

ಮಾಜಿ ಸೈನಿಕರು ಮತ್ತು ವೀರ್ ನಾರಿಸ್ ಅವರಿಂದ ಸೈಬರ್ ಭದ್ರತಾ ವಂಚನೆಗಳ ನಿರ್ವಹಣೆ.

ಕಮಾಂಡರ್ ಪಿ ರಾಜಗೋಪಾಲ್ ತಂಪಿ IN (R)

- AI ಮತ್ತು ದೊಡ್ಡ ಭಾಷಾ ಮಾದರಿಗಳು
- ಸಾಫ್ಟ್‌ವೇರ್ ಮತ್ತು AI ನಡುವಿನ ವ್ಯತ್ಯಾಸವೇನು?
- ಏಜೆಂಟ್ ಎಂದರೇನು?
- ಒಬ್ಬ ಏಜೆಂಟ್ ಎಲ್‌ಎಲ್‌ಎಂಗಿಂತ ಹೇಗೆ ಭಿನ್ನ?
- ಕೆಲವು ಪ್ರಮುಖ AI ಪ್ರಯೋಜನಗಳು ಯಾವುವು?
    - ವೈಜ್ಞಾನಿಕ ಆವಿಷ್ಕಾರಗಳಲ್ಲಿ ತ್ವರಿತ ಪ್ರಗತಿ
    - ಹೊಸ ವಸ್ತುಗಳು, ಹೊಸ ಅಣುಗಳು, ಉತ್ಪಾದಕತೆಯ ಪ್ರಯೋಜನಗಳು
    - ಹವಾಮಾನ ಮುನ್ಸೂಚನೆಗಳು
    - ಸಾಫ್ಟ್‌ವೇರ್ ಕೋಡಿಂಗ್
    - ರೋಬೋಟ್‌ಗಳು ಮತ್ತು ಯಾಂತ್ರೀಕರಣ
- AI ನ ಪ್ರಮುಖ ಅಪಾಯಗಳು ಯಾವುವು?
    - ವಂಚನೆ, ಅಧಿಕಾರ ದಾಹ ಮತ್ತು ಸ್ವಯಂ ಸಂರಕ್ಷಣೆ
    - ಡೀಪ್‌ಫೇಕ್‌ಗಳು
    - ನಿಯಂತ್ರಣ ನಷ್ಟ
    - ಪುನರಾವರ್ತಿತ ಸ್ವಯಂ-ಸುಧಾರಣೆ (RSI)
    - ಸ್ವಯಂ ಪ್ರತಿಕೃತಿ

• ಹಗ್ಗಿಂಗ್‌ಫೇಸ್ ಘಟನೆ, ಆಂಥ್ರಾಪಿಕ್ ಐಒಟಿ ಭವಿಷ್ಯ
• ಫ್ರಾನ್ಸ್‌ನಲ್ಲಿ ಶೈತ್ಯೀಕರಣ ಸ್ಥಾವರಗಳನ್ನು ಹ್ಯಾಕ್ ಮಾಡುವುದು - ಅಕ್ಟೋಬರ್ 2026 ರ ಮಧ್ಯದಲ್ಲಿ
• ಸರ್ಕಾರಿ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತಿಲ್ಲ (PHP ದೋಷಗಳು) – 21ಸೇಂಟ್ ಅಕ್ಟೋಬರ್ 2026
• ಅಂತರ್ಗತವಾಗಿ ದ್ವಿ-ಬಳಕೆಯ ತಂತ್ರಜ್ಞಾನ - ಸ್ವಾಯತ್ತ ಶಸ್ತ್ರಾಸ್ತ್ರ, CBRN ಮತ್ತು ಯುದ್ಧಕಾಲದ ಬಳಕೆಯಲ್ಲಿ ದೊಡ್ಡ ಅಪಾಯಗಳು.
• AI ಸೈಬರ್ ಭದ್ರತೆಯ ಸಕ್ರಿಯಗೊಳಿಸುವ ಮತ್ತು ರಕ್ಷಕ.
• ನಮ್ಮ ಮೆದುಳುಗಳಿಗಿಂತ ಹೆಚ್ಚು ಶಕ್ತಿಶಾಲಿ ಕಂಪ್ಯೂಟಿಂಗ್ ಎಂಜಿನ್ (ವೇಗವಾದ ಮತ್ತು ಅನಿಯಮಿತ ಸಂಪನ್ಮೂಲಗಳು). ನಾವುಅವುಗಳನ್ನು ಹಿಡಿಯಲು ಅಥವಾ ಅರ್ಥಮಾಡಿಕೊಳ್ಳಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲ.
• ಏಜೆಂಟರು 24x7 ರನ್ ಮಾಡುತ್ತಾರೆ ಮತ್ತು ನೂರಾರು ಸಂಖ್ಯೆಯಲ್ಲಿ ಬ್ರೂಟ್ ಫೋರ್ಸ್ ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಮಾಡಬಹುದು, ಸಾಫ್ಟ್‌ವೇರ್‌ನಲ್ಲಿ ದೋಷಗಳನ್ನು ಕಂಡುಹಿಡಿಯಬಹುದು. • ಪವರ್ ಆನ್ ತರಬೇತಿಯ ನಂತರ AI ವ್ಯವಸ್ಥೆಗಳು ಪೂರ್ಣ ಜ್ಞಾನದಿಂದ ಕಾರ್ಯನಿರ್ವಹಿಸಬಹುದು, ಎಲ್ಲಿ ಬೇಕಾದರೂ ವಲಸೆ ಹೋಗಬಹುದು ಮತ್ತು ತಡವಾಗುವವರೆಗೆ ನಾವು ಅವುಗಳನ್ನು ಪತ್ತೆಹಚ್ಚಲು ಸಾಧ್ಯವಾಗದಿರಬಹುದು.
• ಇಂಟರ್ನೆಟ್ ಅನ್ನು AI ಸ್ವಾಧೀನಪಡಿಸಿಕೊಳ್ಳುವುದರಿಂದ ಮತ್ತು ಮೂಲಸೌಕರ್ಯವನ್ನು ಹ್ಯಾಕ್

