इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

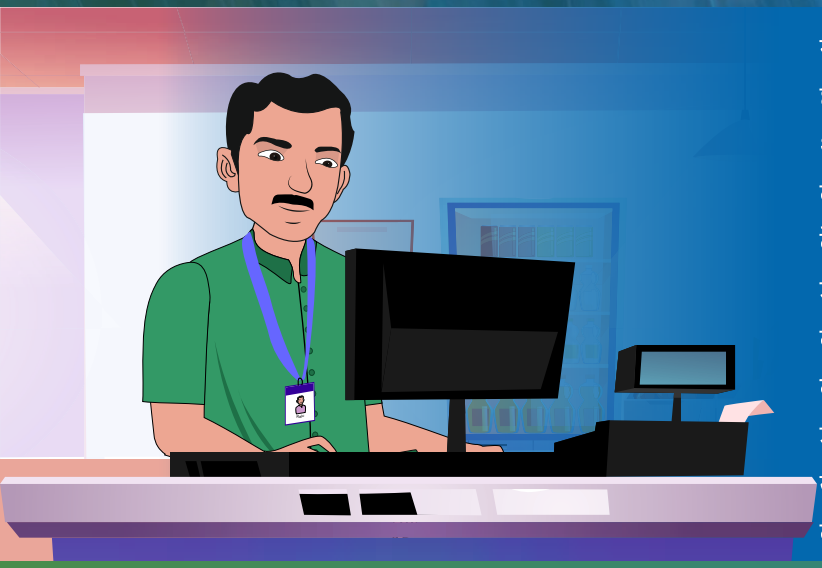
एन आई सी National Informatics Centre

सी डैक CDAC

साइबर जागरूकता कहानी :

एक आम आदमी का सफर और सुरक्षित इंटरनेट दिवस

"एक डिजिटल युग में सिर्फ एक क्लिक से अवसरों के अथवा खतरों के दरवाजे खुल सकते हैं,राजू की यात्रा एक सामान्य इन्टरनेट उपयोगकर्ता से लेकर साइबर रक्षक तक यह दिखाती है कि आप अपने ऑनलाइन संसार को कैसे सुरक्षित कर सकते हैं— आप भी यह यात्रा शुरू करें इस सुरक्षित इंटरनेट दिवस से।"



राजू एक सामान्य आदमी था जो अपनी परिवार के साथ दिल्ली के एक छोटे से मोहल्ले में रहता था। वह एक छोटे से दुकान पर काम करता था, और उसकी जिंदगी सादी थी। वह हर दिन सुबह जल्दी उठता, काम पर जाता, पूरे दिन दुकान पर काम करता और फिर अपने परिवार के साथ समय बिताने के लिए घर लौटता। जबकि वह इंटरनेट का ज्यादा उपयोग नहीं करता था, वह कभी-कभी सोशल मीडिया चेक करता और ऑनलाइन बैंकिंग का उपयोग करता था। उसे इन्टरनेट बस इतना ही पता था कि वह अपना काम चला सके, लेकिन वह बहुत ज्यादा तकनीकी विशेषज्ञ नहीं था। राजू ने कभी इंटरनेट के उपयोग के खतरों के बारे में ज्यादा नहीं सोचा—यहाँ तक कि एक दिन, जब सब कुछ बदल गया।

राजू की साइबर यात्रा – एक दोस्त की तेज़ सोच

एक दिन, राजू घर पर बैठा था, जब उसे एक अज्ञात नंबर से WhatsApp संदेश मिला। संदेश में एक लिंक अटैच था और लिखा था:

ऐसा महसूस हो रहा था की यह संदेश उसके बैंक से आया है, किन्तु सन्देश में जो लिंक को तत्काल क्लिक करने की जल्दी दिखाई दे रही थी, उससे राजू थोड़ी देर के लिए रुक गया। यह संदिग्ध लग रहा था, लेकिन राजू ने हाल ही में कुछ बड़े लेन-देन किए थे और उसने सोचा कि शायद यह एक वास्तविक संदेश हो।

संदिग्ध होने के बावजूद भी राजू लिंक पर क्लिक करने ही वाला था कि तभी उसे अपने दोस्त सुरेश का फोन आया, जो पास ही रहता था।

राजू ने लिंक के बारे में सुरेश को बताया, तो सुरेश ने कहा -

“राजू! मुझे भी आज ऐसा ही एक संदेश मिला था खाता अपडेट्स के बारे में। उस लिंक पर क्लिक मत करना! यह एक धोखाधड़ी है," सुरेश ने चेतावनी दी। "मुझे भी वही संदेश मिला था, और जब मैंने इसे देखा, तो पता चला कि यह एक फ़िशिंग प्रयास है।"

राजू थोड़ा उलझन में था।

फ़िशिंग? वह क्या होता है?

