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

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

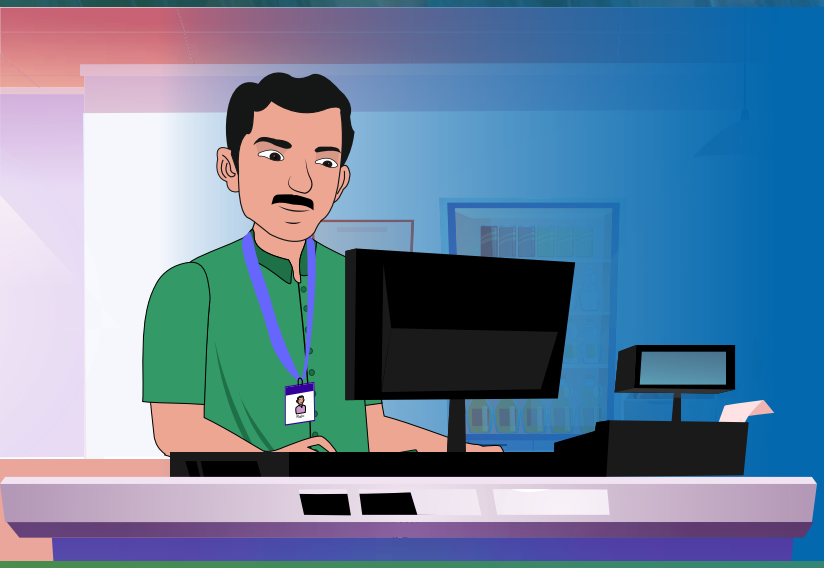
एन आई सी National Informatics Centre

सी डैक CDAC

একটি সাইবার সচেতনতা গল্প:

একটি সাধারণ মানুষের যাত্রা এবং সেফার ইন্টারনেট ডে

"ডিজিটাল যুগে, যেখানে একটি ক্লিকই সুযোগ বা বিপদের কারণ হতে পারে, রাজুর সাধারণ ব্যবহারকারী থেকে সাইবার সুরক্ষাকর্মী হয়ে ওঠার গল্প দেখায় কিভাবে আপনি নিজের অনলাইন জগৎ সুরক্ষিত রাখতে পারেন - এই নিরাপদ ইন্টারনেট দিবস থেকে শুরু করে।"



রাজু ছিলেন এক সাধারণ মানুষ, যিনি তার পরিবারসহ দিল্লির একটি ছোট পাড়ায় বাস করতেন। তিনি একটি ছোট দোকানে কাজ করতেন, এবং তার জীবন ছিল সহজ-সরল। প্রতিদিন, তিনি সকাল সকাল উঠে কাজে যেতেন, সারাদিন দোকানে কাটাতেন, এবং সন্ধ্যায় বাড়ি ফিরে পরিবারের সঙ্গে সময় কাটাতেন। যদিও তিনি বেশি ইন্টারনেট ব্যবহার করতেন না, মাঝে মাঝে সোশ্যাল মিডিয়া দেখতেন এবং অনলাইন ব্যাংকিং ব্যবহার করতেন। তিনি প্রয়োজনীয় জিনিসগুলো জানতেন, তবে খুব বেশি প্রযুক্তি-বোদ্ধা ছিলেন না। রাজু কখনো ইন্টারনেট ব্যবহারের ঝুঁকি নিয়ে বেশি ভাবেননি—যতক্ষণ না একদিন, যখন সবকিছু বদলে গেল।

রাজুর সাইবার যাত্রা – বন্ধুর তৎপর চিন্তা

একদিন, রাজু বাড়িতে বসে ছিল, তখন হঠাৎ সে একটি অচেনা নম্বর থেকে একটি হোয়াটসঅ্যাপ বার্তা পেল। বার্তাটির সাথে একটি লিঙ্ক সংযুক্ত ছিল এবং লেখা ছিল:

বার্তাটি তার ব্যাংকের পক্ষ থেকে এসেছে বলে মনে হচ্ছিল, আর এর জরুরি সুর রাজুকে চিন্তায় ফেলে দিল। এটি সন্দেহজনক লাগছিল, তবে রাজু সম্প্রতি কয়েকটি বড় লেনদেন করেছিল, তাই সে ভাবল এটি হয়তো আসল বার্তা হতে পারে।

