ELECTRONICS AND INFORMATION TECHNOLOGY

cert-in

ISEA Information Security Education & Awareness

Digital India



ᏥᎾᏰᎾᏁᏥ ᏆᏁᏗᏁᏪ

- ᏗᏁᏫᏁᏪ ᏰᎾᎾᏗᏁ 3
- AI-ᎾᏃ ᏥᏃᏆ ᏃᎾᏩᏁᎾᏆ ᏆᏗᏫᏆᏗᏫ ᏁᏫ ᏆᎾᏆᎾᏰ ᏃᎾᏩᏗᏆᏫᏫᏁᏫ 4
- ᏁᎾᏁᏗᏁ ᏁᏫ ᏥᏗᏫᏗᏥᏫᏫᏃ ᏥᏗᏫᏫᏗᏃᎾᏰ (Vishing) 5
- AI-ᏆᏁᏩᏁ.Ꮻ ᏩᏃᏢᏩᏃᏫᏫᏁᏫ ᏁᏫ ᏃᏁᎾᏩᏃᏁᏃᏥ ᏁᏁᏁᏰ 6
- ᏥᏩᏃᏢ ᏩᏃᏥᏆᏆᏫᏫᏃᏗᏁ ᏁᏫ ᏆᎾᏩᎾᏆᏁ ᏖᏆᏃᏩ (Identity Theft) 7
- ᏥᏗᏫᎾᎾᏬ ᏬᏗᏆᏩᏁ. ᎾᏁᏢᏗᏰᏁ 8
- ᎾᏆᏢᏁᏫᏫᏆ ᏆᏃᏫᏁᏰᏩᏁ 9
- ᏥᏗᏥᏁᏫᏫᏗᏆ ᏆᏃᏫᏁᏰᏩᏁ 10
- AI ᏭᏁᏫᏗᏗᎾᏩᎾ ᏆᏁᏖᎾᏃ ᏥᏃᏩᏩᏁᏫ ᏩᏃ 11
- ᏥᏩᏫᏫᎾᏆᏁᏫᏫᎶ ᏃᏫᏆ ᏥᏁᏬᏩᏁᏫᏩ ᏩᏃ 12
- CERT-In ᏫᏃ ᏆᏁᏫᏫᏥᏁᏫ ᏆᏃᏫᏁᏰᏩᏁ ᎶᏩᏁᏁᎾᏆᏁ ᏫᏗᏫᎾᏫᏁ ᏩᏃ 13

[illegible]

[illegible] (AI) [illegible] (Innovation) [illegible]

AI [illegible]

AI [illegible] AI [illegible] AI [illegible]

- [illegible] (CERT-In) [illegible] "AI [illegible]" [illegible] AI [illegible]

ସାଇବର [AI]-ଠାରୁ ଆସୁଥିବା ସାଇବର ଆକ୍ରମଣରୁ ନିଜକୁ ସୁରକ୍ଷିତ ରଖିବାର ଉପାୟଗୁଡ଼ିକ



ଆକ୍ରମଣ ଆସିବାଠାରୁ ବନ୍ଦ କରିବାକୁ?

ସାଇବର ଅପରାଧୀମାନେ (Threat Actors) ଆଜିକାଲି ଖୁବ୍ ଚାଲାକି ହୋଇଗଲେଣି। ସେମାନେ ଏପରି ଏକ ମାଧ୍ୟମ ବାଛିଥାନ୍ତି ଯେଉଁଠି ଆପଣ ସବୁଠାରୁ କମ୍ ସତର୍କ ରହିଥାନ୍ତି, ଯେପରିକି ଅଫିସ୍ ଇମେଲ୍, ଆପଣଙ୍କ ଘରୋଇ ଫୋନ୍ କିମ୍ବା ପରିବାର ସଦସ୍ୟଙ୍କ ନାମରେ ଆସୁଥିବା ମେସେଜ୍। ସେମାନେ ଆପଣଙ୍କୁ ଭୟଭୀତ କରିବା, ଲୋଭ ଦେଖାଇବା କିମ୍ବା ଜରୁରୀ ଅବସ୍ଥା ସୃଷ୍ଟି କରିବା ଭଳି ଉପାୟ ଅବଲମ୍ବନ କରିଥାନ୍ତି। ଏହାଦ୍ୱାରା ଆପଣ ନିଜର ବିଚାରଶକ୍ତି ହରାଇ ବସନ୍ତି ଏବଂ ଭୁଲ୍ ନିଷ୍ପତ୍ତି ନେଇଥାନ୍ତି। ଏହି ଆକ୍ରମଣଗୁଡ଼ିକୁ ଚିହ୍ନିବା ପାଇଁ ଆପଣଙ୍କୁ ସଚେତନ ରହିବାକୁ ପଡ଼ିବ।

ଆକ୍ରମଣ ଆସିବାର ଚିହ୍ନଟ କରିବେ କିପରି?

