সাইবার PASS

কলকাতা পুলিশের সাইবার ক্রাইম ব্রাঞ্চের একটি উদ্যোগ

অনলাইন ব্যাঙ্কিং সুরক্ষার সহজপাঠ
পৃষ্ঠা সংখ্যা - ৩

কলকাতা ✦ সংখ্যা - ১ ✦ প্রকাশিত - ফেব্রুয়ারী ২০২৬ ✦ পৃষ্ঠা - ৪

নিজস্ব চিত্রঃ বইমেলায় কলকাতা পুলিশের স্টল ঘুরে দেখলেন মাননীয়া মুখ্যমন্ত্রী মমতা বন্দোপাধ্যায়

বইমেলার মঞ্চে সাইবার সুরক্ষা নিয়ে জনসচেতনতার বার্তা

কলকাতা আন্তর্জাতিক বইমেলা ২০২৬-এ কলকাতা পুলিশের সাইবার ক্রাইম ব্রাঞ্চের উদ্যোগে একটি বিশেষ জনসচেতনতা স্টল স্থাপন করা হয়। বইমেলায় আগত বিভিন্ন বয়সের মানুষের সঙ্গে সাইবার সুরক্ষা নিয়ে আন্তরিকভাবে মতবিনিময় করেন ব্রাঞ্চের সদস্যরা। তারা সচেতনতামূলক লিফলেট বিতরণ করে অনলাইন প্রতারণা, ফিশিং, ভুয়ো কল, ডিজিটাল লোন অ্যাপসহ বর্তমান সময়ের নানা ট্রেন্ডিং সাইবার অপরাধ যেমন ডিজিটাল এরেস্ট, ইনভেস্টমেন্ট ফ্রড সম্পর্কে বিস্তারিত তথ্য দেন। পাশাপাশি সাইবার জগতে নিরাপদ থাকার জন্য করণীয় ও বর্জনীয় বিষয়গুলি সহজ ভাষায় তুলে ধরা হয়। যে কোনোও পরিস্থিতিতে সাইবার প্রতারণার শিকার হলে দ্রুত ১৯৩০ নম্বরে ফোন করে অভিযোগ জানানোর গুরুত্বও বিশেষভাবে তুলে ধরা হয়।

প্রিয় পাঠক,

কলকাতা পুলিশ সাইবার ক্রাইম ব্রাঞ্চের এই নতুন নিউজলেটারটি (সাইবার Pass) আপনাদের জন্য নিবেদিত - ডিজিটাল দুনিয়ায় নিরাপদ থাকার একটি সহজ ও ব্যবহারিক গাইড। এই উদ্যোগের লক্ষ্য আমাদের 'প্রণাম' প্রকল্পের বয়স্ক সদস্য ও সদস্যাগণ, প্রবীণ নাগরিক, স্কুল ও কলেজের ছাত্রছাত্রীরা শিক্ষক শিক্ষিকা, গৃহকর্মী, চাকুরিজীবী এবং ব্যবসায়ী শ্রেণির মধ্যে সাইবার অপরাধ সম্পর্কে সচেতনতা আরও বাড়ানো। আজকের দিনে প্রতারকেরা নানা কৌশলে মানুষকে ফাঁদে ফেলছে - ভুয়ো ইনভেস্টমেন্ট ফ্রড, নকল লিংক / কিউআর কোড, ব্যাংক, হোটেল, ই-কমার্স সাইটের কাস্টমার কেয়ার সেজে ফোন, এমনকি ভয় দেখিয়ে ডিজিটাল অ্যারেস্টের নাটক। এই সংখ্যায় আমরা ইনভেস্টমেন্ট ফ্রড-এর বিপদ ও প্রতারকদের কৌশল খুব বিস্তারিতভাবে তুলে ধরেছি।

ভুক্তভোগীর মনে অনেক প্রশ্ন থাকে - কী করবেন, কী করবেন না। বিপদে আপনাকে দিশা দেখাতে আমাদের সাইবার ক্রাইম ব্রাঞ্চের তরফে চালু করা হয়েছে একটি টোল-ফ্রি হেল্পলাইন নাম্বার - ১৮০০-৩৪৫-০০৬৬।

