

প্রবীণ সৈনিক এবং বীর নারীস কর্তৃক সাইবার নিরাপত্তা জালিয়াতির মোকাবেলা

কমান্ডার পি রাজাগোপাল টাম্পি আইএন (আর)

- এআই এবং বৃহৎ ভাষা মডেল

সফটওয়্যার এবং এআই-এর মধ্যে পার্থক্য কী?

- এজেন্ট বলতে কী বোঝায়?
- একজন এজেন্ট একজন এলএলএম থেকে কীভাবে আলাদা?
- এআই-এর কিছু গুরুত্বপূর্ণ সুবিধা কী কী?
    - বৈজ্ঞানিক আবিষ্কারে দ্রুত অগ্রগতি
    - নতুন উপকরণ, নতুন অণু, উৎপাদনশীলতার সুবিধা
    - আবহাওয়ার পূর্বাভাস
    - সফটওয়্যার কোডিং
    - রোবট এবং স্বয়ংক্রিয়করণ
- এআই-এর প্রধান ঝুঁকিগুলো কী কী?
    - প্রতারণা, ক্ষমতা লাভের আকাঙ্ক্ষা এবং আত্মরক্ষা
    - ডিপফেকস

    নিয়ন্ত্রণ হারানো
    - পুনরাবৃত্তিমূলক আত্ম-উন্নয়ন (RSI)
    - স্ব-প্রতিলিপিকরণ

- হাগিংফেস ঘটনা, অ্যানথ্রোপিক আইওটি পূর্বাভাস
- ফ্রান্সে রেফ্রিজারেশন প্ল্যান্ট হ্যাকিং – ২০২৬ সালের অক্টোবরের মাঝামাঝি
- সরকারি ওয়েবসাইট বন্ধ (পিএইচপি ত্রুটি) – ২১$^{সেন্ট}$ অক্টোবর ২০২৬
- স্বভাবগতভাবেই এটি একটি দ্বৈত-ব্যবহারের প্রযুক্তি – স্বয়ংক্রিয় অস্ত্র, CBRN (কার্বন ব্ল্যাক রেডেড) এবং যুদ্ধকালীন ব্যবহারে এর ব্যাপক বিপদ রয়েছে।
- এআই সাইবার নিরাপত্তার সহায়ক ও রক্ষাকর্তা
- আমাদের মস্তিষ্কের চেয়েও শক্তিশালী কম্পিউটিং ইঞ্জিন (দ্রুততর এবং সীমাহীন সম্পদ)। আমরাতাদের সাথে তাল মেলাতে বা তাদের কথা বুঝতে পারব না।
- এজেন্টরা ২৪x৭ চলে এবং শত শত সংখ্যায় মিলে এনক্রিপশন ব্রুট ফোর্স করতে ও সফটওয়্যারের বাগ খুঁজে বের করতে পারে। • এআই সিস্টেমগুলো প্রশিক্ষণের পর পাওয়ার অন করার সাথে সাথেই সম্পূর্ণ জ্ঞান নিয়ে চালু হয়ে যেতে পারে, যেকোনো জায়গায় স্থানান্তরিত হতে পারে এবং অনেক দেরি হয়ে যাওয়ার আগে আমরা হয়তো তাদের শনাক্ত করতে পারব না।
- এআই কর্তৃক ইন্টারনেট দখল এবং অবকাঠামো হ্যাকিংয়ের ফলে স্বল্পমেয়াদী ক্ষতি হতে পারে। সিস্টেম এবং ইউটিলিটি।

• এআই সিস্টেমের প্রতি সংশয় ও কম আস্থা রাখুন:

• সোশ্যাল মিডিয়া থেকে প্রাপ্ত কোনো কিছু বিশ্বাস করবেন না।

সিরি বা সমতুল্য কথোপকথন পর্যবেক্ষণকারী অ্যাপগুলো নিষ্ক্রিয় রাখুন।

• আপনি যদি Chat GPT বা Claude-এর মতো AI টুল ব্যবহার করেন, তাহলে “Improve model for everyone” অপশন এবং লোকেশন অপশনটি বন্ধ করে দিন।

বাণিজ্যিকভাবে উপলব্ধ এআই এজেন্ট ব্যবহার করা থেকে বিরত থাকুন, যদি না আপনি নির্ভরযোগ্যভাবে যাচাই করতে পারেন যে এটি আপনার ব্যক্তিগত ডেটা কীভাবে পরিচালনা করে। শুধুমাত্র একান্ত প্রয়োজন হলেই কম ঝুঁকিপূর্ণ অ্যাপ্লিকেশনের জন্য এটি ব্যবহার করুন।