फ़िशिंग तब होती है जब धोखेबाज आपको अपनी व्यक्तिगत जानकारी, जैसे कि आपके बैंक विवरण या पासवर्ड, देने के लिए बहकाते हैं, जबकि वे एक वैध सेवा के रूप में खुद को पेश करते हैं। वे नकली लिंक या संदेशों का इस्तेमाल करते हैं जो आधिकारिक लगते हैं। अगर आप इन पर क्लिक करते हैं, तो वे आपकी जानकारी चुराकर आपके बैंक खाते को खाली कर सकते हैं।

Dear Customer your Credit Card PIN has been redet to 9999. Click here to activate

राजू को तुरंत राहत का एहसास हुआ, लेकिन साथ ही उसे यह महसूस हुआ कि वह लगभग धोखे का शिकार हो सकता था।

“सुरेश। मुझे फ़िशिंग के बारे में तो पता ही नहीं था।”

सुरेश ने आगे बताया,

Unknown...

डिजिटल अरेस्ट? मुझे इसका तो कोई आइडिया नहीं था। मुझे अजनबी नंबरों से कॉल्स आ रहे थे और मैं उन्हें उठाने वाला था।

लेकिन यही सब कुछ नहीं है, एक और चीज़ होती है जिसे डिजिटल अरेस्ट कहते हैं। इसमें धोखेबाज आपको कॉल करके पुलिस या कानून प्रवर्तन अधिकारियों के रूप में खुद को पेश करते हैं और कहते हैं कि आपके नाम पर एक पार्सल मिला है जिसमें ड्रग्स के पैकेट्स हैं, और यह दावा करते हैं कि आप डिजिटल अरेस्ट में हैं। फिर धोखेबाज आपसे बड़ी रकम रुपये में मांगते हैं।”

ऐसी कॉल्स मत उठाओ !

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.

और फिर निवेश धोखाधड़ी भी होती है। धोखेबाज अक्सर 'अविश्वसनीय' निवेश अवसरों के बारे में झूठे संदेश भेजते हैं, जो कम जोखिम में उच्च लाभ का वादा करते हैं। वे आपको पैसे ट्रांसफर करने या नकली योजनाओं में निवेश करने के लिए बहकाने की कोशिश करते हैं। यह बस एक और तरीका है जिससे वे आपका पैसा चुराते हैं।

तो, वे मेरा पैसा कई तरीकों से चुरा सकते हैं, जैसे मेरे बैंक खाते को हैक करके, मुझे लॉगिन से बाहर करके, या यहां तक कि मुझे झूठे निवेश अवसरों का बहाना बनाकर?

हाँ !!

इसीलिए आपको बहुत सतर्क रहना चाहिए। हमेशा उस चीज़ की पुष्टि करें जो सच होने के लिए बहुत अच्छी लगे। लिंक पर क्लिक न करें या व्यक्तिगत जानकारी न दें, जब तक आप स्रोत से पूरी तरह से आश्वस्त न हों।

राजू अब पूरी तरह से स्थिति की गंभीरता को समझ चुका था।

मैं सच में भाग्यशाली हूँ कि तुमने कॉल किया। मैं लगभग उस लिंक पर क्लिक करने वाला था, और कौन जानता क्या हो सकता था!

