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 ಜಾಗೃತಿ ಮಾರ್ಗದರ್ಶಿ

ಸೈಬರ್ ನೈರ್ಮಲ್ಯದ ಸಂಸ್ಕೃತಿಯನ್ನು ನಿರ್ಮಿಸಿ

#ಸೈಬರ್ ನೈರ್ಮಲ್ಯನಮ್ಮ ಸಂಸ್ಕೃತಿ



ರಾಷ್ಟ್ರೀಯ ಸೈಬರ್ ಭದ್ರತಾ ಜಾಗೃತಿ ತಿಂಗಳು (ಅಕ್ಟೋಬರ್ 2026)

ಪ್ರಕಾಶಕರು

ಭಾರತೀಯ ಕಂಪ್ಯೂಟರ್ ತುರ್ತು ಪ್ರತಿಕ್ರಿಯೆ ತಂಡ

ನಮ್ಮನ್ನು ಅನುಸರಿಸಿ:

@IndianCERT

@cert_india

ಪರಿವಿಡಿ

ಮುನ್ನುಡಿ 3

AI-ವರ್ಧಿತ ಫಿಶಿಂಗ್ ಮತ್ತು ಸಾಮಾಜಿಕ ಎಂಜಿನಿಯರಿಂಗ್ 4

ಧ್ವನಿ ಮತ್ತು ವೀಡಿಯೊ ಡೀಪ್‌ಫೇಕ್‌ಗಳು (ವಿಶಿಂಗ್) 5

AI- ನೆರವಿನ ಮಾಲ್‌ವೇರ್ ಮತ್ತು ಸ್ವಯಂಚಾಲಿತ ದಾಳಿಗಳು 6

ನಕಲಿ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಮತ್ತು ಗುರುತಿನ ಕಳ್ಳತನ 7

ಕೆಂಪು ಧ್ವಜಗಳ ಪರಿಶೀಲನಾಪಟ್ಟಿ 8

ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆ 9

ಸಾಧನ ಸುರಕ್ಷತೆ 10

AI ಅನ್ನು ಜವಾಬ್ದಾರಿಯುತವಾಗಿ ಬಳಸಿ 11

ವಿಶ್ವಾಸಾರ್ಹ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಆರಿಸಿ 12

ಸೈಬರ್ ಭದ್ರತಾ ಘಟನೆಗಳನ್ನು CERT-In ಗೆ ವರದಿ ಮಾಡಿ 13

ನಮ್ಮನ್ನು ಅನುಸರಿಸಿ: @IndianCERT @cert_india

ಮುನ್ನುಡಿ

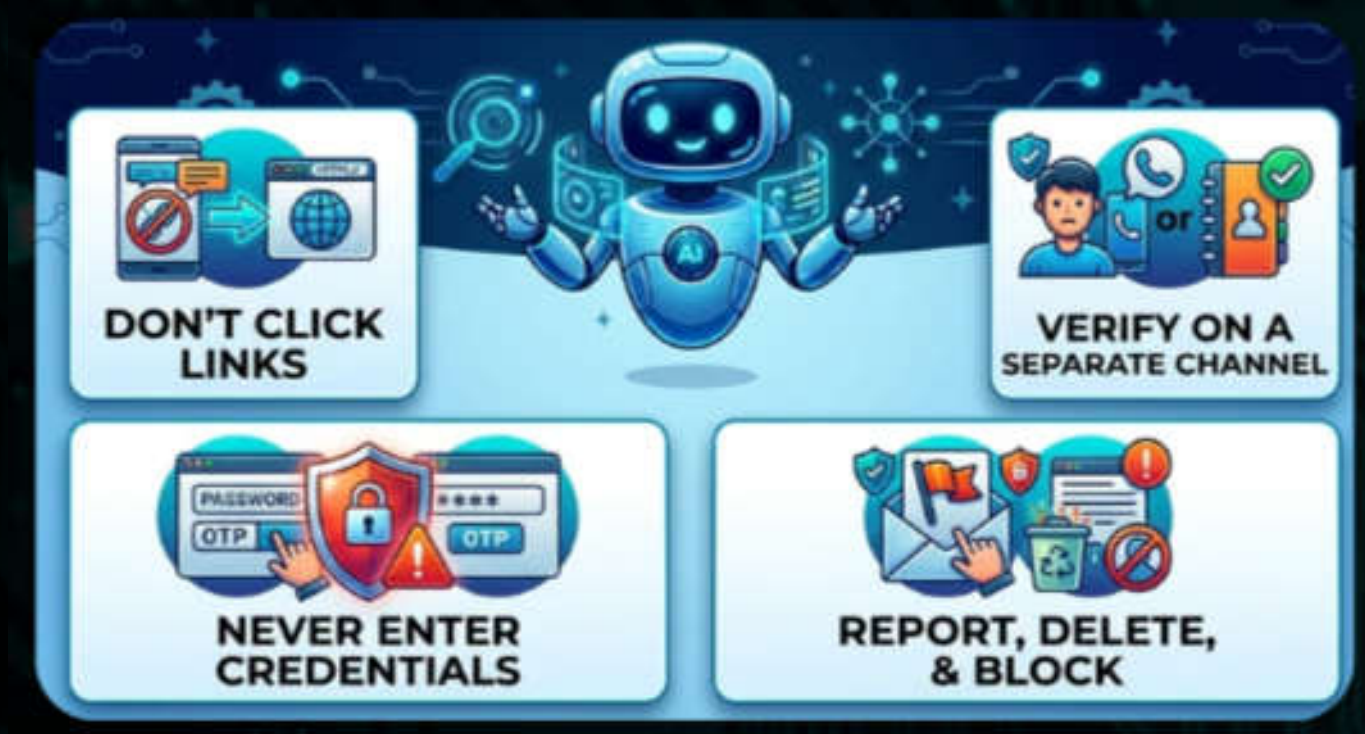
ಕೃತಕ ಬುದ್ಧಿಮತ್ತೆ (AI) ನಾವು ಬದುಕುವ, ಕೆಲಸ ಮಾಡುವ ಮತ್ತು ಸಂವಹನ ನಡೆಸುವ ವಿಧಾನವನ್ನು ಪರಿವರ್ತಿಸುತ್ತಿದೆ. ಇದು ನಾವೀನ್ಯತೆಯನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುತ್ತದೆ, ಉತ್ಪಾದಕತೆಯನ್ನು ಸುಧಾರಿಸುತ್ತದೆ ಮತ್ತು ವಿವಿಧ ವಲಯಗಳಲ್ಲಿ ಸಂಕೀರ್ಣ ಸಮಸ್ಯೆಗಳನ್ನು ಪರಿಹರಿಸಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ. ಆದಾಗ್ಯೂ, ಹೆಚ್ಚು ಮುಂದುವರಿದ ಮತ್ತು ಮನವರಿಕೆಯಾಗುವ ಸೈಬರ್ ಬೆದರಿಕೆಗಳನ್ನು ಸೃಷ್ಟಿಸಲು ಬೆದರಿಕೆ ನೀಡುವವರು ಅದೇ ತಂತ್ರಜ್ಞಾನವನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳುತ್ತಿದ್ದಾರೆ.

