

ويٹرنس ۽ ويرِ ناريس پاران سائبر سيڪيورٽي فراڊ کي سنپالڻ

IN (R) ڪمانڈر پي راجگوپال ٽيمپي

- AI ۽ وڏي پولي جا مادل
- AI سافٽ ويئر ۽ ۾ چا فرق آهي؟
- ايجنٽ چا آهي؟
- هڪ ايجنٽ هڪ ايل ايل ايم کان ڪيئن مختلف آهي؟
- AI ڪجهه اهم فائدا ڪهڙا آهن؟
    - سائنسي دريافتن ۾ تيز ترقي
    - نوان مواد، نوان مالیڪيول، پيداواري فائدا
    - موسم جي اڳڪٿيون
    - سافٽ ويئر ڪوڊنگ
    - روبوٽ ۽ خودڪار
- AI جا وڏا خطرا ڪهڙا آهن؟
    - فريب، طاقت جي ڳولا ۽ پاڻ کي بچائڻ
    - ڊيپ فيڪس
    - ضابطي جو نقصان
    - ورجائيندڙ خود سڌارو (RSI)
    - خود نقل

- هگنگ فيس واقعو، اينٽروپڪ آئي او ٽي جي اڳڪٿي
- فرانس ۾ ريفريجريشن پلانٽس جي هيڪنگ - آڪٽوبر 2026 جي وچ ۾
- بگ) – 21سينٽ آڪٽوبر PHP 2026) سرڪاري ويب سائيٽون بند
- فطري طور تي ٻٹي استعمال واري ٽيڪنالاجي - خودمختيار هٿيارن، سي بي آر اين ۽ جنگ جي وقت جي استعمال ۾ وڏا خطرا.
- AI سائبر سيڪيورٽي جو هڪ فعال ڪندڙ ۽ محافظ آهي.
- اسان جي دماغن کان وڌيڪ طاقتور ڪمپيوٽنگ انجن (تيز ۽ لامحدود وسيلا). اسانانهن کي پڪڙي يا سمجهي نه سگهنداسين
- هلن ٿا ۽ سوين ۾ زبردستي انڪرپشن ڪري سگهن ٿا، سافٽ ويئر ۾ بگ ڳولي سگهن ٿا. • پاور 7xايجنٽ 24 • سسٽم مڪمل ڇاڻ سان ڪم ڪري سگهن ٿا، ڪٽي به منتقل ٿي سگهن ٿا ۽ اسان شايد AI آن تي تربيت کان پوءِ انهن کي ان وقت تائين نه ڳولي سگهون جيستائين تمام دير نه ٿي وڃي.
- جي قبضي ۽ انفراسٽرڪچر کي هيڪ ڪرڻ سان ويجهي مدت جو نقصان ٿي سگهي ٿو.سسٽم ۽ AI انٽرنيٽ تي افاديتون.

• سسٽم ڏانهن رجوع ڪريو AI شڪ ۽ گهٽ سطح جي اعتماد سان:
• سوشل ميڊيا مان حاصل ڪيل شين تي اعتبار نه ڪريو.
• سري يا ان جي برابر گفتگو جي نگراني ڪندڙ ايپس کي غير فعال رکو.
• جيڪڏهن توهان چيٽ جي پي ٽي يا ڪلاڊ جهڙا اي آءِ ٽولز استعمال ڪندا آهيو ته ”امپروو ماڊل فار ايوريو“ آپشن ۽ لوڪيشن آپشن کي بند ڪريو.
• ايجنٽن کي استعمال ڪرڻ کان پاسو ڪريو سواءِ ان جي ته جيڪڏهن توهان قابل اعتماد طور تي تصديق AI تجارتي طور تي موجود ڪري سگهو ته اهو توهان جي ذاتي ڊيٽا کي ڪيئن سنڀالينڊو آهي. ان کي صرف گهٽ خطري واري ايپليڪيشنن لاءِ استعمال ڪريو جيڪڏهن توهان کي بلڪل ضرورت هجي.
• ايجنٽ خاص طور تي پنهنجي ڊائري يا خانگي جرنل جي حوالي نه ڪريو • پنهنجي بينڪ اڪائونٽس، AI پنهنجا خيال ۽ ارادا ڪنهن به ايجنٽن کي رسائي نه ڏيو AI بل، ادائيگين، ٻين مالي معاملن ۽ ٽرانزيڪشن ۾ خودڪار ٽرانزيڪشن لاءِ.
• پنهنجن فولڊرن، اي ميل سروسز ۽ ڪارڊ جي معلومات تائين رسائي فراهم نه ڪريو.
• هميشه "پنهنجي لاءِ سوچيو"، مصنوعي ذهانت کي توهان جي لاءِ سوچڻ لاءِ نه چئو.
• سسٽم سان AI پنهنجي سوچ جي عمل جي تصديق ڪنهن قابل اعتماد دوست سان ڪريو نه ته.
• رازداري ڪنٽرول کي مؤثر طريقي سان استعمال ڪريو، طبي ۽ مالي رڪارڊ صرف ناگزير ضرورت تي اپلوڊ ڪريو.28/10/2026 P