আমাদের আশা, সাইবার ক্রাইম বিভাগের এই নতুন উদ্যোগগুলি মানুষের কাজে লাগবে।

আমার এবং আমাদের শুভকামনা রইলো।

সবাই ভালো থাকবেন।

সুপ্রতিম সরকার

তারিখঃ
০৯, ফেব্রুয়ারী ২০২৬

সুপ্রতিম সরকার, আইপিএস
পুলিশ কমিশনার, কলকাতা পুলিশ

ভুয়ো বিনিয়োগের ফাঁদ, প্রবীণ ব্যবসায়ীর ৪কোটি লোপাট

দেবাশিষ দত্ত, ইনস্পেকটর

নিজস্ব প্রতিবেদনঃ শেয়ার বাজারের মুখোশ আড়ালে সাইবার প্রতারণা, হোয়াটসঅ্যাপের ফাঁদে পড়ে প্রবীণ ব্যবসায়ীর ৪ কোটির বিনিয়োগ, শেষ পর্যন্ত নিখোঁজ ২২ কোটি।

কলকাতার এক প্রবীণ ব্যবসায়ীর জীবন ছিল হিসেবি ও স্থিতিশীল। বহু বছরের পরিশ্রমে গড়া মূলধন তিনি কখনও ঝুঁকিপূর্ণ পথে রাখেননি। কিন্তু একদিন ফেসবুক অ্যাডের আসা একটি বার্তা সেই বিশ্বাসের ভিত কাঁপিয়ে দেয়।

বার্তার প্রেরক নিজেকে পরিচয় দেয় নামী বিনিয়োগ সংস্থার অনুমোদিত প্রতিনিধি হিসেবে। কথাবার্তায় ছিল পেশাদারিত্ব, প্রলোভনে ছিল অস্বাভাবিক উচ্চ রিটার্নের আশ্বাস। কিছুদিনের মধ্যেই তাঁকে যুক্ত করা হয় একটি অনলাইন প্ল্যাটফর্মে—"MO Prosperax।" সেখানে বিনিয়োগের লাইভ ড্যাশবোর্ড, মুনাফার গ্রাফ, সবই নিখুঁতভাবে সাজানো।

পরিকল্পিতভাবে তাঁকে যুক্ত করা হয় একটি হোয়াটসঅ্যাপ গ্রুপে, যেখানে প্রায় শতাধিক সদস্য প্রতিদিন লাভের গল্প শোনাতে থাকে। কেউ বড় অঙ্কের আয়ের কথা লিখছে, কেউ সাফল্যের ছবি শেয়ার করছে। পরে জানা যায়, অধিকাংশ অ্যাকাউন্টই ছিল ভুয়ো।

বিশ্বাস আরও দৃঢ় হয়, যখন ২৫ হাজার টাকা তুলে নেওয়া সম্ভব হয় এবং সেই টাকা সত্যিই তাঁর ব্যাংক অ্যাকাউন্টে জমা পড়ে। এরপর শুরু হয় বড় অঙ্কের বিনিয়োগ। ধাপে ধাপে বিনিয়োগ পৌঁছায় প্রায় ৪ কোটি টাকায়। প্ল্যাটফর্মে দেখানো হতে থাকে, লাভ বেড়ে ১৮ কোটি—মোট মূল্য ২২ কোটি।

নাটকীয় মোড় আসে, যখন তিনি ৫ কোটি টাকা তুলতে চান। তখনই প্ল্যাটফর্মের প্রশাসকরা টাকা তোলার অনুমতি অস্বীকার করে। পরিবর্তে দাবি করা হয় একের পর এক অযৌক্তিক চার্জ - ব্রোকারেজ ও কমিশনের নামে মোটা অঙ্ক, রিডেম্পশনের জন্য সরকারের নামে ৩০% কর, তথাকথিত আরবিআই ট্যাক্স হিসেবে ১০%, এবং প্ল্যাটফর্ম ফি হিসেবে আরও ১০%।

এই অস্বাভাবিক দাবিতেই সন্দেহ দানা বাঁধে। পরিবার ও পরিচিতদের সঙ্গে আলোচনা করে নথি যাচাই করতেই সামনে আসে ভয়াবহ সত্য— SEBI রেজিস্ট্রেশনের কাগজ সম্পূর্ণ জাল, প্ল্যাটফর্মটি একটি সুপরিকল্পিত সাইবার প্রতারণা।

হোয়াটসঅ্যাপের এক ক্লিকে শুরু হওয়া এই বিনিয়োগ শেষ হয় সর্বস্ব হারানোর আতঙ্কে। ডিজিটাল যুগে বিশ্বাসই যে সবচেয়ে বড় ঝুঁকি, তার নির্মম প্রমাণ হয়ে রইল এই ঘটনা।

