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 ସଚେତନତା ମାର୍ଗଦର୍ଶିକା

ସାଇବର ସ୍ୱଚ୍ଛତାର ସଂସ୍କୃତି ଗଠନ କରନ୍ତୁ

#ସାଇବରସ୍ୱାସ୍ଥ୍ୟନିର୍ମିତଆମର ସଂସ୍କୃତି



ଜାତୀୟ ସାଇବର ସୁରକ୍ଷା ସଚେତନତା ମାସ (ଅକ୍ଟୋବର 2026)

ପ୍ରକାଶକ

ଭାରତୀୟ କମ୍ପ୍ୟୁଟର ଜରୁରୀକାଳୀନ ପ୍ରତିକ୍ରିୟା ଦଳ

ଆମକୁ ଅନୁସରଣ କରନ୍ତୁ :

@IndianCERT

@cert_india

ସୂଚୀପତ୍ର

ମୁଖବନ୍ଧ 3

AI-ଉନ୍ନତ ଫିସିଂ ଏବଂ ସାମାଜିକ ଇଞ୍ଜିନିୟରିଂ 4

ଭଏସ୍ ଏବଂ ଭିଡିଓ ଡିପ୍ଫେକ୍ (ଭିସିଂ) 5

AI-ସହାୟକ ମାଲୱେର୍ ଏବଂ ସ୍ୱୟଂଚାଳିତ ଆକ୍ରମଣ 6

ନକଲି ୱେବସାଇଟ୍ ଏବଂ ପରିଚୟ ଚୋରି 7

ଲାଲ ପତାକା ଯାଞ୍ଚ ତାଲିକା 8

ଅନଲାଇନ୍ ସୁରକ୍ଷା 9

ଉପକରଣ ସୁରକ୍ଷା 10

ଦାୟିତ୍ୱର ସହ AI ବ୍ୟବହାର କରନ୍ତୁ 11

ବିଶ୍ୱସ୍ତ ଆପ୍ସ ବାଛନ୍ତୁ 12

ସାଇବର ସୁରକ୍ଷା ଘଟଣାଗୁଡ଼ିକ CERT-In କୁ ରିପୋର୍ଟ କରନ୍ତୁ 13

ମୁଖବନ୍ଧ

କୃତ୍ରିମ ବୁଦ୍ଧିମତ୍ତା (AI) ଆମ ଜୀବନଯାପନ, କାମ ଏବଂ ଯୋଗାଯୋଗ ପଦ୍ଧତିକୁ ପରିବର୍ତ୍ତନ କରୁଛି। ଏହା ନବସୃଜନକୁ ସକ୍ଷମ କରେ, ଉତ୍ପାଦକତାକୁ ଉନ୍ନତ କରେ ଏବଂ ବିଭିନ୍ନ କ୍ଷେତ୍ରରେ ଜଟିଳ ସମସ୍ୟାର ସମାଧାନ କରିବାରେ ସାହାଯ୍ୟ କରେ। ତଥାପି, ସମାନ ପ୍ରଯୁକ୍ତିବିଦ୍ୟାକୁ ବିପଦଜନକ ବ୍ୟକ୍ତିମାନେ ଅଧିକ ଉନ୍ନତ ଏବଂ ବିଶ୍ୱାସଯୋଗ୍ୟ ସାଇବର ବିପଦ ସୃଷ୍ଟି କରିବା ପାଇଁ ଅପବ୍ୟବହାର କରୁଛନ୍ତି।

AI ଡିଜିଟାଲ୍ ବିପଦକୁ ଚିହ୍ନଟ କରିବା ଅଧିକ କଷ୍ଟକର କରୁଛି କାରଣ ଆକ୍ରମଣକାରୀମାନେ ଏବେ ଅତ୍ୟନ୍ତ ବାସ୍ତବବାଦୀ ଇମେଲ୍, ବାର୍ତ୍ତା, ଅଡିଓ, ଭିଡିଓ ଏବଂ ୱେବସାଇଟ୍ ସୃଷ୍ଟି କରିପାରିବେ। ପାରମ୍ପରିକ ଚେତାବନୀ ସଙ୍କେତ, ଯେପରିକି ଖରାପ ବ୍ୟାକରଣ, ଅସ୍ୱାଭାବିକ ଫର୍ମାଟିଂ, କିମ୍ବା ସ୍ପଷ୍ଟ ଭୁଲ, ଆଉ ନିର୍ଭରଯୋଗ୍ୟ ସୂଚକ ହୋଇ ନପାରେ। ଯାଞ୍ଚ ଏବଂ ଦାୟିତ୍ୱପୂର୍ଣ୍ଣ ଡିଜିଟାଲ୍ ଅଭ୍ୟାସ ପୂର୍ବ ଅପେକ୍ଷା ଅଧିକ ଗୁରୁତ୍ୱପୂର୍ଣ୍ଣ ହୋଇଯାଇଛି।

ଆମେ ପ୍ରତିଦିନ ବ୍ୟବହାର କରୁଥିବା AI ଉପକରଣ ଏବଂ ସ୍ମାର୍ଟ ଉପକରଣଗୁଡ଼ିକୁ ସତର୍କତାର ସହ ବ୍ୟବହାର ନ କଲେ ସେଗୁଡ଼ିକ ନୂତନ ଗୋପନୀୟତା ଏବଂ ସୁରକ୍ଷା ବିପଦ ଆଣିପାରେ। ଅବିଶ୍ୱସନୀୟ AI ଆପ୍ଲିକେସନ୍ ସହିତ ବ୍ୟକ୍ତିଗତ କିମ୍ବା ଗୋପନୀୟ ସୂଚନା ବାଣ୍ଟିବା, ଅନାବଶ୍ୟକ ଅନୁମତି ପ୍ରଦାନ କରିବା, କିମ୍ବା ଯାଞ୍ଚ ବିନା AI ଦ୍ୱାରା ଉତ୍ପନ୍ନ ସୂଚନା ଉପରେ ନିର୍ଭର କରିବା ବ୍ୟକ୍ତି ଏବଂ ସଂଗଠନଗୁଡ଼ିକୁ ସୁରକ୍ଷା ବିପଦରେ ପକାଇପାରେ।

"AI ସାଇବର ସଚେତନତା" ଉପରେ ଇଣ୍ଡିଆନ୍ କମ୍ପ୍ୟୁଟର ଜରୁରୀକାଳୀନ ପ୍ରତିକ୍ରିୟା ଦଳ (CERT-In) ଦ୍ୱାରା ପ୍ରସ୍ତୁତ ଏହି ପୁସ୍ତିକାଟି କେବଳ ସାଇବର ସୁରକ୍ଷା ବୃତ୍ତିଗତଙ୍କ ପାଇଁ ନୁହେଁ, ସାଧାରଣ ନାଗରିକ, କର୍ମଚାରୀ ଏବଂ ଡିଜିଟାଲ୍ ବ୍ୟବହାରକାରୀଙ୍କ ପାଇଁ ଡିଜାଇନ୍ କରାଯାଇଛି। ଏହା ବ୍ୟାଖ୍ୟା କରେ ଯେ AI କିପରି ଡିଜିଟାଲ୍ ବିପଦ ପରିଦୃଶ୍ୟକୁ ପରିବର୍ତ୍ତନ କରୁଛି ଏବଂ ବ୍ୟକ୍ତିଗତ ସୂଚନା, ଡିଭାଇସ୍ ଏବଂ ଅନଲାଇନ୍ ପରିଚୟକୁ ସୁରକ୍ଷିତ ରଖିବା ପାଇଁ ପ୍ରତ୍ୟେକ ବ୍ୟକ୍ତି ଅନୁସରଣ କରିପାରିବେ।

ଏଆଇ-ଉନ୍ନତ ଫିସିଙ୍ଗ୍ ଏବଂ ସାମାଜିକ ଇଞ୍ଜିନିୟରିଂ



ଏହା କିପରି କାମ କରେ ?

