OPTIV

DSCI
PROMOTING DATA PROTECTION









ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸುರಕ್ಷಿತವಾಗಿರಲು

ಒಂದು ಸರಳ ಮಾರ್ಗದರ್ಶಿ










Meri Digital Suraksha

ಮಾರ್ಗದರ್ಶಿ ಬಗ್ಗೆ

ಈ ಸುರಕ್ಷತಾ ಮಾರ್ಗದರ್ಶಿಯನ್ನು, ಆಪ್ಟಿವ್ ಸಹಯೋಗದೊಂದಿಗೆ ಡಿಎಸ್‌ಸಿಐ ಕೈಗೊಂಡಿರುವ 'ನನ್ನ ಡಿಜಿಟಲ್ ಸುರಕ್ಷೆ' ಎಂಬ ಸೈಬರ್ ಭದ್ರತಾ ಜಾಗೃತಿ ಉಪಕ್ರಮದ ಭಾಗವಾಗಿ ರಚಿಸಲಾಗಿದೆ.

ಇದು ಡಿಜಿಟಲ್ ಪಾವತಿಗಳು ಮತ್ತು ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್ ಸುರಕ್ಷತೆ, ಇಮೇಲ್ ಹಾಗೂ ಆ್ಯಪ್ ಸುರಕ್ಷತೆ, ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳ ಸುರಕ್ಷತೆ, ಗೌಪ್ಯತೆ ರಕ್ಷಣೆ, ಡಿಜಿಟಲ್ ಕ್ಷೇಮ ಮತ್ತು ಸೈಬರ್ ಅಪರಾಧ ಪರಿಹಾರದಂತಹ ಪ್ರಮುಖ ವಿಷಯಗಳನ್ನು ಒಂದೇ ಪ್ರಾಯೋಗಿಕ ಮಾರ್ಗದರ್ಶಿಯಲ್ಲಿ ಒಗ್ಗೂಡಿಸುತ್ತದೆ.

ಈ ಮಾರ್ಗದರ್ಶಿಯು ಉತ್ತಮ ಕಾರ್ಯವಿಧಾನಗಳು ಹಾಗೂ ಸೈಬರ್ ನೈರ್ಮಲ್ಯದ (ಹೈಜೀನ್) ಅಭ್ಯಾಸಗಳನ್ನು ವಿವರಿಸುತ್ತದೆ. ಜೊತೆಗೆ, ಪ್ರಚಲಿತದಲ್ಲಿರುವ ಸೈಬರ್ ವಂಚನೆಗಳು ಮತ್ತು ಸಂಬಂಧಿತ ಪರಿಭಾಷೆಗಳ ಬಗ್ಗೆ ಅರಿವು ಮೂಡಿಸುತ್ತದೆ. ಈ ಮೂಲಕ, ನೀವು ಡಿಜಿಟಲ್ ಜಗತ್ತಿನಲ್ಲಿ ಹೆಚ್ಚು ಆತ್ಮವಿಶ್ವಾಸದಿಂದ ಹಾಗೂ ಜಾಗರೂಕತೆಯಿಂದ ವ್ಯವಹರಿಸಲು ನೆರವಾಗುತ್ತದೆ.

ವಿಷಯಸೂಚಿ

I. ಸೈಬರ್ ಸುರಕ್ಷತೆಗಾಗಿ ಪಾಲಿಸಬೇಕಾದ ನಿಯಮಗಳು

ಡಿಜಿಟಲ್ ಪಾವತಿಗಳು ಮತ್ತು ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್ ಸುರಕ್ಷತೆ 08

ಆ್ಯಪ್ ಸುರಕ್ಷತೆ 13

ಇ-ಮೇಲ್ ಸುರಕ್ಷತೆ 18

ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಸುರಕ್ಷತೆ 23

II. ಗೌಪ್ಯತೆಗೆ (ಪ್ರೈವೆಸಿ) ಸಂಬಂಧಿಸಿದ ಉತ್ತಮ ಅಭ್ಯಾಸಗಳು 26

III. ಡಿಜಿಟಲ್ ನೈರ್ಮಲ್ಯ (ಹೈಜೀನ್)

ಡಿವೈಸ್ ಮತ್ತು ಅಕೌಂಟ್ ಸುರಕ್ಷತೆ (ಹೈಜೀನ್) 34

ಪಾಸ್‌ವರ್ಡ್ ಸುರಕ್ಷತೆ (ಹೈಜೀನ್) 36

ಡಿಜಿಟಲ್ ಯೋಗಕ್ಷೇಮ 38

IV. ಸೈಬರ್ ಅಪರಾಧ ಪರಿಹಾರ ಕ್ರಮ (ಸೈಬರ್ ಕ್ರೈಮ್ ರಿಡ್ರೆಸಲ್) 39

ಸೈಬರ್ ಸುರಕ್ಷತೆಗಾಗಿ ಪಾಲಿಸಬೇಕಾದ ನಿಯಮಗಳು



ಡಿಜಿಟಲ್ ಪಾವತಿಗಳನ್ನು ಮಾಡುವುದು, ಆ್ಯಪ್‌ಗಳನ್ನು ಬಳಸುವುದು, ಇ-ಮೇಲ್‌ಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸುವುದು ಮತ್ತು ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಸಂವಹನ ನಡೆಸುವುದು ಮುಂತಾದ ದೈನಂದಿನ ಚಟುವಟಿಕೆಗಳು, ವಂಚಕರಿಂದ ನಿರಂತರವಾಗಿ ನಡೆಯುವ ಸೈಬರ್ ದಾಳಿಗಳ ಕಾರಣದಿಂದಾಗಿ ಒಂದಲ್ಲ ಒಂದು ಮಟ್ಟದ ಸೈಬರ್ ಅಪಾಯವನ್ನು ಒಳಗೊಂಡಿರುತ್ತವೆ.

ಬುದ್ಧಿವಂತ ಡಿಜಿಟಲ್ ಅಭ್ಯಾಸಗಳನ್ನು ಅಳವಡಿಸಿಕೊಳ್ಳುವ ವಿಷಯದಲ್ಲಿ ಒಂದು ಪ್ರಮುಖ ನಿಯಮವಿದೆ: ಯಾವುದೇ ಕರೆ, ಸಂದೇಶ ಅಥವಾ ಲಿಂಕ್‌ಗೆ ಪ್ರತಿಕ್ರಿಯಿಸುವ ಮೊದಲು 'ಸ್ವಲ್ಪ ತಾಳಿ, ಪರಿಶೀಲಿಸಿ ಮತ್ತು ನಂತರ ಕ್ರಮ ಕೈಗೊಳ್ಳಿ'.

