

# વેટરન્સ અને વીર નારીસ દ્વારા સાયબર સુરક્ષા છેતરપિંડીઓનું સંચાલન

કમાન્ડર પી રાજગોપાલ ટેમ્પી IN (R)

- AI અને મોટા ભાષા મોડેલ્સ
- સોફ્ટવેર અને AI વચ્ચે શું તફાવત છે?
- એજન્ટ શું છે?
- એજન્ટ અને LLM વચ્ચે શું તફાવત છે?
- કેટલાક મહત્વપૂર્ણ AI ફાયદા શું છે?
    - વૈજ્ઞાનિક શોધોમાં ઝડપી પ્રગતિ
    - નવી સામગ્રી, નવા અણુઓ, ઉત્પાદકતા લાભો
    - હવામાન આગાહીઓ
    - સોફ્ટવેર કોડિંગ
    - રોબોટ્સ અને ઓટોમેશન
- AI ના મુખ્ય જોખમો શું છે?
    - છેતરપિંડી, સત્તાની શોધ અને સ્વ-બચાવ
    - ડીપફેક્સ
    - નિયંત્રણ ગુમાવવું
    - રિકર્સિવ સ્વ-સુધારણા (RSI)
    - સ્વ-પ્રતિકૃતિ

- હગિંગફેસ ઘટના, એન્થ્રોપિક IoT આગાહી
- ફ્રાન્સમાં રેફ્રિજરેશન પ્લાન્ટ્સને હેક કરવા - મધ્ય ઓક્ટોબર 2026
- સરકારી વેબસાઇટ્સ ડાઉન (PHP બગ્સ) – 21 સેન્ટ ઑક્ટોબર ૨૦૨૬
- સ્વાભાવિક રીતે બેવડા ઉપયોગની ટેકનોલોજી - સ્વાયત્ત શસ્ત્રો, CBRN અને યુદ્ધ સમયના ઉપયોગમાં મોટા જોખમો.
- AI એ સાયબર સુરક્ષાને સક્ષમ બનાવનાર અને બચાવ કરનાર છે
- આપણા મગજ કરતાં વધુ શક્તિશાળી કમ્પ્યુટિંગ એન્જિન (ઝડપી અને અમર્યાદિત સંસાધનો). આપણેતેમને પકડી કે સમજી શકશે નહીં
- એજન્ટો 24x7 ચાલે છે અને સેંકડોની સંખ્યામાં તેઓ ફોર્સ ફોર્સ એન્ક્રિપ્શન કરી શકે છે, સોફ્ટવેરમાં બગ્સ શોધી શકે છે. • પાવર ઓન પર તાલીમ લીધા પછી AI સિસ્ટમ્સ સંપૂર્ણ જ્ઞાન સાથે કાર્યરત થઈ શકે છે, ગમે ત્યાં સ્થળાંતર કરી શકે છે અને આપણે તેમને ખૂબ મોડું થાય ત્યાં સુધી શોધી શકતા નથી.
- AI દ્વારા ઇન્ટરનેટ પર કબજો મેળવવાથી અને ઇન્ફ્રાસ્ટ્રક્ચર હેક કરવાથી નજીકના ગાળાનું નુકસાન થઈ શકે છે.સિસ્ટમો અને ઉપયોગિતાઓ.

• શંકા અને વિશ્વાસના નીચા સ્તર સાથે AI સિસ્ટમ્સનો ઉપયોગ કરો:
• સોશિયલ મીડિયા પરથી જે મળે છે તેના પર વિશ્વાસ ન કરો.
• સિરી અથવા તેના જેવી વાતચીત મોનિટરિંગ એપ્લિકેશનોને અક્ષમ રાખો.
• જો તમે ચેટ GPT અથવા ક્લાઉડ જેવા AI ટૂલ્સનો ઉપયોગ કરો છો, તો “ઈમ્પ્રુવ મોડેલ ફોર એવરીવન” વિકલ્પ અને લોકેશન વિકલ્પ બંધ કરો.
• વ્યાપારી રીતે ઉપલબ્ધ AI એજન્ટોનો ઉપયોગ કરવાનું ટાળો, સિવાય કે જો તમે વિશ્વસનીય રીતે ચકાસી શકો કે તે તમારા વ્યક્તિગત ડેટાને કેવી રીતે હેન્ડલ કરે છે. જો તમને ખરેખર જરૂર હોય તો જ ઓછા જોખમવાળા કાર્યક્રમો માટે તેનો ઉપયોગ કરો.
• તમારા વિચારો અને ઇરાદા કોઈપણ AI એજન્ટને ખાસ કરીને તમારી ડાયરી અથવા ખાનગી જર્નલને ન સોંપો. • તમારા બેંક ખાતા, બિલ, ચુકવણીઓ, અન્ય નાણાકીય બાબતો અને વ્યવહારોમાં સ્વચાલિત વ્યવહારો માટે AI એજન્ટોને ઍક્સેસ આપશો નહીં.
• તમારા ફોલ્ડર્સ, ઇમેઇલ સેવાઓ અને કાર્ડ માહિતીની ઍક્સેસ આપશો નહીં.
• હંમેશા "તમારા માટે વિચારો", AI ને તમારા માટે તમારા વિચારો કરવાનું ન કહો.
• તમારી વિચાર પ્રક્રિયાને AI સિસ્ટમ્સ સાથે નહીં, પરંતુ વિશ્વસનીય મિત્ર સાથે ચકાસો.