সাইবার অপরাধ থেকে বাঁচতে কলকাতা পুলিশের নতুন অস্ত্র

অভিষেক মোদি, আইপিএস, ডিসিপি, সাইবার ক্রাইম, কলকাতা পুলিশ

আজকের দিনে মোবাইল, ইন্টারনেট ও অনলাইন লেনদেন আমাদের জীবনের স্বাভাবিক অংশ। এই সুবিধার সঙ্গে সাইবার অপরাধও বাড়ছে, আর অপরাধীদের কৌশল প্রতিদিন বদলাচ্ছে। তাই সাধারণ মানুষের কাছে সহজ ভাষায় সচেতনতার কথা পৌঁছে দিতে শুরু হলো এই মাসিক নিউজলেটার - সাইবার Pass। এটি হার্ডকপি ও ডিজিটাল—দুইভাবেই থাকবে; তবে মূলত ইমেল ও হোয়াটসঅ্যাপের মাধ্যমে দ্রুত এবং সহজে পৌঁছে দেওয়া হবে। আমাদের লক্ষ্য - সাইবার অপরাধের ধরণ ও নতুন কৌশল সম্পর্কে তথ্য তুলে ধরা, যাতে মানুষ আগে থেকেই সতর্ক থাকতে পারেন।

জানুয়ারি সংখ্যার কভার স্টোরি: **বিনিয়োগ প্রতারণা**। এখন অনেকেই "কম সময়ে বেশি লাভ" দেখিয়ে মানুষকে ফাঁদে ফেলছে। কখনও হোয়াটসঅ্যাপ গ্রুপ বানিয়ে, কখনও সোশ্যাল মিডিয়ায় বিজ্ঞাপন দিয়ে, আবার কখনও প্রসিদ্ধ ব্যক্তির নামে বা মুখে তৈরি করা ভুয়ো এ.আই ভিডিও দেখিয়ে বিশ্বাস তৈরি করা হয়। কিছু ক্ষেত্রে ভুয়ো ওয়েবসাইট বা অ্যাপ দেখিয়ে টাকা জমা দিতে বলা হয়। শুরুতে সবকিছু খুব বিশ্বাসযোগ্য মনে হলেও পরে টাকা আটকে যাওয়া, যোগাযোগ বন্ধ হয়ে যাওয়া বা আরও টাকা চাওয়ার মতো ঘটনা ঘটে।

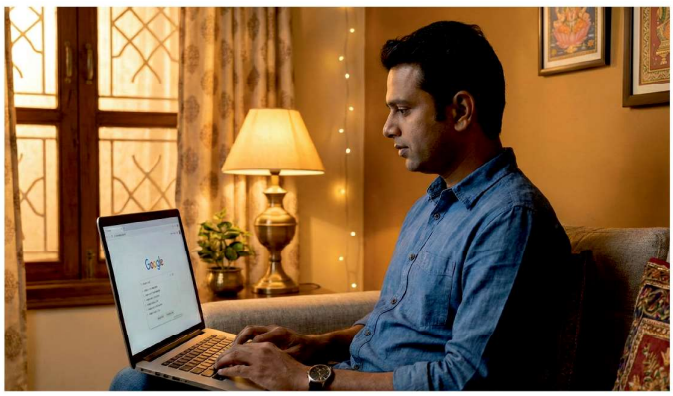
নাগরিক সহায়তার জন্য প্রথমেই মনে রাখুন - **এনসিআরপি পোর্টাল** (cybercrime.gov.in) এবং **জাতীয় হেল্পলাইন নম্বর ১৯৩০**। এর পাশাপাশি কলকাতা পুলিশ চালু করেছে নতুন **টোল-ফ্রি নম্বর ১৮০০-৩৪৫-০০৬৬**। এটি ১৯৩০-এর বিকল্প নয়—বরং ১৯৩০ ব্যবহারে বাড়তি সহায়তা যোগ করে। প্রয়োজনে এটি ভুক্তভোগীকে দ্রুত রিপোর্ট করতে উৎসাহিত করে, রিপোর্টিং প্রক্রিয়া বুঝতে সাহায্য করে, আটকে থাকা অর্থ ফেরতের বিষয়টি নিয়ে দিকনির্দেশ দেয়, সোশ্যাল মিডিয়া-সম্পর্কিত সমস্যায় সহায়তার পথ দেখায় এবং নিকটবর্তী থানা ও ডিভিশন সাইবার সেল-এর সঙ্গে যোগাযোগে সাহায্য করে—দুশ্চিন্তা ও অস্থিরতার সময়ে "বন্ধু ও গাইড" হিসেবে।