• ڪڏهن به ڪنهن ڪال ڪندڙ تي صرف ان ڪري اعتبار نه ڪريو جو آواز بلڪل ڪنهن خاندان جي ميمبر وانگر لڳي ٿو. • جيڪڏهن ڪو ماڻهو ايمرجنسي ۾ مائٽ هجڻ جو دعويٰ ڪري ٿو ۽ پئسا گهري ٿو، ته ان شخص جو رابطو ڪٽيو ۽ ان جي اڳ ۾ محفوظ ڪيل نمبر تي واپس ڪال ڪريو.

• هنگامي حالتن لاءِ هڪ خانگي خانداني تصديق واري جملي تي متفق ٿيو. ان کي سوشل ميڊيا تي شيئر نه ڪريو.ميڊيا.

• صرف ان ڪري نه سمجهو ته وڊيو ڪال حقيقي آهي چاڪاڻ ته توهان ان شخص جي چهري کي سڃاڻو ٿا. • پئسن، رازداري يا فوري ڪارروائي لاءِ فوري درخواستن کي ڊيجاريندڙ نشانين طور سمجهو. • انهن پيغامن تي يقين نه ڪريو جيڪي دعويٰ ڪن ٿا ته پوليس، سي بي آءِ، ڪسٽم، عدالتون يا ٻيا اختيارتوهان کي ڊجيٽل گرفتاري هيٺ رکيو.

• سڃاڻپ جي ثبوت طور ڪالر آئي ڊي، وائس اپ پروفائل تصويرن يا ڏيکاريل تنظيم جي نالن تي اعتبار نه ڪريو.

• پنهنجي آن لائن ڊيٽا پروفائل ۾ فوٽ پرنٽ کي گهٽ ۾ گهٽ ممڪن حد تائين گهٽايو • نقل ڪرڻ جي (مثال (جعلي وڊيو ڪال جي منظوري جي ڪري $25 ملين منتقل ڪيا ويا.