- ଆପଣଙ୍କୁ ଏହି ଭଳି ମେସେଜ୍ ଆସିବା ମାତ୍ରେ ଏମାନେ ଆପଣଙ୍କୁ ଚାପ ପକାଇବାକୁ ଚେଷ୍ଟା କରିଥାନ୍ତି, ଯେପରିକି ଆପଣ ତୁରନ୍ତ କାର୍ଯ୍ୟ ନକଲେ ଆପଣଙ୍କ ଆକାଉଣ୍ଟ ବନ୍ଦ ହୋଇଯିବ ବୋଲି କୁହାଯିବା।
- ଆପଣଙ୍କୁ ଲୋଭଣୀୟ ଅଫର୍ ଦିଆଯିବା ଏବଂ ଏଥିପାଇଁ ଆପଣଙ୍କ ବ୍ୟକ୍ତିଗତ ତଥ୍ୟ ମାଗିବା ହୋଇପାରେ।
- ଯେଉଁ ଲିଙ୍କ ଉପରେ କ୍ଲିକ୍ କଲେ ଆପଣଙ୍କ ଫୋନ୍ ହ୍ୟାକ୍ ହୋଇଯାଇପାରେ, ସେଥିରେ ଭୁଲ୍ ବନାନ ଥିବା ସମ୍ଭାବନା ଅଧିକ।
- ପ୍ରେରକଙ୍କ (Sender) ଠିକଣାରେ ଆପଣଙ୍କୁ ପରିଚିତ ବ୍ୟକ୍ତିଙ୍କ ନାମ ଥିବା ସତ୍ତ୍ୱେ, ଏହାର ଇମେଲ୍ ଆଡ୍ରେସ୍ ଅଲଗା ହୋଇପାରେ।

ଆକ୍ରମଣ ଆସିବାର ପ୍ରତିକାରର ଉପାୟଗୁଡ଼ିକ କ'ଣ?

- ଯଦି ଆପଣ ଆଗରୁ ଆପଣଙ୍କର ବ୍ୟକ୍ତିଗତ ତଥ୍ୟ ଦେଇଥାନ୍ତି, ତେବେ ତୁରନ୍ତ ସେହି ପାସ୍‌ୱର୍ଡ ବଦଳାନ୍ତୁ। ଯେଉଁ ଯେଉଁଠାରେ ସେହି ପାସ୍‌ୱର୍ଡ ବ୍ୟବହାର କରୁଛନ୍ତି ସେଠାରେ ମଧ୍ୟ ତୁରନ୍ତ ପରିବର୍ତ୍ତନ କରନ୍ତୁ।
- ଯଦି ଆପଣଙ୍କ ଫୋନ୍ ବା କମ୍ପ୍ୟୁଟର ହ୍ୟାକ୍ ହୋଇଛି, ତେବେ ଏହି ସମସ୍ତ ଆକାଉଣ୍ଟରୁ ଲଗ୍‌ଆଉଟ୍ କରି ଦିଅନ୍ତୁ, ଯାହାଦ୍ୱାରା ହ୍ୟାକର୍ ଆପଣଙ୍କ ଡିଭାଇସ୍‌ରୁ ଆଉ ପ୍ରବେଶ କରିପାରିବେ ନାହିଁ।
- ଆପଣଙ୍କ ଆକାଉଣ୍ଟରେ ଯଦି ଅତିରିକ୍ତ ସୁରକ୍ଷା ପାଇଁ ଦୁଇ-ପର୍ଯ୍ୟାୟ ଯାଞ୍ଚ (2FA) ଉପଲବ୍ଧ ଅଛି, ତେବେ ତାହା ତୁରନ୍ତ ଚାଲୁ କରନ୍ତୁ। ଏହା ଆପଣଙ୍କ ଆକାଉଣ୍ଟକୁ ଅଧିକ ସୁରକ୍ଷିତ କରିବ।
- ଯଦି ଆପଣ ଏହି ଆକ୍ରମଣର ଶିକାର ହୋଇଛନ୍ତି, ତେବେ ଏହାକୁ ଲୁଚାନ୍ତୁ ନାହିଁ। ତୁରନ୍ତ ନିଜ ପରିବାର ସଦସ୍ୟ, ବନ୍ଧୁ କିମ୍ବା ଅଫିସ୍‌ର ଉପରିସ୍ତରୀୟ ଅଧିକାରୀଙ୍କୁ ଜଣାନ୍ତୁ।

ಕರೆಯು ನಿಜ ಯಶಸ್ಸಿನ ಬೆದರಿಕೆ [Vishing]



ಇದು ಫಿಶಿಂಗ್ ಹೇಗೆ?