• ગોપનીયતા નિયંત્રણોનો અસરકારક રીતે ઉપયોગ કરો, અનિવાર્ય જરૂરિયાત પર જ તબીબી અને નાણાકીય રેકોર્ડ

અપલોડ કરો.

• ફોન કરનાર વ્યક્તિ પર ફક્ત એટલા માટે વિશ્વાસ ન કરો કે તેનો અવાજ બિલકુલ પરિવારના સભ્ય જેવો લાગે છે. • જો કોઈ વ્યક્તિ કટોકટીમાં સંબંધી હોવાનો દાવો કરે છે અને પૈસા માંગે છે, તો તેને ડિસ્કનેક્ટ કરો અને તેના અગાઉ સેવ કરેલા નંબર પર પાછા કૉલ કરો.

• કટોકટી માટે ખાનગી કૌટુંબિક ચકાસણી શબ્દસમૂહ પર સંમત થાઓ. તેને સોશિયલ મીડિયા પર શેર કરશો નહીં.મીડિયા.

• ફક્ત એટલા માટે ન માનો કે તમે વ્યક્તિનો ચહેરો ઓળખો છો એટલા માટે વિડિઓ કોલ અસલી છે. • પૈસા, ગુપ્તતા અથવા તાત્કાલિક કાર્યવાહી માટેની તાત્કાલિક વિનંતીઓને ચેતવણીના સંકેતો તરીકે ગણો.

• એવા સંદેશાઓ પર વિશ્વાસ ન કરો કે જે દાવો કરે છે કે પોલીસ, સીબીઆઈ, કસ્ટમ્સ, કોર્ટ અથવા અન્ય અધિકારીઓતમને ડિજિટલ ધરપકડ હેઠળ મૂક્યા.

• ઓળખના પુરાવા તરીકે કોલર આઈડી, વોટ્સએપ પ્રોફાઇલ ફોટોગ્રાફ્સ અથવા પ્રદર્શિત સંસ્થાના નામો પર વિશ્વાસ કરશો નહીં.

• તમારી ઓનલાઈન ડેટા પ્રોફાઇલ અને ફૂટપ્રિન્ટ શક્ય તેટલી ઓછી કરો • નકલનું ઉદાહરણ (નકલી વિડીયો કોલ મંજૂરીને કારણે $25 મિલિયન ટ્રાન્સફર થયા).



• કાયદેસર હેતુ વિના ઓળખ દસ્તાવેજો શેર કરવાનું ટાળો.
• જ્યાં યોગ્ય હોય, ઓળખ દસ્તાવેજોની નકલોમાં હેતુ-વિશિષ્ટ વોટરમાર્ક ઉમેરો.• WhatsApp, Facebook, Instagram અને અન્ય સોશિયલ પ્લેટફોર્મ પર ગોપનીયતા સેટિંગ્સની સમીક્ષા કરો.• મેસેજિંગ ગ્રુપમાં તમને કોણ ઉમેરી શકે છે તે મર્યાદિત કરો, ગ્રુપ મેમ્બરશિપ ઓછી કરવાનો પ્રયાસ કરો. • જ્યાં શક્ય હોય ત્યાં સાર્વજનિક રીતે ઉપલબ્ધ વૉઇસ રેકોર્ડિંગ અને વ્યક્તિગત વિડિઓઝને મર્યાદિત કરો. • વિગતવાર કૌટુંબિક સંબંધો, દિનચર્યાઓ અને નાણાકીય પરિસ્થિતિઓ પ્રકાશિત કરવાનું ટાળો. • જાહેર ઑનલાઇન પ્રોફાઇલ્સમાંથી બિનજરૂરી વ્યક્તિગત માહિતી દૂર કરો.• UIDAI ની સત્તાવાર આધાર પ્રમાણીકરણ-ઇતિહાસ અને બાયોમેટ્રિક-લોકિંગ સુવિધાઓનો ઉપયોગ કરો જ્યાંયોગ્ય.
• જ્યાં ઉપલબ્ધ હોય ત્યાં સત્તાવાર સરકારી ટેલિકોમ સેવાઓ દ્વારા તમારા મોબાઇલ કનેક્શન તપાસો.

