इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

certin
Enhancing Cyber Security in India

ISEA
Information Security Education & Awareness

Digital India
Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

AI જાગૃતિ માર્ગદર્શિકા

સાયબર સ્વચ્છતાની સંસ્કૃતિ બનાવો

#સાયબર સ્વચ્છતાઆપણી સંસ્કૃતિ



રાષ્ટ્રીય સાયબર સુરક્ષા જાગૃતિ મહિનો (ઓક્ટોબર 2026)

પ્રકાશક

ભારતીય કમ્પ્યુટર ઇમરજન્સી રિસ્પોન્સ ટીમ

અમને અનુસરો : @IndianCERT @cert_india

વિષયસુચીકોષ્ટક

પ્રસ્તાવના ૩

એઆઈ-ઉન્નત ફિશિંગ અને સોશિયલ એન્જિનિયરિંગ ૪

વૉઇસ અને વિડિઓ ડીપફેક્સ (વિશિંગ) ૫

AI-સહાયિત માલવેર અને સ્વચાલિત હુમલાઓ ૬

નકલી વેબસાઇટ્સ અને ઓળખ ચોરી ૭

લાલ ધ્વજ ચેકલિસ્ટ ૮

ઓનલાઇન સલામતી ૯

ઉપકરણ સલામતી ૧૦

AI નો જવાબદારીપૂર્વક ઉપયોગ કરો ૧૧

વિશ્વસનીય એપ્લિકેશનો પસંદ કરો ૧૨

સાયબર સુરક્ષા ઘટનાઓની જાણ CERT-In ને કરો. ૧૩

પ્રસ્તાવના

આર્ટિફિશિયલ ઇન્ટેલિજન્સ (AI) આપણા જીવન, કાર્ય અને વાતચીત કરવાની રીતમાં પરિવર્તન લાવી રહ્યું છે. તે નવીનતાને સક્ષમ બનાવે છે, ઉત્પાદકતામાં સુધારો કરે છે અને વિવિધ ક્ષેત્રોમાં જટિલ સમસ્યાઓ ઉકેલવામાં મદદ કરે છે. જો કે, આ જ ટેકનોલોજીનો દુરુપયોગ જોખમી તત્વો દ્વારા વધુ અદ્યતન અને ખાતરીકારક સાયબર ધમકીઓ બનાવવા માટે પણ થઈ રહ્યો છે.

AI ડિજિટલ ધમકીઓને ઓળખવાનું વધુ મુશ્કેલ બનાવી રહ્યું છે કારણ કે હુમલાખોરો હવે ખૂબ જ વાસ્તવિક ઇમેઇલ્સ, સંદેશાઓ, ઑડિઓ, વિડિઓઝ અને વેબસાઇટ્સ બનાવી શકે છે. પરંપરાગત ચેતવણી ચિહ્નો, જેમ કે નબળું વ્યાકરણ, અસામાન્ય ફોર્મેટિંગ અથવા સ્પષ્ટ ભૂલો, હવે વિશ્વસનીય સૂચક રહી શકશે નહીં. ચકાસણી અને જવાબદાર ડિજિટલ પ્રથાઓ પહેલા કરતાં વધુ મહત્વપૂર્ણ બની ગઈ છે.

આપણે દરરોજ જે AI ટૂલ્સ અને સ્માર્ટ ડિવાઇસનો ઉપયોગ કરીએ છીએ તે જો કાળજીપૂર્વક ઉપયોગ ન કરવામાં આવે તો તે નવા ગોપનીયતા અને સુરક્ષા જોખમો રજૂ કરી શકે છે. અવિશ્વસનીય AI એપ્લિકેશનો સાથે વ્યક્તિગત અથવા ગુપ્ત માહિતી શેર કરવી, બિનજરૂરી પરવાનગીઓ આપવી, અથવા ચકાસણી વિના AI દ્વારા જનરેટ કરેલી માહિતી પર આધાર રાખવો વ્યક્તિઓ અને સંસ્થાઓને સુરક્ષા જોખમોમાં મૂકી શકે છે.

ઇન્ડિયન કોમ્પ્યુટર ઇમરજન્સી રિસ્પોન્સ ટીમ (CERT-In) દ્વારા "AI સાયબર જાગૃતિ" પરની આ પુસ્તિકા ફક્ત સાયબર સુરક્ષા વ્યાવસાયિકો જ નહીં, પરંતુ રોજિંદા નાગરિકો, કર્મચારીઓ અને ડિજિટલ વપરાશકર્તાઓ માટે રચાયેલ છે. તે સમજાવે છે કે AI ડિજિટલ ખતરાના લેન્ડસ્કેપને કેવી રીતે બદલી રહ્યું છે અને વ્યક્તિગત માહિતી, ઉપકરણો અને ઑનલાઇન ઓળખને સુરક્ષિત રાખવા માટે દરેક વ્યક્તિ અનુસરી શકે તેવા સરળ, વ્યવહારુ પગલાં પ્રદાન કરે છે.