দ্বিধান্বিত হলেও কৌতূহলী রাজু লিঙ্কে ক্লিক করতে যাচ্ছিল, ঠিক তখনই তার বন্ধু সুরেশ, যে কাছেই থাকত, তাকে ফোন করল।

রাজু যখন সুরেশকে বার্তা সম্পর্কে জানাল, তখন সুরেশ বলল -

"শোন রাজু! আমি আজ একই ধরনের একটি বার্তা পেয়েছি অ্যাকাউন্ট আপডেট সম্পর্কে। ওই লিঙ্কে ক্লিক কোরো না! এটা একটা প্রতারণা," । "আমিও একই বার্তা পেয়েছি, আর খোঁজ নিয়ে দেখলাম, এটা একটা ফিশিং প্রতারণা।"

রাজু বিভ্রান্ত হয়ে গেল।

ফিশিং?
সেটা আবার কী?

ফিশিং হল প্রতারকদের একটি কৌশল, যেখানে তারা আসল পরিষেবার ছদ্মবেশ ধরে তোমার ব্যক্তিগত তথ্য, যেমন ব্যাংকের বিবরণ বা পাসওয়ার্ড হাতিয়ে নেওয়ার চেষ্টা করে। তারা এমন ভুয়া লিঙ্ক বা বার্তা পাঠায়, যা দেখতে একেবারে আসল ব্যাংকের মতো মনে হয়। তুমি যদি ওগুলিতে ক্লিক করো, তাহলে তারা তোমার তথ্য চুরি করে অ্যাকাউন্টের সব টাকা তুলে নিতে পারে।

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

রাজু তখনই স্বস্তি পেল, কিন্তু একই সঙ্গে লজ্জিতও হল, কারণ সে প্রতারণার ফাঁদে পড়তে যাচ্ছিল।

তুই আমাকে বাঁচালি, সুরেশ! আমি তো ফিশিং সম্পর্কে কিছুই জানতাম না।

সুরেশ আবার বলল

ডিজিটাল অ্যারেস্ট? আমি তো এ বিষয়ে কিছুই জানতাম না! কয়েকদিন ধরে অচেনা নম্বর থেকে ফোন আসছিল, ভাবছিলাম ধরব কিনা।

কিন্তু ব্যাপারটা এতেই শেষ নয়। আরেকটা প্রতারণার কৌশল আছে, যাকে বলে ‘ডিজিটাল অ্যারেস্ট’। এতে প্রতারকরা তোমাকে ফোন করে নিজেদের পুলিশ বা আইনপ্রয়োগকারী সংস্থার কর্মকর্তা পরিচয় দিয়ে বলে, তোমার নামে একটি পার্সেল পাওয়া গেছে, যার মধ্যে মাদকদ্রব্য রয়েছে। এরপর তারা দাবি করে যে তুমি ডিজিটাল অ্যারেস্টের আওতায় পড়েছ এবং মুক্তির জন্য তোমাকে মোটা অঙ্কের টাকা দিতে হবে।

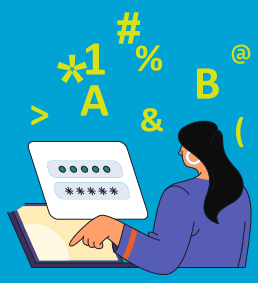
রাজু তার বন্ধুর সময়মতো হস্তক্ষেপের জন্য কৃতজ্ঞতা অনুভব করল, তবে একই সঙ্গে ডিজিটাল জগতের ক্রমবর্ধমান বিপদের ব্যাপারে আরও সচেতন হয়ে উঠল। সে প্রতিজ্ঞা করল যে, ভবিষ্যতে আরও বেশি সতর্ক থাকবে, বিশেষ করে ইমেইল, মেসেজ বা যে কোনো লোভনীয় অফারের ক্ষেত্রে।

