छोटे संगठनों के लिएसाइबर सुरक्षा

सीआईएसओ चेकलिस्ट: आपके ग्राहकों की सुरक्षा करना

व्यक्तिगत स्तर की डेटा की सुरक्षा पर ग्राहकों और कर्मचारियों को सुझाव देना

☐ **उनके डेटा की बेहतर सुरक्षा के लिए कर्मचारियों और ग्राहकों को पालन करने के लिए निम्नलिखित व्यक्तिगत दिशानिर्देशों प्रदान करें:**

- सभी व्यक्तिगत और व्यावसायिक उपकरणों पर शक्तिशाली पासवर्ड का उपयोग करें और पासवर्ड मैनेजर का उपयोग करने पर विचार करें।
- सभी कंप्यूटर और मोबाइल उपकरणों पर ऑपरेटिंग सिस्टम और अन्य सॉफ्टवेयर और एप्लिकेशन को अप टू डेट रखें।
- एंटी-वायरस, एंटी-मालवेयर और एंटी-रैंसमवेयर सॉफ़्टवेयर इंस्टॉल करें जो दुर्भावनापूर्ण प्रोग्राम को रोकता है, उनका पता लगाता है और हटाता है।
- अपने कंप्यूटर पर अनधिकृत पहुँच को रोकने के लिए फायरवॉल प्रोग्राम का उपयोग करें।
- केवल प्रतिष्ठित कंपनियों के सिक्योरिटी प्रोडक्ट का उपयोग करें। कंप्यूटर और उपभोक्ता प्रकाशनों से समीक्षाओं को पढ़ें और अपने कंप्यूटर या ऑपरेटिंग सिस्टम निर्माता के साथ परामर्श करने पर विचार करें।
- संवदेनशील जानकारी के प्रति सावधान रहें। अनएन्क्रिप्टेड ईमेल पर बैंक खाते का पासवर्ड या अन्य संवेदनशील वित्तीय अकाउंट डेटा न भेजें।
- इस बारे में स्मार्ट बनें कि संवेदनशील व्यक्तिगत जानकारी वाले बैंकिंग या अन्य संचार के लिए आप इंटरनेट से कहां और कैसे कनेक्ट होते हैं।
- ईमेल अटैचमेंट को तुरंत न खोलें या अनचाहे या संदिग्ध दिखने वाले ईमेल में लिंक पर क्लिक ना करें। रुकें। सोचें। क्लिक करें।
- यदि कोई व्यक्ति आपसे ऑनलाइन या टेलफोन से अनपेक्षित रूप से संपर्क करता है और आपकी व्यक्तिगत जानकारी मांगता है तो संदेह करें। यहां तक कि जब परिचित पतों के साथ संपर्क करते हैं, तो भी ईमेल के माध्यम से व्यक्तिगत जानकारी को कम से कम साझा करने का प्रयास करें।
- याद रखें कि कोई भी वित्तीय संस्थान आपको ईमेल या कॉल नहीं करेगा और गोपनीय जानकारी का अनुरोध नहीं करेगा जो आपके बारे में उसके पास पहले से मौजूद है।
- मान लें कि आपने जिस बैंक में कभी खाता नहीं खोला है, उससे जानकारी के लिए अनुरोध एक धोखाधड़ी है।
- व्यक्तिगत जानकारी प्रदान करने से पहले एक संदिग्ध दिखने वाले ईमेल या पॉप-अप बॉक्स की वैधता की पुष्टि करें। ईमेल पते पर सावधानी से ध्यान दें।

खातों का प्रबंध

☐ **यह आवश्यक है कि ग्राहक आपकी सेवाओं में लॉग इन करने के लिए शक्तिशाली 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।**

☐ **वास्तविक ग्राहकों को प्रमाणित करने और धोखाधड़ी के अवसर को कम करने के लिए तत्काल सत्यापन, वास्तविक समय के सत्यापन, परीक्षण जमा सत्यापन, पहचान सत्यापन, और/ या आउट ऑफ वॉलेट प्रश्नों का उपयोग करें।**

☐ **अपनी सेवाओं में लॉग इन करते समय ग्राहकों के लिए ऑफ़र या आदर्श रूप से, दो-कारक के प्रमाणीकरण की आवश्यकता होती है।**

☐ **धोखाधड़ी के संकेतों के लिए उपयोगकर्ता खातों की नियमित जांच करें।**

डेटा की सुरक्षा करना

☐ **इस बात पर विचार करें कि आपकी सेवाओं को करने के लिए आपके संगठन को कौन सा ग्राहक डेटा एकत्र करना चाहिए, और उससे आगे जाने वाले किसी भी ग्राहक डेटा को इकट्ठा करने से सावधान रहना चाहिए।**

☐ **डेटा बनाए रखने वाली नीतियों को स्थापित करें और वितरित करें। जब जरूरत ना हो तो ग्राहक के डेटा को नष्ट कर दें।**