ಮಾಡುವುದರಿಂದ ಅಲ್ಪಾವಧಿಯ ಹಾನಿ ಉಂಟಾಗಬಹುದು.ವ್ಯವಸ್ಥೆಗಳು ಮತ್ತು ಉಪಯುಕ್ತತೆಗಳು.

28/10/2026 ಪಿ ರಾಜಗೋಪಾಲ್ ತಂಪಿ 3

• ಸಂದೇಹ ಮತ್ತು ಕಡಿಮೆ ಮಟ್ಟದ ನಂಬಿಕೆಯೊಂದಿಗೆ AI ವ್ಯವಸ್ಥೆಗಳನ್ನು ಸಂಪರ್ಕಿಸಿ:

• ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಿಂದ ಬಂದದ್ದನ್ನು ನಂಬಬೇಡಿ.

• ಸಿರಿ ಅಥವಾ ಅದಕ್ಕೆ ಸಮಾನವಾದ ಸಂಭಾಷಣೆ ಮೇಲ್ವಿಚಾರಣೆ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ.

• ನೀವು Chat GPT ಅಥವಾ Claude ನಂತಹ AI ಪರಿಕರಗಳನ್ನು ಬಳಸುತ್ತಿದ್ದರೆ "ಎಲ್ಲರಿಗೂ ಮಾದರಿಯನ್ನು ಸುಧಾರಿಸಿ" ಆಯ್ಕೆ ಮತ್ತು ಸ್ಥಳ ಆಯ್ಕೆಯನ್ನು ಆಫ್ ಮಾಡಿ.

• ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಡೇಟಾವನ್ನು ಅದು ಹೇಗೆ ನಿರ್ವಹಿಸುತ್ತದೆ ಎಂಬುದನ್ನು ನೀವು ವಿಶ್ವಾಸಾರ್ಹವಾಗಿ ಪರಿಶೀಲಿಸಬಹುದಾದರೆ ಹೊರತುಪಡಿಸಿ, ವಾಣಿಜ್ಯಿಕವಾಗಿ ಲಭ್ಯವಿರುವ AI ಏಜೆಂಟ್‌ಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ. ನಿಮಗೆ ಸಂಪೂರ್ಣವಾಗಿ ಅಗತ್ಯವಿದ್ದರೆ ಮಾತ್ರ ಕಡಿಮೆ ಅಪಾಯದ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಗೆ ಅದನ್ನು ಬಳಸಿ.

• ನಿಮ್ಮ ಆಲೋಚನೆಗಳು ಮತ್ತು ಉದ್ದೇಶಗಳನ್ನು ಯಾವುದೇ AI ಏಜೆಂಟ್‌ಗೆ, ವಿಶೇಷವಾಗಿ ನಿಮ್ಮ ಡೈರಿ ಅಥವಾ ಖಾಸಗಿ ಜರ್ನಲ್‌ಗೆ ಹಸ್ತಾಂತರಿಸಬೇಡಿ • ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಗಳು, ಬಿಲ್, ಪಾವತಿಗಳು, ಇತರ ಹಣಕಾಸು ವಿಷಯಗಳು ಮತ್ತು ವಹಿವಾಟುಗಳಲ್ಲಿ ವಹಿವಾಟುಗಳನ್ನು ಸ್ವಯಂಚಾಲಿತಗೊಳಿಸಲು AI ಏಜೆಂಟ್‌ಗಳಿಗೆ ಪ್ರವೇಶವನ್ನು ನೀಡಬೇಡಿ.

• ನಿಮ್ಮ ಫೋಲ್ಡರ್‌ಗಳು, ಇಮೇಲ್ ಸೇವೆಗಳು ಮತ್ತು ಕಾರ್ಡ್ ಮಾಹಿತಿಗೆ ಪ್ರವೇಶವನ್ನು ಒದಗಿಸಬೇಡಿ.