એઆઈ-એન્હાન્સ્ડ ફિશિંગ અને સોશિયલ એન્જિનિયરિંગ



તે કેવી રીતે કામ કરે છે ?

ધમકી આપનારાઓ હવે એવા ઇમેઇલ અને ટેક્સ્ટ મોકલે છે જે વાસ્તવિક અને ભૂલ મુક્ત લાગે છે. તેઓ તમારા વિશેની વિગતોનો ઉપયોગ કરે છે, જેમ કે તમારી નોકરી, તમે ઉપયોગ કરો છો તે સેવાઓ અથવા તાજેતરની પ્રવૃત્તિઓ, જેથી સંદેશાઓ વ્યક્તિગત લાગે. આ સંદેશાઓ સારી રીતે લખાયેલા હોવાથી, તેમને શોધવા ખૂબ મુશ્કેલ બની શકે છે.

કેવી રીતે ઓળખવું?

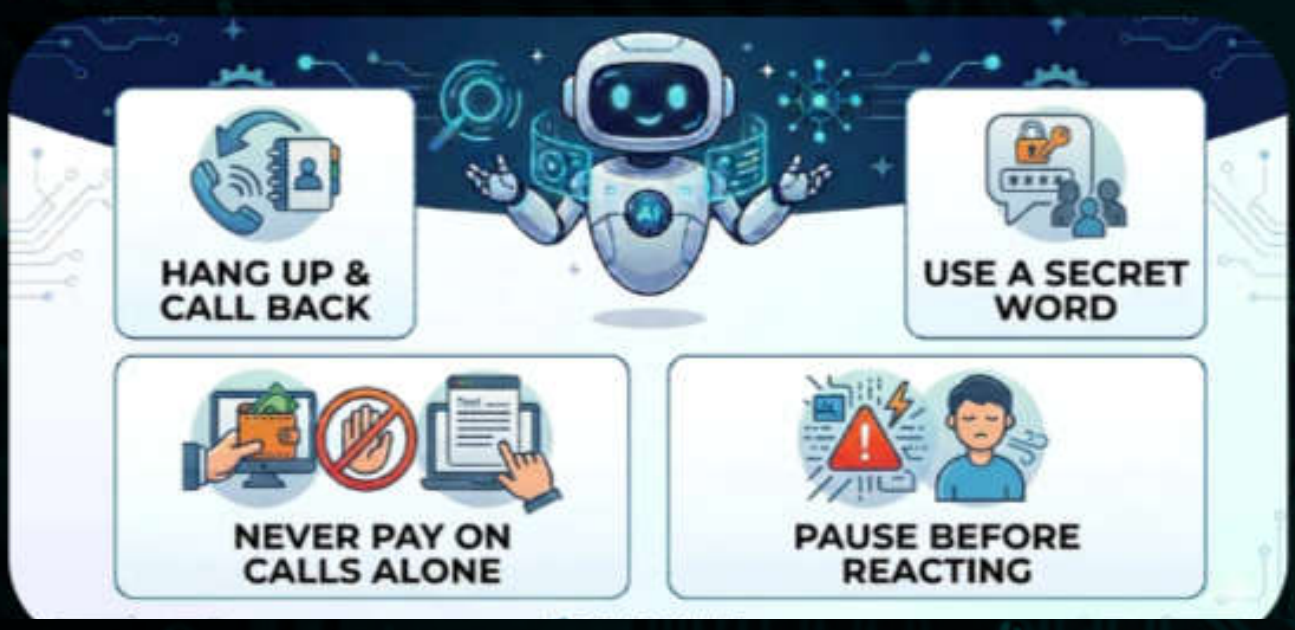
- આ સંદેશ તમારા માટે ખૂબ જ ચોક્કસ લાગે છે પણ અણધારી રીતે આવે છે.
- તે તાત્કાલિક અથવા ધમકીભર્યા સ્વરનો ઉપયોગ કરે છે અને તાત્કાલિક પગલાં લેવાની માંગ કરે છે.
- તે તમને લિંક પર ક્લિક કરવા, એકાઉન્ટ ચકાસવા, પાસવર્ડ રીસેટ કરવા અથવા ચુકવણી કરવા માટે કહે છે.
- મોકલનારનું સરનામું લગભગ સાચું લાગે છે, પણ બરાબર નથી.

સુરક્ષિત કેવી રીતે રહેવું?

- અવાંછિત સંદેશાઓમાં રહેલી લિંક્સ પર ક્લિક કરશો નહીં. તેના બદલે સીધા સત્તાવાર વેબસાઇટ અથવા એપ્લિકેશન પર જાઓ.
- સત્તાવાર ફોન નંબર અથવા એપ્લિકેશન જેવા અલગ, વિશ્વસનીય સંપર્ક ચેનલ દ્વારા વિનંતીઓ ચકાસો.
- મેસેજ લિંક દ્વારા પહોંચેલા પેજ પર ક્યારેય ઓળખપત્રો અથવા OTP દાખલ કરશો નહીં.
- શંકાસ્પદ સંદેશાઓની જાણ કરો અને કાઢી નાખો, પછી મોકલનારને બ્લોક કરો.