• ڪنهن جائز مقصد کان سواءِ سچاٽپ دستاويز شيئر ڪرڻ کان پاسو ڪريو.
• جتي مناسب هجي، سچاٽپ دستاويزن جي ڪاپين ۾ هڪ مقصد لاءِ مخصوص واٽر مارڪ شامل ڪريو.• واٽس اپ، فيس بڪ، انسٽاگرام ۽ ٻين سماجي پليٽ فارمن تي رازداري سيٽنگن جو جائزو وٺو.• محدود ڪريو ته ڪير توهان کي ميسيجنگ گروپن ۾ شامل ڪري سگهي ٿو، ڪوشش ڪريو ۽ گروپ ميمبرشپ کي گهٽ ڪريو. • جتي عملي هجي اتي عوامي طور تي دستياب وائس رڪارڊنگ ۽ ذاتي وڊيوز کي محدود ڪريو. • تفصيلي خانداني رشتن، معمولات ۽ مالي حالتن کي شايع ڪرڻ کان پاسو ڪريو. • عوامي آن لائن پروفائلز مان غير ضروري ذاتي معلومات هٽايو.• UIDAI جي سرڪاري بنياد جي تصديق-تاريخ ۽ بايوميٽرڪ-لاڪنگ سهولتن کي استعمال ڪريو جتيمناسب.
• جتي موجود هجي، سرڪاري ٽيليڪام سروسز ذريعي پنهنجا موبائل ڪنيڪشن چيڪ ڪريو.
• گهٽ اعتماد واري سبسڪرپشن ۽ رجسٽريشن لاءِ الڳ اي ميل پتو استعمال ڪريو.• ڪلائوڊ شيئرنگ لنڪس جو جائزو وٺو ۽ جڏهن ضرورت نه هجي ته عوامي رسائي کي هٽايو.

• ڪڏهن به پنهنجو بينڪنگ پن، يو پي آءِ پن، اي ٽي ايم پن، سي وي وي، پاسورڊ، تاريخ پيدائش يا او ٽي پي ظاهر نه ڪريو.• ياد رکو: پئسا پن داخل ڪرڻ جي ضرورت ناهي. ان کي داخل ڪرڻ سان عام طور تي ادائيگي جي اجازت ملندي آهي.• UPI وصول ڪرڻ لاءِ توهان کي

ڪوڊ کي اسڪين نه ڪريو QR ڪڏهن به ڪنهن اجنبي طرفان پئسا وصول ڪرڻ لاءِ موڪليل.

• گڏ ڪرڻ جي درخواست منظور نه ڪريو UPI ڪڏهن به غير متوقع.

• AI • استعمال ڪندي ضمانت ٿيل اعليٰ واپسي يا غير معمولي منافعي جو واعدو ڪندڙ سيڙپڪاري اسڪيمن تي پروسو نه ڪريو.
ڪڏهن به ايجنٽ ۽ اجنبي ماڻهن کي پنهنجي بينڪنگ ايپليڪيشن کي پري کان هلائڻ جي اجازت نه ڏيو.

• بينڪ ڪارڊ، چيڪ يا مالي دستاويزن جون تصويرون نامعلوم ماڻهن سان شيئر نه ڪريو. • سڀني اهم اڪائونٽس تي
ٽرانزيڪشن الرٽس کي فعال ڪريو.

• جتي توهان جي بينڪ اجازت ڏئي، توهان جي ضرورتن مطابق روزاني منتقلي جي حد مقرر ڪريو.

• ڪاردن جي سنپال: جيڪڏهن توهان آن لائن کان بچي سگهو ٿا ته ڪارڊ جي تفصيلن کي ذخيرو نه ڪريو. ڪارڊ جي تفصيلن جي خودڪار طريقي
سان پرڻ جي طريقيڪار کان پاسو ڪريو. • ڪريڊٽ ڪارڊ آن لائن ٽرانزيڪشن جي حدن کي گهٽايو جڏهن وڌيڪ حدون گهربل نه هجن. • جڏهن
ضرورت نه هجي ته بين الاقوامي ڪارڊ ٽرانزيڪشن کي غير فعال ڪريو.

• خاص طور تي ٻاهرين ملڪ سفر ڪرڻ وقت رابطي کان سواءِ ٽرانزيڪشن کي بند ڪريو - ايمسٽرڊيم واقعو • بار بار آن لائن / يو پي آءِ ادائيگين لاءِ
استعمال ٿيندڙ اڪائونٽس کان وڌي بچت کي الگ رکو.28/10/2026 P Rajagopal Tampi 7

• بينڪنگ، اي ميل ۽ اهم اڪائونٽس لاءِ مختلف پاسورڊ استعمال ڪريو. • ڊگها پاسورڊ يا
پاس فريز استعمال ڪريو جن جو اندازو لڳائڻ ڏکيو هجي.

