



सायबर जागरूकतेची कथा:

एका सामान्य माणसाचा प्रवास आणि सुरक्षित इंटरनेट दिन

डिजिटल युगात, जिथे एका क्लिकवर संधी आणि धोक्याचे दरवाजे उघडू शकतात, राजूचा रोजच्या वापरकर्त्यापासून सायबर संरक्षक होण्यापर्यंतचा प्रवास दाखवतो की तुम्ही तुमचे ऑनलाइन जग कसे सुरक्षित करू शकता



राजू एक सामान्य माणूस होता, जो दिल्लीत एका छोट्याशा वस्तीत आपल्या कुटुंबासोबत राहत होता. तो एका छोट्या दुकानात काम करत असे. त्याचे जीवन अगदी साधे होते. दररोज तो लवकर उठत असे, कामावर जात असे, दिवसभर दुकानात घालवत असे आणि संध्याकाळी घरी परतून कुटुंबासोबत वेळ घालवत असे. तो जास्त इंटरनेट वापर करत नव्हता, पण कधीकधी सोशल मीडिया चेक करत असे आणि ऑनलाइन बँकिंग वापरत असे. तो फक्त इतकेच जाणत होता की तो ऑनलाइन कामे करू शकतो, पण तंत्रज्ञानात फारसा पारंगत नव्हता. राजूने इंटरनेटच्या धोक्यांबद्दल कधीच जास्त विचार केला नव्हता - पण एक दिवस सगळं बदललं.

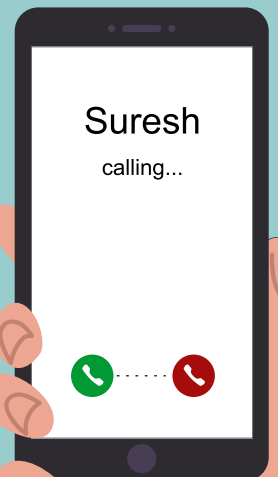
राजूचा सायबर प्रवास - एका मित्राची जलद विचार करण्याची कल्पना

एके दिवशी राजू घरी बसला होता, तेव्हा त्याला एक अज्ञात नंबरवरून WhatsApp मेसेज आला. त्या मेसेजमध्ये एक लिंक होती आणि ते मेसेज असं होतं:

“अत्यावश्यक: तुमच्या बँक खात्यात मोठी रक्कम जमा झाली आहे. कृपया तपशील अपडेट करण्यासाठी येथे क्लिक करा आणि व्यवहाराची पडताळणी करा.”

हा मेसेज त्याच्या बँकेकडून आल्यासारखा वाटत होता आणि त्याच्या टोनमधील गंभीरता पाहून राजू थांबला. तो संशयास्पद वाटत होता, पण राजूने अलीकडेच काही मोठे व्यवहार केले होते आणि त्याला वाटलं की हा मेसेज खरा असू शकतो.

अनिश्चित असूनही, राजू त्या लिंकवर क्लिक करणार होता, तेव्हाच त्याच्या मित्र सुरेशने त्याला फोन केला, जो जवळच राहत होता.



राजूने सुरेशला त्या लिंकबद्दल सांगितल्यावर, सुरेश म्हणाला -

अरे, राजू! मला अशाच प्रकारचा मेसेज आज आला होता. त्या लिंकवर क्लिक करू नकोस! हा एक स्कॅम आहे, ". "मलाही असंच मेसेज आला होता, आणि तपासल्यावर कळलं की हा फिशिंग हल्ल्याचा प्रयत्न आहे ..



राजू गोंधळलेला होता.

फिशिंग?
ते काय असतं?



फिशिंग म्हणजे जेव्हा स्कॅमर्स तुमची वैयक्तिक माहिती, जसे की बँक तपशील किंवा पासवर्ड्स, चुकीच्या मार्गाने मिळवण्याचा प्रयत्न करतात. ते खऱ्यासारखे दिसणारे लिंक किंवा मेसेज वापरतात. जर तुम्ही त्यावर क्लिक केलं, तर ते तुमची माहिती चोरून तुमचं बँक खातं रिकामं करू शकतात.



Dear Customer your
Credit Card PIN has
been redet to 9999.
[Click here to activate](#)

राजूला त्वरित एक दिलासा मिळाला, पण त्याचबरोबर त्याला हे जाणवले की तो जवळजवळ फसवला गेला होता.



सुरेशने पुढे सांगितलं

धन्यवाद, सुरेश, मला वाचवण्याबद्दल. मला फिशिंगबद्दल काहीच माहीत नव्हता.

डिजिटल अरेस्ट? मला काहीच कल्पना नव्हती. मला अज्ञात नंबरवरून कॉल येत होते आणि मी ते उचलणार होतो.



पण इतकंच नाही. डिजिटल अरेस्ट असंही काहीतरी आहे. यात स्कॅमर्स तुमच्याशी फोनद्वारे संपर्क साधतात आणि पोलिस किंवा कायदा अंमलबजावणी अधिकारी असल्याचे बतावणी करतात. ते सांगतात की तुमच्या नावावर ड्रग्सच्या पाकिटांसह एक पार्सल सापडले आहे आणि तुम्ही डिजिटल अरेस्टमध्ये आहात. नंतर ते तुम्हाला मोठी रक्कम भरण्यास सांगतात."



असे कॉल उचलू नका !

Thank you for your support!
Now we are giving higher returns
for your investments
click the link, invest small amount
and gain maximum amount of
returns at very low risk.



आणि नंतर गुंतवणूक फसवणूक आहेत. स्कॅमर्स अनेकदा 'अविश्वसनीय' गुंतवणूक संधींबद्दल खोटे मेसेज पाठवतात, ज्यात कमी जोखमीसह उच्च परताव्याचे आश्वासन दिले जाते. ते तुम्हाला फसवणूक योजनांमध्ये पैसे टाकण्यासाठी प्रलोभन देतात. हा फक्त पैसे चोरण्याचा आणखी एक मार्ग आहे.