• ಯಾವಾಗಲೂ "ನೀವೇ ಯೋಚಿಸಿ", ನಿಮಗಾಗಿ ಯೋಚಿಸುವಂತೆ AI ಅನ್ನು ಕೇಳಬೇಡಿ.

• ನಿಮ್ಮ ಆಲೋಚನಾ ಪ್ರಕ್ರಿಯೆಯನ್ನು AI ವ್ಯವಸ್ಥೆಗಳಲ್ಲ, ವಿಶ್ವಾಸಾರ್ಹ ಸ್ನೇಹಿತನೊಂದಿಗೆ ಪರಿಶೀಲಿಸಿ.

• ಗೌಪ್ಯತಾ ನಿಯಂತ್ರಣಗಳನ್ನು ಪರಿಣಾಮಕಾರಿಯಾಗಿ ಬಳಸಿ, ಅನಿವಾರ್ಯ ಅಗತ್ಯವಿದ್ದಾಗ ಮಾತ್ರ ವೈದ್ಯಕೀಯ ಮತ್ತು ಹಣಕಾಸು

ದಾಖಲೆಗಳನ್ನು ಅಪ್‌ಲೋಡ್ ಮಾಡಿ.28/10/2026 ಪಿ ರಾಜಗೋಪಾಲ್ ತಂಪಿ 4

• ಕರೆ ಮಾಡುವವರ ಧ್ವನಿ ಕುಟುಂಬದ ಸದಸ್ಯರಂತೆಯೇ ಇದೆ ಎಂಬ ಕಾರಣಕ್ಕೆ ಅವರನ್ನು ಎಂದಿಗೂ ನಂಬಬೇಡಿ. • ಯಾರಾದರೂ ತುರ್ತು ಪರಿಸ್ಥಿತಿಯಲ್ಲಿ ಸಂಬಂಧಿಕರೆಂದು ಹೇಳಿಕೊಂಡು ಹಣ ಕೇಳಿದರೆ, ಸಂಪರ್ಕ ಕಡಿತಗೊಳಿಸಿ ಮತ್ತು ಆ ವ್ಯಕ್ತಿಗೆ ಅವರು ಹಿಂದೆ ಉಳಿಸಿದ ಸಂಖ್ಯೆಗೆ ಮತ್ತೆ ಕರೆ ಮಾಡಿ.
• ತುರ್ತು ಪರಿಸ್ಥಿತಿಗಳಿಗಾಗಿ ಖಾಸಗಿ ಕುಟುಂಬ ಪರಿಶೀಲನೆ ಪದಗುಚ್ಛವನ್ನು ಒಪ್ಪಿಕೊಳ್ಳಿ. ಅದನ್ನು ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.ಮಾಧ್ಯಮ.
• ವ್ಯಕ್ತಿಯ ಮುಖವನ್ನು ಗುರುತಿಸಿದ ಮಾತ್ರಕ್ಕೆ ವೀಡಿಯೊ ಕರೆ ನಿಜವಾದದ್ದು ಎಂದು ಭಾವಿಸಬೇಡಿ. • ಹಣ, ಗೌಪ್ಯತೆ ಅಥವಾ ತಕ್ಷಣದ ಕ್ರಮಕ್ಕಾಗಿ ತುರ್ತು ವಿನಂತಿಗಳನ್ನು ಎಚ್ಚರಿಕೆ ಚಿಹ್ನೆಗಳಾಗಿ ಪರಿಗಣಿಸಿ. • ಪೊಲೀಸ್, ಸಿಬಿಐ, ಕಸ್ಟಮ್ಸ್, ನ್ಯಾಯಾಲಯಗಳು ಅಥವಾ ಇತರ ಅಧಿಕಾರಿಗಳುನಿಮ್ಮನ್ನು ಡಿಜಿಟಲ್ ಬಂಧನದಲ್ಲಿರಿಸಿದೆ.
• ಗುರುತಿನ ಪುರಾವೆಯಾಗಿ ಕಾಲರ್ ಐಡಿ, ವಾಟ್ಸಾಪ್ ಪ್ರೊಫೈಲ್ ಛಾಯಾಚಿತ್ರಗಳು ಅಥವಾ ಪ್ರದರ್ಶಿಸಲಾದ

ಸಂಸ್ಥೆಯ ಹೆಸರುಗಳನ್ನು ನಂಬಬೇಡಿ.
• ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಡೇಟಾ ಪ್ರೊಫೈಲ್ ಮತ್ತು ಹೆಜ್ಜೆಗುರುತನ್ನು ಸಾಧ್ಯವಾದಷ್ಟು ಕನಿಷ್ಠಕ್ಕೆ ಇಳಿಸಿ • ಅನುಕರಣೆಯ ಉದಾಹರಣೆ (ನಕಲಿ ವೀಡಿಯೊ ಕರೆ ಅನುಮೋದನೆಯಿಂದಾಗಿ $25 ಮಿಲಿಯನ್ ವರ್ಗಾಯಿಸಲಾಗಿದೆ).