• تصديق کي فعال ڪريو.• پن، فنگر پرنٽ يا FIDO2 جتي به موجود هجي، ٻه عنصر جي تصديق يا

چهري جي تصديق سان پنهنجو فون لاڪ ڪريو.

• پنهنجي فون ۽ ايپليڪيشنن کي تازي رليز سان اپڊيٽ رکو. • صرف سرڪاري ايپ استورن تان ايپليڪيشنون ڊائون لوڊ ڪريو.

• يا ايپليڪيشن انسٽال APK ڪنهن نامعلوم شخص پاران واٽس اپ، ايس ايم ايس يا اي ميل ذريعي موڪليل نه ڪريو.

• ڪنهن اجنبي جي درخواست تي اسڪرين شيئرنگ يا ريموٽ رسائي ايپليڪيشنز انسٽال نه ڪريو. • غير متوقع بينڪ اڪائونٽ، ،Aadhaar ،PAN ،KYC لنڪس تي ڪلڪ نه ڪريو جيڪي دعويٰ ڪن ٿا ته توهان جو بجلي جي فراهمي يا ترسيل بلاڪ ڪئي ويندي.

• پيغامن ۾ لنڪ تي ڪلڪ ڪرڻ بدران سرڪاري بينڪنگ يا سروس ايپليڪيشن پاڻ کوليو.

• جيڪڏهن ممڪن هجي ته اڪائونٽس لاءِ بيڪ اپ سيڪيورٽي کي رجسٽر ڪريو ۽ ان کي محفوظ طور تي محفوظ رکو.

• ذاتي، خاندااني، رشتي جي تفصيل ۽ تصويرون لڳائڻ کان پاسو ڪريو.سوشل ميڊيا تي

• سوشل ميڊيا تي پنهنجي سفر جي پروگرام يا روزاني معمول کي شايع نه ڪريو. • سوشل ميڊيا

تي پنهنجي پسند، ناپسند، سياسي رجحانات، مالي خريداري ۽ نجي سرگرمين کي ظاهر نه ڪريو.

- انڪرپشن استعمال WPA 3 يا WPA2 AES گھر جي وائي فائي لاءِ مضبوط پاسورڊ سان ڪريو.
- جيڪڏهن توهان گھر ۾ ڪيمرا ۽ آئي او ٽي ڊوائيسز استعمال ڪندا آهيو ته پڪ ڪريو ته ڊيٽا توهان جي ڊيٽا ڪارڊ تي رهي. ان کي ڪلائوڊ ڏانهن منتقل نه ڪريو.
- سوشل ميڊيا تي نقلي اڪائونٽس کي بلاڪ ۽ رپورٽ ڪريو.28/10/2026 P Rajagopal Tampi 9

اندر جيڪڏهن جعلسازي ٿي آهي ته ڇا ڪجي؟

1. فوري طور تي 1930 تي ڪال ڪريو - هندستان جي قومي سائبر مالي فراڊ هيلپ لائن.
2. واقعي جي رپورٽ آن لائن ڪريو نيشنل سائبر ڪرائم رپورٽنگ پورٽل
3. فوري طور تي پنهنجي بينڪ سان رابطو ڪريو
4. مناسب طور تي متاثر ٿيل ڪارڊن، اڪائونٽس يا ادائيگي جي رسائي کي بلاڪ ڪرڻ جي درخواست ڪريو.5. ابتدائي رپورٽنگ وڌيڪ منتقلي کي روڪڻ جو موقعو بهتر بڻائي ٿي، جيتوڻيڪ وصولي جي ضمانت نه آهي.پڙ هيٺيان قدم کڻو:
1. شڪي جعلساز سان رابطو ڪرڻ بند ڪريو.

2. ريموٽ رسائي سيشن کي ڊسڪنيڪٽ ڪريو ۽ غير مجاز سافٽ ويئر کي هٽائڻ ۾ مدد ونو. 3. قابل اعتماد ڊوائيس استعمال ڪندي سمجهوتي ٿيل پاسورڊ تبديل ڪريو.