અમને અનુસરો : @IndianCERT @cert_india

વોઇસ અને વિડિયો ડીપફેક્સ [વિશિંગ]



તે કેવી રીતે કામ કરે છે ?

ધમકી આપનારા કલાકારો અવાજોનું ક્લોન બનાવી શકે છે અથવા નકલી વિડિઓઝ બનાવી શકે છે જે વાસ્તવિક લાગે છે અને સંભળાય છે. તેઓ તમારા પરિવાર, સાથીદારો અથવા અધિકારીઓ તરીકે પોતાને રજૂ કરી શકે છે જેથી તમને સંવેદનશીલ માહિતી શેર કરવા, પૈસા મોકલવા અથવા ઝડપથી કાર્યવાહી કરવા દબાણ કરી શકાય.

કેવી રીતે ઓળખવું?

- અસામાન્ય તાકીદ, ગભરાટ, અથવા ગુપ્તતા માટેની વિનંતીઓ, જેમ કે કોઈને ન કહેવું.
- થોડો ઓછો સ્વર, ગતિ, પૃષ્ઠભૂમિ અવાજ અથવા ઑડિઓ ગુણવત્તા.
- સામાન્ય ચકાસણી અથવા મંજૂરી પ્રક્રિયાઓને બાયપાસ કરવાની વિનંતીઓ.
- ગિફ્ટ કાર્ડ, ક્રિપ્ટોકરન્સી અથવા વાયર ટ્રાન્સફર દ્વારા ચુકવણી માટેની વિનંતીઓ.

સુરક્ષિત કેવી રીતે રહેવું?

- ફોન કાપી નાખો અને તે વ્યક્તિને તેમના જાણીતા, સેવ કરેલા નંબરનો ઉપયોગ કરીને પાછો ફોન કરો.
- કટોકટીમાં ઓળખ ચકાસવા માટે કુટુંબ અથવા કાર્યસ્થળ માટે સલામત શબ્દ સેટ કરો.
- ફક્ત કૉલ અથવા વિડિઓના આધારે ચુકવણીઓને ક્યારેય અધિકૃત કરશો નહીં. અલગ ચેનલ દ્વારા લેખિતમાં પુષ્ટિ કરો.
- પ્રતિક્રિયા આપતા પહેલા થોભો. ધમકી આપનારાઓ તમારા નિર્ણયને ધૂંધળો કરવા માટે ગભરાટ પર આધાર રાખે છે.

અમને અનુસરો : @IndianCERT @cert_india

એઆઈ-સહાયિત માલવેર અને સ્વચાલિત હુમલાઓ



તે કેવી રીતે કામ કરે છે ?

ધમકી આપનારાઓ દૂષિત કોડ બનાવવા અથવા છુપાવવા, અનેક સાઇટ્સ પર ચોરાયેલા પાસવર્ડ્સનું પરીક્ષણ કરવા અને અપડેટ્સની જરૂર હોય તેવી સિસ્ટમોને ઓળખવા માટે AI ટૂલ્સનો ઉપયોગ કરે છે. આ હુમલાઓને ઝડપી અને વધુ વ્યાપક બનાવે છે.

કેવી રીતે ઓળખવું?

- અનપેક્ષિત લોગિન ચેતવણીઓ, પાસવર્ડ રીસેટ ઇમેઇલ્સ, અથવા તમે વિનંતી ન કરી હોય તેવા MFA સંકેતો
- તમારી એકાઉન્ટ પ્રવૃત્તિમાં સૂચિબદ્ધ અજાણ્યા ઉપકરણો અથવા સત્રો
- એન્ટિવાયરસ ચેતવણીઓ, પોપ-અપ્સ, અથવા અસામાન્ય રીતે ધીમું ઉપકરણ પ્રદર્શન
- ફાઇલો, સેટિંગ્સ અથવા બ્રાઉઝર એક્સ્ટેન્શન્સ જે તમે ઓળખતા નથી

સુરક્ષિત કેવી રીતે રહેવું?

- દરેક એકાઉન્ટ માટે એક અનોખો, મજબૂત પાસવર્ડ વાપરો.
- બધા મહત્વપૂર્ણ ખાતાઓ પર મલ્ટી ફેક્ટર ઓથેન્ટિકેશન (MFA) સક્ષમ કરો.
- એન્ટીવાયરસ સોફ્ટવેર, સિસ્ટમ્સ અને એપ્સને અપ ટુ ડેટ રાખો.
- અણધાર્યા લોગિન અથવા MFA ચેતવણીઓ પર તાત્કાલિક કાર્યવાહી કરો.

અમને અનુસરો : @IndianCERT @cert_india

નકલી વેબસાઇટ્સ અને ઓળખ ચોરી



તે કેવી રીતે કામ કરે છે ?