• আপনার চিন্তা ও উদ্দেশ্য কোনো এআই এজেন্টের কাছে হস্তান্তর করবেন না, বিশেষ করে আপনার ডায়েরি বা ব্যক্তিগত জার্নাল।

• আপনার ব্যাংক অ্যাকাউন্ট, বিল, পেমেন্ট এবং অন্যান্য আর্থিক বিষয় ও লেনদেন স্বয়ংক্রিয় করার জন্য এআই এজেন্টদের অ্যাক্সেস দেবেন না।

আপনার ফোল্ডার, ইমেল পরিষেবা এবং কার্ডের তথ্যে প্রবেশাধিকার দেবেন না।

• সর্বদা নিজে চিন্তা করুন, আপনার হয়ে চিন্তা করার জন্য এআই-কে বলবেন না।

আপনার চিন্তাভাবনা কোনো বিশ্বস্ত বন্ধুর সাথে যাচাই করুন, এআই সিস্টেমের সাথে নয়।

• গোপনীয়তা নিয়ন্ত্রণ ব্যবস্থা কার্যকরভাবে ব্যবহার করুন, শুধুমাত্র অপরিহার্য প্রয়োজনে চিকিৎসা সংক্রান্ত ও আর্থিক নথি

আপলোড করুন। 28/10/2026 পি রাজাগোপাল টাম্পি 4

• শুধুমাত্র কণ্ঠস্বর হুবহু পরিবারের সদস্যের মতো শোনাচ্ছে বলেই কোনো কলারকে বিশ্বাস করবেন না। • যদি কেউ নিজেকে জরুরি অবস্থার আত্মীয় বলে দাবি করে এবং টাকা চায়, তাহলে সংযোগ বিচ্ছিন্ন করুন এবং সেই ব্যক্তিকে তার আগে থেকে সেভ করা নম্বরে কল করুন।

• জরুরী অবস্থার জন্য একটি ব্যক্তিগত পারিবারিক যাচাইকরণ বাক্যাংশ ঠিক করে নিন। এটি সোশ্যাল মিডিয়ায় শেয়ার করবেন না। গণমাধ্যম।

• শুধুমাত্র ব্যক্তির মুখ চেনার কারণে কোনো ভিডিও কলকে আসল বলে ধরে নেবেন না। • টাকা, গোপনীয়তা বা অবিলম্বে ব্যবস্থা নেওয়ার জন্য জরুরি অনুরোধকে সতর্ক সংকেত হিসেবে বিবেচনা করুন। • পুলিশ, সিবিআই, কাস্টমস, আদালত বা অন্যান্য কর্তৃপক্ষের কাছে পাঠানো হয়েছে বলে দাবি করা বার্তা বিশ্বাস করবেন না। আপনাকে ডিজিটাল গ্রেপ্তারে রাখা হয়েছে।

• পরিচয়পত্র হিসেবে কলার আইডি, হোয়াটসঅ্যাপ প্রোফাইল ছবি বা প্রদর্শিত প্রতিষ্ঠানের নাম বিশ্বাস করবেন না।

• আপনার অনলাইন ডেটা প্রোফাইল এবং ফুটপ্রিন্ট সর্বনিম্ন সম্ভাব্য পর্যায়ে হ্রাস করুন • ছদ্মবেশ ধারণের উদাহরণ (ভুয়া ভিডিও কল অনুমোদনের কারণে ২৫ মিলিয়ন ডলার স্থানান্তরিত হয়েছিল)।

• বৈধ কারণ ছাড়া পরিচয়পত্র আদান-প্রদান করা থেকে বিরত থাকুন।

• যেখানে প্রয়োজন, পরিচয়পত্রের অনুলিপিতে উদ্দেশ্য-নির্দিষ্ট জলছাপ যোগ করুন।• WhatsApp, Facebook, Instagram এবং অন্যান্য সামাজিক প্ল্যাটফর্মের গোপনীয়তা সেটিংস পর্যালোচনা করুন।• মেসেজিং গ্রুপে আপনাকে কে যুক্ত করতে পারবে তা সীমিত করুন, গ্রুপের সদস্যপদ যতটা সম্ভব কম রাখার চেষ্টা করুন। • যেখানে সম্ভব, সর্বজনীনভাবে উপলব্ধ ভয়েস রেকর্ডিং এবং ব্যক্তিগত ভিডিও সীমিত করুন। • বিস্তারিত পারিবারিক সম্পর্ক, দৈনন্দিন রুটিন এবং আর্থিক পরিস্থিতি প্রকাশ করা থেকে বিরত থাকুন। • সর্বজনীন অনলাইন প্রোফাইল থেকে অপ্রয়োজনীয় ব্যক্তিগত তথ্য মুছে ফেলুন।• যেখানে প্রয়োজন সেখানে UIDAI-এর অফিসিয়াল আধার প্রমাণীকরণ-ইতিহাস এবং বায়োমেট্রিক-লকিং সুবিধা ব্যবহার করুন। উপযুক্ত।