ଧମକ ଦେଉଥିବା ବ୍ୟକ୍ତିମାନେ ଏବେ ଏପରି ଇମେଲ୍ ଏବଂ ମେସେଜ୍ ପଠାନ୍ତି ଯାହା ପ୍ରକୃତ ଏବଂ ତ୍ରୁଟିମୁକ୍ତ ଦେଖାଯାଏ। ସେମାନେ ଆପଣଙ୍କ ବିଷୟରେ ବିବରଣୀ ବ୍ୟବହାର କରନ୍ତି, ଯେପରିକି ଆପଣଙ୍କ ଚାକିରି, ଆପଣ ବ୍ୟବହାର କରୁଥିବା ସେବା କିମ୍ବା ସାମ୍ପ୍ରତିକ କାର୍ଯ୍ୟକଳାପ, ଯାହା ଦ୍ୱାରା ମେସଜଗୁଡ଼ିକ ବ୍ୟକ୍ତିଗତ ମନେହୁଏ। ଯେହେତୁ ଏହି ମେସେଜଗୁଡ଼ିକ ଭଲ ଭାବରେ ଲେଖାଯାଇଛି, ସେଗୁଡ଼ିକୁ ଚିହ୍ନିବା ବହୁତ କଷ୍ଟକର ହୋଇପାରେ।

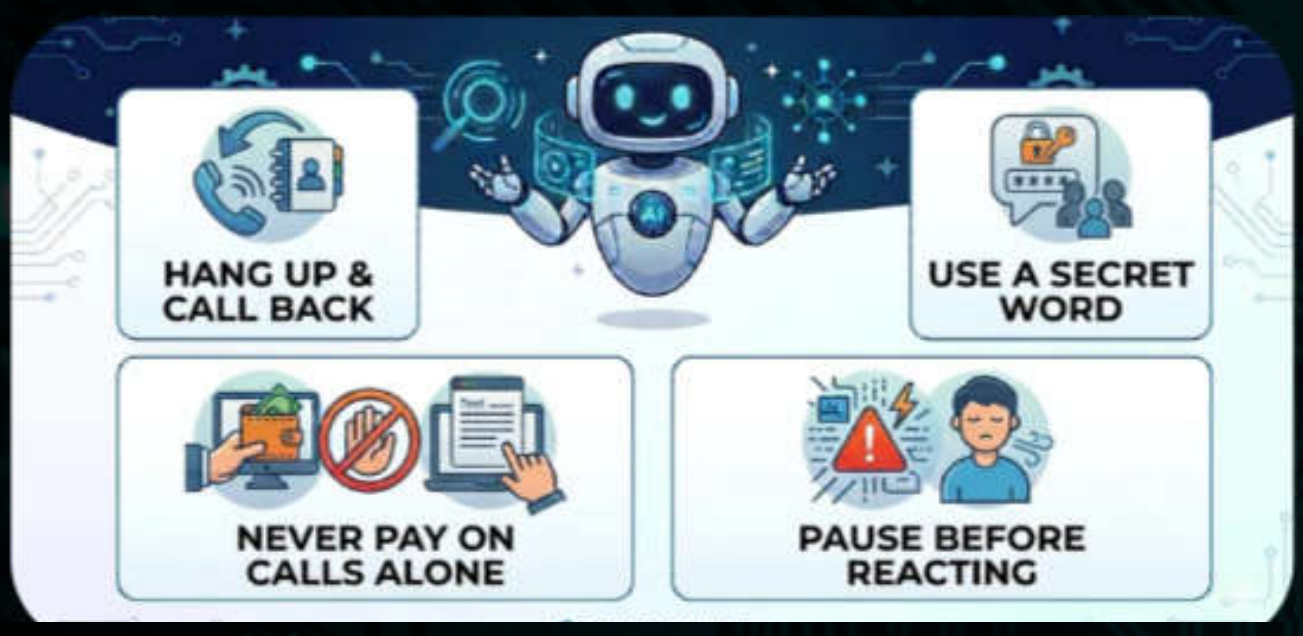
କିପରି ଚିହ୍ନିବେ?

- ବାର୍ତ୍ତାଟି ଆପଣଙ୍କ ପାଇଁ ବହୁତ ନିର୍ଦ୍ଦିଷ୍ଟ ମନେହୁଏ କିନ୍ତୁ ଅପ୍ରତ୍ୟାଶିତ ଭାବରେ ଆସିଯାଏ।
- ଏହା ଏକ ଜରୁରୀ କିମ୍ବା ଧମକପୂର୍ଣ୍ଣ ସ୍ୱର ବ୍ୟବହାର କରେ ଏବଂ ତୁରନ୍ତ କାର୍ଯ୍ୟାନୁଷ୍ଠାନ ଦାବି କରେ।
- ଏହା ଆପଣଙ୍କୁ ଏକ ଲିଙ୍କ୍ କ୍ଲିକ୍ କରିବାକୁ, ଏକ ଆକାଉଣ୍ଟ ଯାଞ୍ଚ କରିବାକୁ, ଏକ ପାସୱାର୍ଡ ପୁନଃସେଟ୍ କରିବାକୁ କିମ୍ବା ଦେୟ କରିବାକୁ କୁହେ।
- ପ୍ରେରକଙ୍କ ଠିକଣା ପ୍ରାୟ ଠିକ୍ ଦେଖାଯାଉଛି, କିନ୍ତୁ ସମ୍ପୂର୍ଣ୍ଣ ନୁହେଁ।

କିପରି ସୁରକ୍ଷିତ ରହିବେ ?

- ଅନାବଶ୍ୟକ ମେସେଜରେ ଥିବା ଲିଙ୍କଗୁଡ଼ିକୁ କ୍ଲିକ୍ କରନ୍ତୁ ନାହିଁ। ଏହା ବଦଳରେ ସିଧାସଳଖ ଅଫିସିଆଲ୍ ୱେବସାଇଟ୍ କିମ୍ବା ଆପ୍ କୁ ଯାଆନ୍ତୁ।
- ଏକ ପୃଥକ, ବିଶ୍ୱସ୍ତ ଯୋଗାଯୋଗ ଚ୍ୟାନେଲ୍, ଯେପରିକି ଏକ ଅଫିସିଆଲ୍ ଫୋନ୍ ନମ୍ବର କିମ୍ବା ଆପ୍ ମାଧ୍ୟମରେ ଅନୁରୋଧଗୁଡ଼ିକୁ ଯାଞ୍ଚ କରନ୍ତୁ।
- ମେସେଜ୍ ଲିଙ୍କ୍ ମାଧ୍ୟମରେ ପହଞ୍ଚିଥିବା ପୃଷ୍ଠାରେ କେବେବି ପ୍ରମାଣପତ୍ର କିମ୍ବା OTP ପ୍ରବେଶ କରନ୍ତୁ ନାହିଁ।
- ସନ୍ଦେହଜନକ ମେସେଜଗୁଡ଼ିକର ରିପୋର୍ଟ କରନ୍ତୁ ଏବଂ ଡିଲିଟ୍ କରନ୍ତୁ, ତା'ପରେ ପ୍ରେରକଙ୍କୁ ଅବରୋଧ କରନ୍ତୁ।

ଭଏସ୍ ଏବଂ ଭିଡିଓ ଡିପ୍ଫେକ୍ [ଭିସିଂ]



ଏହା କିପରି କାମ କରେ ?