ಆಕ್ರಮಣಕಾರರು ಈಗ ಹೆಚ್ಚು ವಾಸ್ತವಿಕ ಇಮೇಲ್‌ಗಳು, ಸಂದೇಶಗಳು, ಆಡಿಯೋ, ವೀಡಿಯೊಗಳು ಮತ್ತು ವೆಬ್‌ಸೈಟ್‌ಗಳನ್ನು ರಚಿಸಬಹುದಾದ್ದರಿಂದ AI ಡಿಜಿಟಲ್ ಬೆದರಿಕೆಗಳನ್ನು ಗುರುತಿಸುವುದನ್ನು ಹೆಚ್ಚು ಕಷ್ಟಕರವಾಗಿಸುತ್ತಿದೆ. ಕಳಪೆ ವ್ಯಾಕರಣ, ಅಸಾಮಾನ್ಯ ಫಾರ್ಮ್ಯಾಟಿಂಗ್ ಅಥವಾ ಸ್ಪಷ್ಟ ತಪ್ಪುಗಳಂತಹ ಸಾಂಪ್ರದಾಯಿಕ ಎಚ್ಚರಿಕೆ ಚಿಹ್ನೆಗಳು ಇನ್ನು ಮುಂದೆ ವಿಶ್ವಾಸಾರ್ಹ ಸೂಚಕಗಳಾಗಿರುವುದಿಲ್ಲ. ಪರಿಶೀಲನೆ ಮತ್ತು ಜವಾಬ್ದಾರಿಯುತ ಡಿಜಿಟಲ್ ಅಭ್ಯಾಸಗಳು ಎಂದಿಗಿಂತಲೂ ಹೆಚ್ಚು ಮುಖ್ಯವಾಗಿವೆ.

ನಾವು ಪ್ರತಿದಿನ ಬಳಸುವ AI ಪರಿಕರಗಳು ಮತ್ತು ಸ್ಮಾರ್ಟ್ ಸಾಧನಗಳನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಬಳಸದಿದ್ದರೆ, ಅವುಗಳನ್ನು ಹೊಸ ಗೌಪ್ಯತೆ ಮತ್ತು ಭದ್ರತಾ ಅಪಾಯಗಳಿಗೆ ಪರಿಚಯಿಸಬಹುದು. ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ AI ಅಪ್ಲಿಕೇಶನ್‌ಗಳೊಂದಿಗೆ ವೈಯಕ್ತಿಕ ಅಥವಾ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದು, ಅನಗತ್ಯ ಅನುಮತಿಗಳನ್ನು ನೀಡುವುದು ಅಥವಾ ಪರಿಶೀಲನೆ ಇಲ್ಲದೆ AI ರಚಿತ ಮಾಹಿತಿಯನ್ನು ಅವಲಂಬಿಸುವುದರಿಂದ ವ್ಯಕ್ತಿಗಳು ಮತ್ತು ಸಂಸ್ಥೆಗಳು ಭದ್ರತಾ ಅಪಾಯಗಳಿಗೆ ಒಳಗಾಗಬಹುದು.

"AI ಸೈಬರ್ ಜಾಗೃತಿ" ಕುರಿತು ಭಾರತೀಯ ಕಂಪ್ಯೂಟರ್ ತುರ್ತು ಪ್ರತಿಕ್ರಿಯೆ ತಂಡ (CERT-In) ಪ್ರಕಟಿಸಿರುವ ಈ ಕಿರುಪುಸ್ತಕವು ಸೈಬರ್ ಭದ್ರತಾ ವೃತ್ತಿಪರರಿಗೆ ಮಾತ್ರವಲ್ಲದೆ ದೈನಂದಿನ ನಾಗರಿಕರು, ಉದ್ಯೋಗಿಗಳು ಮತ್ತು ಡಿಜಿಟಲ್ ಬಳಕೆದಾರರಿಗಾಗಿ ವಿನ್ಯಾಸಗೊಳಿಸಲಾಗಿದೆ. ಇದು AI ಡಿಜಿಟಲ್ ಬೆದರಿಕೆ ಭೂದೃಶ್ಯವನ್ನು ಹೇಗೆ ಬದಲಾಯಿಸುತ್ತಿದೆ ಎಂಬುದನ್ನು ವಿವರಿಸುತ್ತದೆ ಮತ್ತು ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ, ಸಾಧನಗಳು ಮತ್ತು ಆನ್‌ಲೈನ್ ಗುರುತನ್ನು ರಕ್ಷಿಸಲು ಪ್ರತಿಯೊಬ್ಬರೂ ಅನುಸರಿಸಬಹುದಾದ ಸರಳ, ಪ್ರಾಯೋಗಿಕ ಹಂತಗಳನ್ನು ಒದಗಿಸುತ್ತದೆ.

AI-ವರ್ಧಿತ ಫಿಶಿಂಗ್ ಮತ್ತು ಸಾಮಾಜಿಕ ಎಂಜಿನಿಯರಿಂಗ್



ಇದು ಹೇಗೆ ಕೆಲಸ ಮಾಡುತ್ತದೆ?

ಬೆದರಿಕೆ ಹಾಕುವವರು ಈಗ ನೈಜವಾಗಿ ಮತ್ತು ದೋಷಗಳಿಲ್ಲದೆ ಕಾಣುವ ಇಮೇಲ್‌ಗಳು ಮತ್ತು ಪಠ್ಯ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸುತ್ತಾರೆ. ಸಂದೇಶಗಳನ್ನು ವೈಯಕ್ತಿಕವೆಂದು ಭಾವಿಸಲು ಅವರು ನಿಮ್ಮ ಕೆಲಸ, ನೀವು ಬಳಸುವ ಸೇವೆಗಳು ಅಥವಾ ಇತ್ತೀಚಿನ ಚಟುವಟಿಕೆಗಳಂತಹ ನಿಮ್ಮ ಬಗ್ಗೆ ವಿವರಗಳನ್ನು ಬಳಸುತ್ತಾರೆ. ಈ ಸಂದೇಶಗಳು ಚೆನ್ನಾಗಿ ಬರೆಯಲ್ಪಟ್ಟಿರುವುದರಿಂದ, ಅವುಗಳನ್ನು ಗುರುತಿಸುವುದು ತುಂಬಾ ಕಷ್ಟಕರವಾಗಿರುತ್ತದೆ.