ધમકી આપનારાઓ તમારા લોગિન ઓળખપત્રો, OTP અથવા ચુકવણી વિગતો ચોરી કરવા માટે બેંકિંગ અથવા શોપિંગ પોર્ટલ જેવી દેખાતી વાસ્તવિક વેબસાઇટ્સ અને ચેટબોટ્સ બનાવી શકે છે. તેઓ ખોટી ઓળખ બનાવવા માટે નકલી ફોટા અથવા દસ્તાવેજોનો પણ ઉપયોગ કરી શકે છે.

કેવી રીતે ઓળખવું?

- થોડા બદલાયેલા વેબસાઇટ URL, જેમ કે વધારાના અક્ષરો, હાઇફન, અથવા અલગ ડોમેન અંત.
- OTP, PIN, અથવા સંપૂર્ણ કાર્ડ નંબર માંગનારા ચેટબોટ્સ અથવા એજન્ટો.
- પરિચિત સાઇટ પર HTTPS ખૂટે છે અથવા અસામાન્ય ડિઝાઇન અસંગતતાઓ છે.

સુરક્ષિત કેવી રીતે રહેવું?

- લિંક્સ પર ક્લિક કરવાને બદલે હંમેશા સીધા જ સત્તાવાર URL લખો અથવા ચકાસાયેલ બુકમાર્ક્સનો ઉપયોગ કરો.
- કોઈપણ ચેટબોટ અથવા "સપોર્ટ એજન્ટ" સાથે ક્યારેય OTP, PIN અથવા સંપૂર્ણ કાર્ડ વિગતો શેર કરશો નહીં.
- ગમે ત્યાં લોગ ઇન કરતા પહેલા HTTPS તપાસો અને ડોમેન નામ કાળજીપૂર્વક જુઓ.
- અજાણી પ્રવૃત્તિ માટે તમારા બેંક સ્ટેટમેન્ટ અને ક્રેડિટ રિપોર્ટનું નિયમિતપણે નિરીક્ષણ કરો.

અમને અનુસરો : @IndianCERT @cert_india

લાલ ધ્વજ ચેકલિસ્ટ

AI-સક્ષમ હુમલાના આ ચિહ્નો પર નજર રાખો:

- પૈસા, ઓળખપત્રો અથવા મંજૂરી માટે તાત્કાલિક, દબાણયુક્ત વિનંતી
- "જાણીતા" વ્યક્તિના કૉલ અથવા વિડિઓમાં થોડી ઑડિઓ/વિડિઓ અસંગતતાઓ
- સામાન્ય ચકાસણી/મંજૂરી પ્રક્રિયાઓને બાયપાસ કરવાની વિનંતી
- અજાણ્યું મોકલનાર ડોમેન અથવા થોડું બદલાયેલું URL
- તમે વિનંતી ન કરી હોય તેવા અનપેક્ષિત MFA સંકેતો અથવા OTP
- સુરક્ષા સોફ્ટવેરને અક્ષમ કરવા અથવા બિનસત્તાવાર લિંક્સ દ્વારા "ચકાસણી" કરવાની વિનંતીઓ
- નોકરી/રોકાણની ઑફરો જેમાં અગાઉથી ચુકવણી અથવા વ્યક્તિગત નાણાકીય વિગતોની જરૂર હોય

જ્યારે શંકા હોય ત્યારે - થોભો, સ્વતંત્ર રીતે ચકાસણી કરો, અને દબાણ હેઠળ કાર્ય ન કરો.

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते
certin Enhancing Cyber Security in India
ISEA Information Security Education & Awareness
Digital India Power To Empower
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

ઓનલાઇન સલામતી



તમારા એકાઉન્ટ્સનું રક્ષણ કરો

- દરેક એકાઉન્ટ માટે મજબૂત અને અનન્ય પાસવર્ડનો ઉપયોગ કરો; તેમને સુરક્ષિત રીતે સંગ્રહિત કરવા માટે પાસવર્ડ મેનેજરનો ઉપયોગ કરો.
- જ્યાં પણ ઉપલબ્ધ હોય ત્યાં મલ્ટી-ફેક્ટર ઓથેન્ટિકેશન (MFA) સક્ષમ કરો.
- ક્યારેય કોઈની સાથે OTP, PIN, પાસવર્ડ અથવા સુરક્ષા કોડ શેર કરશો નહીં.
- વધારાના સુરક્ષા સ્તર તરીકે બાયોમેટ્રિક પ્રમાણીકરણ (ફિંગરપ્રિન્ટ/ચહેરાની ઓળખ) નો ઉપયોગ કરો.