ଧମକ ଦେଉଥିବା ବ୍ୟକ୍ତିମାନେ ସ୍ୱର ଅବିକଳ କରିପାରିବେ କିମ୍ବା ନକଲି ଭିଡିଓ ତିଆରି କରିପାରିବେ ଯାହା ପ୍ରକୃତ ଦେଖାଯାଏ ଏବଂ ଶୁଭେ। ସେମାନେ ପରିବାର, ସହକର୍ମୀ କିମ୍ବା ଅଧିକାରୀ ଭାବରେ ନିଜର ପରିଚୟ ଦେଇ ସମ୍ବେଦନଶୀଳ ସୂଚନା ସେୟାର କରିବା, ଟଙ୍କା ପଠାଇବା କିମ୍ବା ଶୀଘ୍ର ପଦକ୍ଷେପ ନେବା ପାଇଁ ଚାପ ପକାଇପାରନ୍ତି।

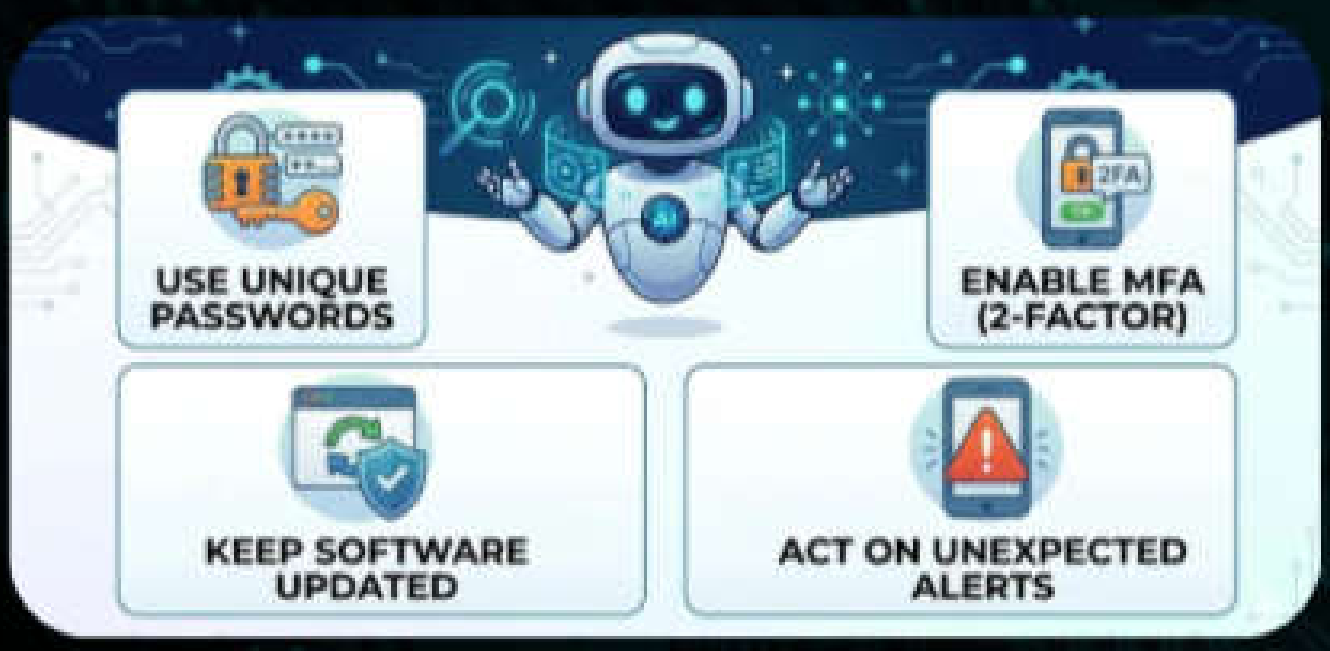
କିପରି ଚିହ୍ନିବେ?

- ଅସାଧାରଣ ଜରୁରୀତା, ଆତଙ୍କ, କିମ୍ବା ଗୋପନୀୟତା ପାଇଁ ଅନୁରୋଧ, ଯେପରିକି କାହାକୁ କୁହନ୍ତୁ ନାହିଁ।
- ଟିକିଏ କମ୍ ସ୍ୱର, ଗତି, ପୃଷ୍ଠଭୂମି ଶବ୍ଦ, କିମ୍ବା ଅଡିଓ ଗୁଣବତ୍ତା।
- ସାଧାରଣ ଯାଞ୍ଚ କିମ୍ବା ଅନୁମୋଦନ ପ୍ରକ୍ରିୟାକୁ ବାଇପାସ୍ କରିବା ପାଇଁ ଅନୁରୋଧ।
- ଉପହାର କାର୍ଡ, କ୍ରିପ୍ଟୋକରେନ୍ସି, କିମ୍ବା ୱାୟାର ଟ୍ରାନ୍ସଫର ମାଧ୍ୟମରେ ଟଙ୍କା ଦେବା ପାଇଁ ଅନୁରୋଧ।

କିପରି ସୁରକ୍ଷିତ ରହିବେ ?

- ଫୋନ୍ କାଟି ଦିଅନ୍ତୁ ଏବଂ ତାଙ୍କ ଜଣାଶୁଣା, ସେଭ୍ କରାଯାଇଥିବା ନମ୍ବର ବ୍ୟବହାର କରି ବ୍ୟକ୍ତିଙ୍କୁ ଫୋନ୍ କରନ୍ତୁ।
- ଜରୁରୀକାଳୀନ ପରିସ୍ଥିତିରେ ପରିଚୟ ଯାଞ୍ଚ କରିବା ପାଇଁ ପରିବାର କିମ୍ବା କର୍ମକ୍ଷେତ୍ରରେ ସୁରକ୍ଷିତ ଶବ୍ଦ ସେଟ୍ କରନ୍ତୁ।
- କେବଳ ଫୋନ୍ କିମ୍ବା ଭିଡିଓ ଆଧାରରେ ପେମେଣ୍ଟକୁ କେବେବି ଅନୁମୋଦନ କରନ୍ତୁ ନାହିଁ। ଏକ ପୃଥକ ଚ୍ୟାନେଲ୍ ମାଧ୍ୟମରେ ଲିଖିତ ଭାବରେ ନିଶ୍ଚିତ କରନ୍ତୁ।
- ପ୍ରତିକ୍ରିୟା ଦେବା ପୂର୍ବରୁ ବିରାମ ନିଅନ୍ତୁ। ଧମକ ଦେଉଥିବା ବ୍ୟକ୍ତିମାନେ ଆପଣଙ୍କ ବିଚାରକୁ ଧୂଳିସାତ କରିବା ପାଇଁ ଆତଙ୍କ ଉପରେ ନିର୍ଭର କରନ୍ତି।

ଏଆଇ-ସହାୟତାପ୍ରାପ୍ତ ମାଲୱେର୍ ଏବଂ ସ୍ୱୟଂଚାଳିତ ଆକ୍ରମଣ



ଏହା କିପରି କାମ କରେ ?