• যেখানে উপলব্ধ, সেখানে সরকারি টেলিযোগাযোগ পরিষেবার মাধ্যমে আপনার মোবাইল সংযোগ যাচাই করে নিন।

• কম নির্ভরযোগ্য সাবস্ক্রিপশন এবং নিবন্ধনের জন্য একটি আলাদা ইমেল ঠিকানা ব্যবহার করুন।• ক্লাউড-শেয়ারিং লিঙ্কগুলো পর্যালোচনা করুন এবং প্রয়োজন ফুরিয়ে গেলে সর্বজনীন প্রবেশাধিকার বন্ধ করে দিন।

• আপনার ব্যাংকিং পিন, ইউপিআই পিন, এটিএম পিন, সিভিভি, পাসওয়ার্ড, জন্ম তারিখ বা ওটিপি কখনো প্রকাশ করবেন না।• মনে রাখবেন: টাকা গ্রহণ করার জন্য আপনাকে ইউপিআই পিন প্রবেশ করাতে হবে না। এটি প্রবেশ করালে সাধারণত অর্থপ্রদান অনুমোদিত হয়।• অপরিচিত ব্যক্তির পাঠানো কিউআর কোড স্ক্যান করে কখনো টাকা গ্রহণ করবেন না।

• অপ্রত্যাশিত কোনো UPI সংগ্রহের অনুরোধ কখনো অনুমোদন করবেন না।

• কৃত্রিম বুদ্ধিমত্তা ব্যবহার করে নিশ্চিত উচ্চ রিটার্ন বা অসাধারণ মুনাফার প্রতিশ্রুতি দেয় এমন বিনিয়োগ প্রকল্পে বিশ্বাস করবেন না।• এজেন্ট এবং অপরিচিত ব্যক্তিদেরকে দূর থেকে আপনার ব্যাংকিং অ্যাপ্লিকেশন পরিচালনা করতে কখনোই অনুমতি দেবেন না।

• অপরিচিত ব্যক্তিদের সাথে ব্যাংক কার্ড, চেক বা আর্থিক নথিপত্রের ছবি শেয়ার করবেন না। • সকল গুরুত্বপূর্ণ অ্যাকাউন্টে লেনদেন সতর্কতা (transaction alerts) চালু করুন।

• আপনার ব্যাংক অনুমতি দিলে, আপনার প্রয়োজন অনুযায়ী দৈনিক স্থানান্তরের সীমা নির্ধারণ করুন।

• কার্ডের যত্ন: অনলাইনে কার্ডের বিবরণ সংরক্ষণ করা এড়ানো সম্ভব হলে তা করবেন না। কার্ডের বিবরণ স্বয়ংক্রিয়ভাবে পূরণ হওয়ার পদ্ধতি পরিহার করুন। • যখন উচ্চ সীমার আর প্রয়োজন নেই, তখন ক্রেডিট-কার্ডের অনলাইন লেনদেনের সীমা কমিয়ে দিন। • অপ্রয়োজনে আন্তর্জাতিক কার্ড লেনদেন নিষ্ক্রিয় করুন।

• বিদেশে ভ্রমণের সময়, বিশেষ করে আমস্টারডামের ঘটনার পর, কন্ট্যাক্টলেস লেনদেন বন্ধ রাখুন। • ঘন ঘন অনলাইন/ইউপিআই পেমেন্টের জন্য ব্যবহৃত অ্যাকাউন্ট থেকে আপনার বড় অঙ্কের সঞ্চয় আলাদা রাখুন। 28/10/2026 পি রাজাগোপাল টাম্পি 7

• ব্যাংকিং, ইমেল এবং গুরুত্বপূর্ণ অ্যাকাউন্টগুলোর জন্য আলাদা পাসওয়ার্ড ব্যবহার করুন। • দীর্ঘ পাসওয়ার্ড অথবা এমন পাসফ্রেজ ব্যবহার করুন যা অনুমান করা কঠিন।