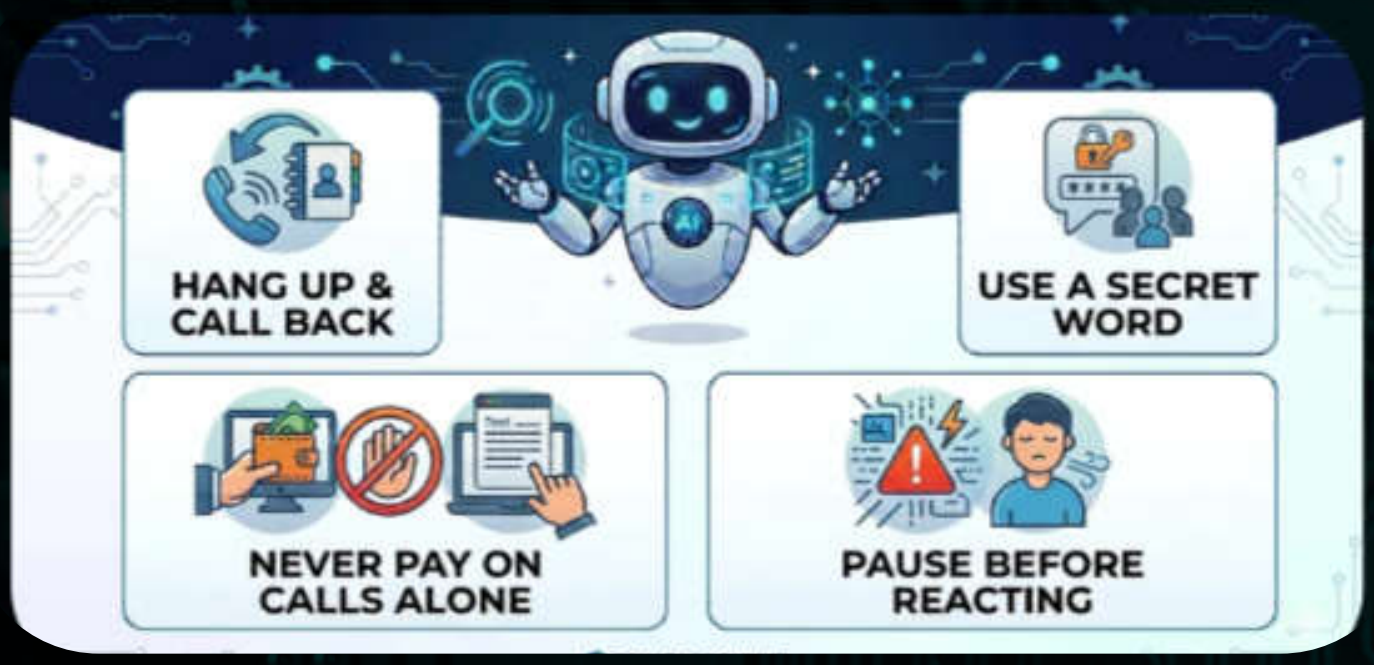
ಗುರುತಿಸುವುದು ಹೇಗೆ?

- ಸಂದೇಶವು ನಿಮಗೆ ತುಂಬಾ ನಿರ್ದಿಷ್ಟವೆನಿಸುತ್ತದೆ ಆದರೆ ಅನಿರೀಕ್ಷಿತವಾಗಿ ಬರುತ್ತದೆ.
- ಇದು ತುರ್ತು ಅಥವಾ ಬೆದರಿಕೆಯ ಸ್ವರವನ್ನು ಬಳಸುತ್ತದೆ ಮತ್ತು ತಕ್ಷಣದ ಕ್ರಮವನ್ನು ಬಯಸುತ್ತದೆ.
- ಅದು ಲಿಂಕ್ ಅನ್ನು ಕ್ಲಿಕ್ ಮಾಡಲು, ಖಾತೆಯನ್ನು ಪರಿಶೀಲಿಸಲು, ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಮರುಹೊಂದಿಸಲು ಅಥವಾ ಪಾವತಿ ಮಾಡಲು ನಿಮ್ಮನ್ನು ಕೇಳುತ್ತದೆ.
- ಕಳುಹಿಸುವವರ ವಿಳಾಸ ಬಹುತೇಕ ಸರಿಯಾಗಿದೆ, ಆದರೆ ಸಂಪೂರ್ಣವಾಗಿ ಅಲ್ಲ.

ಸುರಕ್ಷಿತವಾಗಿರುವುದು ಹೇಗೆ?

- ಅನಪೇಕ್ಷಿತ ಸಂದೇಶಗಳಲ್ಲಿನ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ. ಬದಲಿಗೆ ನೇರವಾಗಿ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್ ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್‌ಗೆ ಹೋಗಿ.
- ಅಧಿಕೃತ ಫೋನ್ ಸಂಖ್ಯೆ ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್‌ನಂತಹ ಪ್ರತ್ಯೇಕ, ವಿಶ್ವಾಸಾರ್ಹ ಸಂಪರ್ಕ ಚಾನಲ್ ಮೂಲಕ ವಿನಂತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಸಂದೇಶ ಲಿಂಕ್ ಮೂಲಕ ತಲುಪಿದ ಪುಟದಲ್ಲಿ ರುಜುವಾತುಗಳು ಅಥವಾ OTP ಗಳನ್ನು ಎಂದಿಗೂ ನಮೂದಿಸಬೇಡಿ.
- ಅನುಮಾನಾಸ್ಪದ ಸಂದೇಶಗಳನ್ನು ವರದಿ ಮಾಡಿ ಮತ್ತು ಅಳಿಸಿ, ನಂತರ ಕಳುಹಿಸುವವರನ್ನು ನಿರ್ಬಂಧಿಸಿ.

ಧ್ವನಿ ಮತ್ತು ವೀಡಿಯೊ ಡೀಪ್‌ಫೇಕ್‌ಗಳು [ವಿಶಿಂಗ್]



ಇದು ಹೇಗೆ ಕೆಲಸ ಮಾಡುತ್ತದೆ?

ಬೆದರಿಕೆ ಹಾಕುವವರು ಧ್ವನಿಗಳನ್ನು ಕ್ಲೋನ್ ಮಾಡಬಹುದು ಅಥವಾ ನಿಜವೆಂದು ತೋರುವ ಮತ್ತು ಧ್ವನಿಸುವ ನಕಲಿ ವೀಡಿಯೊಗಳನ್ನು ರಚಿಸಬಹುದು. ಅವರು ನಿಮ್ಮ ಕುಟುಂಬ, ಸಹೋದ್ಯೋಗಿಗಳು ಅಥವಾ ಅಧಿಕಾರಿಗಳಂತೆ ನಟಿಸಿ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಲು, ಹಣವನ್ನು ಕಳುಹಿಸಲು ಅಥವಾ ತ್ವರಿತವಾಗಿ ಕಾರ್ಯನಿರ್ವಹಿಸಲು ಒತ್ತಡ ಹೇರಬಹುದು.

ಗುರುತಿಸುವುದು ಹೇಗೆ?

- ಅಸಾಮಾನ್ಯ ತುರ್ತು, ಗಾಬರಿ, ಅಥವಾ ಯಾರಿಗೂ ಹೇಳಬೇಡಿ ಎಂಬಂತಹ ಗೌಪ್ಯತೆಯ ವಿನಂತಿಗಳು.
- ಸ್ವಲ್ಪ ಆಫ್ ಟೋನ್, ವೇಗ, ಹಿನ್ನೆಲೆ ಶಬ್ದ ಅಥವಾ ಆಡಿಯೊ ಗುಣಮಟ್ಟ.
- ಸಾಮಾನ್ಯ ಪರಿಶೀಲನೆ ಅಥವಾ ಅನುಮೋದನೆ ಪ್ರಕ್ರಿಯೆಗಳನ್ನು ಬೈಪಾಸ್ ಮಾಡಲು ವಿನಂತಿಗಳು.
- ಉಡುಗೊರೆ ಕಾರ್ಡ್‌ಗಳು, ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿ ಅಥವಾ ವೈರ್ ವರ್ಗಾವಣೆಯ ಮೂಲಕ ಪಾವತಿಗಾಗಿ ವಿನಂತಿಗಳು.

ಸುರಕ್ಷಿತವಾಗಿರುವುದು ಹೇಗೆ?