ବିପଦ ସୃଷ୍ଟିକାରୀମାନେ କ୍ଷତିକାରକ କୋଡ୍ ତିଆରି କିମ୍ବା ଲୁଚାଇବା ପାଇଁ AI ଉପକରଣ ବ୍ୟବହାର କରନ୍ତି, ଅନେକ ସାଇଟରେ ପାସୱାର୍ଡ ଚୋରି ପରୀକ୍ଷା କରନ୍ତି ଏବଂ ଅପଡେଟ୍ ଆବଶ୍ୟକ କରୁଥିବା ସିଷ୍ଟମଗୁଡ଼ିକୁ ଚିହ୍ନଟ କରନ୍ତି। ଏହା ଆକ୍ରମଣକୁ ଦ୍ରୁତ ଏବଂ ବ୍ୟାପକ କରିଥାଏ।

କିପରି ଚିହ୍ନିବେ?

- ଅପ୍ରତ୍ୟାଶିତ ଲଗଇନ୍ ଆଲର୍ଟ, ପାସୱାର୍ଡ ରିସେଟ୍ ଇମେଲ୍, କିମ୍ବା ଆପଣ ଅନୁରୋଧ କରିନଥିବା MFA ପ୍ରମ୍ପ୍ଟ
- ଆପଣଙ୍କ ଆକାଉଣ୍ଟ କାର୍ଯ୍ୟକଳାପରେ ତାଲିକାଭୁକ୍ତ ଅଜଣା ଡିଭାଇସ୍ କିମ୍ବା ସେସନଗୁଡ଼ିକ
- ଆଣ୍ଟିଭାଇରସ୍ ଚେତାବନୀ, ପପ୍-ଅପ୍, କିମ୍ବା ଡିଭାଇସ୍ କାର୍ଯ୍ୟଦକ୍ଷତା ଅସ୍ୱାଭାବିକ ଭାବରେ ଧୀର
- ଆପଣ ଚିହ୍ନଟ କରୁନଥିବା ଫାଇଲ୍, ସେଟିଙ୍ଗ୍ସ କିମ୍ବା ବ୍ରାଉଜର୍ ଏକ୍ସଟେନ୍ସନ୍

କିପରି ସୁରକ୍ଷିତ ରହିବେ ?

- ପ୍ରତ୍ୟେକ ଆକାଉଣ୍ଟ ପାଇଁ ଏକ ଅନନ୍ୟ, ଶକ୍ତିଶାଳୀ ପାସୱାର୍ଡ ବ୍ୟବହାର କରନ୍ତୁ।
- ସମସ୍ତ ଗୁରୁତ୍ୱପୂର୍ଣ୍ଣ ଆକାଉଣ୍ଟରେ ମଲ୍ଟି ଫ୍ୟାକ୍ଟର ଅଥେଣ୍ଟିକେସନ୍ (MFA) ସକ୍ଷମ କରନ୍ତୁ।
- ଆଣ୍ଟିଭାଇରସ୍ ସଫ୍ଟୱେର୍, ସିଷ୍ଟମ୍ ଏବଂ ଆପ୍ସକୁ ଅପ୍ ଟୁ ଡେଟ୍ ରଖନ୍ତୁ।
- ଅପ୍ରତ୍ୟାଶିତ ଲଗଇନ୍ କିମ୍ବା MFA ଆଲର୍ଟ ଉପରେ ତୁରନ୍ତ କାର୍ଯ୍ୟ କରନ୍ତୁ।

ନକଲି ୱେବସାଇଟ୍ ଏବଂ ପରିଚୟ ଚୋରି



ଏହା କିପରି କାମ କରେ ?

ଧମକ ଦେଉଥିବା ବ୍ୟକ୍ତିମାନେ ଆପଣଙ୍କ ଲଗଇନ୍ ପ୍ରମାଣପତ୍ର, OTP, କିମ୍ବା ପେମେଣ୍ଟ ବିବରଣୀ ଚୋରି କରିବା ପାଇଁ ବ୍ୟାଙ୍କିଂ କିମ୍ବା ସପିଂ ପୋର୍ଟାଲ୍ ପରି ସମାନ ଦେଖାଯାଉଥିବା ୱେବସାଇଟ୍ ଏବଂ ଚାଟବଟ୍ ତିଆରି କରିପାରିବେ। ସେମାନେ ମିଥ୍ୟା ପରିଚୟ ସୃଷ୍ଟି କରିବା ପାଇଁ ନକଲି ଫଟୋ କିମ୍ବା ଡକ୍ୟୁମେଣ୍ଟ ମଧ୍ୟ ବ୍ୟବହାର କରିପାରନ୍ତି।

କିପରି ଚିହ୍ନିବେ?

- ସାମାନ୍ୟ ପରିବର୍ତ୍ତିତ ୱେବସାଇଟ୍ URL, ଯେପରିକି ଅତିରିକ୍ତ ଅକ୍ଷର, ହାଇଫେନ୍, କିମ୍ବା ଏକ ଭିନ୍ନ ଡୋମେନ୍ ।
- OTP, PIN, କିମ୍ବା ପୂର୍ଣ୍ଣ କାର୍ଡ ନମ୍ବର ମାଗୁଥିବା ଚାଟବଟ୍ କିମ୍ବା ଏଜେଣ୍ଟମାନେ।
- ଏକ ପରିଚିତ ସାଇଟରେ HTTPS କିମ୍ବା ଅସ୍ୱାଭାବିକ ଡିଜାଇନ୍ ଅସଙ୍ଗତି ନାହିଁ।

କିପରି ସୁରକ୍ଷିତ ରହିବେ ?

- ଲିଙ୍କଗୁଡ଼ିକୁ କ୍ଲିକ୍ କରିବା ପରିବର୍ତ୍ତେ ସର୍ବଦା ସିଧାସଳଖ ଅଫିସିଆଲ୍ URL ଟାଇପ୍ କରନ୍ତୁ କିମ୍ବା ଯାଞ୍ଚ ହୋଇଥିବା ବୁକମାର୍କ ବ୍ୟବହାର କରନ୍ତୁ।
- କେବେବି କୌଣସି ଚାଟବଟ୍ କିମ୍ବା "ସପୋର୍ଟ ଏଜେଣ୍ଟ" ସହିତ OTP, PIN, କିମ୍ବା ସମ୍ପୂର୍ଣ୍ଣ କାର୍ଡ ବିବରଣୀ ସେୟାର କରନ୍ତୁ ନାହିଁ।
- ଯେକୌଣସି ସ୍ଥାନରେ ଲଗ୍ ଇନ୍ କରିବା ପୂର୍ବରୁ HTTPS ଯାଞ୍ଚ କରନ୍ତୁ ଏବଂ ଡୋମେନ୍ ନାମକୁ ଭଲଭାବେ ଦେଖନ୍ତୁ।
- ଅଜଣା କାର୍ଯ୍ୟକଳାପ ପାଇଁ ନିୟମିତ ଭାବରେ ଆପଣଙ୍କର ବ୍ୟାଙ୍କ ଷ୍ଟେଟମେଣ୍ଟ ଏବଂ କ୍ରେଡିଟ୍ କାର୍ଡ ଷ୍ଟେଟମେଣ୍ଟ୍ ଉପରେ ନଜର ରଖନ୍ତୁ।

ସନ୍ଦେହଜନକ ସଙ୍କେତ ଚେକଲିଷ୍ଟ

AI-କ୍ଷମତାସମ୍ପନ୍ନ ଆକ୍ରମଣର ଏହି ସଙ୍କେତଗୁଡ଼ିକ ପ୍ରତି ସତର୍କ ରୁହନ୍ତୁ:

- ଟଙ୍କା, ଲଗଇନ୍ ତଥ୍ୟ (କ୍ରେଡେନସିଆଲ୍), ବା ଅନୁମୋଦନ ପାଇଁ ଜରୁରୀ ଏବଂ ଚାପପୂର୍ଣ୍ଣ ଅନୁରୋଧ
- ଜଣାଶୁଣା ବ୍ୟକ୍ତିଙ୍କ କଲ୍ କିମ୍ବା ଭିଡିଓରେ ସାମାନ୍ୟ ଅଡିଓ/ଭିଡିଓ ଅସଙ୍ଗତି (Inconsistencies)
- ସାଧାରଣ ଯାଞ୍ଚ୍ (verification) କିମ୍ବା ଅନୁମୋଦନ ପ୍ରକ୍ରିୟାକୁ ଏଡ଼ାଇ ଯିବା ପାଇଁ ଅନୁରୋଧ
- ଅପରିଚିତ ପ୍ରେରକ ଡୋମେନ୍ କିମ୍ବା ସାମାନ୍ୟ ପରିବର୍ତ୍ତିତ URL
- ଆପଣ ମାଗି ନଥିବା ଅପ୍ରତ୍ୟାଶିତ MFA ପ୍ରମ୍ପଟ୍ କିମ୍ବା OTP
- ସୁରକ୍ଷା ସଫ୍ଟୱେର୍ ନିଷ୍କ୍ରିୟ (disable) କରିବାକୁ କିମ୍ବା ଅନଧିକୃତ (unofficial) ଲିଙ୍କ୍ ମାଧ୍ୟମରେ "ଯାଞ୍ଚ୍" କରିବା ପାଇଁ ଅନୁରୋଧ
- ଆଗୁଆ ଟଙ୍କା ପେମେଣ୍ଟ୍ କିମ୍ବା ବ୍ୟକ୍ତିଗତ ଆର୍ଥିକ ତଥ୍ୟ ମାଗୁଥିବା ଚାକିରି/ନିବେଶ (Investment) ଅଫର୍

ସନ୍ଦେହ ହେଲେ — ଟିକିଏ ରୁହନ୍ତୁ (pause), ସ୍ୱାଧୀନ ଭାବରେ ଯାଞ୍ଚ୍ କରନ୍ତୁ, ଏବଂ ଚାପରେ ଥାଇ କୌଣସି ପଦକ୍ଷେପ ନିଅନ୍ତୁ ନାହିଁ।

ଅନଲାଇନ୍ ସୁରକ୍ଷା



ଆପଣଙ୍କ ଆକାଉଣ୍ଟଗୁଡ଼ିକୁ ସୁରକ୍ଷିତ ରଖନ୍ତୁ

- ପ୍ରତ୍ୟେକ ଆକାଉଣ୍ଟ ପାଇଁ ଦୃଢ଼ ଏବଂ ଅନନ୍ୟ ପାସୱାର୍ଡ ବ୍ୟବହାର କରନ୍ତୁ; ସେଗୁଡ଼ିକୁ ସୁରକ୍ଷିତ ଭାବରେ ସଂରକ୍ଷଣ କରିବା ପାଇଁ ଏକ ପାସୱାର୍ଡ ପରିଚାଳକ ବ୍ୟବହାର କରନ୍ତୁ।
- ଯେଉଁଠାରେ ଉପଲବ୍ଧ, ମଲ୍ଟି-ଫ୍ୟାକ୍ଟର ଅଥେଣ୍ଟିକେସନ୍ (MFA) ସକ୍ଷମ କରନ୍ତୁ।
- କେବେବି କାହା ସହିତ OTP, PIN, ପାସୱାର୍ଡ କିମ୍ବା ସୁରକ୍ଷା କୋଡ୍ ସେୟାର କରନ୍ତୁ ନାହିଁ।
- ଅତିରିକ୍ତ ସୁରକ୍ଷା ସ୍ତର ଭାବରେ ବାୟୋମେଟ୍ରିକ୍ ପ୍ରମାଣୀକରଣ (ଆଙ୍ଗୁଠି ଚିହ୍ନ/ମୁଖ ଚିହ୍ନଟକରଣ) ବ୍ୟବହାର କରନ୍ତୁ।

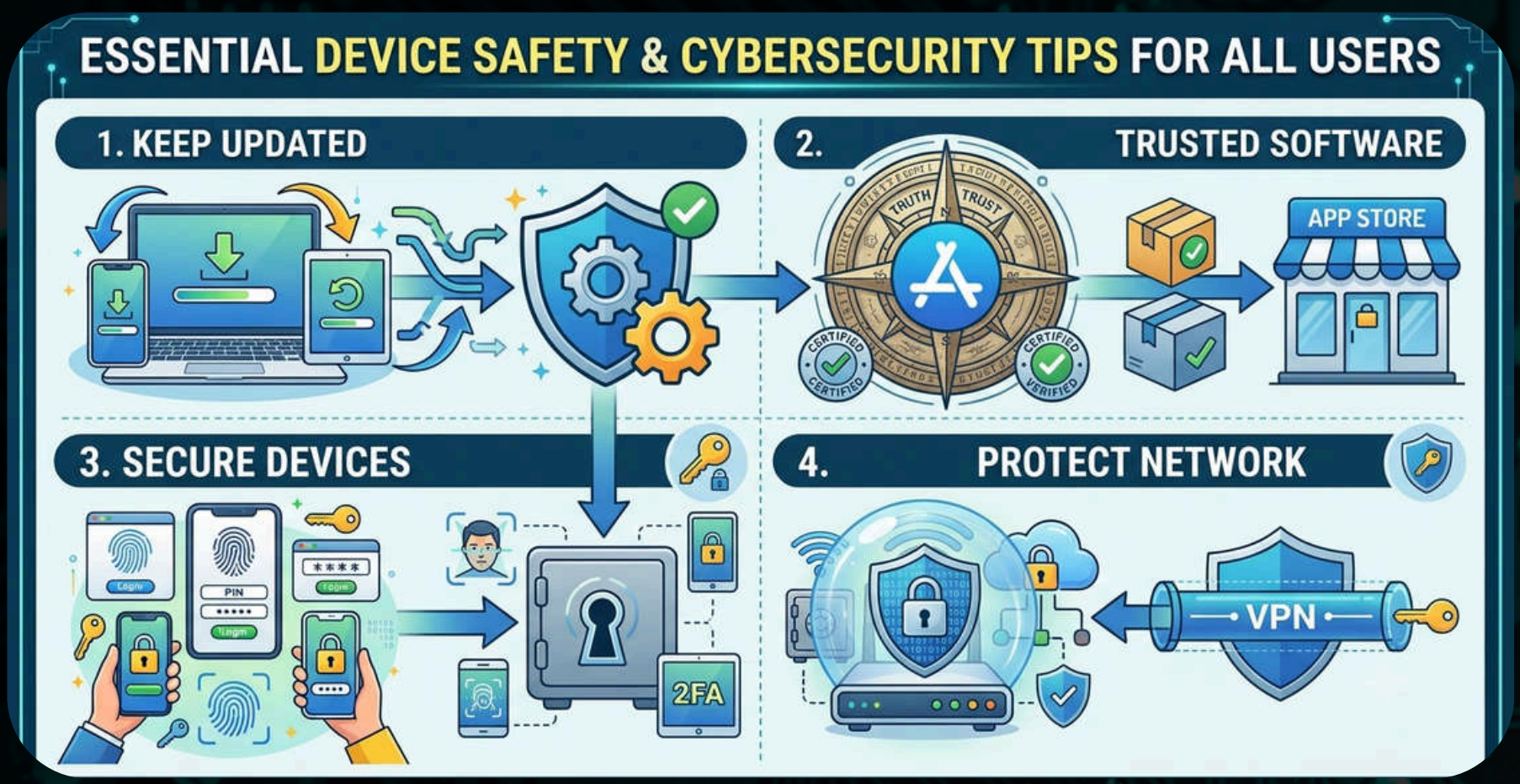
ଇମେଲ୍ ଏବଂ ଇଣ୍ଟରନେଟ୍ ବ୍ୟବହାର କରିବା ସମୟରେ ସୁରକ୍ଷିତ ରୁହନ୍ତୁ