• যেখানে যেখানে উপলব্ধ, সেখানে দ্বি-স্তরীয় প্রমাণীকরণ বা FIDO2 প্রমাণীকরণ সক্রিয় করুন।• পিন, ফিঙ্গারপ্রিন্ট বা ফেস অথেন্টিকেশন দিয়ে আপনার ফোন লক করুন।

• আপনার ফোন ও অ্যাপ্লিকেশনগুলো সর্বশেষ সংস্করণে আপডেট রাখুন। • শুধুমাত্র অফিসিয়াল অ্যাপ স্টোর থেকে অ্যাপ্লিকেশন ডাউনলোড করুন।

• কোনো অপরিচিত ব্যক্তির পাঠানো WhatsApp, SMS বা ইমেলের মাধ্যমে কোনো APK বা অ্যাপ্লিকেশন ইনস্টল করবেন না।

• কোনো অপরিচিত ব্যক্তির অনুরোধে স্ক্রিন-শেয়ারিং বা রিমোট-অ্যাক্সেস অ্যাপ্লিকেশন ইনস্টল করবেন না। • এমন কোনো অপ্রত্যাশিত লিঙ্কে ক্লিক করবেন না, যেখানে দাবি করা হয় যে আপনার KYC, প্যান, আধার, ব্যাঙ্ক অ্যাকাউন্ট, বিদ্যুৎ সরবরাহ বা ডেলিভারি ব্লক করে দেওয়া হবে।
• মেসেজে থাকা লিঙ্কে ক্লিক না করে, নিজে থেকেই অফিসিয়াল ব্যাংকিং বা পরিষেবা অ্যাপ্লিকেশনটি খুলুন।

• সম্ভব হলে অ্যাকাউন্টগুলোর জন্য একটি ব্যাকআপ সিকিউরিটি কী নিবন্ধন করুন এবং এটি নিরাপদে সংরক্ষণ করুন।
• ব্যক্তিগত, পারিবারিক, সম্পর্ক বিষয়ক বিবরণ এবং ছবি পোস্ট করা থেকে বিরত থাকুন।সোশ্যাল মিডিয়ায়।
• সামাজিক মাধ্যমে আপনার ভ্রমণসূচী বা দৈনন্দিন কার্যকলাপ প্রকাশ করবেন না। • সামাজিক মাধ্যমে আপনার পছন্দ, অপছন্দ, রাজনৈতিক মতাদর্শ, আর্থিক কেনাকাটা এবং ব্যক্তিগত কার্যকলাপ প্রকাশ করবেন না।

• বাড়ির ওয়াইফাইয়ের জন্য শক্তিশালী পাসওয়ার্ডসহ WPA2 AES বা WPA 3 এনক্রিপশন ব্যবহার করুন।

• আপনি যদি হোম ক্যামেরা এবং IoT ডিভাইস ব্যবহার করেন, তাহলে নিশ্চিত করুন যে ডেটা আপনার ডেটা কার্ডেই থাকছে। এটি ক্লাউডে স্থানান্তর করবেন না।

• সোশ্যাল মিডিয়ায় ছদ্মবেশী অ্যাকাউন্ট ব্লক করুন এবং রিপোর্ট করুন। 28/10/2026 পি রাজাগোপাল

টাম্পি 9

ইনপ্রতারণা ঘটলে কী করতে হবে?

১. অবিলম্বে ১৯৩০ নম্বরে ফোন করুন - এটি ভারতের জাতীয় সাইবার আর্থিক জালিয়াতি হেল্পলাইন।
২. ঘটনাটি অনলাইনে রিপোর্ট করুনজাতীয় সাইবার অপরাধ রিপোর্টিং পোর্টাল
৩. অবিলম্বে আপনার ব্যাংকের সাথে যোগাযোগ করুন।
৪. প্রয়োজন অনুযায়ী প্রভাবিত কার্ড, অ্যাকাউন্ট বা পেমেন্ট অ্যাক্সেস ব্লক করার জন্য অনুরোধ করুন। ৫. দ্রুত রিপোর্ট করলে আরও অর্থ স্থানান্তর বন্ধ করার সুযোগ বাড়ে, যদিও পুনরুদ্ধারের কোনো নিশ্চয়তা নেই। এছাড়াও এই পদক্ষেপগুলো নিন:
১. সন্দেহভাজন প্রতারকের সাথে যোগাযোগ বন্ধ করুন।