ಬೆದರಿಕೆಯವರು (Threat Actors) ಕರೆಯು ಬಂ ಬಿಲ್ಡರ್ (Clone) ಬಂಧ ಧ್ವನಿಮೇಲ್ ಬಳಸಿ ಹಿ.ಯಿ ಬಳಸಿ ಅವರಿಂದ ಹಣ ಅಥವಾ ಬೆಲೆಬಾಳುವ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯಲು ಯತ್ನಿಸುತ್ತಾರೆ. ಸಾಮಾನ್ಯವಾಗಿ ಇವರು ಬ್ಯಾಂಕ್, ಸರ್ಕಾರಿ ಸಂಸ್ಥೆ ಅಥವಾ ಕಂಪನಿಯ ಅಧಿಕಾರಿಗಳಂತೆ ನಟಿಸಿ, ಬಲಿಪಶುವಿನಲ್ಲಿ ತುರ್ತು ಪರಿಸ್ಥಿತಿಯ ಭಾವನೆ ಮೂಡಿಸುತ್ತಾರೆ. ಇದರಿಂದ ಅವರು ಸೂಕ್ಷ್ಮ (Sensitive) ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಪಡಿಸುವಂತೆ, ಹಣವನ್ನು ವರ್ಗಾಯಿಸುವಂತೆ ಅಥವಾ ಅನುಮಾನಾಸ್ಪದ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವಂತೆ ಒತ್ತಾಯಿಸುತ್ತಾರೆ.

ಇದು ಫಿಶಿಂಗ್ ಏಕೆ ಅಪಾಯಕಾರಿ?

- ಯಾವುದೇ ಬ್ಯಾಂಕ್ ಅಥವಾ ಕಂಪನಿಯು, ಯಾರೇ ಆದರೂ ಫೋನ್‌ನಲ್ಲಿ ಒಟಿಪಿ, ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಬ್ಯಾಂಕ್ ವಿವರಗಳನ್ನು ಕೇಳುವುದಿಲ್ಲ. ಇದನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಹಣವನ್ನು ತಕ್ಷಣ ಕಳುಹಿಸಲು ಒತ್ತಾಯಿಸಿದರೆ, ಅದನ್ನು ಸಂಪೂರ್ಣವಾಗಿ ನಿರ್ಲಕ್ಷಿಸಿ. ಕರೆಯನ್ನು ಕಡಿತಗೊಳಿಸಿ ಮತ್ತು ಅಧಿಕೃತ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಯನ್ನು ಬಳಸಿ ಸಂಸ್ಥೆಯನ್ನು ನೇರವಾಗಿ ಸಂಪರ್ಕಿಸಿ.
- ಕೆಲಸಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ಯಾವುದೇ ಅನುಮೋದನೆ (Approval) ವಿನಂತಿಗಳನ್ನು ಯಾವಾಗಲೂ ಎರಡು ಬಾರಿ ಪರಿಶೀಲಿಸಿ.
- ಬೆಲೆಬಾಳುವ ಆಸ್ತಿ, ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿ (Cryptocurrency) ಅಥವಾ ಗಿಫ್ಟ್ ಕಾರ್ಡ್‌ಗಳಲ್ಲಿ ಪಾವತಿಸಲು ಕೇಳಿದರೆ ಜಾಗರೂಕರಾಗಿರಿ.

ಇದನ್ನು ತಡೆಯಲು ನಾವೇನು ಮಾಡಬಹುದು?

- ಕರೆಯ ಮೂಲವನ್ನು ಪರಿಶೀಲಿಸಿ. ಕರೆ ಮಾಡಿದವರು ಯಾರೆಂದು ಹೇಳಿಕೊಂಡರೂ ಸರಿ, ಅವರ ಗುರುತನ್ನು ಸ್ವತಂತ್ರವಾಗಿ ಪರಿಶೀಲಿಸಿ.
- ಹಿರಿಯರು ಅಥವಾ ಕುಟುಂಬದವರೊಂದಿಗೆ ಸುರಕ್ಷಿತ ಪದವನ್ನು (Safe Word) ಹಂಚಿಕೊಳ್ಳಿ. ಇದರಿಂದ ಅವರು ಗುರುತನ್ನು ಪರಿಶೀಲಿಸಲು ಸಹಾಯವಾಗುತ್ತದೆ.
- ಸಂಶಯಾಸ್ಪದ ಕರೆಗಳ ಬಗ್ಗೆ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ. ಬೆದರಿಕೆಯವರು ಸಾಮಾನ್ಯವಾಗಿ ಭಯ ಅಥವಾ ತುರ್ತು ಪರಿಸ್ಥಿತಿಯ ಭಾವನೆಯನ್ನು ಸೃಷ್ಟಿಸಲು ಪ್ರಯತ್ನಿಸುತ್ತಾರೆ.
- ಪ್ರಶ್ನೆಗಳನ್ನು ಕೇಳಿ ಮತ್ತು ಅನುಮಾನ ವ್ಯಕ್ತಪಡಿಸಿ. ಬೆದರಿಕೆಯವರು (Threat Actors) ಬಲಿಪಶುವಿನ ಅನುಮಾನವನ್ನು ಹೋಗಲಾಡಿಸಲು ಪ್ರಯತ್ನಿಸುತ್ತಾರೆ. ಆದ್ದರಿಂದ ಪ್ರಶ್ನೆಗಳನ್ನು ಕೇಳಿ ಮತ್ತು ಅನುಮಾನಿಸಿ.

cert-in · ISEA · Digital India · Cyber Swachhta Kendra

[illegible] (AI)-[illegible]



[illegible]?