ઇમેઇલ અને ઇન્ટરનેટનો ઉપયોગ કરતી વખતે સુરક્ષિત રહો

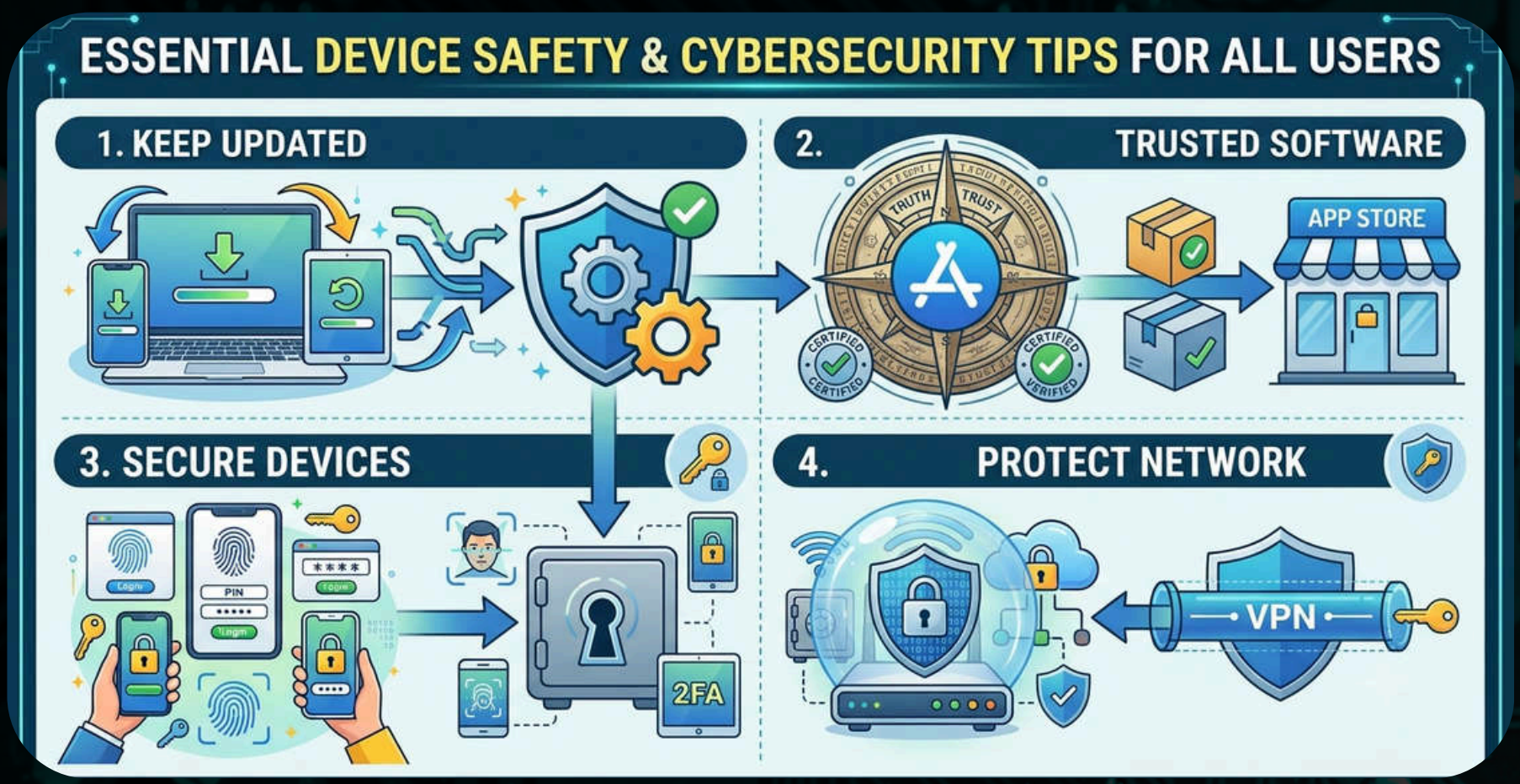
- શંકાસ્પદ અથવા તેના જેવા દેખાતા ઇમેઇલ સરનામાં માટે મોકલનારની વિગતો કાળજીપૂર્વક તપાસો.
- ક્લિક કરતા પહેલા લિંક્સ ચકાસો અને અણધાર્યા જોડાણો ખોલવાનું ટાળો.
- લોગિન અથવા નાણાકીય વિગતો દાખલ કરતા પહેલા વેબસાઇટની અધિકૃતતાની પુષ્ટિ કરો.
- જ્યારે શંકા હોય, ત્યારે કોઈ કાર્ય કરતા પહેલા થોભો અને ચકાસણી કરો.

કંઈક ખોટું થાય તે પહેલાં તૈયારી કરો

- ઑફલાઇન અથવા સુરક્ષિત ક્લાઉડ સેવામાં સંગ્રહિત મહત્વપૂર્ણ ફાઇલોનો નિયમિત બેકઅપ રાખો.
- એકાઉન્ટ પુનઃપ્રાપ્તિ માહિતી (ઈમેલ/ફોન) અપડેટ અને સુરક્ષિત રાખો

અમને અનુસરો : @IndianCERT @cert_india

ઉપકરણ સલામતી



ઉપકરણોને અપડેટ રાખો

- જાણીતી નબળાઈઓને સુધારવા માટે ઓપરેટિંગ સિસ્ટમ્સ, એપ્લિકેશન્સ, બ્રાઉઝર્સ અને સુરક્ષા સોફ્ટવેરને નિયમિતપણે અપડેટ કરો.
- શક્ય હોય ત્યાં સ્વચાલિત અપડેટ્સ સક્ષમ કરો.