- ಫೋನ್ ಕಟ್ ಮಾಡಿ ಮತ್ತು ಆ ವ್ಯಕ್ತಿಗೆ ಅವರ ತಿಳಿದಿರುವ, ಉಳಿಸಿದ ಸಂಖ್ಯೆಯನ್ನು ಬಳಸಿಕೊಂಡು ಮರಳಿ ಕರೆ ಮಾಡಿ.
- ತುರ್ತು ಸಂದರ್ಭಗಳಲ್ಲಿ ಗುರುತನ್ನು ಪರಿಶೀಲಿಸಲು ಕುಟುಂಬ ಅಥವಾ ಕೆಲಸದ ಸ್ಥಳದಲ್ಲಿ ಸುರಕ್ಷಿತ ಪದವನ್ನು ಹೊಂದಿಸಿ.
- ಕೇವಲ ಕರೆ ಅಥವಾ ವೀಡಿಯೊ ಮೂಲಕ ಪಾವತಿಗಳನ್ನು ಎಂದಿಗೂ ಅಧಿಕೃತಗೊಳಿಸಬೇಡಿ. ಪ್ರತ್ಯೇಕ ಚಾನೆಲ್ ಮೂಲಕ ಲಿಖಿತವಾಗಿ ದೃಢೀಕರಿಸಿ.
- ಪ್ರತಿಕ್ರಿಯಿಸುವ ಮೊದಲು ವಿರಾಮಗೊಳಿಸಿ. ಬೆದರಿಕೆ ಹಾಕುವವರು ನಿಮ್ಮ ತೀರ್ಪನ್ನು ಮರೆಮಾಡಲು ಪ್ಯಾನಿಕ್ ಅನ್ನು ಅವಲಂಬಿಸಿರುತ್ತಾರೆ.

AI-ಸಹಾಯದ ಮಾಲ್ವೇರ್ ಮತ್ತು ಸ್ವಯಂಚಾಲಿತ ದಾಳಿಗಳು



ಇದು ಹೇಗೆ ಕೆಲಸ ಮಾಡುತ್ತದೆ?

ಬೆದರಿಕೆಕಾರರು ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್ ಅನ್ನು ರಚಿಸಲು ಅಥವಾ ಮರೆಮಾಡಲು, ಬಹು ಸೈಟ್‌ಗಳಲ್ಲಿ ಕದ್ದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಪರೀಕ್ಷಿಸಲು ಮತ್ತು ನವೀಕರಣಗಳ ಅಗತ್ಯವಿರುವ ವ್ಯವಸ್ಥೆಗಳನ್ನು ಗುರುತಿಸಲು AI ಪರಿಕರಗಳನ್ನು ಬಳಸುತ್ತಾರೆ. ಇದು ದಾಳಿಗಳನ್ನು ವೇಗವಾಗಿ ಮತ್ತು ಹೆಚ್ಚು ವ್ಯಾಪಕವಾಗಿ ಮಾಡುತ್ತದೆ.

ಗುರುತಿಸುವುದು ಹೇಗೆ?

- ನೀವು ವಿನಂತಿಸದ ಅನಿರೀಕ್ಷಿತ ಲಾಗಿನ್ ಎಚ್ಚರಿಕೆಗಳು, ಪಾಸ್‌ವರ್ಡ್ ಮರುಹೊಂದಿಸುವ ಇಮೇಲ್‌ಗಳು ಅಥವಾ MFA ಪ್ರಾಂಪ್ಟ್‌ಗಳು ನಿಮ್ಮ ಖಾತೆಯ ಚಟುವಟಿಕೆಯಲ್ಲಿ ಪಟ್ಟಿ ಮಾಡಲಾದ ಪರಿಚಯವಿಲ್ಲದ ಸಾಧನಗಳು ಅಥವಾ ಸೆಷನ್‌ಗಳು
- ಆಂಟಿವೈರಸ್ ಎಚ್ಚರಿಕೆಗಳು, ಪಾಪ್-ಅಪ್‌ಗಳು ಅಥವಾ ಅಸಾಮಾನ್ಯವಾಗಿ ನಿಧಾನಗೊಂಡ ಸಾಧನದ ಕಾರ್ಯಕ್ಷಮತೆ
- ನೀವು ಗುರುತಿಸದ ಫೈಲ್‌ಗಳು, ಸೆಟ್ಟಿಂಗ್‌ಗಳು ಅಥವಾ ಬ್ರೌಸರ್ ವಿಸ್ತರಣೆಗಳು

ಸುರಕ್ಷಿತವಾಗಿರುವುದು ಹೇಗೆ?

- ಪ್ರತಿಯೊಂದು ಖಾತೆಗೂ ವಿಶಿಷ್ಟವಾದ, ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್ ಬಳಸಿ.
- ಎಲ್ಲಾ ಪ್ರಮುಖ ಖಾತೆಗಳಲ್ಲಿ ಬಹು ಅಂಶ ದೃಢೀಕರಣ (MFA) ಸಕ್ರಿಯಗೊಳಿಸಿ.
- ಆಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್, ಸಿಸ್ಟಮ್‌ಗಳು ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ನವೀಕೃತವಾಗಿಡಿ.
- ಅನಿರೀಕ್ಷಿತ ಲಾಗಿನ್ ಅಥವಾ MFA ಎಚ್ಚರಿಕೆಗಳ ಸಂದರ್ಭದಲ್ಲಿ ತಕ್ಷಣವೇ ಕಾರ್ಯನಿರ್ವಹಿಸಿ.

ನಕಲಿ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಮತ್ತು ಗುರುತಿನ ಕಳ್ಳತನ



ಇದು ಹೇಗೆ ಕೆಲಸ ಮಾಡುತ್ತದೆ?

ಬೆದರಿಕೆ ಹಾಕುವವರು ನಿಮ್ಮ ಲಾಗಿನ್ ರುಜುವಾತುಗಳು, OTP ಗಳು ಅಥವಾ ಪಾವತಿ ವಿವರಗಳನ್ನು ಕದಿಯಲು ಬ್ಯಾಂಕಿಂಗ್ ಅಥವಾ ಶಾಪಿಂಗ್ ಪೋರ್ಟಲ್‌ಗಳಂತಹ ನೈಜವಾಗಿ ಕಾಣುವ ಒಂದೇ ರೀತಿಯ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಮತ್ತು ಚಾಟ್‌ಬಾಟ್‌ಗಳನ್ನು ರಚಿಸಬಹುದು. ಅವರು ಸುಳ್ಳು ಗುರುತುಗಳನ್ನು ರಚಿಸಲು ನಕಲಿ ಫೋಟೋಗಳು ಅಥವಾ ದಾಖಲೆಗಳನ್ನು ಸಹ ಬಳಸಬಹುದು.

ಗುರುತಿಸುವುದು ಹೇಗೆ?

- ಹೆಚ್ಚುವರಿ ಅಕ್ಷರಗಳು, ಹೈಫನ್‌ಗಳು ಅಥವಾ ಬೇರೆ ಡೊಮೇನ್ ಅಂತ್ಯದಂತಹ ವೆಬ್‌ಸೈಟ್ URL ಗಳನ್ನು ಸ್ವಲ್ಪ ಮಾರ್ಪಡಿಸಲಾಗಿದೆ.
- ಚಾಟ್‌ಬಾಟ್‌ಗಳು ಅಥವಾ ಏಜೆಂಟ್‌ಗಳು OTP ಗಳು, PIN ಗಳು ಅಥವಾ ಪೂರ್ಣ ಕಾರ್ಡ್ ಸಂಖ್ಯೆಗಳನ್ನು ಕೇಳುತ್ತಾರೆ.
- ಪರಿಚಿತ ಸೈಟ್‌ನಲ್ಲಿ HTTPS ಕಾಣೆಯಾಗಿದೆ ಅಥವಾ ಅಸಾಮಾನ್ಯ ವಿನ್ಯಾಸ ಅಸಂಗತತೆಗಳು.