এছাড়া কলকাতা পুলিশের আরেকটি নতুন উদ্যোগ হলো **ব্লকিং সেল**। সাইবার অপরাধে ব্যবহার হওয়া মোবাইল নম্বর/ডিভাইস, ওয়েবসাইট, ইউআরএল, এপিকে ফাইল, ক্ষতিকর সোশ্যাল মিডিয়া অ্যাকাউন্ট ইত্যাদি তথ্য সংগ্রহ করে একটি তালিকা তৈরি করা হয় এবং নিয়মমাফিক প্রক্রিয়ায় এগুলি ব্লক করার চেষ্টা করা হয়, যাতে একই রিসোর্স দিয়ে বারবার নতুন মানুষকে প্রতারিত না করা যায়।

সব মিলিয়ে, কলকাতা পুলিশের এই নতুন উদ্যোগগুলি - **১৮০০-৩৪৫-০০৬৬** টোল-ফ্রি সহায়তা, ১৯৩০ ও cybercrime.gov.in রিপোর্টিং ব্যবস্থাকে আরও শক্ত করা, এবং ব্লকিং সেলের মাধ্যমে ক্ষতিকর ডিজিটাল রিসোর্স বন্ধ করা - একটাই লক্ষ্য সামনে রেখে চলছে: নাগরিক যেন দ্রুত সাহায্য পান, ক্ষতি কমে, এবং সাইবার অপরাধীদের কাজের রাস্তা ধাপে ধাপে বন্ধ হয়। আশা করি আপনার নিউজলেটার প্রথম এডিশনকে পছন্দ করবেন।

সার্চ ইঞ্জিনে লুকিয়ে ভুয়ো হোটেল!

রঞ্জন চক্রবর্তী, সাব-ইনস্পেকটর



নিজস্ব প্রতিবেদনঃ ২০২৫ সালের মাঝামাঝি থেকে লক্ষ্য করা যাচ্ছে, অনেকেই সার্চ ইঞ্জিনে হোটেল খুঁজতে গিয়ে একই হোটেলের নামে "কম দামে আকর্ষণীয় অফার" দেখে ভুল ওয়েবসাইটে ঢুকে প্রতারণার শিকার হচ্ছেন। কলকাতার একাধিক ভুক্তভোগীর অভিযোগের ভিত্তিতে সাইবার পুলিশ তদন্ত শুরু করে এবং দেখা যায় - একই ধাঁচের ভুয়ো হোটেল বুকিং ওয়েবসাইট ব্যবহার করে টাকা নেওয়া হচ্ছে, পরে বুকিং কনফার্মেশন, যোগাযোগ বা রিফান্ড - কিছুই মেলে না। এমনই একটি সন্দেহজনক সাইটের উদাহরণ: purihotelkolkatabookingoffice.com।

অভিযুক্ত ব্যক্তি একজন ওয়েবসাইট ডেভেলপার; তিনি অত্যাধুনিক প্রযুক্তি ব্যবহার করে পরিচয় আড়াল করার চেষ্টা করলেও পুলিশ সূক্ষ্ম ডিজিটাল ফুটপ্রিন্ট বিশ্লেষণ করে সূত্র মেলায় এবং পুণে-তে তাঁর বাসস্থান থেকে অভিযান চালিয়ে গ্রেফতার করে । অভিযুক্তের ডিভাইস থেকে ভুয়ো ওয়েবসাইট তৈরি ও পরিচালনার সঙ্গে সম্পর্কিত গুরুত্বপূর্ণ ডিজিটাল প্রমাণ উদ্ধার হয়েছে।

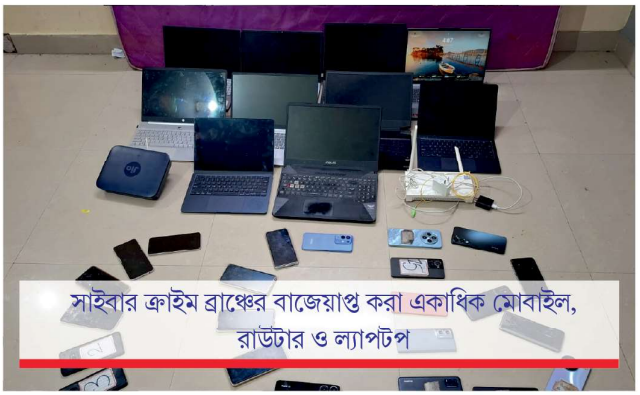
পেমেন্ট করার আগে ওয়েবসাইটটি আসল কি না যাচাই করুন - অফিসিয়াল সাইট/ভেরিফায়েড নম্বর মিলিয়ে নিন, সন্দেহ হলে টাকা দেবেন না।

