**इंटरनेट आणि ईमेल फसवणूक (फिशिंग)**

ऑनलाइन बँकिंग आणि शॉपिंग सारख्या सेवांनी इंटरनेटने आपले जीवन सोयिस्कर बनवले आहे, परंतु त्याखाली नेहमीच सुरक्षा जोखिम असते ज्यांचा आपल्या बँकिंगचे तपशील मिळवण्यासाठी गुन्हेगार इंटरनेटचा दुरुपयोग करतील आणि आपल्या कष्टाची कमाई चोरण्यासाठी याचा वापर करतील.

एखाद्या इलेक्ट्रॉनिक संभाषणामध्ये एक विश्वसनीय संस्था असल्याचे सोंग घेऊन फसवणूक करणारे व्यक्ती युजरनेम, पासवर्ड्स, आणि इतर बँकिंगचे तपशीलांची माहिती मिळवण्याचा प्रयत्न करतात. अशा कृतीला “फिशिंग” म्हणतात.

फिशिंग सामान्यपणे ईमेल्स किंवा इंस्टंट मेसेजिंग द्वारे केले जातात आणि हे नेहमी वापरकर्त्यांना एक खोट्या वेबसाइटवर तपशील प्रविष्ट करण्याची सूचना देतात जी दिसण्यास आणि अनुभवाने जवळजवळ खऱ्या वेबसाइटसारखीच असते.

खाते क्रमांक, लॉगइन आयडीस लॉगइन आणि ट्रांजेक्शन पासवर्ड, मोबाइल क्रमांक, पत्ता, डेबिट कार्डच्या ग्रिड व्हॅल्यू, क्रेडिट कार्ड क्रमांक, सीव्हीव्ही क्रमांक, पॅन, जन्मतारीख, आईचे लग्नाआधीचे नाव, पासपोर्ट क्रमांक इत्यादी सारखे ग्राहकांचे तपशील मिळवण्यासाठी फिशर्स ईमेल फिशिंग, विशिंग (वॉइस फिशिंग) आणि स्मिशिंग (एसएमएस फिशिंग) एकत्र करून वापरतात.

**फिशिंगचा प्रयत्न कसा ओळखाल?**

a. गोपनीय बँकिंग तपशील विचारणाऱ्या वेबसाइट्स किंवा अनोळखी व्यक्तीकडून आलेले अनपेक्षित ईमेल्स, कॉल्स

b. सुरक्षा कारणांमुळे तातडीने कृती करण्यास सांगणारे मेसेजेस

c. परिचित वेबसाइट्स ॲक्सेस करण्यासाठी ईमेलमध्ये प्राप्त झालेल्या लिंक

d. वेबसाइटची विश्वासार्हता तपासण्यासाठी, कर्सर लिंकवर फिरवा किंवा https:// तपासा ज्यात "s" म्हणजे 'सुरक्षित साइट'

**फिशिंगच्या हल्ल्यांचे बळी पडू नये यासाठी टप्पे**

a. फिशिंग ईमेल्सना कधीच उत्तर देऊ नका, आणि कोणत्याही लिंकवर क्लिक करू नका.

b. ईमेल द्वारे किंवा या ईमेल्समधील कोणत्याही लिंक्सवर तुमचा पिन किंवा खात्याचे तपशील यासारखे तुमचे वैयक्तिक तपशील कधीच देऊ नका.

c. नेहमी ॲड्रेसमध्ये बँकांची वेबसाइट टाईप करा.

d. स्पाम ईमेल्स ताबडतोब डीलीट करा. मेलिंग लिस्टमधून तुमचा ईमेल ॲड्रेस काढण्याची विनंती सुद्धा फसवणूक करणाऱ्यांना खात्री करून देईल कि तुमचे ईमेल अकाउंट चालू आहे, आणि तुमच्यावर अधिक हल्ले होण्याचा धोका असू शकतो.

e. मेसेज कोणी पाठवला आहे हे कळल्याशिवाय एखादी ईमेल अटॅचमेंट कधीच उघडू नका.

f. अगदी नवीन ब्राउजर्स वापरा.

तुम्हाला अशी कोणतीही फिशिंग हालचाल आढळल्यास ताबडतोब तुमचा पासवर्ड बदला आणि कोणताही उशीर न करता तुमच्या शाखेत तक्रार करा.

तुमची जागरूकता फिशिंगच्या हल्ल्यांचा बळी पडण्यापासून वाचण्याची चावी आहे.

---

**सायबर फसवणूक झाल्यास तात्काळ तक्रार करा:**

सायबर फसवणुकीचा बळी पडल्यास त्वरित कारवाई करा. राष्ट्रीय सायबर गुन्हे हेल्पलाइन 1930 वर संपर्क साधा आणि https://cybercrime.gov.in/ या संकेतस्थळावर तक्रार नोंदवा. तसेच, तुम्ही Sancharsaathi Portal वरूनही तक्रार दाखल करू शकता. वेळेवर तक्रार केल्यास पुढील फसवणूक टाळता येते आणि इतरांनाही सतर्क करता येते.