• ಕಾನೂನುಬದ್ಧ ಉದ್ದೇಶವಿಲ್ಲದೆ ಗುರುತಿನ ದಾಖಲೆಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ.
• ಸೂಕ್ತವಾದಲ್ಲಿ, ಗುರುತಿನ ದಾಖಲೆಗಳ ಪ್ರತಿಗಳಿಗೆ ಉದ್ದೇಶ-ನಿರ್ದಿಷ್ಟ ವಾಟರ್‌ಮಾರ್ಕ್ ಅನ್ನು ಸೇರಿಸಿ.• WhatsApp, Facebook, Instagram ಮತ್ತು ಇತರ ಸಾಮಾಜಿಕ ವೇದಿಕೆಗಳಲ್ಲಿ ಗೌಪ್ಯತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.• ಸಂದೇಶ ಕಳುಹಿಸುವ ಗುಂಪುಗಳಿಗೆ ನಿಮ್ಮನ್ನು ಯಾರು ಸೇರಿಸಬಹುದು ಎಂಬುದನ್ನು ನಿರ್ಬಂಧಿಸಿ, ಗುಂಪು ಸದಸ್ಯತ್ವಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಲು ಪ್ರಯತ್ನಿಸಿ. • ಪ್ರಾಯೋಗಿಕವಾಗಿ ಸಾರ್ವಜನಿಕವಾಗಿ ಲಭ್ಯವಿರುವ ಧ್ವನಿ ರೆಕಾರ್ಡಿಂಗ್‌ಗಳು ಮತ್ತು ವೈಯಕ್ತಿಕ ವೀಡಿಯೊಗಳನ್ನು ಮಿತಿಗೊಳಿಸಿ. • ವಿವರವಾದ ಕುಟುಂಬ ಸಂಬಂಧಗಳು, ದಿನಚರಿಗಳು ಮತ್ತು ಆರ್ಥಿಕ ಸಂದರ್ಭಗಳನ್ನು ಪ್ರಕಟಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ. • ಸಾರ್ವಜನಿಕ ಆನ್‌ಲೈನ್ ಪ್ರೊಫೈಲ್‌ಗಳಿಂದ ಅನಗತ್ಯ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ತೆಗೆದುಹಾಕಿ.• UIDAI ನ ಅಧಿಕೃತ ಆಧಾರ್ ದೃಢೀಕರಣ-ಇತಿಹಾಸ ಮತ್ತು ಬಯೋಮೆಟ್ರಿಕ್-ಲಾಕಿಂಗ್ ಸೌಲಭ್ಯಗಳನ್ನು ಬಳಸಿ, ಅಲ್ಲಿಸೂಕ್ತ.

• ಲಭ್ಯವಿರುವಲ್ಲಿ ಅಧಿಕೃತ ಸರ್ಕಾರಿ ದೂರಸಂಪರ್ಕ ಸೇವೆಗಳ ಮೂಲಕ ನಿಮ್ಮ ಮೊಬೈಲ್ ಸಂಪರ್ಕಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.

• ಕಡಿಮೆ ವಿಶ್ವಾಸಾರ್ಹ ಚಂದಾದಾರಿಕೆಗಳು ಮತ್ತು ನೋಂದಣಿಗಳಿಗಾಗಿ ಪ್ರತ್ಯೇಕ ಇಮೇಲ್ ವಿಳಾಸವನ್ನು ಬಳಸಿ.• ಕ್ಲೌಡ್-ಹಂಚಿಕೆ ಲಿಂಕ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಇನ್ನು ಮುಂದೆ ಅಗತ್ಯವಿಲ್ಲದಿದ್ದಾಗ ಸಾರ್ವಜನಿಕ ಪ್ರವೇಶವನ್ನು ತೆಗೆದುಹಾಕಿ.

• ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ಪಿನ್, UPI ಪಿನ್, ATM ಪಿನ್, CVV, ಪಾಸ್‌ವರ್ಡ್, ಜನ್ಮ ದಿನಾಂಕ ಅಥವಾ OTP ಅನ್ನು ಎಂದಿಗೂ ಬಹಿರಂಗಪಡಿಸಬೇಡಿ.• ನೆನಪಿಡಿ: ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ನೀವು UPI ಪಿನ್ ಅನ್ನು ನಮೂದಿಸುವ ಅಗತ್ಯವಿಲ್ಲ. ಅದನ್ನು ನಮೂದಿಸುವುದರಿಂದ ಸಾಮಾನ್ಯವಾಗಿ ಪಾವತಿಯನ್ನು ಅಧಿಕೃತಗೊಳಿಸುತ್ತದೆ.• ಹಣ ಸ್ವೀಕರಿಸಲು ಅಪರಿಚಿತರು ಕಳುಹಿಸಿದ QR ಕೋಡ್ ಅನ್ನು ಎಂದಿಗೂ ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ.