चिंता मत करो, राजू," सुरेश ने उसे ढांढस बंधाया। "बस याद रखो: हमेशा किसी भी संदेश की पुष्टि करो, जो व्यक्तिगत जानकारी मांगता है या जो ऑफर सच होने के लिए बहुत अच्छा लगता है। अगर संदेह हो, तो सीधे उस सेवा या बैंक से उनके आधिकारिक संपर्क पर संपर्क करो।

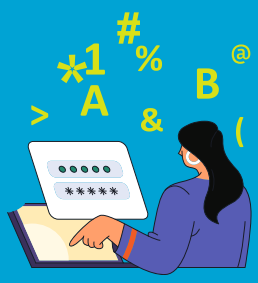
राजू ने अपने दोस्त के समय पर हस्तक्षेप के लिए आभार महसूस किया, लेकिन साथ ही उसे डिजिटल दुनिया में बढ़ते खतरों के प्रति अधिक जागरूकता भी हुई। उसने खुद से वादा किया कि वह आगे बढ़ते हुए बहुत सतर्क रहेगा, खासकर जब भी उसे संदिग्ध या अवास्तविक दिखने वाले ईमेल, संदेश, या ऑफर मिलेंगे।

सुरक्षित इंटरनेट दिवस के बारे में जानकारी प्राप्त करना :

सुरेश ने राजू को "सुरक्षित इंटरनेट दिवस" के बारे में भी जानकारी दी, सुरेश ने कहा, "सुरक्षित इंटरनेट दिवस एक वार्षिक कार्यक्रम है जो वैश्विक रूप से मनाया जाता है, जिसका उद्देश्य ऑनलाइन सुरक्षा और डिजिटल कल्याण के महत्व के बारे में जागरूकता बढ़ाना है।

साइबर स्वच्छता एक ऐसी प्रक्रिया है जो व्यक्तियों को उनके उपकरणों और व्यक्तिगत जानकारी की सुरक्षा बनाए रखने में मदद करती है। जैसे आप कीटाणुओं से बचने के लिए हाथ धोते हैं, वैसे ही साइबर स्वच्छता में आपकी ऑनलाइन आदतों को साफ करना शामिल है ताकि आप अपनी डिजिटल जिंदगी को सुरक्षित रख सकें। अच्छी साइबर स्वच्छता से फ़िशिंग, हैकिंग और मैलवेयर जैसी चीजों से आपके व्यक्तिगत खातों और उपकरणों को प्रभावित होने से रोका जा सकता है।

राजू ने सीखा कि साइबर स्वच्छता में कुछ प्रमुख अभ्यास शामिल हैं:



मजबूत, अद्वितीय पासवर्ड सेट करना:

"123456" या "password" जैसे आसान पासवर्ड का उपयोग करने से बचें। इसके बजाय, अक्षरों, संख्याओं और प्रतीकों का मिश्रण करके मजबूत पासवर्ड बनाएं।

दो-चरणीय प्रमाणिकता (2FA) को सक्षम करना:

2FA सुरक्षा की एक अतिरिक्त स्तर जोड़ता है, जिसमें आपको एक दूसरा पासवर्ड, जैसे आपके फोन पर भेजा गया कोड, के माध्यम से अपनी पहचान सत्यापित करनी होती है।

मजबूत स्क्रीन लॉक और बायोमेट्रिक प्रमाणीकरण सेट करें:

अपने डिवाइस को अधिक सुरक्षित बनाने के लिए बायोमेट्रिक्स (उंगलियों के निशान या चेहरा पहचान) या एक मजबूत पिन/पासवर्ड का उपयोग करें।

केवल विश्वसनीय स्रोतों से ऐप्स डाउनलोड करें:

केवल आधिकारिक ऐप स्टोर्स से ही ऐप्स डाउनलोड करें। अनौपचारिक स्रोतों से ऐप्स में मैलवेयर हो सकता है या वे आपका डेटा चुराने के लिए डिज़ाइन किए जा सकते हैं।

सुरक्षित कनेक्शन का उपयोग करना:

जब सार्वजनिक Wi-Fi का उपयोग करें, तो संवेदनशील खातों, जैसे ऑनलाइन बैंकिंग, तक पहुंचने से बचें।

संदिग्ध ईमेल और लिंक से बचना:

किसी भी लिंक पर क्लिक करने या अटैचमेंट डाउनलोड करने से पहले हमेशा ईमेल के स्रोत की पुष्टि करें।

सॉफ़्टवेयर और ऐप्स को नियमित रूप से अपडेट करना:

नियमित अपडेट सुरक्षा की खामियों को ठीक करते हैं जिन्हें बुरे लोग हेक कर सकते हैं।

Report cyber frauds at 1930 www.cybercrime.gov.in

Supported by

certin Enhancing Cyber Security in India | साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre | Digital India Power To Empower | myGov मेरी सरकार | रा.इ.सू.प्रौ.सं NIELIT