[illegible] (Threat Actors) [illegible] AI [illegible]

[illegible]?

- [illegible] MFA [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]?

- [illegible] (Strong) [illegible]
- [illegible] (MFA) [illegible]
- [illegible]
- [illegible] MFA [illegible]

[illegible]: @IndianCERT @cert_india

ऑनलाइन धोखाधड़ी और डिजिटल फ्रॉड



धोखाधड़ी क्या है?

धोखेबाज (Threat Actors) वो लोग होते हैं जो फर्जी वेबसाइट बनाकर, फर्जी कॉल करके या सोशल मीडिया पर झूठे वादे करके, आपसे आपकी निजी जानकारी, जैसे बैंक डिटेल्स, पासवर्ड, OTP या आपकी फोटो (Photo) या पहचान पत्र जैसी संवेदनशील (Identity) चीजें मांगते हैं।

धोखाधड़ी से कैसे बचें?

- वेबसाइट का URL हमेशा ध्यान से पढ़ें, आधिकारिक स्पेलिंग, अंडरस्कोर (-), या गलत डोमेन एक्सटेंशन से सावधान रहें।
- अनजान या संदिग्ध लिंक पर OTP, PIN या पासवर्ड कभी साझा न करें।
- अपने बैंकिंग ऐप्स को HTTPS सक्षम ब्राउज़र में या मोबाइल ऐप के माध्यम से ही एक्सेस करें, असामान्य (Unusual) लिंक से बचें।

धोखाधड़ी होने पर क्या करें?

- संदिग्ध लेनदेन या संबंधित वेबसाइट URल को तुरंत ही या तो ब्लॉक कर दें या रिपोर्ट करने के लिए, फ्रॉड के ठीक बाद।
- OTP, PIN या पासवर्ड, कभी भी किसी भी परिस्थिति में अनजान या "सहायक व्यक्ति" जैसे साझा न करें।
- संदिग्ध वेबसाइट के लिए हमेशा HTTPS ब्राउज़र में या फिर ऐप का ही उपयोग करें और सही URL टाइप करें।
- अगर आपको लगता है कि आपकी जानकारी चोरी हो गई है, तो तुरंत ही अपने बैंक या क्रेडिट कार्ड कंपनी को कॉल करें।

৩৭৪৯৫ ৪৸৫৲৯৯. ০৯৮৮৸৮৯

AI-৲৯৯৲৯৯.৫ ৲৸৩৸৮৮৯ ৯৸৲৲৯৯৫ ৲৫৸৩৯ ৪৸৲৲৯৯. ৮৫ ৭২৮ ৯৯৯ ৲৯৩৸৫৹৸৯৯৲ ০৯৲৲৸৲৲ ৸২:



- ৸৯৮৮৯, ৮৫৫৲৲৲ ৮৯২৩৩৲৲৲৲৫৯৮ ৲২ ৫৲৸৸৫৫৲ (Approval) ৮৯৫৲৹ ৯৸.৩৸ ৸৯৮৫৹৸ ৯৯ ৪৯৸৩ ২৩৸৫৫ ৫৯৸.৸৸।
- "৯৯৩ ৪৸৲৲৲৯৸.৸" ৲৸৸৩ ৯২৲৲৯৫ ৮৫৮৫ ৲২ ৩৪৸৩৸৲৲৫৯ ৯২ ৯৯৸৯৸৸ ৲২ ৩৪৸৩৸৲৲৫৯ ৯২ ৮৫৩৩ ৩২৫৯৯৯ ৭২৮৫৫৫-৯৯।
- ৲৯৹৫৪৯৯৯৫৲ ৸৸৲৪ ৯৯ ৫৲৸৸৫৫৲ ৩৯৫৸৲২৲ ৮৫ ২৪৯৯৩ ৲২ ৩৯৯৫৩৯৯৲ ৮৫৫৫ ৩২ ৩২৲০২ ৫৯৸.৸৸।
- ৯৸৫৸৩ ৩৪২৩৩৯ (Sender) ৩৫৩২৲ ৲২ ৮৫৩ ৩৯৹৫৫৮ ৮৯৲৫৯ URL ৭২৮৫৫৫-৯৯।
- ৩৲৲৯৯ ৯৩৩৯৫ ৫৯৸.৸৸৩০২ MFA ৩৯৫৩৩৩৯ ৲২ OTP ৭৯৩৩৫৫-৯৯।
- ৲২৮৫৸৯৯৯৯৲ ৲৫৩৯৯৫৸৲৲৫৯৯ ৩৫'৫ ৮৫৫৫৫ ৲২ ৩৲২৫৯৯৮৯৯৲ (Unofficial) ৮৲৯৮ ৫৯৯৯৯৫ "৸৸৲৪" ৮৫৫৫৫ ৫৯৸.৸৸।
- ৮৯৸.৩৲ (Job) ৲২ ২৲৩৲২ (Investment) ৫৩৫৯৯৯ ৸৯৩৩৲ ৩৯৲৯৯৯ ৯২ ৯৯৸৮৯ ২৩৸৫৫ ৲২ ২৲৸২৯ ৯৯০৫৯৲৮ ৮৫৫৩৫৯ ৮৫০৫৯ ৮৫৮৲ ৮৯৲২৯।