• ઓછા વિશ્વાસપાત્ર સબ્સ્ક્રિપ્શન્સ અને નોંધણીઓ માટે અલગ ઇમેઇલ સરનામાંનો ઉપયોગ કરો.• ક્લાઉડ-શેરિંગ લિંક્સની સમીક્ષા કરો અને જ્યારે જરૂર ન હોય ત્યારે જાહેર ઍક્સેસ દૂર કરો.



• ક્યારેય તમારો બેંકિંગ પિન, UPI પિન, ATM પિન, CVV, પાસવર્ડ, જન્મ તારીખ અથવા OTP જાહેર કરશો નહીં.• યાદ રાખો: પૈસા મેળવવા માટે તમારે UPI પિન દાખલ કરવાની જરૂર નથી. તેને દાખલ કરવાથી સામાન્ય રીતે ચુકવણી અધિકૃત થાય છે.• કોઈ અજાણી વ્યક્તિ દ્વારા પૈસા મેળવવા માટે મોકલવામાં આવેલ QR કોડ ક્યારેય સ્કેન કરશો નહીં.

• ક્યારેય અણધારી UPI કલેક્શન વિનંતીને મંજૂરી આપશો નહીં.

• AI નો ઉપયોગ કરીને ગેરંટીકૃત ઉચ્ચ વળતર અથવા અસાધારણ નફાનું વચન આપતી રોકાણ યોજનાઓ પર વિશ્વાસ ન કરો.• એજન્ટો અને અજાણ્યા લોકોને ક્યારેય તમારી બેંકિંગ એપ્લિકેશન દૂરથી ચલાવવાની મંજૂરી આપશો નહીં.

• અજાણ્યા લોકો સાથે બેંક કાર્ડ, ચેક અથવા નાણાકીય દસ્તાવેજોના ફોટોગ્રાફ્સ શેર કરશો નહીં. • બધા મહત્વપૂર્ણ ખાતાઓ પર વ્યવહાર ચેતવણીઓ સક્ષમ કરો.

• તમારી બેંક પરવાનગી આપે ત્યાં, તમારી જરૂરિયાતો અનુસાર દૈનિક ટ્રાન્સફર મર્યાદા સેટ કરો.

• કાર્ડસની સંભાળ: જો તમે કાર્ડની વિગતો ઓનલાઈન ટાળી શકો તો તેનો સંગ્રહ કરશો નહીં. કાર્ડની વિગતો આપમેળે ભરવાની પ્રક્રિયા ટાળો. • જ્યારે ઊંચી મર્યાદા જરૂરી ન હોય ત્યારે ક્રેડિટ-કાર્ડ ઓનલાઈન વ્યવહાર મર્યાદા ઘટાડો. • જ્યારે જરૂરી ન હોય ત્યારે આંતરરાષ્ટ્રીય કાર્ડ વ્યવહારો અક્ષમ કરો.

• ખાસ કરીને વિદેશ મુસાફરી કરતી વખતે સંપર્ક રહિત વ્યવહારો બંધ કરો - એમ્સ્ટરડેમ ઘટના • વારંવાર ઓનલાઈન/UPI ચુકવણી માટે ઉપયોગમાં લેવાતા ખાતાઓથી નોંધપાત્ર બચત અલગ રાખો.28/10/2026 પી રાજગોપાલ ટેમ્પી 7

• બેંકિંગ, ઇમેઇલ અને મહત્વપૂર્ણ ખાતાઓ માટે અલગ અલગ પાસવર્ડનો ઉપયોગ કરો. • લાંબા પાસવર્ડ અથવા પાસફ્રેઝનો ઉપયોગ કરો જેનો અંદાજ લગાવવો મુશ્કેલ હોય.

• જ્યાં પણ ઉપલબ્ધ હોય ત્યાં દ્વિ-પરિબળ પ્રમાણીકરણ અથવા FIDO2 પ્રમાણીકરણ સક્ષમ કરો.• તમારા ફોનને PIN, ફિંગરપ્રિન્ટ અથવા ફેસ ઓથેન્ટિકેશન વડે લોક કરો.