ಈ ವಿಭಾಗವು ಡಿಜಿಟಲ್ ಪಾವತಿಗಳು, ಆ್ಯಪ್ ಭದ್ರತೆ, ಇಮೇಲ್ ಮತ್ತು ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ಪ್ರಾಯೋಗಿಕ ಭದ್ರತಾ ಅಭ್ಯಾಸಗಳನ್ನು ವಿವರಿಸುತ್ತದೆ.

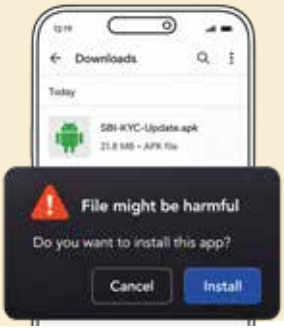
ಡಿಜಿಟಲ್ ಪಾವತಿಗಳು ಮತ್ತು ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್ ಸುರಕ್ಷತೆ

ಡಿಜಿಟಲ್ ಪಾವತಿಗಳು ದಿನನಿತ್ಯದ ವಹಿವಾಟುಗಳನ್ನು ವೇಗವಾಗಿ ಮತ್ತು ಸುಲಭವಾಗಿಸುತ್ತವೆ, ಆದರೆ ಅವು ನಮ್ಮ ಹಣ ಮತ್ತು ಹಣಕಾಸಿನ ಮಾಹಿತಿಯನ್ನು ಒಳಗೊಂಡಿರುತ್ತವೆ.
ಇದಕ್ಕಾಗಿಯೇ ಡಿಜಿಟಲ್ ಪಾವತಿಗಳು ಮತ್ತು ಬ್ಯಾಂಕಿಂಗ್ ಭದ್ರತೆ ಮುಖ್ಯವಾಗುತ್ತದೆ: ಒಂದು ವಂಚನೆಯ ಅಥವಾ ತಪ್ಪಾದ ವಹಿವಾಟು ನಿಮ್ಮ ಹಣವನ್ನು ಅಪಾಯಕ್ಕೆ ಸಿಲುಕಿಸಬಹುದು ಮತ್ತು ಅದನ್ನು ಮರಳಿ ಪಡೆಯುವುದು ಕಷ್ಟವಾಗಬಹುದು.

ಸಾಮಾನ್ಯವಾಗಿ ಬಳಸುವ ಡಿಜಿಟಲ್ ಪದಗಳನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳೋಣ

1 ಫೈಲ್

ಎಪಿಕೆ (ಆಂಡ್ರಾಯ್ಡ್ ಪ್ಯಾಕೇಜ್ ಕಿಟ್) ಫೈಲ್ ಎಂಬುದು ಆಂಡ್ರಾಯ್ಡ್ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ನಲ್ಲಿ ಮೊಬೈಲ್ ಆಪ್‌ಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಲು ಬಳಸುವ ಒಂದು ಸ್ಟ್ಯಾಂಡರ್ಡ್ ಫಾರ್ಮ್ಯಾಟ್ ಆಗಿದೆ. ಅಪರಿಚಿತ ವೆಬ್‌ಸೈಟ್‌ಗಳು, ಲಿಂಕ್‌ಗಳು ಅಥವಾ ಮೆಸೇಜ್‌ಗಳಿಂದ ಎಪಿಕೆ ಫೈಲ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮತ್ತು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡುವುದು ಮಾಲ್‌ವೇರ್, ಡೇಟಾ ಕಳ್ಳತನ ಮತ್ತು ಹಣಕಾಸಿನ ವಂಚನೆಯಂತಹ ಪ್ರಮುಖ ಭದ್ರತಾ ಅಪಾಯಗಳನ್ನು ಉಂಟುಮಾಡುತ್ತದೆ.



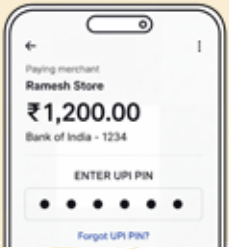
2 ದೂರಸ್ಥ ಪ್ರವೇಶ (ರಿಮೋಟ್ ಆಕ್ಸೆಸ್) /ಸ್ಕ್ರೀನ್-ಶೇರಿಂಗ್ ಆಪ್

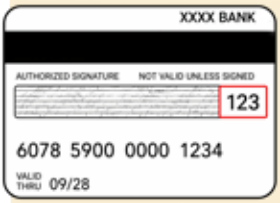


ಇದು ನಿಮ್ಮ ಸಾಧನವನ್ನು ಇನ್ನೊಬ್ಬರಿಗೆ ತೋರಿಸಲು, ಬೇರೆ ಸ್ಥಳದಿಂದ ಅದನ್ನು ನಿಯಂತ್ರಿಸಲು ಅಥವಾ ನಿಮ್ಮ ಪರದೆಯನ್ನು (ಸ್ಕ್ರೀನ್) ನೇರಪ್ರಸಾರದಂತೆ (ಲೈವ್ ಆಗಿ) ವೀಕ್ಷಿಸಲು ಅನುವು ಮಾಡಿಕೊಡುವ ಒಂದು ಸಾಫ್ಟ್‌ವೇರ್ ಪ್ರೋಗ್ರಾಂ ಆಗಿದೆ. ಇದರ ಸಾಮಾನ್ಯ ಉದಾಹರಣೆಗಳೆಂದರೆ **ಎನಿಡೆಸ್ಕ್, ಟೀಮ್‌ವೀವರ್, ಕ್ವಿಕ್‌ಸಪೋರ್ಟ್ ಮತ್ತು ರಸ್ಟ್‌ಡೆಸ್ಕ್.**

3 ಯುಪಿಐ (ಯೂನಿಫೈಡ್ ಪೇಮೆಂಟ್ಸ್ ಇಂಟರ್‌ಫೇಸ್) ಪಿನ್

ಯುಪಿಐ ಪಿನ್ ಎಂಬುದು ಯುಪಿಐ ಆಪ್‌ಗಳ ಮೂಲಕ ಹಣ ವರ್ಗಾವಣೆಯನ್ನು ಅನುಮೋದಿಸಲು ಬಳಸುವ ವೈಯಕ್ತಿಕ ಭದ್ರತಾ ಕೋಡ್ ಆಗಿದೆ.