ફક્ત વિશ્વસનીય સોફ્ટવેર ઇન્સ્ટોલ કરો

- વાસ્તવિક સોફ્ટવેરનો ઉપયોગ કરો અને ફક્ત સત્તાવાર એપ સ્ટોર્સ અથવા વિશ્વસનીય સ્ત્રોતોમાંથી જ એપ્લિકેશનો ઇન્સ્ટોલ કરો.
- વિશ્વસનીય એન્ટીવાયરસ અથવા સુરક્ષા ઉકેલોનો ઉપયોગ કરો અને તેમને અપડેટ રાખો.

તમારા ઉપકરણો અને એકાઉન્ટ્સને સુરક્ષિત કરો

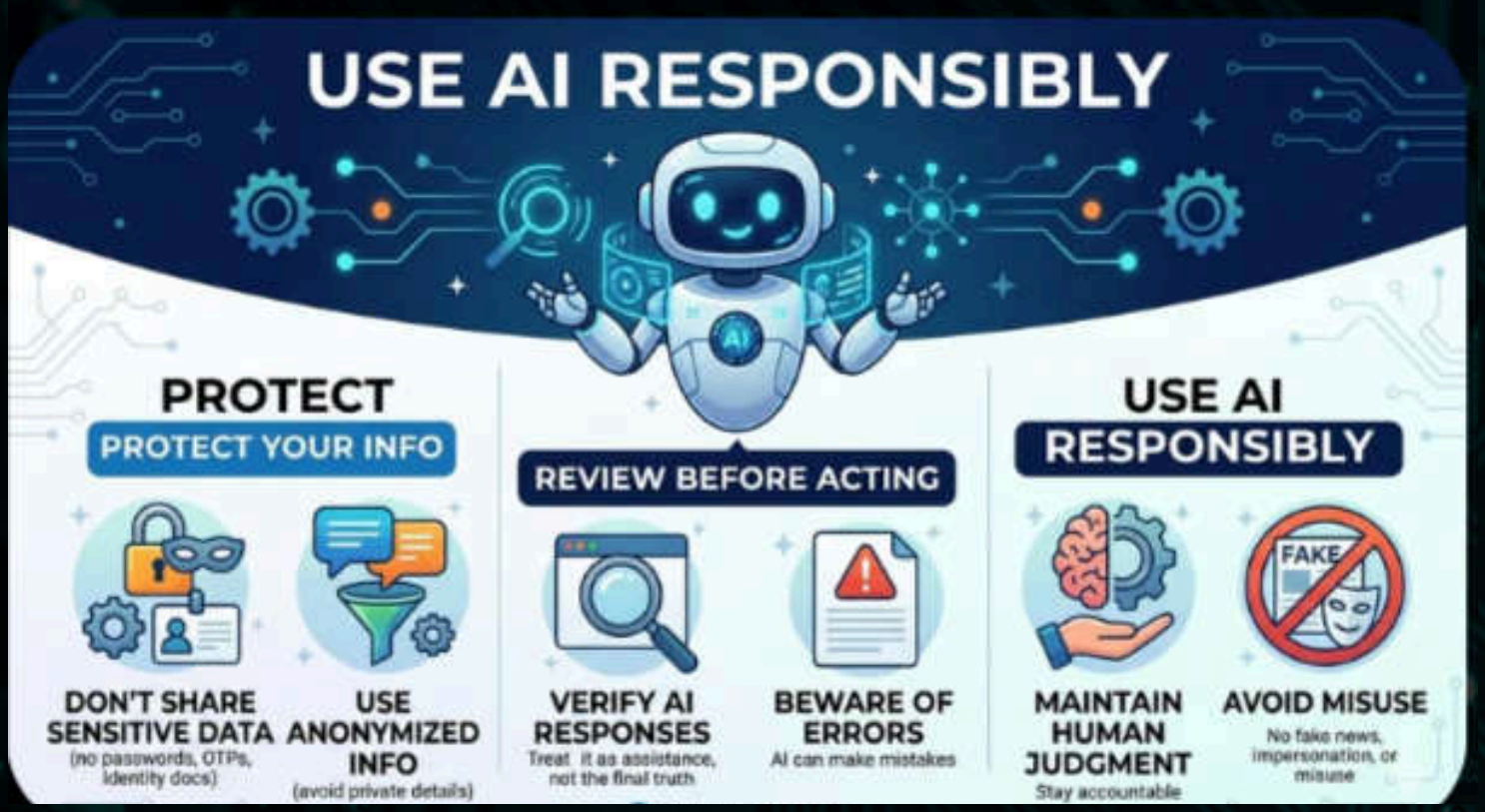
- બધા ઉપકરણો પર મજબૂત પાસવર્ડ અથવા સ્ક્રીન લોકનો ઉપયોગ કરો.
- જ્યારે પણ ઉપલબ્ધ હોય ત્યારે ઉપકરણ એન્ક્રિપ્શન અને સુરક્ષા સુવિધાઓ સક્ષમ કરો.
- બિનજરૂરી એપ્લિકેશનો અને પરવાનગીઓની સમીક્ષા કરો અને દૂર કરો.