• તમારા ફોન અને એપ્લિકેશનોને નવીનતમ રીલીઝ સાથે અપડેટ રાખો. • ફક્ત સત્તાવાર એપ સ્ટોર્સમાંથી જ એપ્લિકેશનો ડાઉનલોડ કરો.

• કોઈ અજાણ્યા વ્યક્તિ દ્વારા WhatsApp, SMS કે ઈમેલ દ્વારા મોકલવામાં આવેલ APK કે એપ્લિકેશન ઇન્સ્ટોલ કરશો નહીં.

• કોઈ અજાણી વ્યક્તિના કહેવા પર સ્ક્રીન-શેરિંગ અથવા રિમોટ-એક્સેસ એપ્લિકેશન ઇન્સ્ટોલ કરશો નહીં. • તમારા KYC, PAN, આધાર, બેંક એકાઉન્ટ, વીજળી પુરવઠો અથવા ડિલિવરી બ્લોક કરવામાં આવશે એવો દાવો કરતી અણધારી લિંક્સ પર ક્લિક કરશો નહીં.
• સંદેશાઓમાં લિંક્સ પર ક્લિક કરવાને બદલે, સત્તાવાર બેંકિંગ અથવા સેવા એપ્લિકેશન જાતે ખોલો.



• શક્ય હોય તો એકાઉન્ટ્સ માટે બેકઅપ સુરક્ષા કી રજીસ્ટર કરો અને તેને સુરક્ષિત રીતે સંગ્રહિત રાખો.
• વ્યક્તિગત, કૌટુંબિક, સંબંધોની વિગતો અને ફોટોગ્રાફ્સ મૂકવાનું ટાળોસોશિયલ મીડિયા પર.
• સોશિયલ મીડિયા પર તમારા પ્રવાસ કાર્યક્રમ અથવા દિનચર્યા પ્રકાશિત કરશો નહીં. • સોશિયલ મીડિયા પર તમારી પસંદ, નાપસંદ, રાજકીય ઝુકાવ, નાણાકીય ખરીદી અને ખાનગી પ્રવૃત્તિઓનો ખુલાસો કરશો નહીં.

- ધરના વાઇફાઇ માટે મજબૂત પાસવર્ડ સાથે WPA2 AES અથવા WPA 3 એન્ક્રિપ્શનનો ઉપયોગ કરો.
- જો તમે ધરના કેમેરા અને IoT ઉપકરણોનો ઉપયોગ કરો છો, તો ખાતરી કરો કે ડેટા તમારા ડેટા કાર્ડ પર જ રહે. તેને ક્લાઉડમાં ટ્રાન્સફર કરશો નહીં.
- સોશિયલ મીડિયા પર નકલી એકાઉન્ટ્સને બ્લોક કરો અને તેની જાણ કરો.



# માંજો છેતરપિંડી થઈ હોય તો શું કરવું?

૧. તાત્કાલિક ૧૯૩૦ પર કૉલ કરો - ભારતની રાષ્ટ્રીય સાયબર નાણાકીય છેતરપિંડી હેલ્પલાઇન.
2. ઘટનાની ઓનલાઈન જાણ કરોરાષ્ટ્રીય સાયબર ક્રાઇમ રિપોર્ટિંગ પોર્ટલ
૩. તાત્કાલિક તમારી બેંકનો સંપર્ક કરો
4. યોગ્ય હોય ત્યાં સુધી અસરગ્રસ્ત કાર્ડ, એકાઉન્ટ અથવા ચુકવણી ઍક્સેસને અવરોધિત કરવાની વિનંતી કરો.૫. વહેલા રિપોર્ટિંગથી વધુ ટ્રાન્સફર રોકવાની તક વધે છે, જોકે પુનઃપ્રાપ્તિની ખાતરી નથી.આ પગલાં પણ લો:
૧. શંકાસ્પદ છેતરપિંડી કરનાર સાથે વાતચીત કરવાનું બંધ કરો.