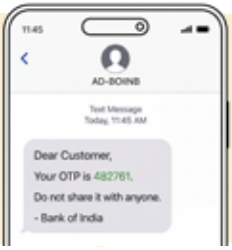


4 ಸಿವಿವಿ

ಸಿವಿವಿ ಎನ್ನುವುದು ಆನ್‌ಲೈನ್ ಪಾವತಿಗಳಿಗಾಗಿ ನಿಮ್ಮ ಡೆಬಿಟ್ ಅಥವಾ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್‌ನಲ್ಲಿ ಮುದ್ರಿಸಲಾದ ಭದ್ರತಾ ಕೋಡ್ ಆಗಿದೆ.

5 ಒಟಿಪಿ (ಒಂದು ಬಾರಿಯ (ಒನ್-ಟೈಮ್) ಪಾಸ್ವರ್ಡ್)

ಲಾಗಿನ್ ಅಥವಾ ವಹಿವಾಟನ್ನು ಪರಿಶೀಲಿಸಲು ನಿಮ್ಮ ಮೊಬೈಲ್ ಸಂಖ್ಯೆ ಅಥವಾ ಇ-ಮೇಲ್‌ಗೆ ಕಳುಹಿಸಲಾದ ತಾತ್ಕಾಲಿಕ ಭದ್ರತಾ ಕೋಡ್.





6 ಕೆವೈಸಿ (ನಿಮ್ಮ ಗ್ರಾಹಕರನ್ನು ತಿಳಿಯಿರಿ-ನೌ ಯುವರ್ ಕಸ್ಟಮರ್)

ಬ್ಯಾಂಕ್‌ಗಳು ಮತ್ತು ಆ್ಯಪ್‌ಗಳು ಅಧಿಕೃತ ದಾಖಲೆಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಗ್ರಾಹಕರ ನೈಜ ಗುರುತನ್ನು ಪರೀಕ್ಷಿಸಲು ಮತ್ತು ಪರಿಶೀಲಿಸಲು ಬಳಸುವ ಪ್ರಕ್ರಿಯೆ. ಬಳಕೆದಾರರನ್ನು ದೃಢೀಕರಿಸಲು ಇಕೆವೈಸಿ (ಇ-ಕೆವೈಸಿ), ವಿಡಿಯೋ ಕೆವೈಸಿ ಮತ್ತು ಸೆಂಟ್ರಲ್ ಕೆವೈಸಿ (ಸಿಕೆವೈಸಿ) ವಿಧಾನಗಳನ್ನು ಹೆಚ್ಚಾಗಿ ಬಳಸಲಾಗುತ್ತದೆ.

7 ಕ್ಯೂಆರ್ ಕೋಡ್

ಕ್ಯೂಆರ್ ಕೋಡ್ ಎಂಬುದು ಒಂದು ಚೌಕಾಕಾರದ ಬಾರ್‌ಕೋಡ್ ಆಗಿದ್ದು, ಪೇಮೆಂಟ್‌ಗಳಂತಹ ಡಿಜಿಟಲ್ ಕಾರ್ಯಗಳನ್ನು ಪೂರ್ಣಗೊಳಿಸಲು ನಿಮ್ಮ ಫೋನ್ ಕ್ಯಾಮೆರಾವನ್ನು ಬಳಸಿ ಇದನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬಹುದು.



ಪಾಲಿಸಬೇಕಾದ ನಿಯಮಗಳು

- ಅಧಿಕೃತ ಬ್ಯಾಂಕಿಂಗ್ ಮತ್ತು ಪೇಮೆಂಟ್ ಆಪ್‌ಗಳನ್ನು ಬಳಸಿ. ಅವುಗಳನ್ನು ನಿಮ್ಮ ಫೋನ್‌ನ ಅಧಿಕೃತ ಆಪ್ ಸ್ಟೋರ್‌ನಿಂದ ಮಾತ್ರ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ; ಮೆಸೇಜ್‌ಗಳ ಮೂಲಕ ಕಳುಹಿಸಲಾದ ಲಿಂಕ್‌ಗಳು ಅಥವಾ ಎಪಿಕೆ ಫೈಲ್‌ಗಳನ್ನು ತೆರೆಯಬೇಡಿ.

- ನಿಮ್ಮ ಯುಪಿಐ ಪಿನ್, ಓಟಿಪಿ, ಕ್ರೆಡಿಟ್/ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಸಿವಿವಿ ಮತ್ತು ಪಿನ್ ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಪೂರ್ಣ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

- ಯಾವುದೇ ಯುಪಿಐ ಪಾವತಿಯನ್ನು (Payment) ಅಪ್ರೂವ್ ಮಾಡುವ ಮೊದಲು, ಹಣ ಪಡೆಯುವವರ ಹೆಸರು ಮತ್ತು ಮೊತ್ತವನ್ನು ಕಡ್ಡಾಯವಾಗಿ ಪರಿಶೀಲಿಸಿ. ಅದು "ರಿಫಂಡ್", "ಕ್ಯಾಶ್‌ಬ್ಯಾಕ್" ಅಥವಾ "ಬಹುಮಾನ (ಪ್ರೈಜ್)" ಎಂದು ಬಂದಿದ್ದರೂ ಸಹ ಎಚ್ಚರದಿಂದಿರಿ.

- ಪಾವತಿ ಮಾಡಲು ಓಟಿಪಿ ನಮೂದಿಸುವ ಮೊದಲು, ವಹಿವಾಟಿನ ಮೊತ್ತ ಮತ್ತು ಸ್ವೀಕರಿಸುವವರ ವಿವರಗಳನ್ನು ಪರಿಶೀಲಿಸಲು ಯಾವಾಗಲೂ ಮೊದಲು ಓಟಿಪಿ ಎಸ್‌ಎಂಎಸ್ ಅನ್ನು ಪರೀಕ್ಷಿಸಿ.