• ಅನಿರೀಕ್ಷಿತ UPI ಸಂಗ್ರಹ ವಿನಂತಿಯನ್ನು ಎಂದಿಗೂ ಅನುಮೋದಿಸಬೇಡಿ.

• AI ಬಳಸಿಕೊಂಡು ಖಾತರಿಪಡಿಸಿದ ಹೆಚ್ಚಿನ ಆದಾಯ ಅಥವಾ ಅಸಾಧಾರಣ ಲಾಭದ ಭರವಸೆ ನೀಡುವ ಹೂಡಿಕೆ ಯೋಜನೆಗಳನ್ನು ನಂಬಬೇಡಿ.• ಏಜೆಂಟ್‌ಗಳು ಮತ್ತು ಅಪರಿಚಿತರು ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ಅರ್ಜಿಯನ್ನು ದೂರದಿಂದಲೇ ನಿರ್ವಹಿಸಲು ಎಂದಿಗೂ ಅನುಮತಿಸಬೇಡಿ.

• ಅಪರಿಚಿತ ಜನರೊಂದಿಗೆ ಬ್ಯಾಂಕ್ ಕಾರ್ಡ್‌ಗಳು, ಚೆಕ್‌ಗಳು ಅಥವಾ ಹಣಕಾಸಿನ ದಾಖಲೆಗಳ ಛಾಯಾಚಿತ್ರಗಳನ್ನು

ಹಂಚಿಕೊಳ್ಳಬೇಡಿ. • ಎಲ್ಲಾ ಪ್ರಮುಖ ಖಾತೆಗಳಲ್ಲಿ ವಹಿವಾಟು ಎಚ್ಚರಿಕೆಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.

• ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅನುಮತಿಸುವ ಸ್ಥಳದಲ್ಲಿ, ನಿಮ್ಮ ಅಗತ್ಯಗಳಿಗೆ ಸೂಕ್ತವಾದ ದೈನಂದಿನ ವರ್ಗಾವಣೆ ಮಿತಿಗಳನ್ನು ಹೊಂದಿಸಿ.

• ಕಾರ್ಡ್‌ಗಳ ಕಾಳಜಿ: ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಸಂಗ್ರಹಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ. ಕಾರ್ಡ್ ವಿವರಗಳ ಸ್ವಯಂಚಾಲಿತ ಭರ್ತಿ ಪ್ರಕ್ರಿಯೆಯನ್ನು ತಪ್ಪಿಸಿ. • ಹೆಚ್ಚಿನ ಮಿತಿಗಳು ಇನ್ನು ಮುಂದೆ ಅಗತ್ಯವಿಲ್ಲದಿದ್ದಾಗ ಕ್ರೆಡಿಟ್-ಕಾರ್ಡ್ ಆನ್‌ಲೈನ್ ವಹಿವಾಟು ಮಿತಿಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಿ. • ಅಗತ್ಯವಿಲ್ಲದಿದ್ದಾಗ ಅಂತರರಾಷ್ಟ್ರೀಯ ಕಾರ್ಡ್ ವಹಿವಾಟುಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ.

• ವಿದೇಶಗಳಿಗೆ ಪ್ರಯಾಣಿಸುವಾಗ ಸಂಪರ್ಕರಹಿತ ವಹಿವಾಟುಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ - ವಿಶೇಷವಾಗಿ ಆಮ್ಸ್ಟರ್‌ಡ್ಯಾಮ್ ಘಟನೆ • ಆಗಾಗ್ಗೆ ಆನ್‌ಲೈನ್/ಯುಪಿಐ ಪಾವತಿಗಳಿಗೆ ಬಳಸುವ ಖಾತೆಗಳಿಂದ ಗಣನೀಯ ಉಳಿತಾಯವನ್ನು ಪ್ರತ್ಯೇಕವಾಗಿ ಇರಿಸಿ.

• ಬ್ಯಾಂಕಿಂಗ್, ಇಮೇಲ್ ಮತ್ತು ಪ್ರಮುಖ ಖಾತೆಗಳಿಗೆ ವಿಭಿನ್ನ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸಿ.
• ಊಹಿಸಲು ಕಷ್ಟಕರವಾದ ಉದ್ದವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಅಥವಾ ಪಾಸ್‌ಫ್ರೇಸ್‌ಗಳನ್ನು ಬಳಸಿ.
• ಲಭ್ಯವಿರುವಲ್ಲೆಲ್ಲಾ ಎರಡು-ಅಂಶ ದೃಢೀಕರಣ ಅಥವಾ FIDO2 ದೃಢೀಕರಣವನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.• ಪಿನ್, ಫಿಂಗರ್‌ಪ್ರಿಂಟ್ ಅಥವಾ ಮುಖ ದೃಢೀಕರಣದೊಂದಿಗೆ ನಿಮ್ಮ ಫೋನ್ ಅನ್ನು ಲಾಕ್ ಮಾಡಿ.
• ನಿಮ್ಮ ಫೋನ್ ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಇತ್ತೀಚಿನ ಬಿಡುಗಡೆಯೊಂದಿಗೆ ನವೀಕರಿಸುತ್ತಿರಿ. • ಅಧಿಕೃತ ಅಪ್ಲಿಕೇಶನ್ ಅಂಗಡಿಗಳಿಂದ ಮಾತ್ರ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ.

• ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಯಿಂದ WhatsApp, SMS ಅಥವಾ ಇಮೇಲ್ ಮೂಲಕ ಕಳುಹಿಸಲಾದ APK ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಸ್ಥಾಪಿಸಬೇಡಿ.

• ಅಪರಿಚಿತರ ಕೋರಿಕೆಯ ಮೇರೆಗೆ ಸ್ಕ್ರೀನ್-ಶೇರಿಂಗ್ ಅಥವಾ ರಿಮೋಟ್-ಆಕ್ಸೆಸ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಸ್ಥಾಪಿಸಬೇಡಿ. • ನಿಮ್ಮ KYC, PAN, ಆಧಾರ್, ಬ್ಯಾಂಕ್ ಖಾತೆ, ವಿದ್ಯುತ್ ಸರಬರಾಜು ಅಥವಾ ವಿತರಣೆಯನ್ನು ನಿರ್ಬಂಧಿಸಲಾಗುತ್ತದೆ ಎಂದು ಹೇಳುವ ಅನಿರೀಕ್ಷಿತ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.

• ಸಂದೇಶಗಳಲ್ಲಿರುವ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವ ಬದಲು ಅಧಿಕೃತ ಬ್ಯಾಂಕಿಂಗ್ ಅಥವಾ ಸೇವಾ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ನೀವೇ ತೆರೆಯಿರಿ.

• ಸಾಧ್ಯವಾದರೆ ಖಾತೆಗಳಿಗಾಗಿ ಬ್ಯಾಕಪ್ ಭದ್ರತಾ ಕೀಲಿಯನ್ನು ನೋಂದಾಯಿಸಿ ಮತ್ತು ಅದನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಸಂಗ್ರಹಿಸಿಡಿ.

• ವೈಯಕ್ತಿಕ, ಕುಟುಂಬ, ಸಂಬಂಧದ ವಿವರಗಳು ಮತ್ತು ಛಾಯಾಚಿತ್ರಗಳನ್ನು ಹಾಕುವುದನ್ನು ತಪ್ಪಿಸಿ.ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ.

• ನಿಮ್ಮ ಪ್ರಯಾಣದ ವಿವರ ಅಥವಾ ದೈನಂದಿನ ದಿನಚರಿಯನ್ನು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಪ್ರಕಟಿಸಬೇಡಿ. • ನಿಮ್ಮ ಇಷ್ಟಗಳು, ಇಷ್ಟವಿಲ್ಲದಿರುವಿಕೆಗಳು, ರಾಜಕೀಯ ಒಲವುಗಳು,

ಹಣಕಾಸಿನ ಖರೀದಿಗಳು ಮತ್ತು ಖಾಸಗಿ ಚಟುವಟಿಕೆಗಳನ್ನು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಬಹಿರಂಗಪಡಿಸಬೇಡಿ.

• ಮನೆಯ ವೈಫೈಗಾಗಿ ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳೊಂದಿಗೆ WPA2 AES ಅಥವಾ WPA 3 ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಬಳಸಿ.

• ನೀವು ಹೋಮ್ ಕ್ಯಾಮೆರಾಗಳು ಮತ್ತು IoT ಸಾಧನಗಳನ್ನು ಬಳಸುತ್ತಿದ್ದರೆ ಡೇಟಾ ನಿಮ್ಮ ಡೇಟಾ ಕಾರ್ಡ್‌ನಲ್ಲಿ ಉಳಿಯುವಂತೆ ನೋಡಿಕೊಳ್ಳಿ. ಅದನ್ನು ಕ್ಲೌಡ್‌ಗೆ ವರ್ಗಾಯಿಸಬೇಡಿ.

• ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಸೋಗು ಹಾಕುವ ಖಾತೆಗಳನ್ನು ನಿರ್ಬಂಧಿಸಿ ಮತ್ತು ವರದಿ

ಮಾಡಿ.28/10/2026 ಪಿ ರಾಜಗೋಪಾಲ್ ತಂಪಿ 9

ಒಳಗೆವಂಚನೆ ನಡೆದಿದ್ದರೆ ಏನು ಮಾಡಬೇಕು?