- ସନ୍ଦିଗ୍ଧ କିମ୍ବା ସମାନ ଦେଖାଯାଉଥିବା ଇମେଲ୍ ଠିକଣା ପାଇଁ ପ୍ରେରକଙ୍କ ବିବରଣୀକୁ ସାବଧାନତାର ସହ ଯାଞ୍ଚ କରନ୍ତୁ।
- କ୍ଲିକ୍ କରିବା ପୂର୍ବରୁ ଲିଙ୍କଗୁଡ଼ିକୁ ଯାଞ୍ଚ କରନ୍ତୁ ଏବଂ ଅପ୍ରତ୍ୟାଶିତ ସଂଲଗ୍ନଗୁଡ଼ିକୁ ଖୋଲିବା ଏଡ଼ାନ୍ତୁ।
- ଲଗଇନ୍ କିମ୍ବା ଆର୍ଥିକ ବିବରଣୀ ପ୍ରବେଶ କରିବା ପୂର୍ବରୁ ୱେବସାଇଟ୍ ପ୍ରାମାଣିକତା ଯାଞ୍ଚ କରନ୍ତୁ।
- ସନ୍ଦେହ ହେଲେ, କିଛି କରିବା ପୂର୍ବରୁ ଅଟକି ଯାଆନ୍ତୁ ଏବଂ ଯାଞ୍ଚ କରନ୍ତୁ।

କିଛି ଭୁଲ ହେବା ପୂର୍ବରୁ ପ୍ରସ୍ତୁତ ହୁଅ

- ଅଫଲାଇନରେ କିମ୍ବା ସୁରକ୍ଷିତ କ୍ଲାଉଡ୍ ସେବାରେ ସଂରକ୍ଷିତ ଗୁରୁତ୍ୱପୂର୍ଣ୍ଣ ଫାଇଲଗୁଡ଼ିକର ନିୟମିତ ବ୍ୟାକଅପ୍ ବଜାୟ ରଖନ୍ତୁ।
- ଆକାଉଣ୍ଟ ପୁନରୁଦ୍ଧାର ସୂଚନା (ଇମେଲ୍/ଫୋନ୍)କୁ ଅପଡେଟ୍ ଏବଂ ସୁରକ୍ଷିତ ରଖନ୍ତୁ।

ଡିଭାଇସ୍ ସୁରକ୍ଷା



ଡିଭାଇସ୍‌ଗୁଡ଼ିକୁ ଅପଡେଟ୍ ରଖନ୍ତୁ

- ଜଣାଶୁଣା ଦୁର୍ବଳତାଗୁଡ଼ିକୁ ସମାଧାନ କରିବା ପାଇଁ ଅପରେଟିଂ ସିଷ୍ଟମ୍, ଆପ୍ଲିକେସନ୍, ବ୍ରାଉଜର୍ ଏବଂ ସୁରକ୍ଷା ସଫ୍ଟୱେର୍ ନିୟମିତ ଭାବରେ ଅପଡେଟ୍ କରନ୍ତୁ।
- ଯେଉଁଠାରେ ସମ୍ଭବ ସ୍ୱୟଂଚାଳିତ ଅପଡେଟ୍ ସକ୍ଷମ କରନ୍ତୁ।

କେବଳ ବିଶ୍ୱସ୍ତ ସଫ୍ଟୱେର୍ ସଂସ୍ଥାପନ କରନ୍ତୁ

- ପ୍ରକୃତ ସଫ୍ଟୱେର୍ ବ୍ୟବହାର କରନ୍ତୁ ଏବଂ କେବଳ ଅଫିସିଆଲ୍ ଆପ୍ ଷ୍ଟୋର କିମ୍ବା ବିଶ୍ୱସ୍ତ ଉତ୍ସରୁ ଆପ୍ଲିକେସନ୍ ସଂସ୍ଥାପନ କରନ୍ତୁ।
- ନିର୍ଭରଯୋଗ୍ୟ ଆଣ୍ଟିଭାଇରସ୍ କିମ୍ବା ସୁରକ୍ଷା ସମାଧାନ ବ୍ୟବହାର କରନ୍ତୁ ଏବଂ ସେଗୁଡ଼ିକୁ ଅପଡେଟ୍ ରଖନ୍ତୁ।

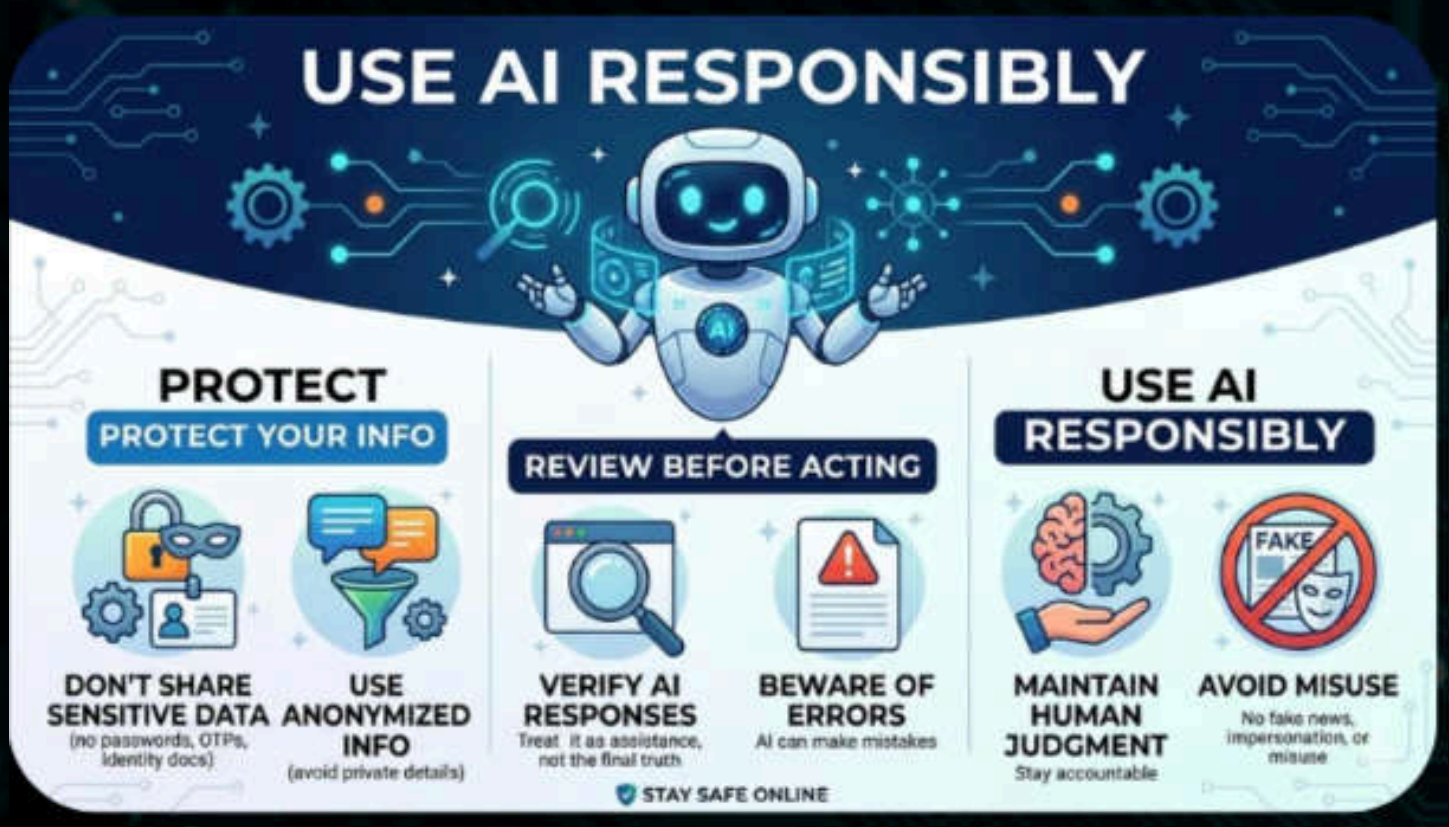
ଆପଣଙ୍କର ଡିଭାଇସ୍ ଏବଂ ଆକାଉଣ୍ଟଗୁଡ଼ିକୁ ସୁରକ୍ଷିତ ରଖନ୍ତୁ