તમારા નેટવર્ક કનેક્શનને સુરક્ષિત કરો

- તમારા Wi-Fi ને મજબૂત પાસવર્ડથી સુરક્ષિત કરો અને ડિફોલ્ટ રાઉટર ઓળખપત્રો બદલો.
- અપડેટેડ રાઉટર ફર્મવેર અને સુરક્ષિત નેટવર્ક સેટિંગ્સનો ઉપયોગ કરો.
- સંવેદનશીલ એકાઉન્ટ્સ ઍક્સેસ કરવાનું અથવા અસુરક્ષિત નેટવર્ક્સ પર ગુપ્ત માહિતી શેર કરવાનું ટાળો.

અમને અનુસરો : @IndianCERT @cert_india

AI નો જવાબદારીપૂર્વક ઉપયોગ કરો



તમારી વ્યક્તિગત માહિતીને સુરક્ષિત કરો

- જાહેર *AI* ટૂલ્સ અથવા અજાણી ઓનલાઈન સેવાઓમાં વ્યક્તિગત, નાણાકીય, આરોગ્ય, સત્તાવાર અથવા ગુપ્ત માહિતી દાખલ કરશો નહીં.
- પાસવર્ડ, OTP, એકાઉન્ટ નંબર, ઓળખ દસ્તાવેજો, ગ્રાહક ડેટા અથવા ખાનગી વાતચીત જેવી સંવેદનશીલ વિગતો શેર કરવાનું ટાળો.
- AI ટૂલ્સ પાસેથી મદદ માંગતી વખતે અનામી અથવા સામાન્ય માહિતીનો ઉપયોગ કરો.

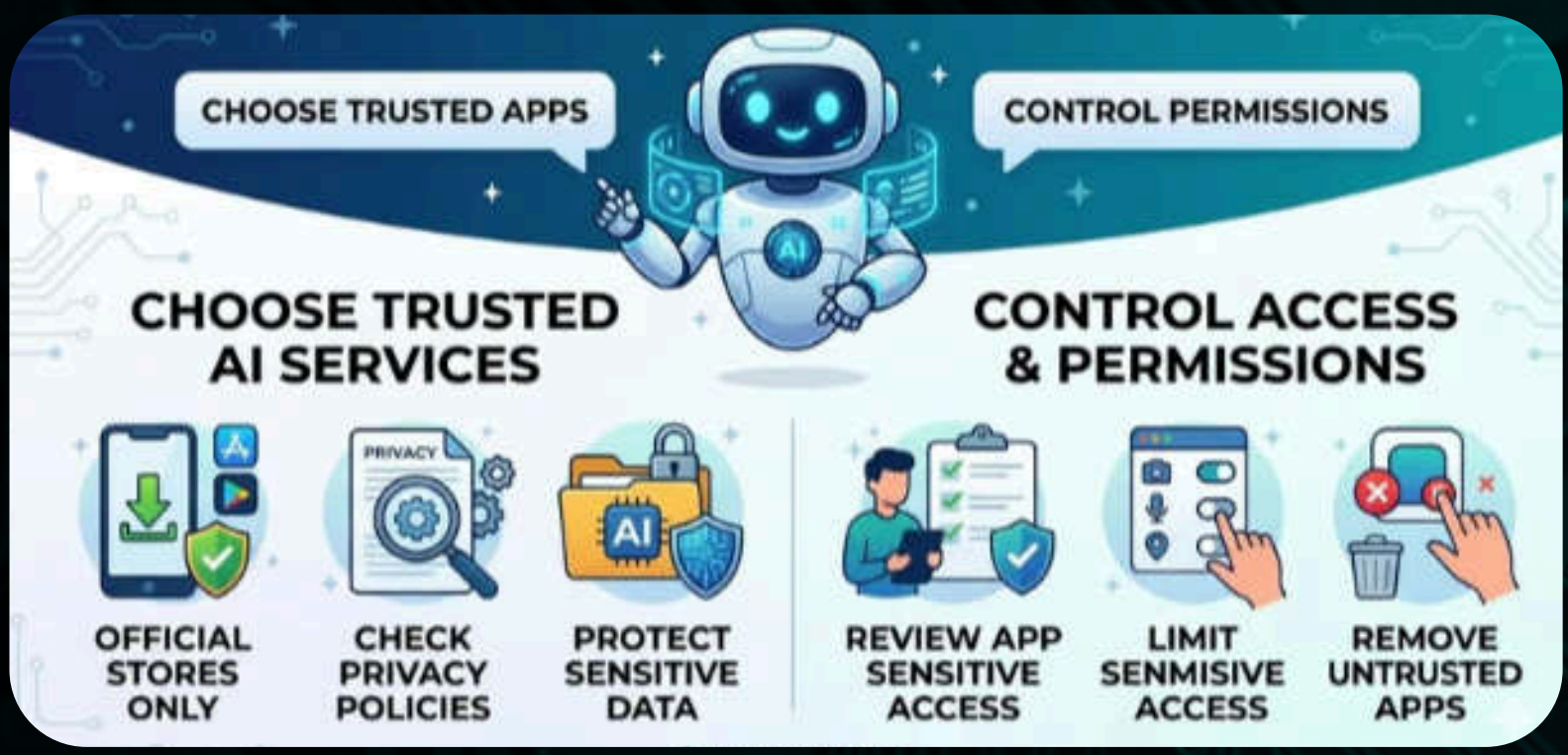
શેર કરતા પહેલા કે કાર્ય કરતા પહેલા સમીક્ષા કરો