ಸುರಕ್ಷಿತವಾಗಿರುವುದು ಹೇಗೆ?

- ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವ ಬದಲು ಯಾವಾಗಲೂ ಅಧಿಕೃತ URL ಗಳನ್ನು ನೇರವಾಗಿ ಟೈಪ್ ಮಾಡಿ ಅಥವಾ ಪರಿಶೀಲಿಸಿದ ಬುಕ್‌ಮಾರ್ಕ್‌ಗಳನ್ನು ಬಳಸಿ.
- ಯಾವುದೇ ಚಾಟ್‌ಬಾಟ್ ಅಥವಾ "ಬೆಂಬಲ ಏಜೆಂಟ್" ಜೊತೆ OTP ಗಳು, PIN ಗಳು ಅಥವಾ ಪೂರ್ಣ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಎಲ್ಲಿಯಾದರೂ ಲಾಗಿನ್ ಆಗುವ ಮೊದಲು HTTPS ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಡೊಮೇನ್ ಹೆಸರನ್ನು ಹತ್ತಿರದಿಂದ ನೋಡಿ.
- ಪರಿಚಯವಿಲ್ಲದ ಚಟುವಟಿಕೆಗಳಿಗಾಗಿ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಹೇಳಿಕೆಗಳು ಮತ್ತು ಕ್ರೆಡಿಟ್ ವರದಿಯನ್ನು ನಿಯಮಿತವಾಗಿ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ.

ಕೆಂಪು ಧ್ವಜಗಳ ಪರಿಶೀಲನಾಪಟ್ಟಿ

AI-ಸಕ್ರಿಯಗೊಳಿಸಿದ ದಾಳಿಯ ಈ ಚಿಹ್ನೆಗಳಿಗಾಗಿ ಗಮನಿಸಿ:

- ಹಣ, ರುಜುವಾತುಗಳು ಅಥವಾ ಅನುಮೋದನೆಗಾಗಿ ತುರ್ತು, ಒತ್ತಡದ ವಿನಂತಿ.
- "ಪರಿಚಿತ" ವ್ಯಕ್ತಿಯಿಂದ ಬಂದ ಕರೆ ಅಥವಾ ವೀಡಿಯೊದಲ್ಲಿ ಸ್ವಲ್ಪ ಆಡಿಯೋ/ವಿಡಿಯೋ ಅಸಂಗತತೆಗಳು ಕಂಡುಬಂದರೆ
- ಸಾಮಾನ್ಯ ಪರಿಶೀಲನೆ/ಅನುಮೋದನೆ ಕಾರ್ಯವಿಧಾನಗಳನ್ನು ಬೈಪಾಸ್ ಮಾಡಲು ವಿನಂತಿ
- ಪರಿಚಯವಿಲ್ಲದ ಕಳುಹಿಸುವವರ ಡೊಮೇನ್ ಅಥವಾ ಸ್ವಲ್ಪ ಬದಲಾದ URL
- ನೀವು ವಿನಂತಿಸದ ಅನಿರೀಕ್ಷಿತ MFA ಪ್ರಾಂಪ್ಟ್‌ಗಳು ಅಥವಾ OTP ಗಳು
- ಅನಧಿಕೃತ ಲಿಂಕ್‌ಗಳ ಮೂಲಕ ಭದ್ರತಾ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲು ಅಥವಾ "ಪರಿಶೀಲಿಸಲು" ವಿನಂತಿಗಳು.
- ಮುಂಗಡ ಪಾವತಿ ಅಥವಾ ವೈಯಕ್ತಿಕ ಹಣಕಾಸಿನ ವಿವರಗಳ ಅಗತ್ಯವಿರುವ ಉದ್ಯೋಗ/ಹೂಡಿಕೆ ಕೊಡುಗೆಗಳು

ಸಂದೇಹವಿದ್ದಾಗ – ವಿರಾಮಗೊಳಿಸಿ, ಸ್ವತಂತ್ರವಾಗಿ ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಒತ್ತಡದಲ್ಲಿ ವರ್ತಿಸಬೇಡಿ.

ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆ



ನಿಮ್ಮ ಖಾತೆಗಳನ್ನು ರಕ್ಷಿಸಿ

- ಪ್ರತಿಯೊಂದು ಖಾತೆಗೂ ಬಲವಾದ ಮತ್ತು ವಿಶಿಷ್ಟವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸಿ; ಅವುಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಸಂಗ್ರಹಿಸಲು ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕವನ್ನು ಬಳಸಿ.
- ಲಭ್ಯವಿರುವಲ್ಲೆಲ್ಲಾ ಬಹು-ಅಂಶ ದೃಢೀಕರಣ (MFA) ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.
- OTP ಗಳು, PIN ಗಳು, ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಅಥವಾ ಭದ್ರತಾ ಕೋಡ್‌ಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಹೆಚ್ಚುವರಿ ಭದ್ರತಾ ಪದರವಾಗಿ ಬಯೋಮೆಟ್ರಿಕ್ ದೃಢೀಕರಣವನ್ನು (ಬೆರಳಚ್ಚು/ಮುಖ ಗುರುತಿಸುವಿಕೆ) ಬಳಸಿ.