- ସମସ୍ତ ଡିଭାଇସରେ ଦୃଢ଼ ପାସୱାର୍ଡ କିମ୍ବା ସ୍କ୍ରିନ୍ ଲକ୍ ବ୍ୟବହାର କରନ୍ତୁ।
- ଯେତେବେଳେ ଉପଲବ୍ଧ ହେବ, ଡିଭାଇସ୍ ଏନକ୍ରିପ୍ସନ୍ ଏବଂ ସୁରକ୍ଷା ବୈଶିଷ୍ଟ୍ୟଗୁଡ଼ିକୁ ସକ୍ଷମ କରନ୍ତୁ।
- ଅନାବଶ୍ୟକ ଆପ୍ଲିକେସନ୍ ଏବଂ ଅନୁମତିଗୁଡ଼ିକୁ ସମୀକ୍ଷା କରନ୍ତୁ ଏବଂ ହଟାନ୍ତୁ।

ଆପଣଙ୍କର ନେଟୱାର୍କ ସଂଯୋଗକୁ ସୁରକ୍ଷିତ ରଖନ୍ତୁ

- ଏକ ଦୃଢ଼ ପାସୱାର୍ଡ ସହିତ ଆପଣଙ୍କର Wi-Fi କୁ ସୁରକ୍ଷିତ କରନ୍ତୁ ଏବଂ ଡିଫଲ୍ଟ ରାଉଟର କ୍ରେଡେନସିଆଲ୍ ପରିବର୍ତ୍ତନ କରନ୍ତୁ।
- ଅପଡେଟ୍ ହୋଇଥିବା ରାଉଟର ଫାର୍ମୱେର୍ ଏବଂ ସୁରକ୍ଷିତ ନେଟୱାର୍କ ସେଟିଙ୍ଗ୍ସ ବ୍ୟବହାର କରନ୍ତୁ।
- ଅସୁରକ୍ଷିତ ନେଟୱାର୍କରେ ସମ୍ବେଦନଶୀଳ ଆକାଉଣ୍ଟଗୁଡ଼ିକୁ ଆକ୍ସେସ୍ କରିବା କିମ୍ବା ଗୋପନୀୟ ସୂଚନା ସେୟାର କରିବାରୁ ଦୂରେଇ ରୁହନ୍ତୁ।

ଦାୟିତ୍ୱର ସହିତ AI ବ୍ୟବହାର କରନ୍ତୁ



ଆପଣଙ୍କର ବ୍ୟକ୍ତିଗତ ସୂଚନାକୁ ସୁରକ୍ଷିତ ରଖନ୍ତୁ

- ସାର୍ବଜନୀନ *AI* ଉପକରଣ କିମ୍ବା ଅଜଣା ଅନଲାଇନ୍ ସେବାରେ ବ୍ୟକ୍ତିଗତ, ଆର୍ଥିକ, ସ୍ୱାସ୍ଥ୍ୟ, ସରକାରୀ କିମ୍ବା ଗୋପନୀୟ ସୂଚନା ପ୍ରବେଶ କରନ୍ତୁ ନାହିଁ।
- ପାସୱାର୍ଡ, OTP, ଆକାଉଣ୍ଟ ନମ୍ବର, ପରିଚୟ ଡକ୍ୟୁମେଣ୍ଟ, ଗ୍ରାହକ ତଥ୍ୟ କିମ୍ବା ବ୍ୟକ୍ତିଗତ କଥାବାର୍ତ୍ତା ଭଳି ସମ୍ବେଦନଶୀଳ ବିବରଣୀ ସେୟାର କରିବାରୁ ଦୂରେଇ ରୁହନ୍ତୁ।
- AI ଉପକରଣଗୁଡ଼ିକୁ ସହାୟତା ମାଗିବା ସମୟରେ ଅଜ୍ଞାତ କିମ୍ବା ସାଧାରଣ ସୂଚନା ବ୍ୟବହାର କରନ୍ତୁ।