২. রিমোট-অ্যাক্সেস সেশনগুলো বিচ্ছিন্ন করুন এবং অননুমোদিত সফটওয়্যার অপসারণের জন্য সাহায্য নিন। ৩. একটি বিশ্বস্ত ডিভাইস ব্যবহার করে ফাঁস হওয়া পাসওয়ার্ডগুলো পরিবর্তন করুন। ৪. সন্দেহজনক লগইন সেশনগুলো বাতিল করুন এবং প্রয়োজনে প্রমাণীকরণ পদ্ধতিগুলো রিসেট করুন। ৫. মেসেজ, স্ক্রিনশট, ফোন নম্বর, লেনদেনের তথ্য এবং অন্যান্য প্রমাণ সংরক্ষণ করুন। ৬. ভুয়া প্রোফাইল, ডিপফেক এবং ছদ্মবেশ ধারণের বিষয়বস্তু সম্পর্কে সংশ্লিষ্ট প্ল্যাটফর্ম ও কর্তৃপক্ষকে জানান। ৭. আপনার অ্যাকাউন্ট প্রতারণামূলক মেসেজ পাঠানোর জন্য ব্যবহার করা হলে, ক্ষতিগ্রস্ত পরিচিতদের সতর্ক করুন।

১. স্বাধীনভাবে যাচাই না করে কোনো পরিচিত কণ্ঠস্বর বা মুখ বিশ্বাস করবেন না। ২. কখনো ওটিপি, পিন, পাসওয়ার্ড বা ব্যাংকিং তথ্য প্রকাশ করবেন না।

৩. হুমকি, জরুরি অবস্থা বা গোপনীয়তার কারণে কখনো টাকা পাঠাবেন না।

৪. ডিজিটাল গ্রেপ্তার বা পুলিশের নিরাপদ অ্যাকাউন্টের দাবি কখনো বিশ্বাস করবেন না।

৫. টাকা গ্রহণ করার জন্য কখনো কিউআর কোড স্ক্যান করবেন না বা ইউপিআই পিন প্রবেশ করাবেন না।

৬. কোনো অপরিচিত ব্যক্তির অনুরোধে কখনো সফটওয়্যার ইনস্টল করবেন না বা আপনার স্ক্রিন শেয়ার করবেন না।

৭. অপ্রত্যাশিত লিঙ্ক, বিনিয়োগের অফার বা পেনশন-সংক্রান্ত বার্তা কখনও বিশ্বাস করবেন না। ৮. ফোন আপডেট রাখুন এবং শক্তিশালী অ্যাকাউন্ট প্রমাণীকরণ সক্রিয় করুন।

৯. অস্বাভাবিক আর্থিক সিদ্ধান্ত নেওয়ার আগে একজন বিশ্বস্ত ব্যক্তির সাথে পরামর্শ করুন। ১০. প্রতারণা ঘটলে, অবিলম্বে আপনার ব্যাঙ্কের সাথে যোগাযোগ করুন এবং ১৯৩০ নম্বরে ফোন করুন।

১১. মনে রাখার মতো সবচেয়ে কার্যকর নীতিটি হলো:

১২. কোনো কণ্ঠস্বর, মুখ, বার্তা বা ভিডিও দেখতে আসল মনে হলেই তা বিশ্বাস করবেন না। কোনো পদক্ষেপ নেওয়ার আগে পরিচয় এবং অনুরোধটি আলাদাভাবে যাচাই করে নিন।

	মোবাইল ফোনের নি
সেটিংস	প্রস্তাবিত সেটিং
অবস্থান	শুধুমাত্র অ্যাপটি ব্যবহা
ক্যামেরা	শুধুমাত্র অ্যাপটি ব্যবহা
মাইক্রোফোন	প্রতিবার জিজ্ঞাসা করু
যোগাযোগ এবং এসএমএস	প্রতিবার জিজ্ঞাসা করু
ক্যালেন্ডার	প্রতিবার জিজ্ঞাসা করু

স্বাস্থ্য তথ্য	না
ছবি এবং ভিডিও	না
শারীরিক কার্যকলাপ	না
বিজ্ঞপ্তি	না
ব্লুটুথ	শুধুমাত্র ব্যবহারের সময়
এআই অ্যাপস	প্রশিক্ষণের জন্য ডেটা ব্য

সৌভাগ্য সেখানেই যেখানে সুযোগ এবং প্রস্তুতি মিলিত হয়।

এআইপি রিসার্চ ওয়েবসাইট HTTPS:AIPATHFINDER.ORG

ফলিত মানব-কেন্দ্রিক এআই –HTTPS://www.amazon.com/dp/B0CYXHYPHC

আপনার বুদ্ধিমত্তাকে শক্তিশালী করুন -https://www.amazon.in/dp/B0D3WZXY99

ধন্যবাদ!