☐ **पारगमन और स्थायी ग्राहक डेटा को एन्क्रिप्ट करें।**

☐ **यह स्पष्ट करने के लिए डेटा सुरक्षा नीतियों को लागू करें कि डेटा ट्रांसफर के कौन से तरीकों को मंजूर बनाम प्रतिबंधित किया गया है या उल्लेख करें कि जब ग्राहक डेटा से निपटने की बात आती है तो सभी कर्मचारियों के लिए क्या स्वीकार्य है। सुनिश्चित करें कि इन नीतियों को दस्तावेजीकृत किया गया है, सभी कर्मचारियों को बताया गया, लागू किया गया है, और समय-समय पर समीक्षा और अपडेट किया जाता है।**

सार्वजनिक वेब एप्लीकेशंस को सुरक्षित करना

- ☐ अपने संगठन के सार्वजनिक उपयोग वाले वेब एप्लिकेशन(एप्लिकेशनों) पर HTTPS लागू करें और सभी HTTP ट्रैफ़िक को HTTPS में पुनर्निर्देशित करें।
- ☐ अपनी वेबसाइट(वेबसाइटों) पर सामग्री सुरक्षा नीति का उपयोग करें।
- ☐ अपनी वेबसाइट(वेबसाइटों) पर पब्लिक की पिनिंग सक्षम करें।
- ☐ सुनिश्चित करें कि आपका सार्वजनिक उपोग वाला वेब एप्लिकेशन (एप्लिकेशंस) कभी भी ग्राहक की अत्यधिक संवेदनशील या महत्वपूर्ण जानकारी (जैसे पासवर्ड) को संग्रहीत करने के लिए कुकीज़ का उपयोग नहीं करता है और कि कुकीज़ के लिए उनकी सतर्क समाप्ति की तारीखें हैं (जितनी जल्दी हो सके)।
- ☐ उस जानकारी को एन्क्रिप्ट करने पर विचार करें जो आपके द्वारा उपयोग की जाने वाली कुकीज़ में संग्रहीत है।
- ☐ वर्ष में कम से कम एक बार अपने सार्वजनिक-उपयोग वाले वेब एप्लिकेशन (एप्लिकेशनों) की सुरक्षा का आकलन करने के लिए एक पेनीट्रेशन टेस्टिंग सर्विस को हायर करने पर विचार करें।

कर्मचारियों को प्रशिक्षित करना

- ☐ ऐसी मानवीय त्रुटि को कम करने के लिए अपने कर्मचारियों की जवाबदेही और रणनीति सिखाएं जो ग्राहक के डेटा को उजागर कर सकती है। इसका मतलब है कि उन्हें निम्नलिखित के लिए सुझाव दें:
  - ग्राहक डेटा तक उनकी पहुँच और संचार को वहां तक सीमित करें, जितना उनके कार्य को करने के लिए आवश्यक है,
  - शक्तिशाली पासवर्ड का उपयोग करके, दो कारकों वाले प्रमाणीकरण को सक्षम करके, सॉफ्टवेयर को अपडेट रखकर, और संदिग्ध लिंक पर क्लिक न करके उन सभी डिवाइसों और खातों पर शक्तिशाली सुरक्षा व्यवहार बनाए रखें जो ग्राहक के डेटा के साथ डील करते हैं, और
  - किसी भी संभावित आंतरिक या बाहरी सुरक्षा घटनाओं, खतरों या ग्राहक डेटा से छेड़छाड़ की सूचना अपने संगठन के तकनीकी कर्मचारियों और/ या उच्च प्रबंधन को दें।
- ☐ सुनिश्चित करें कि आपके कर्मचारी आपके संगठन के डेटा की सुरक्षा और अपने कर्मचारियों को समझते हैं और उसका पालन करने के लिए दस्तावेजों पर हस्ताक्षर किए हैं।

ग्राहकों को सूचित करना

- ☐ जब ग्राहक डेटा के उल्लंघनों को संभालने की बात आती है तो यह सुनिश्चित करने के लिए कि जब घटनाएं घटती हैं, तो आप उसका अनुपालन करने के लिए तैयार हैं, आप अपने संगठन के विनियामक वातावरण के बारे में जागरूकता का निर्माण करें।
- ☐ जब आपके संगठन को ग्राहक की संवेदनशील जानकारी तक अनधिकृत पहुंच की घटना के बारे में पता चलता है तो, तो इस संभावना की तुरंत जांच कर लें कि जानकारी का दुरुपयोग हुआ है या नहीं। अधिसूचना की सर्वोत्तम प्रथाओं का पालन करें और प्रभावित ग्राहक(ग्राहकों) को जल्द से जल्द सूचित करें:
  - घटना और जानकारी का सामान्य विवरण जिसका उल्लंघन हुआ था;
  - अधिक जानकारी और सहायता के लिए एक टेलीफोन नंबर;
  - अगले 12 से 24 महीनों में "सतर्क रहने के लिए" एक अनुस्मारक;
  - एक सिफारिश कि संदिग्ध पहचान की चोरी की घटनाओं को तुरंत सूचित किया जाए;
  - वित्तीय संस्था द्वारा जानकारी तक आगे अनधिकृत पहुंच या उपयोग से बचाने के लिए उठाए गए कदमों का एक सामान्य विवरण;
  - क्रेडिट रिपोर्टिंग एजेंसियों के लिए संपर्क जानकारी; और
  - आपके संगठन को जिन नियमों का पालन करना चाहिए, उनके लिए अन्य आवश्यक जानकारी।

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America®