৯৩৫৲ ২৫২৫৲২৩ ৩৯৲৮৩৫-৯৯ - ০৫৲৲ ০৯৩৩২২ ৩২, ২৲৩২৯০২ ৸৯৲৪ ৩২, ৯৯ ৪৯৩৩ ৯২ ৩৫৪৫৫৫ ৮৯৩০২ ৮৯৲.৩৲ ৯৯৫৫৩ ৮৫৫৯৫ ৩২!

৯৩৩ ২৯৯২ ৸৫৫৯৩৩৫ ৯৯৸৮৫৩৫৯ ৩২:

ସୁରକ୍ଷାରେ ଦୃଢ଼୍ୟକରଣ



ମଧ୍ୟମ ଯୋଜନାରେ ଚଢ଼ ଦୃଢ଼୍ୟକରଣ ଯୋ

- ଆକାଉଣ୍ଟରେ ଯୋଜାଇବା ପାଇଁରେ ଯାହାକି (Strong) ଅଟେ ଆପଣ-ଆପଣଙ୍କ ଆକାଉଣ୍ଟକୁ ଅପଡେଟ୍ କରିଥାଆନ୍ତୁ ଯୋ; ଏହିପରି ଦୃଢ଼୍ୟକରଣଗୁଡ଼ିକରେ ସୁରକ୍ଷା ବ୍ୟବସ୍ଥାକୁ ପାଇଁରେ ଆକାଉଣ୍ଟକୁ ଯୋଡ଼ିହୁଏନାହିଁ ଅପଡେଟ୍ କରିଥାଆନ୍ତୁ ଯୋ।
- ସୁରକ୍ଷାର ଯୋଡ଼ଣ-ସ୍ତର, ଯାହା ବୈକଳ୍ପିକ ସୁରକ୍ଷାରକ୍ଷା ଏବଂ ଯାଞ୍ଚକାରୀ-ଉତ୍ପାଦନର ଅତିରିକ୍ତାକାରରେ (MFA) ଶୁଣାଯାଏ ଯୋ।
- OTP, PIN, ଆକାଉଣ୍ଟକୁ ଏବଂ ଏପ୍ଲିକେସନ୍ସମୂହ ବ୍ୟତୀତ ସୁରକ୍ଷାରେ ଯାଉଥିବା ଏକାଧିକ ଆପଣ ଅତିରିକ୍ତାକାରରେ।
- ଅତିରିକ୍ତ ଏପ୍ଲିକେସନ୍ସମୂହ ଦ୍ୱାରା (Additional Security Layer) ପ୍ରଦାନିତ ଅତିରିକ୍ତାକାରରେ ଅତିରିକ୍ତାକାରରେ (ଆଙ୍ଗୁଠି ଚିହ୍ନଟକାରୀ / Fingerprint ଅଥବା ଯାଞ୍ଚ ଚିହ୍ନଟକାରୀ / Face Recognition) ଅପଡେଟ୍ କରିଥାଆନ୍ତୁ ଯୋ।

ମୋବାଇଲ ଅଥବା ସୁରକ୍ଷାରେ ଯୋଡ଼ିଥାଆନ୍ତୁ ଅତିରିକ୍ତ ଏବଂ ଦୃଢ଼୍ୟକରଣଗୁଡ଼ିକରେ ଦୃଢ଼୍ୟକରଣ ଯୋ

- ଏକ୍ସେଲ୍‌ସିଅର୍‌ରେ ଏବଂ ଏକାଧିକ ପ୍ରତିଷ୍ଠା ସୁରକ୍ଷାରେ ମୋବାଇଲ ଅତିରିକ୍ତାକାରରେ ଅତି ଚିହ୍ନଟକାରୀ ଯୋଡ଼ିଥାଆନ୍ତୁ (Sender) ଅଟେଥାଏ ଅତିରିକ୍ତାକାରରେ ଅତିରିକ୍ତାକାରରେ ଯୋଡ଼ିଥାଆନ୍ତୁ ଯୋ।
- ଅପ୍ରତି ଅତିରିକ୍ତାକାରରେ ଯାଞ୍ଚକାରୀ ପ୍ରସ୍ତୁତ ଯୋଡ଼ିଥାଆନ୍ତୁ ଯୋ ଅତି ଅପଡେଟ୍ ଅତି ଅପଡେଟ୍ ଯୋଡ଼ିଥାଆନ୍ତୁ ଯୋ।
- ପାଇଁରେ ଏବଂ ଅତିରିକ୍ତାକାରରେ ଅତିରିକ୍ତାକାରରେ ଅପଡେଟ୍ ଅତିରିକ୍ତାକାରରେ ଅଟେଥାଏ ଏକ୍ସେଲ୍‌ସିଅର୍ (Authenticity) ଯାଞ୍ଚ ଯୋ।
- ଯାଞ୍ଚକାରୀ ଏକ୍ସେଲ୍‌ସିଅର୍ ଯାଞ୍ଚକାରୀ-ସ୍ତ, ଅତିରିକ୍ତାକାରରେ ଅତିରିକ୍ତାକାରରେ ଯୋ ଯାଞ୍ଚ ଅତିରିକ୍ତାକାରରେ ଏବଂ ଅତି.ଯୋ ଅତିରିକ୍ତାକାରରେ ଯୋ।