- ಕ್ಯೂಆರ್ ಕೋಡ್‌ಗಳ ವಿಷಯದಲ್ಲಿ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ. ಕ್ಯೂಆರ್ ಕೋಡ್ ಅನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡುವುದರಿಂದ ಹಣ ಪಾವತಿಯಾಗಬಹುದು; ಕೇವಲ ಹಣ ಅಥವಾ ಮರುಪಾವತಿಯನ್ನು ಪಡೆಯಲು ಅದನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ.

- ನಿಮ್ಮ ಫೋನ್‌ಗೆ ರಿಮೋಟ್ ಆಕ್ಸೆಸ್ ನೀಡಬೇಡಿ. ಅಪರಿಚಿತ ಕರೆ ಮಾಡುವವರು ಕೇಳುತ್ತಾರೆ ಎಂಬ ಕಾರಣಕ್ಕೆ ರಿಮೋಟ್-ಆಕ್ಸೆಸ್ ಅಥವಾ ಸ್ಕ್ರೀನ್-ಶೇರಿಂಗ್ ಆ್ಯಪ್ ಅನ್ನು ಎಂದಿಗೂ ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಬೇಡಿ.



- ಅನಿರೀಕ್ಷಿತ ಕೆವೈಸಿ ಕರೆಗಳು ಅಥವಾ ಸಂದೇಶಗಳನ್ನು ನಿರ್ಲಕ್ಷಿಸಿ ಮತ್ತು ನಿಮ್ಮ ಬ್ಯಾಂಕಿನ ಅಧಿಕೃತ ಚಾನಲ್ ಮೂಲಕ ಅವರನ್ನು ಸಂಪರ್ಕಿಸಿ.

- ಪೇಮೆಂಟ್ ಮಾಡುವಾಗ ಆತುರಕ್ಕೆ ಒಳಗಾಗಬೇಡಿ. ಭಯ, ಒತ್ತಡ ಅಥವಾ ಗಡುವುಗಳನ್ನು ಒಳಗೊಂಡಿರುವ ವಿನಂತಿಗಳನ್ನು ಸ್ವತಂತ್ರವಾಗಿ ಪರಿಶೀಲಿಸಲು ಸಮಯ ತೆಗೆದುಕೊಳ್ಳಿ.

- ಎಸ್ಎಂಎಸ್ (SMS) ಮೂಲಕ ಬರುವ ಟ್ರಾನ್ಸಾಕ್ಷನ್ ಅಲರ್ಟ್ ಮತ್ತು ನೋಟಿಫಿಕೇಶನ್ಗಳನ್ನು ಯಾವಾಗಲೂ ಆನ್ನಲ್ಲಿ ಇರಿಸಿ. ಯಾವುದೇ ಅಸಹಜ ಅಥವಾ ಶಂಕಾಸ್ಪದ ವಹಿವಾಟು ಕಂಡುಬಂದಲ್ಲಿ ತಕ್ಷಣವೇ ಬ್ಯಾಂಕಿಗೆ ವರದಿ ಮಾಡಿ.

- ನಿಮ್ಮ ದೈನಂದಿನ ಅಗತ್ಯಕ್ಕೆ ತಕ್ಕಂತೆ ಯುಪಿಐ ವಹಿವಾಟಿನ ಮಿತಿಯನ್ನು ನಿಗದಿಪಡಿಸಿಕೊಳ್ಳಿ. ಏನಾದರೂ ತೊಂದರೆಯಾದಲ್ಲಿ ನಿಮ್ಮ ಮೇಲಾಗುವ ಪರಿಣಾಮವನ್ನು ಕಡಿಮೆ ಮಾಡಲು, ನಿಮ್ಮ ಅಗತ್ಯಗಳಿಗೆ ಸೂಕ್ತವಾದ ದೈನಂದಿನ ಮಿತಿಯೊಂದನ್ನು ನಿಗದಿಪಡಿಸಿಕೊಳ್ಳಿ.

- ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅಕೌಂಟ್ ಅನ್ನು ನಿಮ್ಮ ಸ್ವಂತ ವಹಿವಾಟುಗಳಿಗಾಗಿ ಮಾತ್ರ ಬಳಸಿ. ಕಮಿಷನ್ ಆಸೆಗಾಗಿ ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ಅಥವಾ ವರ್ಗಾಯಿಸಲು ನಿಮ್ಮ ಅಕೌಂಟ್ ಅನ್ನು ಬೇರೆಯವರಿಗೆ ಎಂದಿಗೂ ಬಳಸಲು ಬಿಡಬೇಡಿ.

- ಯಾವುದೇ ಅಪರಿಚಿತ ಸಂದೇಶಗಳು (SMS) ಅಥವಾ ಇಂಟರ್ನೆಟ್ ಸರ್ಚ್ ಫಲಿತಾಂಶಗಳಲ್ಲಿ ಕಂಡುಬರುವ ಸಂಖ್ಯೆಗಳನ್ನು ಅವಲಂಬಿಸಬೇಡಿ. ಅಧಿಕೃತ ಗ್ರಾಹಕ ಸೇವಾ (ಕಸ್ಟಮರ್-ಕೇರ್) ವಿವರಗಳನ್ನೇ ಬಳಸಿ. ನಿಮ್ಮ ಬ್ಯಾಂಕಿನ ಅಧಿಕೃತ ವೆಬ್ಸೈಟ್, ಆ್ಯಪ್ ಅಥವಾ ಪಾಸ್ಬುಕ್ನಿಂದ ಬ್ಯಾಂಕಿನ ಸಂಖ್ಯೆಯನ್ನು ಪಡೆದುಕೊಳ್ಳಿ.





ಯಾವಾಗಲೂ ನೆನಪಿಡಿ

ಹಣವನ್ನು ಕಳುಹಿಸಲು ಮಾತ್ರ ಒಂದು ಯುಪಿಐ ಪಿನ್ ಅಗತ್ಯವಿರುತ್ತದೆ, ಅದನ್ನು ಸ್ವೀಕರಿಸಲು ಎಂದಿಗೂ ಬೇಕಾಗಿರುವುದಿಲ್ಲ. ನಿಮಗೆ ರಿಫಂಡ್ ಅಥವಾ ಕ್ಯಾಶ್ಬ್ಯಾಕ್ ನೀಡಲು ಯಾರಾದರೂ ನಿಮ್ಮ ಪಿನ್ ಕೇಳಿದರೆ, ಅದು ಯಾವಾಗಲೂ ವಂಚನೆಯೇ (ಸ್ಕ್ಯಾಮ್) ಆಗಿರುತ್ತದೆ.