সেফার ইন্টারনেট ডে সম্পর্কে জানা

সুরেশ রাজুকে "সেফার ইন্টারনেট ডে" সম্পর্কেও জানাল, যা আসন্ন ছিল। সুরেশ বলল, "সেফার ইন্টারনেট ডে একটি বার্ষিক ইভেন্ট, যা বিশ্বব্যাপী অনলাইন নিরাপত্তা ও ডিজিটাল সুস্থতা সম্পর্কে সচেতনতা বৃদ্ধির জন্য উদযাপিত হয়।

সাইবার হাইজিন হল এমন কিছু অভ্যাসের সমষ্টি, যা ব্যক্তিগত তথ্য ও ডিভাইস সুরক্ষিত রাখতে সাহায্য করে। যেমন আমরা জীবাণু থেকে রক্ষা পেতে হাত ধুই, তেমনি আমাদের ডিজিটাল জীবন রক্ষা করতে হলে অনলাইন ব্যবহারের ক্ষেত্রে কিছু নিয়ম মেনে চলতে হবে। সঠিক সাইবার হাইজিন মেনে চললে ফিশিং, হ্যাকিং ও ম্যালওয়্যার আক্রমণ থেকে ব্যক্তিগত অ্যাকাউন্ট ও ডিভাইস সুরক্ষিত রাখা যায়।

রাজু জানল যে, সাইবার হাইজিনের কিছু গুরুত্বপূর্ণ অভ্যাস হলঃ



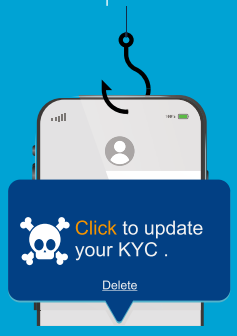
শক্তিশালী ও ইউনিক পাসওয়ার্ড সেট করা :
সহজ অনুমেয় পাসওয়ার্ড, যেমন "123456" বা "password" ব্যবহার না করে, বড় হাতের ও ছোট হাতের অক্ষর, সংখ্যা ও বিশেষ চিহ্ন মিশিয়ে শক্তিশালী পাসওয়ার্ড তৈরি করা।

দুই স্তরের প্রমাণীকরণ (2FA) চালু করা :
2FA আপনার অ্যাকাউন্টের নিরাপত্তা আরও শক্তিশালী করে। এটি লগইনের জন্য পাসওয়ার্ড ছাড়াও ফোনে পাঠানো একটি কোড চায়.

শক্তিশালী স্ক্রিন লক ও বায়োমেট্রিক অথেনটিকেশন চালু করা
ফোনের নিরাপত্তা বাড়াতে শক্তিশালী পাসওয়ার্ড বা PIN ব্যবহার করা উচিত। এছাড়া ফিঙ্গারপ্রিন্ট বা ফেস আইডি চালু করলে ফোনে অননুমোদিত প্রবেশ রোধ করা সম্ভব।

শুধুমাত্র বিশ্বস্ত উৎস থেকে অ্যাপ ডাউনলোড করা
শুধুমাত্র অফিসিয়াল অ্যাপ স্টোর থেকে অ্যাপ ডাউনলোড করা উচিত। অজানা উৎস থেকে ডাউনলোড করা অ্যাপে ভাইরাস থাকতে পারে বা এটি আপনার তথ্য চুরি করতে পারে।

নিরাপদ সংযোগ ব্যবহার করা:
পাবলিক Wi-Fi ব্যবহার করার সময় অনলাইন ব্যাংকিং বা গুরুত্বপূর্ণ অ্যাকাউন্টে লগইন করা এড়িয়ে চলা উচিত।



সন্দেহজনক লিংক এড়িয়ে চলা:
কোনো ইমেইলের লিংকে ক্লিক করার আগে তার উৎস যাচাই করা উচিত।

সফটওয়্যার ও অ্যাপ নিয়মিত আপডেট করা :
পুরনো সফটওয়্যারে নিরাপত্তা ত্রুটি থাকতে পারে, যা সাইবার অপরাধীরা কাজে লাগাতে পারে।

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.सु.प्रौ.सं NIELIT