ভুয়ো সরকারি অ্যাপ

লক্ষাধিক টাকার প্রতারণা, গ্রেফতার ৫

রথিন সিং, ইনস্পেকটর

বিশেষ প্রতিবেদনঃ জানুয়ারির শেষ সপ্তাহে কলকাতা পুলিশ সাইবার ক্রাইম ব্রাঞ্চের সফল অভিযানে "জামতাড়া" গ্যাংয়ের ৫ জন সদস্য গ্রেফতার হয়েছে। তারা দেশের বিভিন্ন প্রান্তের সহযোগীদের কাছ থেকে ক্রিপ্টিক মেসেজিং প্ল্যাটফর্মে এপিকে ফাইল কিনে এনে তা হোয়াটসঅ্যাপ, এসএমএস ও সোশ্যাল মিডিয়া বিজ্ঞাপনের মাধ্যমে ভুক্তভোগীদের ফোনে পাঠাত। সোশ্যাল ইঞ্জিনিয়ারিংয়ের মাধ্যমে এসব ফাইলকে এম.পরিবহন চালান, বিয়ের কার্ড ইনভিটেশন, কে.ওয়াই.সি আপডেট বা সরকারি কল্যাণ প্রকল্পের "অফিসিয়াল অ্যাপ" বলে বিশ্বাস করানো হতো। ফাইল ইনস্টল করালেই ডিভাইসের সংবেদনশীল তথ্য ও ব্যাংক-সম্পর্কিত অনুমতি নিয়ে প্রতারণা করে আর্থিক ক্ষতি ঘটানো হতো। অভিযানে ১০টি ল্যাপটপ, ২৪টি মোবাইল, ২টি রাউটার এবং বিপুল ইলেকট্রনিক প্রমাণ উদ্ধার করা হয়েছে। অচেনা নম্বরের পাঠানো এপিকে ডাউনলোড করবেন না, অ্যাপকে প্রয়োজনের বেশি পারমিশন দেবেন না।



সাইবার ক্রাইম ব্রাঞ্চের বাজেয়াপ্ত করা একাধিক মোবাইল, রাউটার ও ল্যাপটপ

আদালতের অনুমতি ছাড়াই ফেরৎ পাবেন ৫০হাজার টাকা

সাইবার জালিয়াতির টাকা ফেরত পাওয়া আরও সহজ

মৃণ্ময় ব্যানার্জী, ইনস্পেকটর

নিজস্ব প্রতিবেদনঃ বর্তমান ব্যবস্থায় সাইবার আর্থিক প্রতারণার শিকার হলে ভুক্তভোগীরা প্রায়ই একই সমস্যায় পড়েন—অভিযোগের অগ্রগতি স্পষ্ট বোঝা যায় না, একাধিক দফতর/ব্যাংকের মধ্যে সমন্বয়ের অভাবে বারবার যোগাযোগ করতে হয়, আর টাকা "ফ্রিজ/লিয়েন" হয়ে দীর্ঘদিন আটকে থাকে। এতে মানসিক চাপ যেমন বাড়ে, তেমনই প্রাথমিক পর্যায়ে দ্রুত পদক্ষেপ না হলে অর্থ ফেরতের সম্ভাবনাও কমে যায়। নতুন এসওপি (এখন বাস্তবায়নের পথে) এই জায়গাতেই বড় পরিবর্তন আনছে - পুরো প্রক্রিয়াকে আরও সময়বদ্ধ, স্বচ্ছ এবং ভুক্তভোগী-কেন্দ্রিক করার কাঠামো তৈরি হচ্ছে।

এখানে দু'টি মডিউল সবচেয়ে গুরুত্বপূর্ণ—

Grievance Redressal Module: অভিযোগ গ্রহণ থেকে শুরু করে ট্র্যাকিং, দায়িত্ব ভাগ, এবং নির্দিষ্ট সময়সীমার মধ্যে নিষ্পত্তির একটি পরিষ্কার রূপরেখা। ফলে ভুক্তভোগী জানবেন কোন ধাপে কী হচ্ছে, কার দায়িত্ব কী, এবং অপ্রয়োজনীয় দেরি কমবে। একই সঙ্গে "ফলো-আপ" করার নিয়মও আরও সংগঠিত হবে, যাতে প্রতিটি পদক্ষেপ নথিভুক্ত থাকে। এমনকি কলকাতার কোনো প্রকৃত ব্যবসায়ী/ট্রেডারের বৈধ ব্যবসায়িক অ্যাকাউন্ট যদি অন্য রাজ্যের কোনো মামলার কারণে ভুলবশত ফ্রিজ হয়ে যায়, এই মডিউলের মাধ্যমে সময়সীমার মধ্যে তাঁর অভিযোগ নিষ্পত্তি ও প্রয়োজনীয় প্রতিকার পাওয়ার পথ আরও পরিষ্কার হবে।