ಸಾಮಾನ್ಯ ಡಿಜಿಟಲ್ ಪಾವತಿಗಳು ಮತ್ತು ಬ್ಯಾಂಕಿಂಗ್ ಭದ್ರತೆಯ ಸಂಬಂಧಿತ ಸ್ಕ್ಯಾಮ್‌ಗಳು



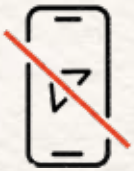
ನಕಲಿ (ಫೇಕ್) ಕೆವೈಸಿ/ಅಕೌಂಟ್ ಬ್ಲಾಕ್ ಮಾಡುವ ಸ್ಕ್ಯಾಮ್

ಯಾರಾದರೂ ಕರೆ ಅಥವಾ ಸಂದೇಶದ ಮೂಲಕ ನಿಮ್ಮ ಬ್ಯಾಂಕಿನಿಂದ ಮಾತನಾಡುತ್ತಿರುವುದಾಗಿ ನಟಿಸಿ, 'ನಿಮ್ಮ KYC ನವೀಕರಿಸದಿದ್ದರೆ ಖಾತೆ ಬ್ಲಾಕ್ ಆಗುತ್ತದೆ' ಎಂದು ಹೆದರಿಸಬಹುದು. ಅಷ್ಟೇ ಅಲ್ಲದೆ, ನಕಲಿ ವೆಬ್ಸೈಟ್‌ಗಳ ಲಿಂಕ್ ನೀಡಿ ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಕೇಳಬಹುದು ಅಥವಾ ಹಣ ಪಾವತಿಸಲು ಒತ್ತಾಯಿಸಬಹುದು.

ನಕಲಿ (ಫೇಕ್) ರೀಫಂಡ್ / ಕ್ಯಾಶ್‌ಬ್ಯಾಕ್ ವಂಚನೆ (ಸ್ಕ್ಯಾಮ್)



ನೀವು ರಿಫಂಡ್, ಕ್ಯಾಶ್‌ಬ್ಯಾಕ್ ಅಥವಾ ರಿವಾರ್ಡ್ ಪಡೆಯಲು ಅರ್ಹರಿದ್ದೀರಿ ಎಂದು ಸಂದೇಶ ಅಥವಾ ಕರೆ ಬರಬಹುದು. ಅದನ್ನು ಪಡೆಯಲು ಯುಪಿಐ ವಿನಂತಿಯನ್ನು ಅನುಮೋದಿಸಲು, ಕ್ಯೂಆರ್ ಕೋಡ್ ಸ್ಕ್ಯಾನ್ ಮಾಡಲು ಅಥವಾ ಪಾವತಿ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ನಿಮ್ಮನ್ನು ಕೇಳಬಹುದು.



ರಿಮೋಟ್ ಆಕ್ಸೆಸ್ ಸ್ಕ್ಯಾಮ್

ಬ್ಯಾಂಕಿಂಗ್ ಅಥವಾ ಪೇಮೆಂಟ್ ಸಮಸ್ಯೆಯನ್ನು ಬಗೆಹರಿಸಲು ಅಗತ್ಯವಿದೆ ಎಂದು ಹೇಳಿ, ವಂಚಕರು ನಿಮ್ಮನ್ನು ರಿಮೋಟ್-ಆಕ್ಸೆಸ್ ಅಥವಾ ಸ್ಕ್ರೀನ್-ಶೇರಿಂಗ್ ಆ್ಯಪ್ ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡುವಂತೆ ನಂಬಿಸುತ್ತಾರೆ. ಒಮ್ಮೆ ಆಕ್ಸೆಸ್ ನೀಡಿದ ನಂತರ, ಅವರು ನಿಮ್ಮ ಡಿವೈಸ್‌ನಲ್ಲಿನ ಚಟುವಟಿಕೆಯನ್ನು ನೋಡಲು ಅಥವಾ ನಿಯಂತ್ರಿಸಲು ಸಾಧ್ಯವಾಗಬಹುದು.

ಮನಿ ಮ್ಯೂಲ್ / ಖಾತೆ ದುರುಪಯೋಗದ ವಂಚನೆ



ಯಾರಾದರೂ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅಕೌಂಟ್ ಮೂಲಕ ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ಮತ್ತು ವರ್ಗಾಯಿಸಲು ಹಣ ಅಥವಾ ಕಮಿಷನ್ ನೀಡುತ್ತಾರೆ. ಆ ಹಣವನ್ನು ವಂಚನೆಯಿಂದ ಪಡೆಯಲಾಗಿರಬಹುದು, ಇದರಿಂದ ನಿಮ್ಮ ಅಕೌಂಟ್ ಕೂಡ ಅಂತಹ ವಂಚನೆಯ ಭಾಗವಾಗುತ್ತದೆ.



ಕ್ಯೂಆರ್ ಕೋಡ್ ಪಾವತಿ ವಂಚನೆ

ವಂಚಕರು ನಿಮಗೆ ಹಣ, ಮರುಪಾವತಿ (ರಿಫಂಡ್) ಅಥವಾ ಬಹುಮಾನವನ್ನು ನೀಡುವ ನೆಪದಲ್ಲಿ QR ಕೋಡ್ ಅನ್ನು ಕಳುಹಿಸಬಹುದು ಅಥವಾ ತೋರಿಸಬಹುದು. ಅದನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಿದರೆ, ನಿಮ್ಮ ಖಾತೆಯಿಂದ ಹಣ ಕಡಿತವಾಗುವ ಪೇಮೆಂಟ್ ಪ್ರಕ್ರಿಯೆ ಶುರುವಾಗಬಹುದು (ನಿಮ್ಮ ಖಾತೆಯಿಂದಲೇ ಹಣ ಕಡಿತವಾಗುವ ಅಪಾಯವಿರುತ್ತದೆ).