ಇಮೇಲ್ ಮತ್ತು ಇಂಟರ್ನೆಟ್ ಬಳಸುವಾಗ ಸುರಕ್ಷಿತವಾಗಿರಿ

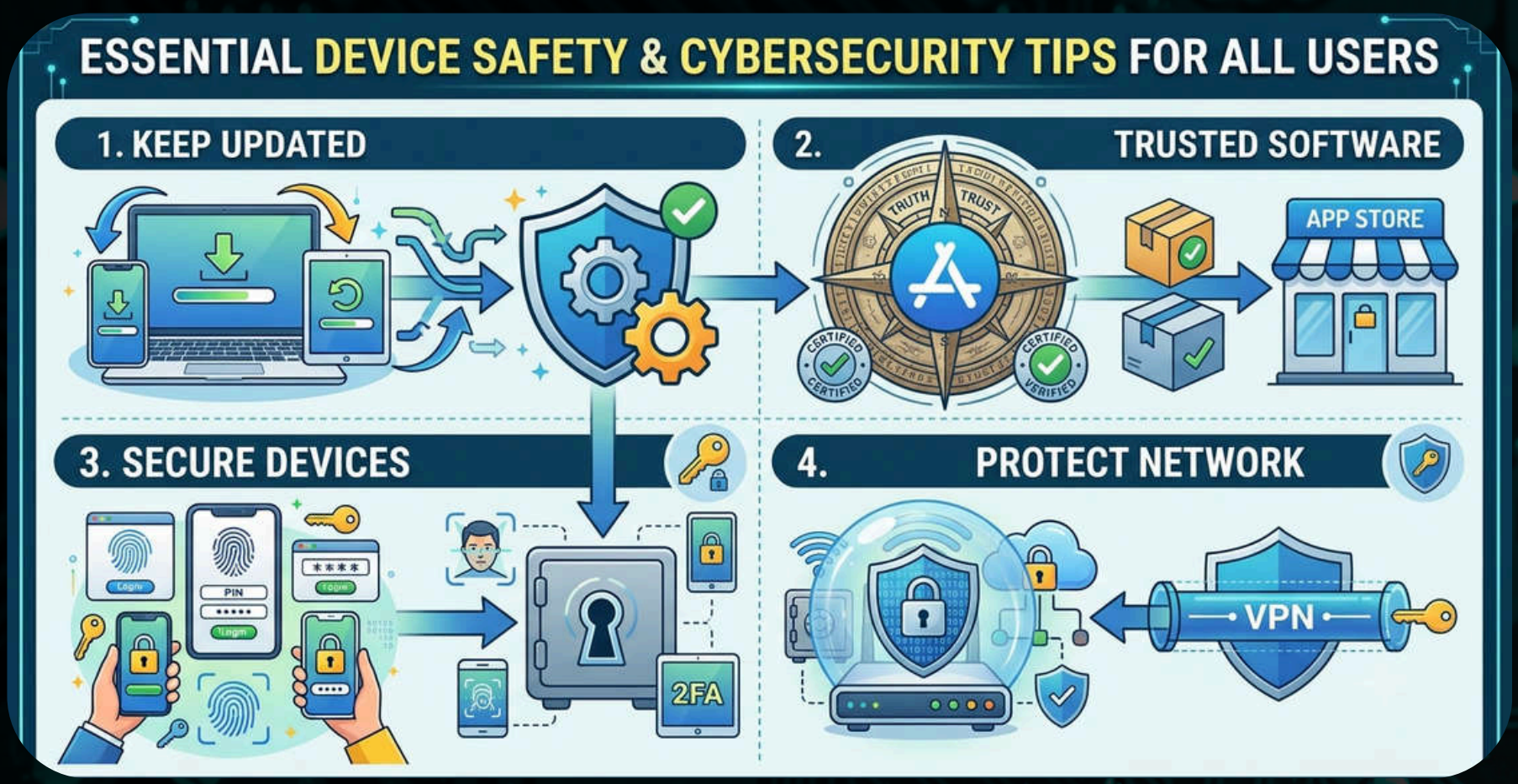
- ಅನುಮಾನಾಸ್ಪದ ಅಥವಾ ಒಂದೇ ರೀತಿಯ ಇಮೇಲ್ ವಿಳಾಸಗಳಿಗಾಗಿ ಕಳುಹಿಸುವವರ ವಿವರಗಳನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಪರಿಶೀಲಿಸಿ.
- ಕ್ಲಿಕ್ ಮಾಡುವ ಮೊದಲು ಲಿಂಕ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಅನಿರೀಕ್ಷಿತ ಲಗತ್ತುಗಳನ್ನು ತೆರೆಯುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಲಾಗಿನ್ ಅಥವಾ ಹಣಕಾಸಿನ ವಿವರಗಳನ್ನು ನಮೂದಿಸುವ ಮೊದಲು ವೆಬ್‌ಸೈಟ್ ದೃಢೀಕರಣವನ್ನು ದೃಢೀಕರಿಸಿ.
- ಸಂದೇಹವಿದ್ದಲ್ಲಿ, ನೀವು ಕಾರ್ಯನಿರ್ವಹಿಸುವ ಮೊದಲು ನಿಲ್ಲಿಸಿ ಮತ್ತು ಪರಿಶೀಲಿಸಿ.

ಏನಾದರೂ ತಪ್ಪಾಗುವ ಮುನ್ನ ಸಿದ್ಧರಾಗಿರಿ

- ಆಫ್‌ಲೈನ್‌ನಲ್ಲಿ ಅಥವಾ ಸುರಕ್ಷಿತ ಕ್ಲೌಡ್ ಸೇವೆಯಲ್ಲಿ ಸಂಗ್ರಹಿಸಲಾದ ಪ್ರಮುಖ ಫೈಲ್‌ಗಳ ನಿಯಮಿತ ಬ್ಯಾಕಪ್‌ಗಳನ್ನು ನಿರ್ವಹಿಸಿ.
- ಖಾತೆ ಮರುಪಡೆಯುವಿಕೆ ಮಾಹಿತಿಯನ್ನು (ಇಮೇಲ್/ಫೋನ್) ನವೀಕರಿಸಿ ಮತ್ತು ಸುರಕ್ಷಿತವಾಗಿರಿಸಿ.

ನಮ್ಮನ್ನು ಅನುಸರಿಸಿ: @IndianCERT @cert_india

ಸಾಧನ ಸುರಕ್ಷತೆ



ಸಾಧನಗಳನ್ನು ನವೀಕೃತವಾಗಿಡಿ

- ತಿಳಿದಿರುವ ದೋಷಗಳನ್ನು ಸರಿಪಡಿಸಲು ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಂಗಳು, ಅಪ್ಲಿಕೇಶನ್‌ಗಳು, ಬ್ರೌಸರ್‌ಗಳು ಮತ್ತು ಭದ್ರತಾ ಸಾಫ್ಟ್‌ವೇರ್‌ಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ನವೀಕರಿಸಿ.
- ಸಾಧ್ಯವಾದಲ್ಲೆಲ್ಲಾ ಸ್ವಯಂಚಾಲಿತ ನವೀಕರಣಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.

ವಿಶ್ವಾಸಾರ್ಹ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಮಾತ್ರ ಸ್ಥಾಪಿಸಿ

- ನಿಜವಾದ ಸಾಫ್ಟ್‌ವೇರ್ ಬಳಸಿ ಮತ್ತು ಅಧಿಕೃತ ಅಪ್ಲಿಕೇಶನ್ ಸ್ಟೋರ್‌ಗಳು ಅಥವಾ ವಿಶ್ವಾಸಾರ್ಹ ಮೂಲಗಳಿಂದ ಮಾತ್ರ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಸ್ಥಾಪಿಸಿ.
- ವಿಶ್ವಾಸಾರ್ಹ ಆಂಟಿವೈರಸ್ ಅಥವಾ ಭದ್ರತಾ ಪರಿಹಾರಗಳನ್ನು ಬಳಸಿ ಮತ್ತು ಅವುಗಳನ್ನು ನವೀಕೃತವಾಗಿಡಿ.