Money Restoration Module: ব্যাংক/আর্থিক প্রতিষ্ঠানের সমন্বয়ে প্রতারিত অর্থ দ্রুত ফেরানোর প্রক্রিয়াকে এক ছাতার নিচে আনা। বিশেষ করে ৫০,০০০ টাকার কম প্রতারণায় অনেক ক্ষেত্রে আদালতের নির্দেশ ছাড়াই রিফান্ড এগোনোর সুবিধা সাধারণ মানুষের জন্য বড় স্বস্তি—কারণ এতে সময় ও হয়রানি দুটোই কমে । পাশাপাশি সময়সীমা নির্ধারিত থাকায় "ফ্রিজ/লিয়েন" অবস্থা দীর্ঘায়িত হওয়ার ঝুঁকিও কমবে।

সারকথা—এই পরিবর্তনে সাধারণ মানুষ কম হয়রান হবেন, অভিযোগ দ্রুত এগোবে, এবং টাকা ফেরার সম্ভাবনা বাস্তবে আরও বাড়বে—এটাই প্রত্যাশা।

#StopDropInform

অনলাইন ব্যাঙ্কিং সুরক্ষার সহজপাঠ

নিজস্ব প্রতিবেদনঃ OTP / UPI PIN /CVV কখনও কারও সঙ্গে শেয়ার করবেন না। ব্যাংক/পুলিশ/কাস্টমার কেয়ারও এগুলো চায় না।

শুধুমাত্র ব্যাঙ্কের অফিসিয়াল ডোমেইন বা অফিসিয়াল অ্যাপ ব্যবহার করুন - ভারতে ব্যাংকের অনুমোদিত ওয়েবসাইট সাধারণত .bank.in ডোমেইনের অধীনে থাকে; লিংক খুলে লগইন না করে নিজে টাইপ করে বা বুকমার্ক থেকে যান।

অ্যাকাউন্টে অ্যালার্ট অন রাখুন - এসএমএস / ইমেল ট্রান্সাকশন অ্যালার্ট, এবং ছোট অংকের ডেবিট/অনলাইন ট্রান্সাকশন লিমিট সেট করুন।

ডিভাইস সুরক্ষিত রাখুন - সিস্টেম/অ্যাপ আপডেট, স্ক্রিন লক, এবং অচেনা এপিকে ফাইল / অ্যাপ ইনস্টল নয়; অ্যাপের পারমিশন প্রয়োজনের বেশি দেবেন না।

সন্দেহ হলেই সঙ্গে সঙ্গেই পদক্ষেপ নিন - কার্ড / ইউপিআই ব্লক করুন, ব্যাংকে জানান, এবং প্রতারণা হলে দ্রুত **১৯৩০-এ কল করুন** ও cybercrime.gov.in-এ **অভিযোগ করুন।**

একটুখানি বিশ্বাস, আর একটুখানি অসতর্কতা

শান্তনু গাইন, সার্জেন্ট (ইনভেস্টিগেশন)

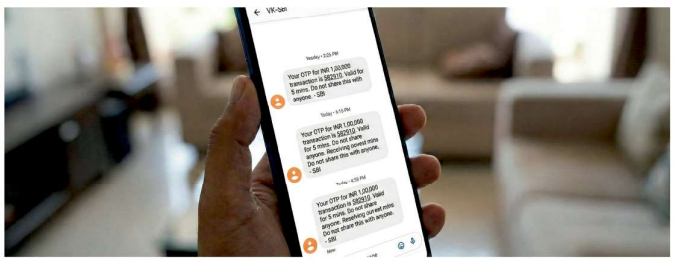
নিজস্ব প্রতিবেদনঃ ফোনটা বেজে ওঠে। পরিচিত নাম, পরিচিত নম্বর। হোয়াটসঅ্যাপ মেসেজে লেখা - "ভুল করে তোমার নম্বরে একটা ওটিপি চলে গেছে, দয়া করে ওটিপিটা বলবে? খুব দরকার।"