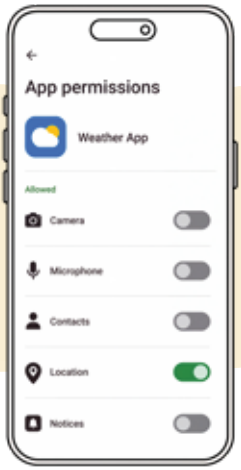
ಆ್ಯಪ್ ಸುರಕ್ಷತೆ

ಆಪ್ಸ್ ನಮ್ಮ ದೈನಂದಿನ ಕೆಲಸಗಳನ್ನು ಸುಲಭಗೊಳಿಸುತ್ತವೆ, ಆದರೆ ಅವು ನಮ್ಮ ಫೋನ್‌ಗಳಲ್ಲಿನ ವಿವಿಧ ಫೀಚರ್ಸ್ ಮತ್ತು ಮಾಹಿತಿಯನ್ನು ಆಕ್ಸೆಸ್ ಮಾಡಬಲ್ಲವು. **ಇದಕ್ಕಾಗಿಯೇ ಆಪ್ ಭದ್ರತೆ ಮುಖ್ಯವಾಗುತ್ತದೆ: ಅಸುರಕ್ಷಿತ ಆಪ್ ಈ ಆಕ್ಸೆಸ್ ಅನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳಬಹುದು, ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಪಡಿಸಬಹುದು ಅಥವಾ ನಿಮ್ಮ ಖಾತೆ ಮತ್ತು ಹಣವನ್ನು ಅಪಾಯಕ್ಕೆ ಸಿಲುಕಿಸಬಹುದು.**

ಸಾಮಾನ್ಯವಾದ ಡಿಜಿಟಲ್ ಪ್ರಮುಖ ಪದಗಳನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳೋಣ

1 ಆ್ಯಪ್ ಅನುಮತಿಗಳು (ಪರ್ಮಿಷನ್ಸ್)

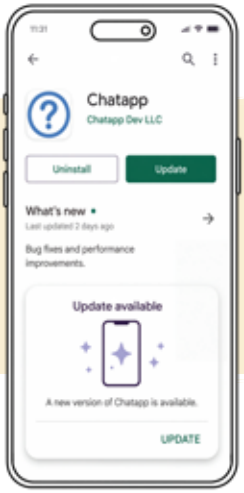
ಆ್ಯಪ್ ಅನುಮತಿಗಳು ಎಂದರೆ ನಿಮ್ಮ ಫೋನ್‌ನಲ್ಲಿರುವ ಕ್ಯಾಮೆರಾ, ಮೈಕ್ರೋಫೋನ್, ಸಂಪರ್ಕಗಳು, ಫೋಟೋಗಳು ಅಥವಾ ಲೊಕೇಶನ್‌ನಂತಹ ಕೆಲವು ಫೀಚರ್‌ಗಳು ಅಥವಾ ಮಾಹಿತಿಯನ್ನು ಆಕ್ಸೆಸ್ ಮಾಡಲು ನೀವು ಆ್ಯಪ್‌ಗೆ ನೀಡುವ ಅನುಮೋದನೆಗಳಾಗಿವೆ.



2 ಅಧಿಕೃತ ಆಪ್ ಸ್ಟೋರ್

Google Play Store Apple App Store

ಅಧಿಕೃತ ಆ್ಯಪ್ ಸ್ಟೋರ್ ಎಂಬುದು ನಿಮ್ಮ ಫೋನ್ ತಯಾರಕರು ಮತ್ತು ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್ (ಒಎಸ್) ಒದಗಿಸುವವರು ಅಧಿಕೃತವಾಗಿ ಪರಿಶೀಲಿಸಿದ ಆ್ಯಪ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ಒದಗಿಸಿದ ನಂಬಿಕಸ್ತ ಸ್ಥಳವಾಗಿದೆ. ಆಂಡ್ರಾಯ್ಡ್ ಫೋನ್‌ಗಳಲ್ಲಿ, ಇದು ಸಾಮಾನ್ಯವಾಗಿ **ಗೂಗಲ್ ಪ್ಲೇ ಸ್ಟೋರ್** ಆಗಿರುತ್ತದೆ ಮತ್ತು ಐಫೋನ್‌ಗಳಲ್ಲಿ, ಇದು **ಆಪಲ್ ಆ್ಯಪ್ ಸ್ಟೋರ್** ಆಗಿರುತ್ತದೆ.



3 ಅಪ್‌ಡೇಟ್

ಆ್ಯಪ್ ಅಪ್‌ಡೇಟ್ ಎಂಬುದು ಆ್ಯಪ್ ಡೆವಲಪರ್ ಬಿಡುಗಡೆ ಮಾಡಿದ ಹೊಸ ಆವೃತ್ತಿಯಾಗಿದೆ. ಇದು ಸಮಸ್ಯೆಗಳನ್ನು ಸರಿಪಡಿಸಬಹುದು, ಭದ್ರತೆಯನ್ನು ಸುಧಾರಿಸಬಹುದು ಅಥವಾ ಹೊಸ ಫೀಚರ್‌ಗಳನ್ನು ಸೇರಿಸಬಹುದು.



4 ಆ್ಯಪ್ ಸಂಗ್ರಹ (ಕ್ಯಾಶೆ)/ ದತ್ತಾಂಶ (ಡೇಟಾ)

ಆ್ಯಪ್ ಕ್ಯಾಶೆ ಮತ್ತು ಡೇಟಾ ಎಂಬುದು ನಿಮ್ಮ ಫೋನ್‌ನಲ್ಲಿರುವ ಆ್ಯಪ್‌ನಿಂದ ಸ್ಥಳೀಯವಾಗಿ ಸಂಗ್ರಹಿಸಲಾದ ಮಾಹಿತಿಯಾಗಿದೆ. ಕ್ಯಾಶ್ ಸಾಮಾನ್ಯವಾಗಿ ತಾತ್ಕಾಲಿಕ ಫೈಲ್‌ಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ, ಆದರೆ ಆ್ಯಪ್ ಡೇಟಾವು ಉಳಿಸಿದ ಸೆಟ್ಟಿಂಗ್‌ಗಳು, ಆದ್ಯತೆಗಳು ಮತ್ತು ಇತರ ಮಾಹಿತಿಯನ್ನು ಒಳಗೊಂಡಿರಬಹುದು.



ಅನುಸರಿಸಬೇಕಾದ ಉತ್ತಮ ಪದ್ಧತಿಗಳು

- ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡುವ ಮೊದಲು ಅಧಿಕೃತ ಆ್ಯಪ್ ಸ್ಟೋರ್ ಅನ್ನು ಮಾತ್ರ ಬಳಸಿ ಮತ್ತು ಆ್ಯಪ್ ಹೆಸರು, ಡೆವಲಪರ್, ರಿವ್ಯೂಗಳು ಮತ್ತು ರೇಟಿಂಗ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.

