

سابق فوجیوں اور ویر ناریوں کے ذریعہ سائبرسیکیوریٹی فراڈ سے نمٹنا

کمانڈر پی راجگوپال ٹمپی IN (R)

- AI اور بڑی زبان کے ماڈل
- AI سافٹ ویئر اور میں کیا فرق ہے؟
- ایجنٹ کیا ہے؟
- ایک ایجنٹ ایل ایل ایم سے کیسے مختلف ہے؟

AI کے کچھ اہم فوائد کیا ہیں؟

- سائنسی دریافتوں میں تیزی سے پیش رفت
- نئے مواد، نئے مالیکیولز، پیداواری فوائد
- موسم کی پیشین گوئیاں
- سافٹ ویئر کوڈنگ
- روبوٹ اور آٹومیشن

- AI کے بڑے خطرات کیا ہیں؟

دھوکہ دہی، طاقت کی تلاش اور خود کو بچانا

- ڈیپ فیکس
- کنٹرول کا نقصان
- بار بار خود کی بہتری (RSI)
- خود نقل

- پیشین گوئی IoT گلے لگنے والا واقعہ، انتھروپک
- فرانس میں ریفریجریشن پلانٹس کو ہیک کرنا - اکتوبر 2026 کے وسط میں
- اکتوبر 2026 st کیڑے) - PHP 21) سرکاری ویب سائٹس ڈاؤن
- اور جنگ کے وقت کے استعمال CBRN ،فطری طور پر دوہری استعمال کی ٹیکنالوجی – خود مختار ہتھیار میں بڑے خطرات۔
- سائبرسیکیوریٹی کا ایک فعال اور محافظ ہے۔ AI
- ہمارے دماغ سے زیادہ طاقتور کمپیوٹنگ انجن (تیز اور لامحدود وسائل)۔ ہم انہیں پکڑنے یا سمجھنے کے قابل نہیں ہوں گے۔
- چلاتے ہیں اور سینکڑوں کی تعداد میں زبردستی خفیہ کاری کر سکتے ہیں، سافٹ ویئر میں x7ایجنٹ 24
- سسٹمز پاور آن ٹریننگ کے بعد پوری جانکاری کے ساتھ چل سکتے ہیں، AI • کیڑے تلاش کر سکتے ہیں۔ کہیں بھی ہجرت کر سکتے ہیں اور ہو سکتا ہے کہ ہم ان کا پتہ نہ لگا سکیں جب تک کہ بہت دیر نہ ہو جائے۔
- کو انٹرنیٹ پر قبضہ کرنے اور انفراسٹرکچر کو ہیک کرنے سے قریبی مدت کا نقصان ہو سکتا ہے۔ نظام AI اور افادیت.

• سسٹمز تک پہنچیں AI شکوک و شبہات اور اعتماد کی کم سطح کے ساتھ:
• سوشل میڈیا سے جو کچھ حاصل ہوتا ہے اس پر بھروسہ نہ کریں۔
• یا مساوی گفتگو کی نگرانی کرنے والی ایپس کو غیر فعال رکھیں۔ Siri
• اگر آپ چیٹ جی پی ٹی یا کلاڈ جیسے اے آئی ٹولز استعمال کرتے ہیں تو "ہر ایک کے لیے ماڈل کو بہتر بنائیں" کے آپشن اور لوکیشن آپشن کو آف کر دیں۔
• ایجنٹوں کے استعمال سے گریز کریں سوائے اس کے کہ آپ قابل اعتماد طریقے سے تصدیق کر سکیں کہ یہ AI تجارتی طور پر دستیاب آپ کے ذاتی ڈیٹا کو کیسے ہینڈل کرتا ہے۔ اسے کم خطرے والے ایپلی کیشنز کے لیے صرف اس صورت میں استعمال کریں جب آپ کو بالکل ضرورت ہو۔
• ایجنٹ کے حوالے نہ کریں خاص طور پر اپنی ڈائری یا پرائیویٹ جرنل • اپنے بینک اکاؤنٹس، AI اپنے خیالات اور ارادے کسی بھی ایجنٹس تک رسائی نہ دیں۔ AI بل، ادائیگیوں، دیگر مالی معاملات اور لین دین میں خودکار لین دین کے لیے
• اپنے فولڈرز، ای میل سروسز اور کارڈ کی معلومات تک رسائی فراہم نہ کریں۔
• سے نہ کہیں کہ وہ آپ کے لیے اپنی سوچ کرے۔ AI ،"ہمیشہ "اپنے لیے سوچیں
• سسٹمز سے۔ AI اپنے سوچنے کے عمل کی تصدیق کسی قابل اعتماد دوست سے کریں نہ کہ
• پرائیویسی کنٹرولز کو مؤثر طریقے سے استعمال کریں، طبی اور مالیاتی ریکارڈز صرف ناگزیر ضرورت پر اپ لوڈ کریں۔ 28/10/2026