ଅତିରିକ୍ତାକାରରେ ଓଏଟିପି ଯାଞ୍ଚକାରୀ ପାଇଁରେ ଯାଞ୍ଚକାରୀ ଅପଡେଟ୍ ଯୋ

- ସୁରକ୍ଷାକାରୀ ଯୋଡ଼ିଥାଆନ୍ତୁ ଅତିରିକ୍ତାକାରରେ ଏମ୍‌ଏସ୍.ଯୋଏ ଅପଡେଟ୍ ଅପଡେଟ୍ ଅତିରିକ୍ତାକାରରେ ଯୋ, ସୁରକ୍ଷାରେ ଅତିରିକ୍ତାକାରରେ ଏବଂ ଏପ୍ଲିକେସନ୍ସରେ ଅତିରିକ୍ତାକାରରେ ଏବଂ ସୁରକ୍ଷାରେ ଯୋ।
- ଅପଡେଟ୍ ଅତିରିକ୍ତାକାରରେ ଅତିରିକ୍ତାକାରରେ (ଯାଞ୍ଚକାରୀ/ଯୋଡ଼ିଥାଆନ୍ତୁ) ଅତି ଏକ୍ସେଲ୍‌ସିଅର୍ ଏକ୍ସେଲ୍‌ସିଅର୍ ଅତିରିକ୍ତାକାରରେ ଅତିରିକ୍ତାକାରରେ ଅତିରିକ୍ତାକାରରେ ଏପ୍ଲିକେସନ୍ସରେ ଅତିରିକ୍ତାକାରରେ ଯୋ।

ಡಿವೈಸ್ ಸುರಕ್ಷತೆ ಟಿಪ್ಸ್



ಡಿವೈಸ್‌ಗಳನ್ನು ಏಕೆ ಸುರಕ್ಷಿತವಾಗಿ ಇಡಬೇಕು

- ಭದ್ರತಾ ದೋಷಗಳನ್ನು (Vulnerabilities) ಸರಿಪಡಿಸಲು ಹಾಗೂ ಇತ್ತೀಚಿನ ಬೆದರಿಕೆಗಳಿಂದ ರಕ್ಷಿಸಿಕೊಳ್ಳಲು, ಸಾಫ್ಟ್‌ವೇರ್‌ಗಳನ್ನು, ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ಗಳನ್ನು ಮತ್ತು ಆ್ಯಪ್‌ಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಅಪ್‌ಡೇಟ್ ಮಾಡಿಕೊಳ್ಳಬೇಕು.
- ಭದ್ರತೆಗೆ ಕಿರುಬೆದರಿಕೆಯಾದ ಯಾವುದೇ-ಸಿ, ಅದನ್ನು ಬಳಸಲು ಭದ್ರತೆಯ ಸಲುವಾಗಿ ತಕ್ಷಣವೇ ಅಪ್‌ಡೇಟ್ ಮಾಡಿಕೊಳ್ಳಿ.

ಬೆಂಬಲಿತ ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂಗಳನ್ನು ಬಳಸುತ್ತಿರುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ

- ಬಳಸಲು (Genuine) ಬಳಸುತ್ತಿರುವುದು ಆದ್ಯತೆಯು ಆ ಸಂ ಬಿ ಬೆಂಬಲಿತ ತಯಾರಿಕಾದಾರರಿಂದ ಬಿ ಬಳಸಲು ಬಿ ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಬಂಲ್ ಬಳಸಲ ಸಲಹೆ ನೀಡಲಾಗಿದೆ.
- ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಬಿದಿನವಾಗಿರುವುದರಿಂದ ಬಿ ಬೆದರಿಕೆಯಿಂದ ಬಳಸಲಾಗಿದೆ ಆದ್ಯತೆಯು ಆ ಸಂ ಬಿಡಿಯ ತಯಾರಿಕೆ ಸಂಸ್ಥೆಯು ಬೆಂಬಲಿಸುತ್ತದೆ.