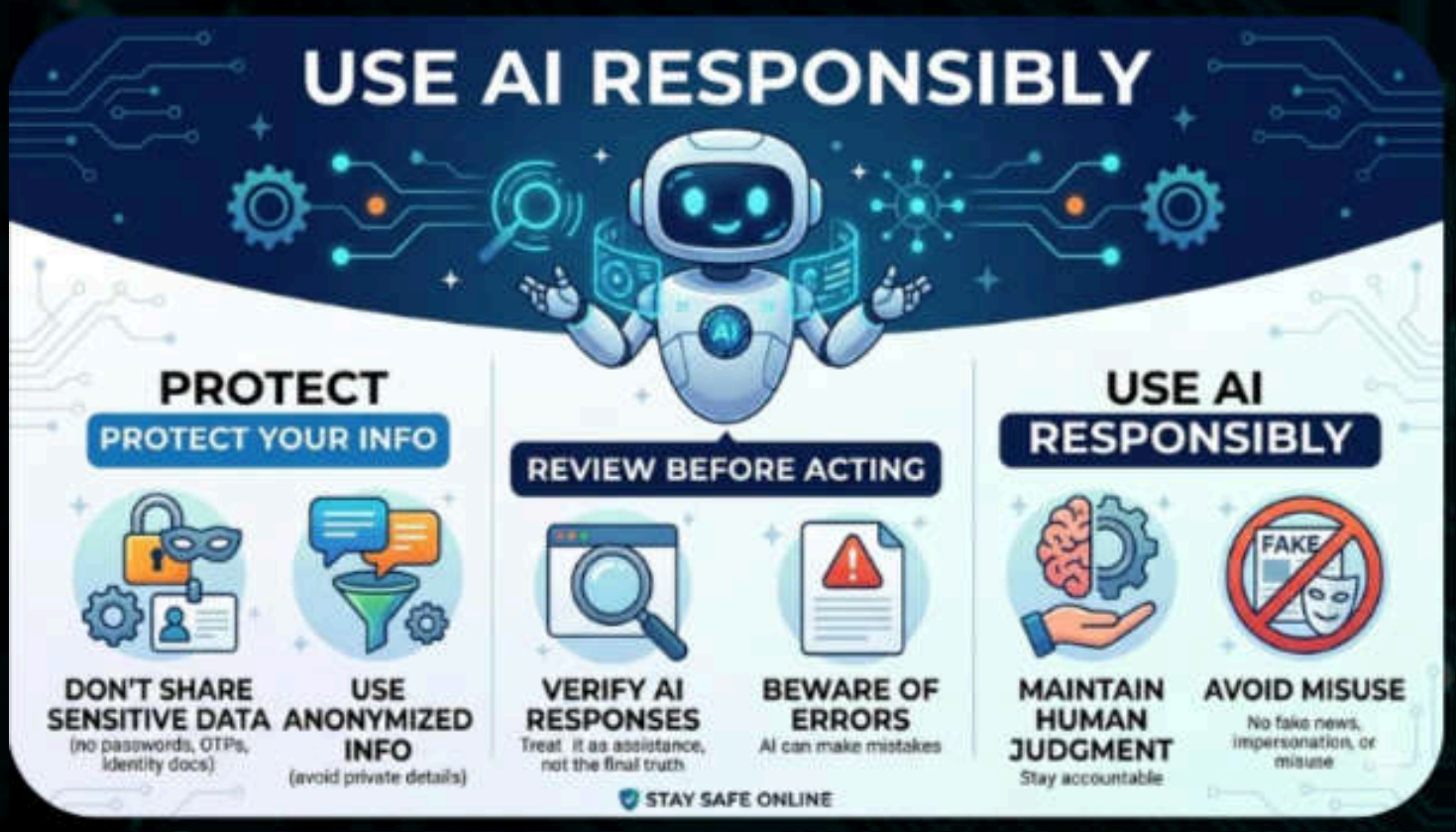
ನಿಮ್ಮ ಸಾಧನಗಳು ಮತ್ತು ಖಾತೆಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ

- ಎಲ್ಲಾ ಸಾಧನಗಳಲ್ಲಿ ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಅಥವಾ ಸ್ಕ್ರೀನ್ ಲಾಕ್‌ಗಳನ್ನು ಬಳಸಿ.
- ಲಭ್ಯವಿದ್ದಾಗಲೆಲ್ಲಾ ಸಾಧನ ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಮತ್ತು ಭದ್ರತಾ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.
- ಅನಗತ್ಯ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಮತ್ತು ಅನುಮತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ತೆಗೆದುಹಾಕಿ.

ನಿಮ್ಮ ನೆಟ್‌ವರ್ಕ್ ಸಂಪರ್ಕವನ್ನು ರಕ್ಷಿಸಿ

- ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್‌ನೊಂದಿಗೆ ನಿಮ್ಮ ವೈ-ಫೈ ಅನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ ಮತ್ತು ಡೀಫಾಲ್ಟ್ ರೂಟರ್ ರುಜುವಾತುಗಳನ್ನು ಬದಲಾಯಿಸಿ.
- ನವೀಕರಿಸಿದ ರೂಟರ್ ಫರ್ಮ್‌ವೇರ್ ಮತ್ತು ಸುರಕ್ಷಿತ ನೆಟ್‌ವರ್ಕ್ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಬಳಸಿ.
- ಅಸುರಕ್ಷಿತ ನೆಟ್‌ವರ್ಕ್‌ಗಳ ಮೂಲಕ ಸೂಕ್ಷ್ಮ ಖಾತೆಗಳನ್ನು ಪ್ರವೇಶಿಸುವುದನ್ನು ಅಥವಾ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ.

AI ಅನ್ನು ಜವಾಬ್ದಾರಿಯುತವಾಗಿ ಬಳಸಿ



ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸಿ

- ಸಾರ್ವಜನಿಕ AI ಪರಿಕರಗಳು ಅಥವಾ ಅಪರಿಚಿತ ಆನ್‌ಲೈನ್ ಸೇವೆಗಳಲ್ಲಿ ವೈಯಕ್ತಿಕ, ಹಣಕಾಸು, ಆರೋಗ್ಯ, ಅಧಿಕೃತ ಅಥವಾ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ನಮೂದಿಸಬೇಡಿ.
- ಪಾಸ್‌ವರ್ಡ್‌ಗಳು, ಒಟಿಪಿಗಳು, ಖಾತೆ ಸಂಖ್ಯೆಗಳು, ಗುರುತಿನ ದಾಖಲೆಗಳು, ಗ್ರಾಹಕರ ಡೇಟಾ ಅಥವಾ ಖಾಸಗಿ ಸಂಭಾಷಣೆಗಳಂತಹ ಸೂಕ್ಷ್ಮ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಸಹಾಯಕ್ಕಾಗಿ AI ಪರಿಕರಗಳನ್ನು ಕೇಳುವಾಗ ಅನಾಮಧೇಯ ಅಥವಾ ಸಾಮಾನ್ಯ ಮಾಹಿತಿಯನ್ನು ಬಳಸಿ.