• کبھی بھی فون کرنے والے پر بھروسہ نہ کریں کیونکہ آواز بالکل خاندان کے کسی فرد کی طرح ہے۔ • اگر کوئی ہنگامی حالت میں اپنے رشتہ دار ہونے کا دعوی کرتا ہے اور پیسے مانگتا ہے، تو اس شخص کو اس کے پہلے محفوظ کردہ نمبر پر رابطہ منقطع کریں اور واپس کال کریں۔

• ہنگامی حالات کے لیے نجی خاندان کی تصدیق کے فقرے پر اتفاق کریں۔ اسے سوشل پر شیئر نہ کریں۔ میڈیا

• یہ نہ سمجھیں کہ ویڈیو کال حقیقی ہے کیونکہ آپ اس شخص کے چہرے کو پہچانتے ہیں۔ رقم، رازداری یا فوری کارروائی کی فوری درخواستوں کو انتباہی علامات کے طور پر سمجھیں۔ • پولیس، سی بی آئی، کسٹمز، عدالتوں یا دیگر حکام کے پاس موجود پیغامات پر یقین نہ کریں۔ آپ کو ڈیجیٹل گرفتاری میں رکھا۔

• شناخت کے ثبوت کے طور پر کالر آئی ڈی، واٹس ایپ پروفائل فوٹوز یا ظاہر کردہ تنظیم کے ناموں پر بھروسہ نہ کریں۔

• اپنے آن لائن ڈیٹا پروفائل اور فوٹ پرنٹ کو کم سے کم ممکنہ حد تک کم کریں • نقالی کی مثال (جعلی ویڈیو کال کی منظوری کی وجہ سے $25 ملین منتقل ہوئے)۔

• بغیر کسی جائز مقصد کے شناختی دستاویزات کا اشتراک کرنے سے گریز کریں۔
• جہاں مناسب ہو، شناختی دستاویزات کی کاپیوں میں مقصد کے لیے مخصوص واٹر مارک شامل کریں۔
• WhatsApp، Facebook، Instagram اور دیگر سماجی پلیٹ فارمز پر رازداری کی ترتیبات کا جائزہ لیں۔
محدود کریں کہ کون آپ کو میسجنگ گروپس میں شامل کرسکتا ہے، گروپ کی رکنیت کو کم سے کم کرنے کی کوشش کریں۔ عوامی طور پر دستیاب صوتی ریکارڈنگ اور ذاتی ویڈیوز کو محدود کریں جہاں عملی ہوں۔ • تفصیلی خاندانی تعلقات، معمولات اور مالی حالات کو شائع کرنے سے گریز کریں۔ عوامی آن لائن پروفائلز سے غیر ضروری ذاتی کی سرکاری آدھار کی توثیق کی تاریخ اور بائیو میٹرک لاکنگ سہولیات کا استعمال UIDAI • معلومات کو ہٹا دیں۔
کریں جہاں مناسب
• جہاں دستیاب ہو سرکاری ٹیلی کام سروسز کے ذریعے اپنے موبائل کنکشن چیک کریں۔
کم بھروسہ سبسکرپشنز اور رجسٹریشن کے لیے علیحدہ ای میل ایڈریس استعمال کریں۔ • کلاؤڈ شیئرنگ لنکس کا جائزہ لیں اور جب مزید ضرورت نہ ہو تو عوامی رسائی کو ہٹا دیں۔

