फ़िशिंग मेल एडवाइजरी

क्या करें

1. सतर्क और संदेहवादी रहें : हमेशा सावधानी से ईमेल खोलें, खासकर अज्ञात या संदिग्ध स्रोतों से।

2. प्रेषक को सत्यापित करें : प्रेषक के ईमेल पते की जांच करें और सुनिश्चित करें कि यह उस संगठन की आधिकारिक संपर्क जानकारी से मेल खाता है जिसका वे प्रतिनिधित्व करने का दावा करते हैं।

3. वर्तनी और व्याकरण की त्रुटियों की जाँच करें : फ़िशिंग ईमेल में अक्सर टाइपिंग संबंधी व्याकरण संबंधी गलतियाँ या अजीब भाषा होती है।

4. क्लिक करने से पहले होवर करें : वास्तविक यूआरएल देखने के लिए ईमेल में किसी भी लिंक पर अपने माउस को होवर करें। सुनिश्चित करें कि यूआरएल ईमेल में प्रदर्शित यूआरएल से मेल खाता है और एक भ्रामक लिंक नहीं है।

5. सॉफ़्टवेयर को अद्यतन रखें : ज्ञात कमजोरियों से बचाने के लिए अपने ईमेल क्लाइंट ,वेब ब्राउज़र और ऑपरेटिंग सिस्टम को नियमित रूप से अपडेट करें।

6. मजबूत, यूनिक पासवर्ड का उपयोग करें : मजबूत पासवर्ड बनाएं और उन्हें सुरक्षित रूप से संग्रहीत करने के लिए पासवर्ड मैनेजर का उपयोग करें।

7. टू-फैक्टर प्रमाणीकरण (2 एफए) इनेबल करें : अपने ईमेल खाते के लिए सुरक्षा का एक अतिरिक्त स्तर प्रदान करने के लिए जब भी संभव हो 2 एफए इनेबल करें।

8. स्वयं को शिक्षित करें : नवीनतम फ़िशिंग तकनीकों और घोटालों को बेहतर ढंग से पहचानने और उनसे बचने के लिए उनके बारे में सतर्क रहें।

क्या न करें

1. संदिग्ध लिंक पर क्लिक न करें : ईमेल में दिए गए लिंक पर तब तक क्लिक करने से बचें जब तक आप उनकी प्रामाणिकता के बारे में आश्वस्त न हों।

2. अज्ञात स्रोतों से अटैचमेंट डाउनलोड न करें : अटैचमेंट डाउनलोड करते समय सावधान रहें ,खासकर यदि वे अप्रत्याशित हों या अपरिचित प्रेषकों से हों।

3. व्यक्तिगत जानकारी प्रदान न करें : वैध संगठन कभी भी ईमेल के माध्यम से व्यक्तिगत या वित्तीय जानकारी नहीं मांगेंगे। ईमेल के माध्यम से पासवर्ड, क्रेडिट कार्ड विवरण या सामाजिक सुरक्षा नंबर जैसे संवेदनशील डेटा को शेयर करने से बचें।

4. अत्यावश्यक या धमकी भरे संदेशों पर भरोसा न करें : फ़िशिंग ईमेल अक्सर पीड़ितों को धोखा देने के लिए अत्यावश्यक या धमकी भरी भाषा का उपयोग करते हैं। ऐसे संदेशों पर संदेह करें और अन्य माध्यमों से उनकी वैधता की पुष्टि करें।

साइबर स्वच्छता कदम

1. मजबूत ईमेल फ़िल्टर का उपयोग करें : मजबूत स्पैम फ़िल्टर इनेबल करें और संदिग्ध ईमेल को स्पैम फ़ोल्डर में चिह्नित करने या डायवर्ट करने के लिए उन्हें कॉन्फ़िगर करें।

2. एंटीवायरस और एंटी-मैलवेयर सॉफ़्टवेयर इंस्टॉल करें : फ़िशिंग प्रयासों का पता लगाने और उन्हें रोकने के लिए अपने कंप्यूटर को अद्यतन सुरक्षा सॉफ़्टवेयर से सुरक्षित रखें।

3. नियमित रूप से अपने डेटा का बैकअप लें : किसी भी संभावित फ़िशिंग खतरे के प्रभाव को कम करने के लिए महत्वपूर्ण फ़ाइलों और डेटा का नियमित बैकअप बनाएं।

4. फ़िशिंग प्रयासों की रिपोर्ट करें : यदि आपको कोई फ़िशिंग ईमेल प्राप्त होता है ,तो अपने ईमेल प्रदाता और संबंधित अधिकारियों को इसकी रिपोर्ट करें ताकि उचित कार्रवाई की जा सके।

5. सुरक्षा की सर्वोत्तम पद्धतियों के बारे में अपडेट रहें : साइबर सुरक्षा की सर्वोत्तम पद्धतियों के बारे में खुद को लगातार शिक्षित करें और अपनी ऑनलाइन सुरक्षा बढ़ाने के लिए नवीनतम अनुशंसाओं का पालन करें।