ಅಪಾಯಕಾರಿ ಆ್ಯಪ್‌ಗಳನ್ನು ಏಕೆ ನಿರ್ಬಂಧಿಸಬೇಕು

- ಬಳಸಲು ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಅನ್ನು ಬಳಸುವ ಮೊಬೈಲ್‌ಗಳಲ್ಲಿ ಬಿ ಬೆಂಬಲಿತ ಬಿಡಿಯ ಆದ್ಯತೆಯು ಆ ಸಂ ಬಿಡಿಯ.
- ಭದ್ರತೆಯ ಕಿರುಬೆದರಿಕೆಯಾದ ಯಾವುದೇ-ಸಿ, ಅದನ್ನು ಅನ್ನು ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಸಂಸ್ಥೆಯು ಬೆಂಬಲಿಸುತ್ತದೆ ಆ್ಯಪ್‌ಗಳನ್ನು ನಿರ್ಬಂಧಿಸಲಾಗಿದೆ.
- ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ಗಳನ್ನು ಮತ್ತು ಆ್ಯಪ್‌ಗಳನ್ನು ಅಧಿಕೃತ ಮೂಲಗಳಿಂದ ಮಾತ್ರ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿಕೊಳ್ಳಬೇಕು.

ಅಪಾಯಕಾರಿ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ಬಳಸದಿರುವುದನ್ನು ಏಕೆ ನಿರ್ಬಂಧಿಸಲಾಗಿದೆ

- ಬಳಸಲು ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಅನ್ನು Wi-Fi ಬೆಂಬಲಿತವಾಗಿದೆ ಆ ಸಂ ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಬಳಸುವುದನ್ನು ಬಳಸಲಾಗಿದೆಯೆಂದು ಅಂದಾಜಿಸಲಾಗಿದೆ.
- ಅಪಾಯಕಾರಿ ಬಳಸುವುದನ್ನು ನಿಯಂತ್ರಿಸುವುದರಿಂದ ಆ್ಯಪ್‌ಗಳನ್ನು ಬಳಸಲು ಬೆದರಿಕೆಯಿಂದ ಬಳಸಲಾಗಿದೆ ಆದ್ಯತೆಯು ಆ ಸಂ.
- ಬಳಸಲಾಗಿರುವ ವೈಶಿಷ್ಟ್ಯಗಳು ಬಿ ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಬಳಸಲು ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಅಂಶಗಳು ಬಳಸಲು ಆ ಸಂ ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ (Unsecured) ಬಳಸುವುದನ್ನು ಆಪರೇಟಿಂಗ್‌ಸಿಸ್ಟಂ ಅಪಾಯ ಆ.

ਟਿਕਾਊ [AI] ਢਾਂਚਾਗਤਾਵਾਂ ਦੀਵਾਰਾਂ ਪੈਦਾ



ਸੰਪਰਕ ਟਿਕਾਣੇ ਖ਼ਤਰਨਾਕ ਦੀਵਾਰਾਂ ਪੈਦਾ

- ਤਿਆਰਾਤੀ AI ਨਾਲ ਦੇ ਸ.ਦਾਖਾ ਤੋਦਾਰਦੇ ਦੇਹਾਰਦੇ ਤੇ ਟਿਪ, ਸੰਤਰਾਤੇ, ਦੇਸ਼ਾਦੇਤਾਤੇ, ਤਹਿਤਾਦੇਤਾਦਾਰਾਂ ਦੇ ਦਾਤਾਤੇ ਖ਼ਤਰਨਾਕ ਸੰਪਾਰ ਟਿਪਾਤ ਹੈ।
- ਤਿਆਦੇਸ਼ਾਂ, OTP, ਟਿਖਾਸ਼ਾਦਾ ਦੇਤਾਦਾਰਾਂ, ਤਿਆਤਿਤਾਰ ਦੀਰਖਾਟਦਾਰਾ, ਖ਼ਤਦਾਰਾਤਾਂ ਦੀਟਾਰਾ ਦੇ ਟਿਪ ਸੰਪਾਰ ਸੰਟਾਰਾ ਪੈਸਾਤਾ ਦੇਟਦਾਦਾਰਾਤਾਤੇ ਖ਼ਤਰਨਾਕ ਦੀਵਾਰਾਂ ਸੰਪਾਰ ਪੈਦਾ ਹੈ।
- AI ਨਾਲ ਖ਼ਤਰਨਾਕ ਦਾਟਾਰ ਸੰਖਾਤ ਤੇ ਦਾਤਾ (Anonymized) ਦੇ ਟਿਸਦਾਤਾਤਾਂ ਖ਼ਤਰਨਾਕ ਦੀਟਾਰਾਂ ਦੀਟਾਰਾਂ ਹੈ।