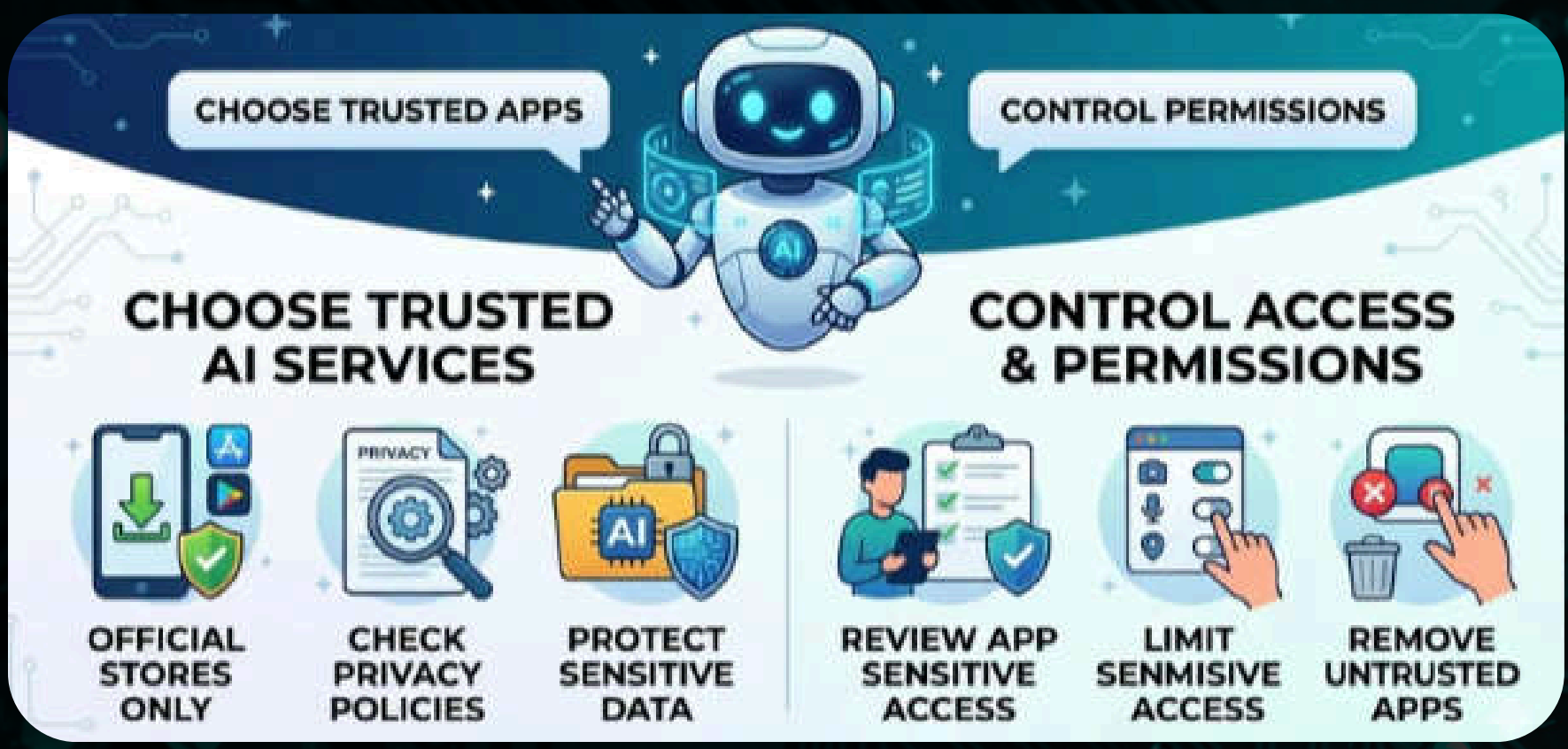
ನೀವು ಹಂಚಿಕೊಳ್ಳುವ ಅಥವಾ ಕಾರ್ಯನಿರ್ವಹಿಸುವ ಮೊದಲು ಪರಿಶೀಲಿಸಿ

- AI-ರಚಿತ ಪ್ರತಿಕ್ರಿಯೆಗಳನ್ನು ಸತ್ಯದ ಅಂತಿಮ ಮೂಲವಾಗಿ ಪರಿಗಣಿಸದೆ, ಸಹಾಯವಾಗಿ ಪರಿಗಣಿಸಿ.
- ಆರ್ಥಿಕ, ಕಾನೂನು, ವೃತ್ತಿಪರ ಅಥವಾ ವೈಯಕ್ತಿಕ ನಿರ್ಧಾರಗಳಿಗಾಗಿ ಪ್ರಮುಖ ಮಾಹಿತಿಯನ್ನು ಬಳಸುವ ಮೊದಲು ಅದನ್ನು ಪರಿಶೀಲಿಸಿ.
- AI ಪರಿಕರಗಳು ತಪ್ಪಾದ, ಅಪೂರ್ಣ ಅಥವಾ ದಾರಿತಪ್ಪಿಸುವ ಮಾಹಿತಿಯನ್ನು ನೀಡಬಹುದು ಎಂಬುದನ್ನು ನೆನಪಿನಲ್ಲಿಡಿ.

AI ಪರಿಕರಗಳನ್ನು ಜವಾಬ್ದಾರಿಯುತವಾಗಿ ಬಳಸಿ

- ನಿಮ್ಮ ಕೆಲಸ ಮತ್ತು ಕಲಿಕೆಯನ್ನು ಬೆಂಬಲಿಸಲು AI ಬಳಸಿ, ಆದರೆ ಮಾನವ ತೀರ್ಪು ಮತ್ತು ಹೊಣೆಗಾರಿಕೆಯನ್ನು ಕಾಪಾಡಿಕೊಳ್ಳಿ.
- ಸುಳ್ಳು ಮಾಹಿತಿಯನ್ನು ರಚಿಸಲು ಅಥವಾ ಹರಡಲು, ಇತರರಂತೆ ನಟಿಸಲು ಅಥವಾ ಯಾರೊಬ್ಬರ ವೈಯಕ್ತಿಕ ಡೇಟಾವನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳಲು AI ಅನ್ನು ಬಳಸಬೇಡಿ.

ವಿಶ್ವಾಸಾರ್ಹ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಆರಿಸಿ



ಅಪ್ಲಿಕೇಶನ್ ಪ್ರವೇಶ ಮತ್ತು ಅನುಮತಿಗಳನ್ನು ನಿಯಂತ್ರಿಸಿ

- AI ಅರ್ಜಿಗಳು ಮತ್ತು ಡಿಜಿಟಲ್ ಸಹಾಯಕರಿಗೆ ನೀಡಲಾದ ಅನುಮತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಕ್ಯಾಮೆರಾ, ಮೈಕ್ರೊಫೋನ್, ಸಂಪರ್ಕಗಳು ಅಥವಾ ಸ್ಥಳದಂತಹ ವೈಶಿಷ್ಟ್ಯಗಳಿಗೆ ಅಗತ್ಯವಿದ್ದಾಗ ಮಾತ್ರ ಪ್ರವೇಶವನ್ನು ಅನುಮತಿಸಿ.
- ಅನಗತ್ಯ ಅನುಮತಿಗಳನ್ನು ತೆಗೆದುಹಾಕಿ ಮತ್ತು ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ಮೂಲಗಳಿಂದ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಅಸ್ಥಾಪಿಸಿ.

ವಿಶ್ವಾಸಾರ್ಹ AI ಸೇವೆಗಳನ್ನು ಆರಿಸಿ

- ಪ್ರತಿಷ್ಠಿತ ಪೂರೈಕೆದಾರರಿಂದ *AI* ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿ ಮತ್ತು ಅವುಗಳನ್ನು ಅಧಿಕೃತ ಅಪ್ಲಿಕೇಶನ್ ಸ್ಟೋರ್‌ಗಳಿಂದ ಮಾತ್ರ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ.
- *AI* ಸೇವೆಗಳನ್ನು ಬಳಸುವ ಮೊದಲು ಗೌಪ್ಯತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳು, ಬಳಕೆಯ ನಿಯಮಗಳು ಮತ್ತು ಡೇಟಾ ನಿರ್ವಹಣಾ ಅಭ್ಯಾಸಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಭದ್ರತಾ ನಿಯಂತ್ರಣಗಳನ್ನು ಪರಿಶೀಲಿಸದ ಹೊರತು *AI* ಪರಿಕರಗಳನ್ನು ಸೂಕ್ಷ್ಮ ಖಾತೆಗಳು ಅಥವಾ ಫೈಲ್‌ಗಳಿಗೆ ಸಂಪರ್ಕಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ.

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