म्हणजे ते माझे पैसे अनेक मार्गांनी चोरू शकतात, जसे की माझं बँक खातं हॅक करून, मला लॉक आउट करून किंवा गुंतवणूक संधींचे आश्वासन देऊन?

होय !!

म्हणूनच तुम्हाला अतिरिक्त सावधगिरी बाळगणे आवश्यक आहे. जे काही खूप चांगलं वाटतं त्याची नेहमी पडताळणी करा. जोपर्यंत तुम्हाला स्रोताची पूर्ण खात्री होत नाही, तोपर्यंत लिंकवर क्लिक करू नका किंवा वैयक्तिक तपशील सामायिक करू नका.

राजू आता परिस्थितीची गंभीरता पूर्णपणे समजून घेत होता.

तू मला वेळेवर कॉल केल्याबद्दल खरोखर आभारी आहे. मी जवळजवळ त्या लिंकवर क्लिक केलं असतं, आणि काय झालं असतं कोण जाणे!

काळजी करू नका, राजू, फक्त लक्षात ठेवा: जो कोणताही मेसेज वैयक्तिक माहिती मागतो किंवा खूप चांगला वाटतो, त्याची नेहमी पडताळणी करा. जर शंका वाटत असेल, तर थेट सेवा किंवा बँकेशी त्यांच्या अधिकृत संपर्क माध्यमातून संपर्क साधा.

राजू त्याच्या मित्राच्या वेळेवरच्या हस्तक्षेपाबद्दल आभारी होता, पण त्याच वेळी डिजिटल जगातील वाढत्या धोक्यांबद्दल अधिक जागरूक झाला होता. त्याने स्वतःशी वचन दिले की पुढे तो अधिक सावध राहील, विशेषतः जेव्हा संशयास्पद किंवा अवास्तव वाटणारी ईमेल, मेसेज किंवा ऑफर्स येतात तेव्हा.

सुरक्षित इंटरनेट दिनाबद्दल शिकणे

सुरेशने राजूला "सुरक्षित इंटरनेट दिन" बद्दलही माहिती दिली, जो जवळपास येत होता. सुरेश म्हणाला, "सुरक्षित इंटरनेट दिन हा एक वार्षिक कार्यक्रम आहे जो संपूर्ण जगात ऑनलाइन सुरक्षा आणि डिजिटल चांगुलपणाबद्दल जागरूकता वाढवण्यासाठी साजरा केला जातो.

सायबर हायजीन म्हणजे अशा पद्धतींचा संच, ज्यामुळे व्यक्ती त्यांच्या उपकरणांची आणि वैयक्तिक माहितीची सुरक्षितता राखू शकतात. जसे तुम्ही रोगांपासून बचाव करण्यासाठी हात धुतात, तसेच सायबर हायजीनमध्ये तुमच्या ऑनलाइन सवयी साफ करून तुमच्या डिजिटल जीवनाचे संरक्षण करणे समाविष्ट आहे. चांगली सायबर हायजीन फिशिंग, हॅकिंग आणि मालवेअरपासून तुमच्या वैयक्तिक खाती आणि उपकरणांना बचावू शकते.

राजूने शिकलं की सायबर हायजीनमध्ये पुढील गोष्टींचा समावेश होतो:



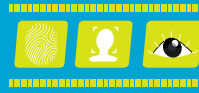
मजबूत, अद्वितीय पासवर्ड सेट करणे:

"123456" किंवा "password" सारखे सहज अंदाज लावता येणारे पासवर्ड वापरू नका. त्याऐवजी अक्षरे, संख्या आणि चिन्हे यांचा मिश्रण असलेले मजबूत पासवर्ड तयार करा.



दोन-चरणीय प्रमाणीकरण (2FA) सक्षम करणे:

2FA द्वारे तुमच्या ओळखीची पुष्टी करण्यासाठी दुसरा घटक आवश्यक असतो, जसे की तुमच्या फोनवर पाठवलेला कोड.



मजबूत स्क्रीन लॉक आणि बायोमेट्रिक प्रमाणीकरण सेट करा:

आपल्या डिव्हाइसला अधिक सुरक्षित बनवण्यासाठी बायोमेट्रिक्स (अंगठ्याचा ठसा किंवा चेहऱ्याची ओळख) किंवा एक मजबूत पिन/पासवर्ड वापरा.



फक्त विश्वासाई स्रोतांवरून ॲप्स डाउनलोड करा:

- फक्त अधिकृत ॲप स्टोअर्सवरून ॲप्स डाउनलोड करा. अनधिकृत स्रोतांवरील ॲप्समध्ये मालवेअर असू शकते किंवा ते आपली माहिती चोरण्यासाठी डिझाइन केलेले असू शकतात.



सुरक्षित कनेक्शन वापरणे:

सार्वजनिक Wi-Fi वापरताना, ऑनलाइन बँकिंग सारख्या संवेदनशील खात्यांमध्ये प्रवेश करू नका.



संशयास्पद लिंक टाळणे:

कोणत्याही लिंकवर क्लिक करण्यापूर्वी किंवा अटॅचमेंट डाउनलोड करण्यापूर्वी ईमेलचा स्रोत नेहमी पडताळा.



सॉफ्टवेअर आणि ॲप्स नियमितपणे अपडेट करणे:

नियमित अपडेट्सद्वारे सुरक्षा कमकुवतता दूर केल्या जातात, ज्याचा वापर वाईट लोक करू शकतात.

Report cyber frauds at

1930



www.cybercrime.gov.in

Supported by