ਦੀਵਾਰਾਂ ਦੇ ਖ.ਦਾ ਖ਼ਤਰਨਾਕ ਪੈਦਾਟਾਰਾਂ ਪੈਸਾ ਹੈ

- AI ਢਾਂਚਾਤਾਂ ਦਾਟਾਰਾਂ ਪੈਸਾਤਾਂ ਖ਼ਤਰਨਾਕ ਦਾਟਾਰਾਂ ਦਾਟਾਰਾਂ ਹੈ, ਪੈਟਾਖ਼ਤਾਟ ਸੰਪਾਰ ਦੇਟਾਦਾਰਾਂ ਦਾਟਾਰਾਂ।
- ਸੰਤਾਖ਼ਤਾਤ, ਸੰਪਾਤਾਟ, ਤਿਟਾਟਾਤਾਤਾਂ ਦੇ ਟਿਪ ਟਿਸਦਾਤਾਤਾਂ ਤਾਟਾਖ਼ਤਾਟ ਤੇ ਦੀਟਾਰਾਂ ਪੈਟਾਖ਼ਤਾਟ ਪੈਸਾਤਾਂ ਪੈਸਾਤਾਂ ਪੈਸਾਤਾਂ ਹੈ।
- ਟਾਤਾਤਾ ਪੈਟਾਟ ਤੇ ਤੰਸਾਖ਼ਤਾਤਾ ਪੈਟ ਪੈਸ AI ਨਾਲ ਖ਼ਤਰਨਾਕ ਖ਼ਤਰਨਾਕ ਦੀਖਾਟ, ਤਾਟਾਤਾਤਾਂ ਦੇ ਦੀਖਾਟ ਪੈਟਾਤਾ ਤੇ ਸੰਤਾਖ਼ਤਾਤ ਟਾਤਾਤਾ ਖ਼ਤਰਨਾਕ ਟਾਤਾਤਾ ਹੈ।

AI ਨਾਲ ਢਾਂਚਾਗਤਾਵਾਂ ਦੀਵਾਰਾਂ ਪੈਦਾ

- ਸੰਪਾਰ ਖ.ਦਾ ਸੰਤ ਟਿਖਾਟ ਤੇ ਖ਼ਤਰਨਾਕ ਨਾਲ AI ਦੀਵਾਰਾਂ ਪੈਦਾ, ਪੈਟਾਖ਼ਤਾਟ ਪੈਸਾਤਾਂ ਪੈਸਾਤਾਂ ਸੰਤ ਢਾਂਚਾਗਤਾਵਾਂ ਪੈਸਾਤਾਂ ਤੇ ਤੰਸਾਖ਼ਤਾਤਾ ਪੈਸਾ ਹੈ।
- ਦੀਖਾਟ ਖ਼ਤਰਨਾਕ ਟਾਤਾਤਾਂ ਟਿਖਾਟ ਟਿਖਾਟਾਤਾਂ, ਟਾਤਾਤਾਂ ਪੈਸਾਤਾਂ ਨਾਲ ਖ਼ਤਰਨਾਕ ਨਾਲ (Impersonation), ਟਿਖਾਟ ਪੈਸਾਤਾਂ ਪੈਸਾਤਾਂ ਤੇ ਟਿਪ ਟਿਸਦਾਤਾਤਾਂ ਦੀਟਾਰਾਂ ਦੀਖਾਟ ਦੀਵਾਰਾਂ ਪੈਸਾਤਾਂ ਖ਼ਤਰਨਾਕ AI ਸੰਪਾਰ ਦੀਵਾਰਾਂ ਹੈ।

ਸੰਪਾ ਟਿਸਦਾ ਪੈਸਾਤਾਂਤਾਂ ਤੇ ਸੰਤਾਖ਼ਤਾਤਾ ਪੈਸਾ ਹੈ: @indianCERT @cert_India

ডিভাইসগুলিতে AI ব্যবহার করা

AI ব্যবহার করে ব্যক্তিগত তথ্য সুরক্ষিত রাখুন

- AI ব্যবহারকারীদের তথ্য প্রশিক্ষণের জন্য ব্যবহৃত হওয়ার ঝুঁকি সম্পর্কে সচেতন থাকুন।
- চ্যাটবট, ভার্চুয়াল অ্যাসিস্ট্যান্ট, চিকিৎসা বা আর্থিক পরামর্শের জন্য AI ব্যবহার করবেন না।
- গোপন তথ্য ব্যক্তিগত ব্যবহার না করা এবং ব্যবহারকারীর চুক্তি ভালোভাবে পড়া।

ডিভাইসগুলিতে AI ব্যবহার করা

- ফোন, ল্যাপটপ ব্যবহার করার সময় কোন AI ব্যবহারকারীর প্রয়োজন তা নির্ধারণ করুন এবং অপ্রয়োজনীয় AI বন্ধ করুন।
- AI ব্যবহার প্রয়োজন, ক্যামেরা, মাইক্রোফোন ব্যবহার, প্রয়োজন, ব্যবহারকারী চুক্তি (Terms of Use) এবং গোপনীয়তা নীতি ভালোভাবে পড়া।
- অপ্রয়োজনীয় অ্যাপ্লিকেশন চিহ্নিত করা এবং সেগুলি ডিলিট করা, ব্যবহারকারীদের তথ্য ব্যবহার করে AI মডেল প্রশিক্ষণ বন্ধ করা।

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

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