें जिसका वे अन्य खातों के लिए उपयोग करते हैं।
- अविलम्ब सत्यापन, रीयल-टाइम सत्यापन, ट्रायल डिपॉजिट सत्यापन का इस्तेमाल करें, सत्यापन की पहचान करें और/अथवा आउट ऑफ वैलेट सवाल करें ताकि वास्तविक ग्राहकों का मान्यकरण हो सके और धोखाधड़ी के अवसर को कम किया जा सके।
- आपकी सेवा में लॉग करने के लिए दो-कारक सत्यापन की पेशकश करें जो आदर्श स्थिति के लिए आवश्यक होता है।
- धोखाधड़ी के किसी संकेत की जांच हेतु नियमित रूप यूजर खाते की जांच करते रहें।

डेटा की सुरक्षा करना

- इस बात पर विचार करें कि आपका संगठन किस ग्राहक डेटा को अपनी सेवा के लिए *अवश्य संग्रह* करता है और इससे इतर के ग्राहक डेटा के संग्रहण को लेकर सजग रहें।
- डेटा संधारण नीतियों का निर्धारण और वितरण करें। जब जरूरत ना हो तो ग्राहक के डेटा को नष्ट कर दें।
- पारगमन और स्थिर स्थिति में ग्राहक के डेटा को इन्क्रिप्ट करें।
- यह स्पष्ट करने के लिए कि प्रतिबंधित के विरुद्ध कौन सी डेटा स्थानांतरण नीति अनुमोदित है और यह विनिर्दिष्ट करने के लिए ग्राहकों डेटा से निपटते समय कर्मियों के हेतु क्या स्वीकार करने योग्य है, डेटा सुरक्षा की नीति को सामने रखें। यह सुनिश्चित करें कि ये नीतियां दस्तावेजित और संचारित है जोकि सभी कर्मियों के लिए प्रवर्तनीय है और आवर्ती रूप से समीक्षित एवं अपडेट किया हुआ है।

सार्वजनिक वेब एप्लिकेशन को सुरक्षित करना

- अपने संगठन के जन-मुखी वेब एप्लिकेशन (एप्लिकेशंस) पर HTTPS को लागू करें और सभी HTTP ट्रॉफिक को HTTPS पर पुनर्निर्देशित करें।
- अपनी वेबसाइट (वेबसाइटों) पर एक कंटेंट सुरक्षा नीति का उपयोग करें ताकि क्रॉस साइट स्क्रिप्टिंग हमले, क्लिकजैकिंग और अन्य कोड इंजेक्शन को रोका जा सके।
- अपनी वेबसाइट (वेबसाइटों) पर पब्लिक की पिनिंग को सक्षम करें ताकि हमलावर को हमला के बीच रोका जा सके।
- सुनिश्चित करें कि आपके जन-मुखी एप्लिकेशन (एप्लिकेशनों) कभी कूकी का उपयोग नहीं करे जिससे कि ग्राहकों की अतिसंवेदनशील या महत्वपूर्ण सूचना (जैसे कि पासवर्ड) भंडारित न हो, कूकी के लिए संरक्षित एक्सपायरेशन तिथियों का अनुपालन करें (बाद में नहीं बल्कि तुरंत) और आपके द्वारा उपयोग किए जाने वाले कूकीज में भंडारित सूचना हेतु इन्क्रिप्शन पर विचार करें।
- अपने जन-मुखी वेब एप्लिकेशन (एप्लिकेशनों) की सुरक्षा के आकलन हेतु साल में कम से कम एक बार पेनेट्रेशन टेस्टिंग सेवा नियुक्त करने पर विचार करें।

वित्तीय डेटा की रक्षा के लिए ग्राहकों और कर्मियों को व्यक्तिगत स्तर पर सलाह देना

अपने कर्मियों और ग्राहकों को सलाह दें कि वे अपने निजी आचरणों में निम्नलिखित दिशा-निर्देशों का पालन करें ताकि उनकी तैयारी बेहतर हो और साइबर हमले के विरुद्ध वे अपने वित्तीय डेटा की रक्षा कर सकें।

1. आधारभूत साइबर स्वच्छता के अभ्यास को सभी डिवाइसेज पर लागू करना।

- सभी व्यक्तिगत और पेशेवर डिवाइस पर मजबूत पासवर्ड का उपयोग करना और एक पासवर्ड मैनेजर के उपयोग पर विचार करना।
- अपने कंप्यूटर और मोबाइल डिवाइस पर सभी ऑपरेटिंग सिस्टम और अन्य सॉफ्टवेयर और एप्लिकेशंस को अद्यतन रखें।
- ऐसे एंटी-वायरस, एंटी-मैलवेयर और एंटी-रैंसमवेयर सॉफ्टवेयर इंस्टॉल करें जो दुर्भावनापूर्ण प्रोग्राम को रोक सकें, उसकी पहचान कर उन्हें हटा सकें।
- आपके कंप्यूटर का अनाधिकृत एक्सेस नहीं हो इसके लिए एक फायरवॉल प्रोग्राम का इस्तेमाल करें।
- केवल प्रतिष्ठित कंपनी के सुरक्षा प्रोडक्ट का इस्तेमाल करें। कंप्यूटर और उपभोक्ता प्रकाशनों से समीक्षाओं को पढ़ें और अपने कंप्यूटर या ऑपरेटिंग सिस्टम निर्माता के साथ परामर्श करने पर विचार करें।