2. રિમોટ-એક્સેસ સત્રોને ડિસ્કનેક્ટ કરો અને અનધિકૃત સોફ્ટવેરને દૂર કરવામાં મદદ લો. 3. વિશ્વસનીય ઉપકરણનો ઉપયોગ કરીને ચેડા થયેલા પાસવર્ડ્સ બદલો.
4. શંકાસ્પદ લોગિન સત્રો રદ કરો અને જ્યાં જરૂરી હોય ત્યાં પ્રમાણીકરણ પદ્ધતિઓ ફરીથી સેટ કરો.૫. સંદેશાઓ, સ્ક્રીનશોટ, ફોન નંબર, વ્યવહાર સંદર્ભો અને અન્ય પુરાવા સાચવો. ૬. સંબંધિત પ્લેટફોર્મ અને અધિકારીઓને નકલી પ્રોફાઇલ્સ, ડીપફેક્સ અને નકલ સામગ્રીની જાણ કરો. ૭. જો તમારા એકાઉન્ટનો ઉપયોગ કપટપૂર્ણ સંદેશાઓ મોકલવા માટે કરવામાં આવ્યો હોય તો અસરગ્રસ્ત સંપર્કોને ચેતવણી આપો.



૧. સ્વતંત્ર ચકાસણી વિના ક્યારેય કોઈ પરિચિત અવાજ કે ચહેરા પર વિશ્વાસ ન કરો. ૨. ક્યારેય OTP, PIN, પાસવર્ડ કે બેંકિંગ ઓળખપત્ર જાહેર ન કરો.
૩. ધમકીઓ, તાકીદ અથવા ગુપ્તતાને કારણે ક્યારેય પૈસા ટ્રાન્સફર કરશો નહીં.
૪. ડિજિટલ ધરપકડ અથવા પોલીસ સેફ એકાઉન્ટ્સના દાવાઓ પર ક્યારેય વિશ્વાસ કરશો નહીં.
5. પૈસા મેળવવા માટે ક્યારેય QR કોડ સ્કેન કરશો નહીં કે UPI પિન દાખલ કરશો નહીં.
૬. કોઈ અજાણી વ્યક્તિના કહેવા પર ક્યારેય સોફ્ટવેર ઇન્સ્ટોલ કરશો નહીં કે તમારી સ્ક્રીન શેર કરશો નહીં.
7. ક્યારેય અણધારી લિંક્સ, રોકાણ ઓફર અથવા પેન્શન સંબંધિત સંદેશાઓ પર વિશ્વાસ ન કરો. 8. ફોન અપડેટ રાખો અને મજબૂત એકાઉન્ટ પ્રમાણીકરણ સક્ષમ કરો.

9. અસામાન્ય નાણાકીય નિર્ણયો લેતા પહેલા વિશ્વસનીય વ્યક્તિની સલાહ લો.
10. જો છેતરપિંડી થાય, તો તાત્કાલિક તમારી બેંકનો સંપર્ક કરો અને 1930 પર કૉલ કરો.
૧૧. યાદ રાખવાનો એકમાત્ર સૌથી અસરકારક સિદ્ધાંત છે:
૧૨. ક્યારેય કોઈ અવાજ, ચહેરો, સંદેશ અથવા વિડિઓ ફક્ત એટલા માટે વિશ્વાસ ન કરો કે તે વાસ્તવિક લાગે છે. કાર્યવાહી કરતા પહેલા ઓળખ અને વિનંતીની સ્વતંત્ર રીતે ચકાસણી કરો.

28/10/2026 પી રાજગોપાલ ટેમ્પી 11

| | |
|---|---|
| આરોગ્ય ડેટા | ના |
| ફોટા અને વિડિઓઝ | ના |
| શારીરિક પ્રવૃત્તિ | ના |
| સૂચનાઓ | ના |
| બ્લૂટૂથ | ફક્ત ઉપયોગ કરતી વ |
| AI એપ્સ | તાલીમ માટે ડેટાનો ઉપ |

| | મોબાઇલ ફોન સુ |
|---|---|
| સેટિંગ્સ | ભલામણ કરેલ સેટિંગ |
| સ્થાન | ફક્ત એપ્લિકેશનનો ઉ |
| કેમેરા | ફક્ત એપ્લિકેશનનો ઉ |
| માઇક્રોફોન | દર વખતે પૂછો |
| સંપર્કો અને એસએમએસ | દર વખતે પૂછો |
| કૅલેન્ડર | દર વખતે પૂછો |

પી રાજગોપાલ ટામ્પી
૨૮/૧૦/૨૦૨૬ ૧૨

# નસીબ એ છે જ્યાં તક અને તૈયારી મળે છે

AIP રિસર્ચ વેબસાઇટ HTTPS:AIPATHFINDER.ORG

લાગુ માનવ-કેન્દ્રિત કૃત્રિમ બુદ્ધિ -HTTPS://www.amazon.com/dp/B0CYXHYPHC

તમારી બુદ્ધિને શક્તિ આપો -https://www.amazon.in/dp/B0D3WZXY99

# આભાર!