- **AI-જનરેટેડ પ્રતિભાવોને સત્યના અંતિમ સ્ત્રોત તરીકે નહીં, પરંતુ સહાય તરીકે ગણો.**
- નાણાકીય, કાનૂની, વ્યાવસાયિક અથવા વ્યક્તિગત નિર્ણયો માટે મહત્વપૂર્ણ માહિતીનો ઉપયોગ કરતા પહેલા તેની ચકાસણી કરો.
- ધ્યાન રાખો કે AI ટૂલ્સ ખોટી, અપૂર્ણ અથવા ગેરમાર્ગે દોરતી માહિતી ઉત્પન્ન કરી શકે છે.

AI ટૂલ્સનો જવાબદારીપૂર્વક ઉપયોગ કરો

- તમારા કાર્ય અને શિક્ષણને ટેકો આપવા માટે AI નો ઉપયોગ કરો, પરંતુ માનવીય નિર્ણય અને જવાબદારી જાળવી રાખો.
- ખોટી માહિતી બનાવવા કે ફેલાવવા, બીજાઓનો ઢોંગ કરવા અથવા કોઈના અંગત ડેટાનો દુરુપયોગ કરવા માટે AI નો ઉપયોગ કરશો નહીં.

વિશ્વસનીય એપ્લિકેશનો પસંદ કરો



એપ્લિકેશન ઍક્સેસ અને પરવાનગીઓનું નિયંત્રણ કરો

- AI એપ્લિકેશનો અને ડિજિટલ સહાયકોને આપવામાં આવેલી પરવાનગીઓની સમીક્ષા કરો.
- કેમેરા, માઇક્રોફોન, સંપર્કો અથવા સ્થાન જેવી સુવિધાઓ માટે જરૂરી હોય ત્યારે જ ઍક્સેસની મંજૂરી આપો.
- બિનજરૂરી પરવાનગીઓ દૂર કરો અને અવિશ્વસનીય સ્ત્રોતોમાંથી એપ્લિકેશનો અનઇન્સ્ટોલ કરો.

વિશ્વસનીય AI સેવાઓ પસંદ કરો

- પ્રતિષ્ઠિત પ્રદાતાઓ પાસેથી AI એપ્લિકેશનોનો ઉપયોગ કરો અને તેમને ફક્ત સત્તાવાર એપ સ્ટોર્સ પરથી જ ડાઉનલોડ કરો.
- AI સેવાઓનો ઉપયોગ કરતા પહેલા ગોપનીયતા સેટિંગ્સ, ઉપયોગની શરતો અને ડેટા હેન્ડલિંગ પ્રથાઓની સમીક્ષા કરો.
- જ્યાં સુધી સુરક્ષા નિયંત્રણો ચકાસાયેલ ન હોય ત્યાં સુધી સંવેદનશીલ એકાઉન્ટ્સ અથવા ફાઇલો સાથે AI ટૂલ્સને કનેક્ટ કરવાનું ટાળો.

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

certin Enhancing Cyber Security in India

ISEA Information Security Education & Awareness

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

Digital India Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Report Cyber Security Incidents to CERT-In

For reporting Cyber Security Incidents to CERT-In:

Visit website: ***https://www.cert-in.org.in***

Email: ***incident@cert-in.org.in***

Toll Free Phone: ***+91-1800-11-4949***

Toll Free Fax: ***+91-1800-11-6969***

Information Desk

Phone: ***+91-11-22902657***

Follow us :

@IndianCERT

@cert_india

WEBSITE
https://www.cert-in.org.in/

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Awareness Booklet
https://cert-in.org.in/AwarenessBooklets.jsp

Security Tools
https://www.csk.gov.in/security-tools.html