2. संवेदनशील सूचना के प्रति सावधान रहें।

- अनक्रिप्टेड ईमेल के माध्यम से बैंक खातों का पासवर्ड या अन्य संवेदनशील वित्तीय खाता डेटा नहीं भेजें।
- इस बात को लेकर बुद्धिमता दिखाएं कि आप कहां और कैसे बैंकिंग या संवेदनशील सूचना से युक्त संचार के कार्य हेतु इंटरनेट से कनेक्ट होते/होती हैं। सार्वजनिक वाई-फाई नेटवर्क और पुस्तकालय या होटल व्यवसाय केंद्र जैसे स्थानों के कंप्यूटर जोखिमपूर्ण हो सकते हैं।

3. फिशिंग का प्रतिरोध करना।

- ईमेल अटैमेंट्स को तत्काल नहीं खोलें या ऐसे लिंकों पर क्लिक नहीं करें जो अविश्वसनीय या संदेहास्पद ईमेल हो। रूकें। सोचें। क्लिक करें।
- अगर कोई अप्रत्याशित रूप से ऑनलाइन या टेलीफोन के जरिए संपर्क करें और आपकी व्यक्तिगत सूचना की जानकारी मांगे तो संदेह करें। यहां तक कि ज्ञात पते के साथ संचार करते हुए ईमेल के जरिए व्यक्तिगत सूचना के साझाकरण को न्यूनतम रखें।
- याद रखें कि कोई भी वित्तीय संस्था आपसे ईमेल या फोन कर गोपनीय सूचना की मांग नहीं करती है जिसके बारे में उसे पहले से ही पता रहता है।
- मानकर चलें कि किसी ऐसे बैंक से अगर सूचना के लिए अनुरोध किया जाता है जहां आपका कभी कोई खाता नहीं रहा है तो यह स्कैम है।
- व्यक्तिगत सूचना प्रदान करने से पूर्व संदिग्ध नजर आने वाले ईमेल या किसी पॉप अप बाक्स की मान्यता का सत्यापन करें। ईमेल पते पर सावधानी से ध्यान दें।

कर्मियों को प्रशिक्षण देना

- मानवीय त्रुटि जोकि ग्राहकों के डेटा को असुरक्षित कर सकती है उसे कम से कम करने हेतु अपने कर्मियों को जवाबदेही और रणनीतियों के प्रति शिक्षित करें। इसका मतलब है कि उन्हें निम्नलिखित के लिए सुझाव दें:
  - ग्राहकों के डेटा तक उनकी पहुंच और प्रसारण के एक्सेस को सिर्फ वहीं तक सीमित करें जो उनके कार्य दायित्व के निर्वहन के लिए आवश्यक हो,
  - मजबूत पासवर्ड, टू-फैक्टर सत्यापन, सॉफ्टवेयर को अपडेट रखते हुए और संदिग्ध लिंक पर क्लिक नहीं करते हुए ग्राहकों के डेटा से निपटने वाले डिवाइस और खातों पर मजबूत सुरक्षा अभ्यास बरतें, और
  - अपने संगठन के तकनीकी कर्मी और/अथवा उच्च प्रबंधन को किसी वास्तविक आंतरिक या बाह्य खतरे या डेटा दुरुपयोग की रिपोर्ट करें।
- यह सुनिश्चित करें कि आपके कर्मी समझते हैं और उन्होंने आपके संगठन के डेटा सुरक्षा और सुरक्षा नीतियों के प्रति समर्पित रहने वाले दस्तावेज पर हस्ताक्षर कर रखा है ताकि वे इसका उल्लंघन नहीं करें और वे ग्राहकों से निपटते समय सहज रहें और उनसे असुरक्षित अंदाज में बातचीत नहीं करें।

ग्राहकों को अधिसूचित करना

- अपने संगठन के नियामक माहौल को समझे जब बात ग्राहकों के डेटा के उल्लंघन से निपटने की बात हो ताकि घटना होने पर आप अनुपालन के लिए तैयार रहें।
- जब आपके संगठन को पता चले कि ग्राहक की संवेदनशील सूचना के अनाधिकृत एक्सेस की घटना हुई है तो इसकी जांच कर प्रमुखता से तय करें इस घटना के कारण सूचना के अब तक दुरुपयोग होने और भविष्य में होने की संभावना क्या है। अधिसूचना के श्रेष्ठ अभ्यास का पालन करें और प्रभावित ग्राहक (ग्राहकों) को यथाशीघ्र इससे अधिसूचित करें:
  - जिस सूचना की सेंधमारी हुई उसकी सूचना और घटना का सामान्य विवरण,
  - सूचना और सहायता के लिए एक टेलीफोन नंबर,
  - अगले 12 से 24 महीने तक "सजग रहने का" रीमाइंडर,
  - इस बात की अनुशंसा कि संदिग्ध चोरी पहचान की घटना की प्रमुखता से रिपोर्ट करें,
  - सूचना का आगे और अनाधिकृत एक्सेस या उपयोग न हो इसके लिए वित्त संस्थान द्वारा उठाए कदमों के बारे में एक सामान्य विवरण,
  - क्रेडिट रिपोर्टिंग एजेंसियों की संपर्क सूचना और
  - आपके संगठन को जिन नियमों का पालन करना चाहिए, उनके लिए अन्य आवश्यक जानकारी।