• یاد رکھیں: رقم وصول کرنے کے OTP پاس ورڈ، تاریخ پیدائش یا CVV، پن ATM، پن UPI، کبھی بھی اپنا بینکنگ پن ظاہر نہ کریں۔
• رقم وصول کرنے کے UPI PIN لیے آپ کو درج کرنے کی ضرورت نہیں ہے۔ اس میں داخل ہونا عام طور پر ادائیگی کی اجازت دیتا ہے۔
QR کوڈ کو کبھی بھی اسکین نہ کریں۔ لیے کسی اجنبی کی طرف سے بھیجے گئے
• UPI کبھی بھی غیر متوقع جمع کرنے کی درخواست کو منظور نہ کریں۔
• AI کا استعمال کرتے ہوئے اعلیٰ منافع یا غیر معمولی منافع کی ضمانت دینے والی سرمایہ کاری کی اسکیموں پر بھروسہ نہ کریں۔
ایجنٹوں اور اجنبیوں کو کبھی بھی اپنی بینکنگ ایپلیکیشن کو دور سے چلانے کی اجازت نہ دیں۔
بینک کارڈز، چیک یا مالیاتی دستاویزات کی تصویریں نامعلوم لوگوں کے ساتھ شیئر نہ کریں۔ • تمام اہم اکاؤنٹس پر ٹرانزیکشن الرٹس کو فعال کریں۔
• اپنی ضروریات کے مطابق روزانہ کی منتقلی کی حدیں مقرر کریں، جہاں آپ کا بینک اجازت دیتا ہے۔
• کارڈز کی دیکھ بھال: اگر آپ آن لائن اس سے بچ سکتے ہیں تو کارڈ کی تفصیلات کو ذخیرہ نہ کریں۔ کارڈ کی تفصیلات کو خودکار طریقے سے بھرنے سے گریز کریں۔ • کریڈٹ کارڈ آن لائن لین دین کی حد کو کم کریں جب زیادہ حدوں کی ضرورت نہ ہو۔ • ضرورت نہ ہونے پر بین الاقوامی کارڈ کے لین دین کو غیر فعال کریں۔
• خصوصی طور پر بیرون ملک سفر کرتے وقت کنٹیکٹ لیس لین دین کو غیر فعال کریں - ایمسٹرڈیم کا واقعہ • خاطر خواہ بچتوں کو ان اکاؤنٹس سے UPI/الگ رکھیں جو اکثر آن لائن ادائیگیوں کے لیے استعمال ہوتے ہیں۔

• بینکنگ، ای میل اور اہم اکاؤنٹس کے لیے مختلف پاس ورڈ استعمال کریں۔ • لمبے پاسورڈز یا پاس ورڈز استعمال کریں جن کا اندازہ لگانا مشکل ہو۔

• تصدیق کو فعال کریں۔ • اپنے فون کو FIDO2 جہاں کہیں بھی دستیاب ہو دو عنصر کی تصدیق یا پن، فنگر پرنٹ یا چہرے کی تصدیق کے ساتھ لاک کریں۔

• اپنے فون اور ایپلیکیشنز کو تازہ ترین ریلیز کے ساتھ اپ ڈیٹ رکھیں۔ • صرف سرکاری ایپ اسٹورز سے ایپلیکیشنز ڈاؤن لوڈ کریں۔

• کسی نامعلوم شخص کے ذریعے واٹس ایپ، ایس ایم ایس یا ای میل کے ذریعے بھیجی گئی APK یا ایپلیکیشن انسٹال نہ کریں۔

• کسی اجنبی کی درخواست پر اسکرین شیئرنگ یا ریموٹ ایکسیس ایپلی کیشنز انسٹال نہ کریں۔ • غیر متوقع آدھار، بینک اکاؤنٹ، بجلی کی ،PAN ،KYC لنکس پر کلک نہ کریں جس میں یہ دعویٰ کیا جائے کہ آپ کا فراہمی یا ترسیل بلاک کر دی جائے گی۔

• پیغامات میں لنکس پر کلک کرنے کے بجائے خود سرکاری بینکنگ یا سروس ایپلیکیشن کھولیں۔

• اگر ممکن ہو تو اکاؤنٹس کے لیے بیک اپ سیکیورٹی کلید رجسٹر کریں اور اسے محفوظ طریقے سے اسٹور کریں۔

.ذاتی، خاندانی، رشتے کی تفصیلات اور تصویریں لگانے سے گریز کریں۔ سوشل میڈیا پر

• اپنے سفری پروگرام یا روزمرہ کے معمولات کو سوشل میڈیا پر شائع نہ کریں۔ • سوشل میڈیا پر اپنی پسند، ناپسند، سیاسی جھکاؤ، مالی خریداری اور نجی سرگرمیوں کو ظاہر نہ کریں۔

• انکرپشن WPA 3 یا WPA2 AES ہوم وائی فائی کے لیے مضبوط پاس ورڈز کے ساتھ استعمال کریں۔

• آلات استعمال کرتے ہیں تو یقینی بنائیں کہ ڈیٹا آپ کے ڈیٹا IoT اگر آپ گھر کے کیمرے اور کارڈ میں موجود رہے۔ اسے بادل میں منتقل نہ کریں۔