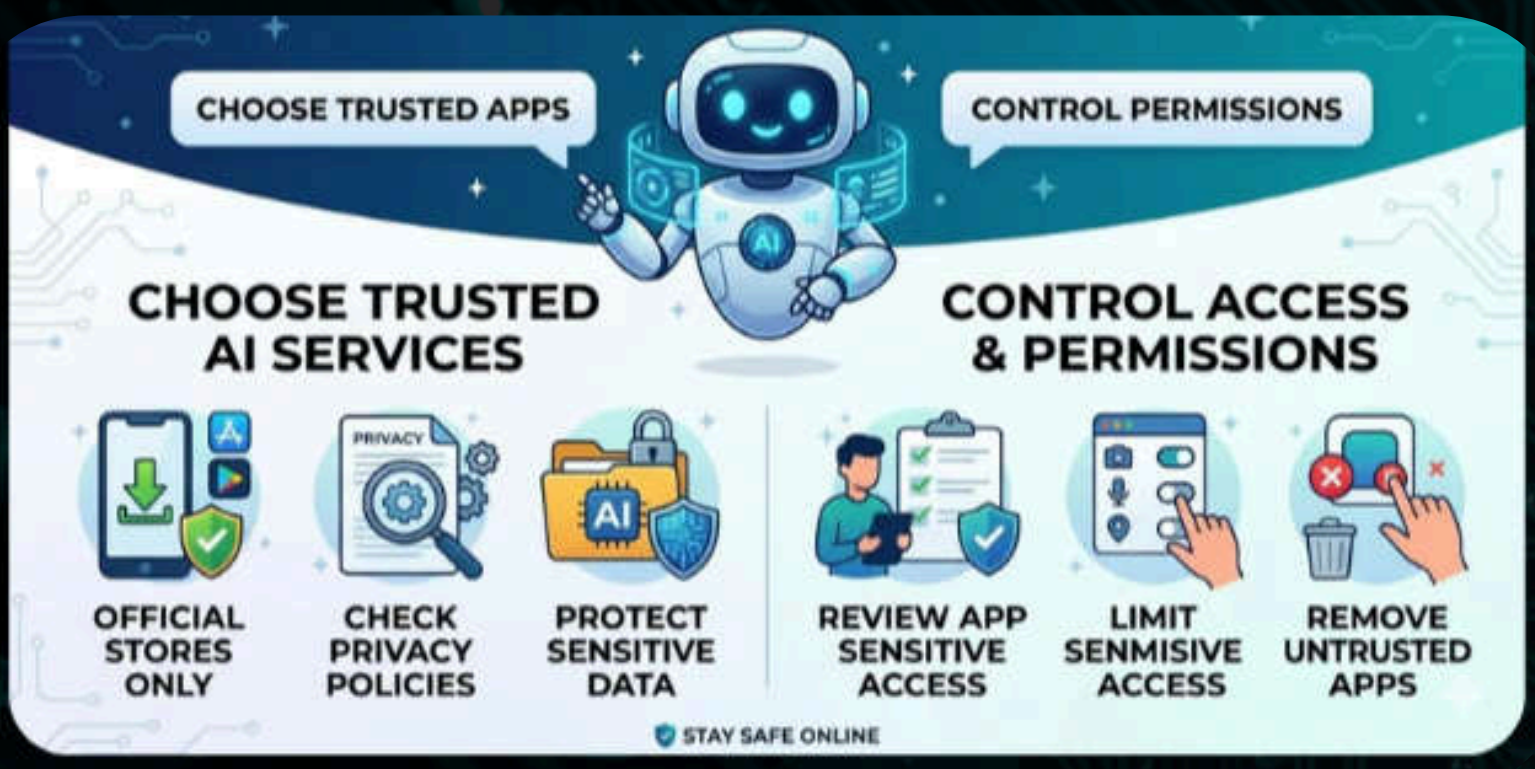
ସେୟାର କରିବା କିମ୍ବା କାର୍ଯ୍ୟ କରିବା ପୂର୍ବରୁ ସମୀକ୍ଷା କରନ୍ତୁ

- ସତ୍ୟର ଅନ୍ତିମ ଉତ୍ସ ଭାବରେ ନୁହେଁ, ବରଂ AI-ଉତ୍ପନ୍ନ ପ୍ରତିକ୍ରିୟାଗୁଡ଼ିକୁ ସହାୟତା ଭାବରେ ବ୍ୟବହାର କରନ୍ତୁ।
- ଆର୍ଥିକ, ଆଇନଗତ, ବୃତ୍ତିଗତ କିମ୍ବା ବ୍ୟକ୍ତିଗତ ନିଷ୍ପତ୍ତି ପାଇଁ ଗୁରୁତ୍ୱପୂର୍ଣ୍ଣ ସୂଚନା ବ୍ୟବହାର କରିବା ପୂର୍ବରୁ ଯାଞ୍ଚ କରନ୍ତୁ।
- ସଚେତନ ରୁହନ୍ତୁ ଯେ AI ଉପକରଣଗୁଡ଼ିକ ଭୁଲ, ଅସମ୍ପୂର୍ଣ୍ଣ କିମ୍ବା ଭ୍ରାମକ ସୂଚନା ସୃଷ୍ଟି କରିପାରେ।

AI ଉପକରଣଗୁଡ଼ିକୁ ଦାୟିତ୍ୱର ସହିତ ବ୍ୟବହାର କରନ୍ତୁ

- ଆପଣଙ୍କ କାମ ଏବଂ ଶିକ୍ଷାକୁ ସମର୍ଥନ କରିବା ପାଇଁ AI ବ୍ୟବହାର କରନ୍ତୁ, କିନ୍ତୁ ମାନବୀୟ ବିଚାର ଏବଂ ଦାୟିତ୍ୱ ବଜାୟ ରଖନ୍ତୁ।
- ମିଥ୍ୟା ସୂଚନା ସୃଷ୍ଟି କିମ୍ବା ପ୍ରସାର କରିବା, ଅନ୍ୟମାନଙ୍କ ପରି ବ୍ୟବହାର କରିବା କିମ୍ବା କାହାର ବ୍ୟକ୍ତିଗତ ତଥ୍ୟର ଅପବ୍ୟବହାର କରିବା ପାଇଁ AI ବ୍ୟବହାର କରନ୍ତୁ ନାହିଁ।

ବିଶ୍ୱସ୍ତ ଆପ୍ସ ବାଛନ୍ତୁ



ଆପ୍ ଆକ୍ସେସ୍ ଏବଂ ଅନୁମତିଗୁଡ଼ିକ ନିୟନ୍ତ୍ରଣ କରନ୍ତୁ

- AI ଆପ୍ଲିକେସନ୍ ଏବଂ ଡିଜିଟାଲ୍ ସହାୟକମାନଙ୍କୁ ଦିଆଯାଇଥିବା ଅନୁମତିଗୁଡ଼ିକର ସମୀକ୍ଷା କରନ୍ତୁ।
- କ୍ୟାମେରା, ମାଇକ୍ରୋଫୋନ୍, ଯୋଗାଯୋଗ କିମ୍ବା ଲୋକେସନ୍ ଭଳି ବୈଶିଷ୍ଟ୍ୟଗୁଡ଼ିକ ପାଇଁ ଆବଶ୍ୟକ ହେଲେ କେବଳ ଆକ୍ସେସ୍ ଅନୁମତି ଦିଅନ୍ତୁ।
- ଅନାବଶ୍ୟକ ଅନୁମତିଗୁଡ଼ିକ କାଢ଼ିଦିଅନ୍ତୁ ଏବଂ ଅବିଶ୍ୱସନୀୟ ଉତ୍ସଗୁଡ଼ିକରୁ ଆପ୍ସ ଅନଇନଷ୍ଟଲ୍ କରନ୍ତୁ।

ବିଶ୍ୱସ୍ତ AI ସେବାଗୁଡ଼ିକୁ ବାଛନ୍ତୁ

- ସୁନାମଧନ୍ୟ ପ୍ରଦାନକାରୀଙ୍କଠାରୁ AI ଆପ୍ଲିକେସନ୍ ବ୍ୟବହାର କରନ୍ତୁ ଏବଂ ସେଗୁଡ଼ିକୁ କେବଳ ସରକାରୀ ଆପ୍ ଷ୍ଟୋରରୁ ଡାଉନଲୋଡ୍ କରନ୍ତୁ।
- AI ସେବା ବ୍ୟବହାର କରିବା ପୂର୍ବରୁ ଗୋପନୀୟତା ସେଟିଙ୍ଗ୍ସ, ବ୍ୟବହାରର ସର୍ତ୍ତାବଳୀ ଏବଂ ଡାଟା ପରିଚାଳନା ଅଭ୍ୟାସଗୁଡ଼ିକର ସମୀକ୍ଷା କରନ୍ତୁ।
- ସୁରକ୍ଷା ନିୟନ୍ତ୍ରଣ ଯାଞ୍ଚ ନହେବା ପର୍ଯ୍ୟନ୍ତ AI ଟୁଲ୍ସକୁ ସମ୍ବେଦନଶୀଳ ଆକାଉଣ୍ଟ କିମ୍ବା ଫାଇଲଗୁଡ଼ିକ ସହିତ ସଂଯୋଗ କରିବାରୁ ଦୂରେଇ ରୁହନ୍ତୁ।

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