- ನಿಮಗೆ ಅಗತ್ಯವಿರುವ ಆಪ್‌ಗಳನ್ನು ಮಾತ್ರ ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಿ. ಸಾಮಾಜಿಕ ಜಾಲತಾಣ, ವಾಟ್ಸಾಪ್ ಅಥವಾ ಮೆಸೇಜ್‌ಗಳ ಮೂಲಕ ಸೂಚಿಸಲಾದ ಸಂಬಂದವಿಲ್ಲದ ಆಪ್‌ಗಳನ್ನು ತಪ್ಪಿಸಿ, ವಿಶೇಷವಾಗಿ ಟ್ರೆಂಡಿಂಗ್ ಫೀಚರ್‌ಗಳು, ರಿವಾರ್ಡ್‌ಗಳು ಅಥವಾ ಗೇಮ್‌ಗಳನ್ನು ನೀಡುವ ಆಪ್‌ಗಳಿಂದ ದೂರವಿರಿ.

- ಆ್ಯಪ್ ಪರ್ಮಿಷನ್‌ಗಳನ್ನು ಚೆಕ್ ಮಾಡಿ. ಆ್ಯಪ್‌ಗೆ ಅದಕ್ಕೆ ಬೇಕಾದ ಆಕ್ಸೆಸ್ ಅನ್ನು ಮಾತ್ರ ನೀಡಿ. ಕ್ಯಾಲ್ಕುಲೇಟರ್‌ಗೆ ನಿಮ್ಮ ಕಾಂಟ್ಯಾಕ್ಟ್‌ಗಳ ಅಗತ್ಯವಿರುವುದಿಲ್ಲ ಮತ್ತು ಒಂದು ಸಾಧಾರಣ ಫೋಟೋ-ಎಡಿಟಿಂಗ್ ಆ್ಯಪ್‌ಗೆ ನಿಮ್ಮ ಲೊಕೇಶನ್ ಆಕ್ಸೆಸ್ ಅಗತ್ಯವಿರುವುದಿಲ್ಲ.

- ನಿಮ್ಮ ಫೋನ್ ಮತ್ತು ಆಪ್‌ಗಳನ್ನು ಅಪ್‌ಡೇಟ್ ಆಗಿ ಇರಿಸಿ. ಭದ್ರತೆ ದೋಷಗಳನ್ನು ಸರಿಪಡಿಸಲು ಅಪ್‌ಡೇಟ್‌ಗಳು ಲಭ್ಯವಿದ್ದಾಗ ಅವುಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಿ.

- ಅಗತ್ಯವಿದ್ದಾಗ ಮಾತ್ರ ಅಕೌಂಟ್‌ಗಳನ್ನು ಕ್ರಿಯೇಟ್ ಮಾಡಿ. ಆ್ಯಪ್ ಯಾವ ಮಾಹಿತಿಯನ್ನು ಕೇಳುತ್ತದೆ ಮತ್ತು ನಿಮಗೆ ನಿಜವಾಗಿಯೂ ಅಕೌಂಟ್ ಅಗತ್ಯವಿದೆಯೇ ಎಂದು ಚೆಕ್ ಮಾಡಿ.



- ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ತಡೆಯಲು ನಿಮ್ಮ ಫೋನ್ ಮತ್ತು ಸೂಕ್ಷ್ಮ ಆ್ಯಪ್‌ಗಳನ್ನು ಪಿನ್ (PIN), ಫಿಂಗರ್‌ಪ್ರಿಂಟ್ ಅಥವಾ ಫೇಸ್ ಲಾಕ್‌ನೊಂದಿಗೆ ಸುರಕ್ಷಿತಗೊಳಿಸಿ ಮತ್ತು ಹಣಕಾಸಿನ ಹಾಗೂ ಇತರ ಸೂಕ್ಷ್ಮ ಆ್ಯಪ್‌ಗಳಿಗಾಗಿ 2-ಫ್ಯಾಕ್ಟರ್ ಅಥೆಂಟಿಕೇಶನ್ (2FA) ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.

- ನಿಮ್ಮ ನಿಮ್ಮ ಆ್ಯಪ್‌ಗಳು ಮತ್ತು ಅನುಮತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ. ಇನ್ನು ಮುಂದೆ ಬಳಸದ ಆ್ಯಪ್‌ಗಳನ್ನು ತೆಗೆದುಹಾಕಿ ಮತ್ತು ಪ್ರಸ್ತುತ ಇರುವ ಆ್ಯಪ್‌ಗಳಿಗೆ ಅಗತ್ಯವಿರುವ ಅನುಮತಿಗಳು ಮಾತ್ರ ಇವೆಯೇ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

- ಭದ್ರತೆ ವಾರ್ನಿಂಗ್‌ಗಳ ಬಗ್ಗೆ ಗಮನವಿರಲಿ. ನಿಮ್ಮ ಫೋನ್ ಅಥವಾ ಆ್ಯಪ್ ಭದ್ರತೆ ವಾರ್ನಿಂಗ್ ತೋರಿಸಿದರೆ, ಮುಂದುವರಿಯುವ ಮೊದಲು ನಿಲ್ಲಿ ಮತ್ತು ಪರಿಶೀಲಿಸಿ.

- ಯಾವುದೇ ಆ್ಯಪ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡುವ ಮೊದಲು ಮತ್ತು ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ನಮೂದಿಸುವ ಮೊದಲು ಅದನ್ನು ಪರಿಶೀಲಿಸಿ. ಆ್ಯಪ್ ಅಸಲಿ ಎಂದು ನಿಮಗೆ ಖಚಿತವಾಗದ ಹೊರತು ನಿಮ್ಮ ಓಟಿಪಿ, ಪಿನ್, ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಬ್ಯಾಂಕಿಂಗ್ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ನಮೂದಿಸಬೇಡಿ.