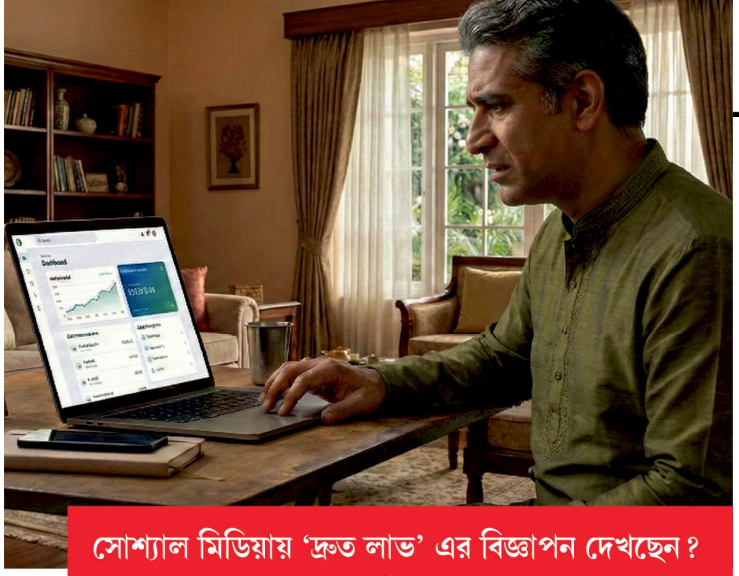
এক মুহূর্তের বিশ্বাস, আর পরক্ষণেই বিপর্যয়। ওটিপি শেয়ার করার সঙ্গে সঙ্গেই হোয়াটসঅ্যাপ অ্যাকাউন্ট চলে যায় অপরাধীর দখলে। অ্যাকাউন্ট দখলের পর অপরাধীরা ভুক্তভোগীর নামেই পরিচিতদের বার্তা পাঠায় - "আমি বিপদে পড়েছি, টাকা পাঠাও।" মেসেজ আসে পরিচিত নম্বর থেকে, তাই সন্দেহ কমে। অনেক সময় কাছের পরিবার বা বন্ধু-বান্ধবও প্রতারকদের টাকা পাঠিয়ে দেন।

এতে শুরু হয় এক ধরনের শৃঙ্খল প্রতিক্রিয়া - আপনার বন্ধুদের কাছেও একই কৌশলে বার্তা গিয়ে তাদের হোয়াটসঅ্যাপ অ্যাকাউন্টও দখল হয়ে যেতে পারে।

সাইবার অপরাধীরা আজ আর জটিল হ্যাকিংয়ে যায় না। তারা লক্ষ্য করে মানুষের বিশ্বাসকে। কখনও ব্যাংক কর্মী, কখনও পরিচিত বন্ধুর ছদ্মবেশ - লক্ষ্য একটাই; ওটিপি । ওটিপি পেলেই হোয়াটসঅ্যাপ অ্যাকাউন্ট দখল। ওটিপি কখনও কারও সঙ্গে শেয়ার করবেন না - পরিচিত হলেও না। টু-স্টেপ ভেরিফিকেশন চালু রাখুন। টাকা চাওয়ার মেসেজ এলে আগে ফোন করে তা যাচাই করুন।

হোয়াটসঅ্যাপ হ্যাক মানে শুধু অ্যাকাউন্ট হারানো নয় - ভেঙে পড়ে বিশ্বাস, নষ্ট হয় মানসিক শান্তি। অপরাধীরা ফোন নয়, তারা ভাঙে সতর্কতার দেওয়াল। আজ একটু সাবধান থাকলেই আগামীতে বাঁচবে আপনার পরিচয়, আপনার বিশ্বাস, আর আপনার গল্প।





সোশ্যাল মিডিয়ায় ‘দ্রুত লাভ’ এর বিজ্ঞাপন দেখছেন?
সাবধান, আপনার জন্যও ফাঁদ পাতা আছে!

স্পনসরড্ বিজ্ঞাপন মানেই বিশ্বাসযোগ্য নয়!

পিগ-বুচারিং হলো দীর্ঘ সময় ধরে বিশ্বাস তৈরি করে পরে ভুয়ো “বিনিয়োগ” প্ল্যাটফর্মে টাকা ঢোকানো এবং শেষ পর্যন্ত টাকা আটকে/হাতিয়ে নেওয়ার একটি পরিকল্পিত প্রতারণা।

ক) সোশ্যাল মিডিয়া বিজ্ঞাপন: ফেসবুক/ইনস্টা/ইউটিউবে “কম সময়ে বেশি লাভ”, “প্রিমিয়াম সিগন্যাল”, “সেলিব্রিটি-অনুমোদিত” ধরনের টার্গেটেড অ্যাড চলে। এখানে ট্র্যাকিং লিংক/লিড-ফর্মে ক্লিক করলেই হোয়াটসঅ্যাপ/টেলিগ্রামে “অ্যাডভাইজরি ডেস্ক” যুক্ত হয়—এই লিড-জেনারেশনই স্ক্যামের এন্ট্রি-পয়েন্ট।