4. مشڪوڪ لاگ ان سيشن کي رد ڪريو ۽ جتي ضروري هجي تصديق جي طريقن کي ري سيٽ ڪريو.5. پيغام، اسڪرين شاٽ، فون نمبر، ٽرانزيڪشن جا حوالا ۽ ٻيا ثبوت محفوظ ڪريو. 6. جعلي پروفائلز، ڊيپ فيڪس ۽ نقالي واري مواد جي لاڳاپيل پليٽ فارمن ۽ اختيارين کي رپورٽ ڪريو. 7. متاثر ٿيل رابطن کي خبردار ڪريو جيڪڏهن توهان جو اڪائونٽ جعلي پيغام موڪلڻ لاءِ استعمال ڪيو ويو آهي.

1. ڪڏهن به ڪنهن واقف آواز يا چهري تي آزاد تصديق کان سواءِ اعتبار نه ڪريو. 2. ڪڏهن به OTP، پن، پاسورڊ يا بينڪنگ سند ظاهر نه ڪريو.

3. ڪڏهن به ڏمڪين، تڪڙ يا رازداري جي ڪري پئسا منتقل نه ڪريو.

4. ڊجيٽل گرفتاري يا پوليس جي محفوظ اڪائونٽس جي دعوائن تي ڪڏهن به يقين نه ڪريو.

5. UPI پن داخل نه ڪريو يا QR ڪوڊ اسڪين نه ڪريو پئسا وصول ڪرڻ لاءِ ڪڏهن به.

6. ڪڏهن به ڪنهن اجنبي جي درخواست تي سافٽ ويئر انسٽال نه ڪريو يا پنهنجي اسڪرين شيئر نه ڪريو.

7. ڪڏهن به غير متوقع لنڪس، سيڙپڪاري آڇون يا پينشن سان لاڳاپيل پيغامن تي پروسو نه ڪريو. 8. فونز کي اپڊيٽ رکو ۽ مضبوط اڪائونٽ جي تصديق کي فعال ڪريو.

9. .10 غير معمولي مالي فيصلا ڪرڻ کان اڳ ڪنهن قابل اعتماد شخص سان صلاح ڪريو.
جيڪڏهن فراڊ ٿئي ٿو، ته پنهنجي بينڪ سان رابطو ڪريو ۽ فوري طور تي 1930 تي ڪال ڪريو.

11. ياد رکڻ لاءِ سڀ کان وڌيڪ اثرائتو اصول هي آهي:

12. ڪڏهن به ڪنهن آواز، چهري، پيغام يا وڊيو تي صرف ان ڪري اعتبار نه ڪريو جو اهو حقيقي لڳي ٿو. ڪارروائي ڪرڻ کان اڳ سڃاڻپ ۽ درخواست جي آزادانه طور تي تصديق ڪريو.

نه	صحت جو ڊيٽا
نه	تصويرون ۽ وڊيوز
نه	جساني سرگرمي
نه	اطلاع
صرف استعمال ڪرڻ وقت	بلوٽوٿ
ڪ لاءِ ڊيٽا استعمال نه ڪريو	ايپس AI

جورٽي ۽ سيٽنگون	
تجويز ڪيل سيٽنگ	سيٽنگون
، ايپ استعمال ڪرڻ وقت	جڳهه
، ايپ استعمال ڪرڻ وقت	ڪئميرا
هر پيري پچو	مائڪروفون
هر پيري پچو	رابطا ۽ ايس ايم ايس
هر پيري پچو	ڪئلينڈر

قسمت اها آهي جتي موقعو ۽ تياري ملندي آهي

AIP ريسرچ ويب سائيٽ HTTPS:AIPATHFINDER.ORG

ايچ ٽي ٽي پي ايس-لاڳو ٿيل انساني-مرڪزي مصنوعي ذهانت -https://www.amazon.com/dp/B0CYXHYPHC

پنهنجي ذهانت کي مضبوط ڪريو -https://www.amazon.in/dp/B0D3WZXY99

تنهنجي مهرباني!