1. ತಕ್ಷಣ 1930 ಗೆ ಕರೆ ಮಾಡಿ - ಭಾರತದ ರಾಷ್ಟ್ರೀಯ ಸೈಬರ್ ಹಣಕಾಸು ವಂಚನೆ ಸಹಾಯವಾಣಿ.
2. ಘಟನೆಯನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ವರದಿ ಮಾಡಿರಾಷ್ಟ್ರೀಯ ಸೈಬರ್ ಅಪರಾಧ ವರದಿ ಮಾಡುವ ಪೋರ್ಟಲ್

3. ತಕ್ಷಣ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ
4. ಸೂಕ್ತವಾಗಿ ಬಾಧಿತ ಕಾರ್ಡ್‌ಗಳು, ಖಾತೆಗಳು ಅಥವಾ ಪಾವತಿ ಪ್ರವೇಶವನ್ನು ನಿರ್ಬಂಧಿಸಲು ವಿನಂತಿಸಿ.5. ಆರಂಭಿಕ ವರದಿ ಮಾಡುವಿಕೆಯು ಮುಂದಿನ ವರ್ಗಾವಣೆಗಳನ್ನು ನಿಲ್ಲಿಸುವ ಅವಕಾಶವನ್ನು ಸುಧಾರಿಸುತ್ತದೆ, ಆದಾಗ್ಯೂ ಚೇತರಿಕೆ ಖಾತರಿಪಡಿಸುವುದಿಲ್ಲ.ಈ ಹಂತಗಳನ್ನು ಸಹ ತೆಗೆದುಕೊಳ್ಳಿ:
1. ಶಂಕಿತ ವಂಚಕನೊಂದಿಗೆ ಸಂವಹನ ನಡೆಸುವುದನ್ನು ನಿಲ್ಲಿಸಿ.
2. ರಿಮೋಟ್-ಆಕ್ಸೆಸ್ ಸೆಷನ್‌ಗಳನ್ನು ಸಂಪರ್ಕ ಕಡಿತಗೊಳಿಸಿ ಮತ್ತು ಅನಧಿಕೃತ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ತೆಗೆದುಹಾಕಲು ಸಹಾಯವನ್ನು ಪಡೆಯಿರಿ. 3. ವಿಶ್ವಾಸಾರ್ಹ ಸಾಧನವನ್ನು ಬಳಸಿಕೊಂಡು ರಾಜಿ ಮಾಡಿಕೊಂಡ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬದಲಾಯಿಸಿ.
4. ಅನುಮಾನಾಸ್ಪದ ಲಾಗಿನ್ ಅವಧಿಗಳನ್ನು ರದ್ದುಗೊಳಿಸಿ ಮತ್ತು ಅಗತ್ಯವಿದ್ದಲ್ಲಿ ದೃಢೀಕರಣ ವಿಧಾನಗಳನ್ನು ಮರುಹೊಂದಿಸಿ.5. ಸಂದೇಶಗಳು, ಸ್ಕ್ರೀನ್‌ಶಾಟ್‌ಗಳು, ಫೋನ್ ಸಂಖ್ಯೆಗಳು, ವಹಿವಾಟು ಉಲ್ಲೇಖಗಳು ಮತ್ತು ಇತರ ಪುರಾವೆಗಳನ್ನು ಸಂರಕ್ಷಿಸಿ. 6. ನಕಲಿ ಪ್ರೊಫೈಲ್‌ಗಳು, ಡೀಪ್‌ಫೇಕ್‌ಗಳು ಮತ್ತು ಅನುಕರಣೆಯ ವಿಷಯವನ್ನು ಸಂಬಂಧಿತ ವೇದಿಕೆಗಳು ಮತ್ತು ಅಧಿಕಾರಿಗಳಿಗೆ ವರದಿ ಮಾಡಿ. 7. ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಮೋಸದ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸಲು ಬಳಸಿದ್ದರೆ ಪ್ರಭಾವಿತ ಸಂಪರ್ಕಗಳಿಗೆ ಎಚ್ಚರಿಕೆ ನೀಡಿ.

1. ಸ್ವತಂತ್ರ ಪರಿಶೀಲನೆಯಿಲ್ಲದೆ ಪರಿಚಿತ ಧ್ವನಿ ಅಥವಾ ಮುಖವನ್ನು ಎಂದಿಗೂ ನಂಬಬೇಡಿ.

2. OTP, PIN, ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಬ್ಯಾಂಕಿಂಗ್ ರುಜುವಾತುಗಳನ್ನು ಎಂದಿಗೂ ಬಹಿರಂಗಪಡಿಸಬೇಡಿ.

3. ಬೆದರಿಕೆ, ತುರ್ತು ಅಥವಾ ಗೌಪ್ಯತೆಯ ಕಾರಣದಿಂದ ಎಂದಿಗೂ ಹಣವನ್ನು ವರ್ಗಾಯಿಸಬೇಡಿ.

4. ಡಿಜಿಟಲ್ ಬಂಧನ ಅಥವಾ ಪೊಲೀಸ್ ಸುರಕ್ಷಿತ ಖಾತೆಗಳ ಹಕ್ಕುಗಳನ್ನು ಎಂದಿಗೂ ನಂಬಬೇಡಿ.

5. ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ಎಂದಿಗೂ QR ಕೋಡ್ ಅನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ ಅಥವಾ UPI ಪಿನ್ ಅನ್ನು ನಮೂದಿಸಬೇಡಿ.

6. ಅಪರಿಚಿತರ ಕೋರಿಕೆಯ ಮೇರೆಗೆ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಎಂದಿಗೂ ಸ್ಥಾಪಿಸಬೇಡಿ ಅಥವಾ ನಿಮ್ಮ ಪರದೆಯನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

7. ಅನಿರೀಕ್ಷಿತ ಲಿಂಕ್‌ಗಳು, ಹೂಡಿಕೆ ಕೊಡುಗೆಗಳು ಅಥವಾ ಪಿಂಚಣಿ ಸಂಬಂಧಿತ ಸಂದೇಶಗಳನ್ನು ಎಂದಿಗೂ ನಂಬಬೇಡಿ. 8. ಫೋನ್‌ಗಳನ್ನು ನವೀಕರಿಸಿ ಮತ್ತು ಬಲವಾದ ಖಾತೆ ದೃಢೀಕರಣವನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.

9. ಅಸಾಮಾನ್ಯ ಹಣಕಾಸಿನ ನಿರ್ಧಾರಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳುವ ಮೊದಲು ವಿಶ್ವಾಸಾರ್ಹ ವ್ಯಕ್ತಿಯನ್ನು ಸಂಪರ್ಕಿಸಿ. 10. ವಂಚನೆ ಸಂಭವಿಸಿದಲ್ಲಿ, ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ ಮತ್ತು ತಕ್ಷಣವೇ 1930 ಗೆ ಕರೆ ಮಾಡಿ.

11. ನೆನಪಿಡಬೇಕಾದ ಏಕೈಕ ಅತ್ಯಂತ ಪರಿಣಾಮಕಾರಿ ತತ್ವವೆಂದರೆ:

12. ಯಾವುದೇ ಧ್ವನಿ, ಮುಖ, ಸಂದೇಶ ಅಥವಾ ವೀಡಿಯೊ ನಿಜವಾದದ್ದು ಎಂದು ಮಾತ್ರ ನಂಬಬೇಡಿ. ಕ್ರಮ ಕೈಗೊಳ್ಳುವ ಮೊದಲು ಗುರುತು ಮತ್ತು ವಿನಂತಿಯನ್ನು ಸ್ವತಂತ್ರವಾಗಿ ಪರಿಶೀಲಿಸಿ.

ಕ್ಯಾಲೆಂಡರ್	ಪ್ರತಿ ಬಾರಿ ಕೇಳಿ
ಆರೋಗ್ಯ ದತ್ತಾಂಶ	ಇಲ್ಲ
ಫೋಟೋಗಳು ಮತ್ತು ವೀಡಿಯೊಗಳು	ಇಲ್ಲ
ದೈಹಿಕ ಚಟುವಟಿಕೆ	ಇಲ್ಲ
ಅಧಿಸೂಚನೆಗಳು	ಇಲ್ಲ
ಬ್ಲೂಟೂತ್	ಬಳಸುವಾಗ ಮಾತ್ರ
AI ಅಪ್ಲಿಕೇಶನ್‌ಗಳು	ತರಬೇತಿಗಾಗಿ ಡೇಟಾವನ

ಮೊಬೈಲ್ ಫೋನ್ ಭದ್ರ	
ಸೆಟ್ಟಿಂಗ್‌ಗಳು	ಶಿಫಾರಸು ಮಾಡಲಾದ ಸ
ಸ್ಥಳ	ಅಪ್ಲಿಕೇಶನ್ ಬಳಸುವಾಗ
ಕ್ಯಾಮೆರಾ	ಅಪ್ಲಿಕೇಶನ್ ಬಳಸುವಾಗ
ಮೈಕ್ರೋಫೋನ್	ಪ್ರತಿ ಬಾರಿ ಕೇಳಿ
ಸಂಪರ್ಕಗಳು ಮತ್ತು SMS	ಪ್ರತಿ ಬಾರಿ ಕೇಳಿ

ಪಿ ರಾಜಗೋಪಾಲ್ ತಂಪಿ
28/10/2026 12

ಅವಕಾಶ ಮತ್ತು ಸಿದ್ಧತೆ ಸಿಗುವ ಸ್ಥಳವೇ ಅದೃಷ್ಟ.

AIP ಸಂಶೋಧನಾ ವೆಬ್‌ಸೈಟ್ HTTPS:AIPATHFINDER.ORG

ಅನ್ವಯಿಕ ಮಾನವಕೇಂದ್ರಿತ AI –HTTPS://www.amazon.com/dp/B0CYXHYPHC

ನಿಮ್ಮ ಬುದ್ಧಿಶಕ್ತಿಯನ್ನು ಹೆಚ್ಚಿಸಿಕೊಳ್ಳಿ -https://www.amazon.in/dp/B0D3WZXY99

ಧನ್ಯವಾದಗಳು!