খ) অনলাইন ট্রেনিং/কোচিং: “ফ্রি ওয়েবিনার”, “লাইভ ট্রেডিং ক্লাস”, “মেন্টরশিপ” দেখিয়ে ধাপে ধাপে বিশ্বাস গড়ে। স্ক্যাম অপারেশনগুলোতে কথোপকথনের স্ক্রিপ্ট/ম্যানুয়াল থাকে—কখন কী বলতে হবে, কীভাবে FOMO তৈরি করতে হবে, কখন ‘VIP গ্রুপে’ ঢোকাতে হবে—সবই প্রক্রিয়াগত।

গ) ফেক অ্যাপ / প্ল্যাটফর্মে হাই রিটার্ন: হাই রিটার্ন ড্যাশবোর্ড: দেখতে আসল ট্রেডিং অ্যাপের মতো, কিন্তু ভেতরে ফেক লেজার/ড্যাশবোর্ড: কৃত্রিম লাভ, চার্ট, ব্যালান্স, এমনকি “উইথড্র সফল” দেখিয়ে আরও টাকা ঢোকায়। পরে টাকা তুলতে গেলে “ট্যাক্স”, “চার্জ”, “মার্জিন”, “ভেরিফিকেশন ফি”—এই অজুহাতে আরও ডিপোজিট চাইতে থাকে।

ঘ) ফেক হোয়াটসঅ্যাপ গ্রুপ: বড় গ্রুপে “বিশেষজ্ঞ”, “অ্যাসিস্ট্যান্ট”, “সফল বিনিয়োগকারী”—অনেকেই আসলে বট/সহযোগী। নিয়মিত স্ক্রিনশট, “আজ ১২শতাংশ প্রফিট”, “আমি উইথড্র পেলাম”—এভাবে সোশ্যাল প্রুফ তৈরি করে এবং একাধিক অ্যাকাউন্টে টাকা পাঠাতে প্ররোচিত করে। সাম্প্রতিক রিপোর্টে এ ধরনের গ্রুপ-ভিত্তিক ট্রেডিং স্ক্যামের উদাহরণও দেখা যাচ্ছে।

ঙ) জনপ্রিয় ব্যক্তির ফেক এআই ভিডিও/ডিপফেক: ডিপফেক ভিডিও/ভয়েস ক্লোনিং দিয়ে পরিচিত মুখ/অ্যাঙ্কর/বিশেষজ্ঞের “এন্ডোর্সমেন্ট” বানানো হয়—এটা মূলত ট্রাস্ট-অ্যাক্সিলারেটর। মানুষ “চেনা মুখ” দেখলেই সন্দেহ কমায়, আর প্রতারকরা সেই মানসিক শর্টকাট কাজে লাগায়।

এই পাঁচটি মাত্রা আলাদা দেখালেও মূল সূত্র এক - টার্গেটেড রিচ → ট্রাস্ট বিল্ডিং → ভুয়ো প্রুফ → উইথড্র আটকে আরও টাকা দাবি। “গ্যারান্টিড রিটার্ন”, অচেনা গ্রুপ/অ্যাপ, বা তাড়াহুড়ো করে পেমেন্ট - এই তিনটি দেখলেই থামুন; প্ল্যাটফর্ম/রেগুলেশন/ডোমেইন যাচাই না করে টাকা দেবেন না।

#StopDropInform

সাইবার সুরক্ষা অভিযান!

সাইবার প্রতারণা ঠেকাতে সুরক্ষায় জোর কলকাতা পুলিশের

পশ্চিমবঙ্গ ট্রেডার্স অ্যাসোসিয়েশনের সহযোগিতায় সচেতনতা কর্মসূচি

কলকাতা বইমেলায় সেবি-র স্টলে সচেতনতামূলক কর্মসূচি

Cy-Buzz-র সাথে সচেতনতামূলক কর্মসূচি

কলকাতার রোমান ক্যাথলিক আর্চডায়োসিসে সচেতনতামূলক কর্মসূচি

কলকাতা পুলিশের সাইবার ক্রাইম ব্রাঞ্চের সমস্ত সোশ্যাল মিডিয়া অ্যাকাউন্ট

WHATSAPP CHANNEL	FACEBOOK PAGE	INSTAGRAM HANDLE	X ACCOUNT (TWITTER)

কলকাতা পুলিশের সাইবার ক্রাইম ব্রাঞ্চের সঙ্গে যোগাযোগ করতে পারেন

ইমেল আইডি - cscss-dd@kolkatapolice.gov.in
সাইবার থানা - +91 98365 13000/ 033-2214-3000
প্রণাম টোল ফ্রী নম্বর - 94779 55555

ডিজিটাল প্রহরী হেল্পলাইন নম্বর **১৮০০ ৩৪৫ ০০৬৬**