• سوشل میڈیا پر نقالی اکاؤنٹس کو بلاک اور رپورٹ کریں۔

میناگر فراڈ ہوا ہے تو کیا کرنا ہے؟

1. فوری طور پر 1930 پر کال کریں - ہندوستان کی قومی سائبر مالیاتی فراڈ ہیلپ لائن۔
2. واقعہ کی آن لائن اطلاع دیں۔ نیشنل سائبر کرائم رپورٹنگ پورٹل
3. فوری طور پر اپنے بینک سے رابطہ کریں۔
4. متاثرہ کارڈز، اکاؤنٹس یا ادائیگی تک رسائی کو مسدود کرنے کی درخواست کریں۔ 5. ابتدائی رپورٹنگ مزید منتقلی کو روکنے کے موقع کو بہتر بناتی ہے، حالانکہ بحالی کی ضمانت نہیں ہے۔ یہ اقدامات بھی کریں:
1. مشتبہ دھوکے باز کے ساتھ بات چیت کرنا بند کریں۔
2. دور دراز تک رسائی کے سیشن منقطع کریں اور غیر مجاز سافٹ ویئر کو ہٹانے میں مدد طلب کریں۔ 3. ایک قابل اعتماد آلہ کا استعمال کرتے ہوئے سمجھوتہ شدہ پاس ورڈز کو تبدیل کریں۔
4. مشکوک لاگ ان سیشنز کو منسوخ کریں اور جہاں ضروری ہو توثیق کے طریقوں کو دوبارہ ترتیب دیں۔ 5. پیغامات، اسکرین شاٹس، فون نمبرز، لین دین کے حوالے اور دیگر شواہد محفوظ رکھیں۔ 6. جعلی پروفائلز، ڈیپ فیکس اور نقالی مواد کی متعلقہ پلیٹ فارمز اور حکام کو اطلاع دیں۔ 7. متاثرہ رابطوں کو خبردار کریں اگر آپ کا اکاؤنٹ دھوکہ دہی کے پیغامات بھیجنے کے لیے استعمال ہوا ہے۔

پی راجگوپال تمپی 10 28/10/2026

1. آزاد تصدیق کے بغیر کسی مانوس آواز یا چہرے پر کبھی بھروسہ نہ کریں۔ 2. کبھی بھی

پاس ورڈ یا بینکنگ اسناد کا انکشاف نہ کریں۔ OTP، PIN،

3. دھمکیوں، عجلت یا رازداری کی وجہ سے کبھی بھی رقم منتقل نہ کریں۔

4. ڈیجیٹل گرفتاری یا پولیس کے محفوظ اکاؤنٹس کے دعووں پر کبھی یقین نہ کریں۔

5. درج نہ کریں۔ UPI PIN کوڈ کو اسکین نہ کریں یا QR رقم وصول کرنے کے لیے کبھی بھی

6. کسی اجنبی کی درخواست پر کبھی بھی سافٹ ویئر انسٹال نہ کریں یا اپنی اسکرین کا اشتراک نہ کریں۔

7. کبھی بھی غیر متوقع لنکس، سرمایہ کاری کی پیشکش یا پنشن سے متعلق پیغامات پر بھروسہ نہ کریں۔

8. فون کو اپ ڈیٹ رکھیں اور مضبوط اکاؤنٹ کی تصدیق کو فعال کریں۔

9. غیر معمولی مالی فیصلے کرنے سے پہلے کسی قابل اعتماد شخص سے مشورہ کریں۔ 10.

اگر فراڈ ہوتا ہے تو اپنے بینک سے رابطہ کریں اور 1930 پر فوراً کال کریں۔

11. یاد رکھنے کا واحد سب سے مؤثر اصول ہے:

12. کبھی بھی کسی آواز، چہرے، پیغام یا ویڈیو پر صرف اس لیے بھروسہ نہ کریں کہ یہ حقیقی معلوم ہوتا ہے۔ کارروائی کرنے سے پہلے شناخت اور درخواست کی آزادانہ تصدیق کریں۔

پی راجگوپال تمپی 11 28/10/2026

ف ایپ استعمال کرتے وقت	مقام
ف ایپ استعمال کرتے وقت	کیمرے
ہر بار پوچھیں	مائکروفون
ہر بار پوچھیں	رابطے اور ایس ایم ایس

یورٹی اور ترتیبات	
تجویز کردہ ترتیب	سیٹنگز

کیلنڈر	ہر بار پوچھیں
صحت کے اعداد و شمار	نہیں
تصاویر اور ویڈیوز	نہیں
جسمانی سرگرمی	نہیں
اطلاعات	نہیں

بلوٹوتھ	صرف استعمال کرتے وقت
ایپس AI	لیے ڈیٹا استعمال نہ کریں۔

پی راجگوپال ٹمپی۔
28/10/2026 12

خوش قسمتی ہے جہاں موقع اور تیاری مل جاتی ہے۔

AIP ریسرچ ویب سائٹ HTTPS:AIPATHFINDER.ORG

AI اپلائیڈ ہیومن سینٹرک - HTTPS://www.amazon.com/dp/B0CYXHYPHC

اپنی ذہانت کو طاقت دیں - https://www.amazon.in/dp/B0D3WZXY99

آپ کا شکریہ!