- ಸಾಲ ಮತ್ತು ಹೂಡಿಕೆ ಸಂಬಂದಿತ ಆ್ಯಪ್‌ಗಳ ವಿಷಯದಲ್ಲಿ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ. ತ್ವರಿತ ಸಾಲ, ಖಚಿತ ಆದಾಯ ಅಥವಾ ಶೀಘ್ರ ಲಾಭದ ಭರವಸೆ ನೀಡುವ ಆ್ಯಪ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವ ಮುನ್ನ, ಸಾಲ ನೀಡುವ ಸಂಸ್ಥೆ ಅಥವಾ ಹೂಡಿಕೆ ಕಂಪನಿಯ ಬಗ್ಗೆ ಪರಿಶೀಲಿಸಿ.



ಯಾವಾಗಲೂ ನೆನಪಿಡಿ

ಅಧಿಕೃತ ಆ್ಯಪ್ ಸ್ಟೋರ್‌ನಲ್ಲಿರುವ ಆ್ಯಪ್‌ಗಳು ಕೂಡ ಕೆಲವೊಮ್ಮೆ ವಂಚನೆಯಿಂದ ಕೂಡಿರಬಹುದು ಅಥವಾ ಹಾನಿಕಾರಕವಾಗಿರಬಹುದು. ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡುವ ಮೊದಲು, ನೀವು ಅಸಲಿ ಆ್ಯಪ್ ಅನ್ನೇ ಡೌನ್ಲೋಡ್ ಮಾಯಾಡುತ್ತಿದ್ದೀರಿ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಆ್ಯಪ್ ಹೆಸರು, ಲೋಗೋ, ಡೆವಲಪರ್ ಮತ್ತು ರಿವ್ಯೂಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.



ನಕಲಿ ಆ್ಯಪ್ ವಂಚನೆಗಳು

ನೀವು ತಪ್ಪಾಗಿ ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಿಕೊಳ್ಳಲಿ ಎಂಬ ಕಾರಣಕ್ಕೆ ನಕಲಿ ಆ್ಯಪ್ ಅನ್ನು ಅಸಲಿ ಆ್ಯಪ್‌ನಂತೆಯೇ ಕಾಣುವಂತೆ ತಯಾರಿಸಲಾಗಿರುತ್ತದೆ. ಇದು ನಂಬಿಕಸ್ತ ಆ್ಯಪ್‌ನಂತೆಯೇ ಲೋಗೋ, ಬಣ್ಣಗಳು ಮತ್ತು ಹೆಸರನ್ನು ಹೊಂದಿರಬಹುದು, ಆದರೆ ಸಣ್ಣಪುಟ್ಟ ವಿವರಗಳು ಬೇರೆಯಾಗಿರಬಹುದು.



ನಕಲಿ ಶಾಪಿಂಗ್ ಆ್ಯಪ್

ವಂಚಕರು ಭಾರಿ ರಿಯಾಯಿತಿ ದರದ ಉತ್ಪನ್ನಗಳು, ಸೀಮಿತ ಅವಧಿಯ ಡೀಲ್‌ಗಳು ಅಥವಾ ವಿಶೇಷ ಆಫರ್‌ಗಳನ್ನು ನೀಡುವ ಆ್ಯಪ್‌ಗಳನ್ನು ರಚಿಸಬಹುದು. ಗೂಗಲ್ ಸರ್ಚ್‌ಗಳು, ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಅಥವಾ ಮೆಸೇಜ್‌ಗಳ ಮೂಲಕ ನೀವು ಇಂತಹ ಪ್ರಚಾರಗಳನ್ನು ನೋಡಬಹುದು. ಈ ಆ್ಯಪ್ ಅಸಲಿ ಶಾಪಿಂಗ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ನಂತೆ ಕಾಣಿಸಬಹುದು ಮತ್ತು ಉತ್ಪನ್ನವನ್ನು ತಲುಪಿಸದೆಯೇ ನಿಮ್ಮ ಪೇಮೆಂಟ್ ಅನ್ನು ಪಡೆದುಕೊಳ್ಳಬಹುದು.



ನಕಲಿ ಸರ್ಕಾರಿ ಅಥವಾ ಸೇವಾ ಆ್ಯಪ್

ವಂಚಕರು ಸರ್ಕಾರಿ ಸೇವೆಗಳು, ಸಬ್ಸಿಡಿಗಳು, ಪ್ರಮಾಣಪತ್ರಗಳು, ಯುಟಿಲಿಟಿ ಸೇವೆಗಳು ಅಥವಾ ಇತರ ಸಾರ್ವಜನಿಕ ಸೇವೆಗಳನ್ನು ನೀಡುವಂತೆ ನಟಿಸುವ ಆ್ಯಪ್‌ಗಳನ್ನು ರಚಿಸಬಹುದು. ಗೂಗಲ್ ಸರ್ಚ್‌ಗಳು, ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಅಥವಾ ಮೆಸೇಜ್‌ಗಳ ಮೂಲಕ ನೀವು ಇಂತಹ ಆ್ಯಪ್‌ಗಳನ್ನು ಕಾಣಬಹುದು. ಈ ಆ್ಯಪ್ ಅಸಲಿಯಂತೆ ಕಾಣಿಸಬಹುದು ಮತ್ತು ನಿಮ್ಮ ಆಧಾರ್, ಪ್ಯಾನ್, ಓಟಿಪಿ ಅಥವಾ ಇತರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಕೇಳಬಹುದು.



ಫೇಕ್ ಬ್ಯಾಂಕಿಂಗ್ ಅಥವಾ ಕಸ್ಟಮರ್ ಸಪೋರ್ಟ್ ಆಪ್

ವಂಚಕರು ಬ್ಯಾಂಕಿಂಗ್, ಪಾವತಿ ಅಥವಾ ಗ್ರಾಹಕ ಸೇವಾ (ಕಸ್ಟಮರ್ ಸಪೋರ್ಟ್) ವಿಭಾಗದ ಸೇವೆಗಳಂತೆ ನಟಿಸುವ ಆ್ಯಪ್‌ಗಳನ್ನು ಸೃಷ್ಟಿಸಬಹುದು. ನಿಮ್ಮ ಖಾತೆಗೆ ಸಂಬಂಧಿಸಿದ ಸಹಾಯವನ್ನು ನೀಡುವುದಾಗಿ ಹೇಳಿಕೊಳ್ಳುವ ಸಂದೇಶಗಳು, ಕರೆಗಳು ಅಥವಾ ಸರ್ಚ್ ಫಲಿತಾಂಶಗಳ ಮೂಲಕ ನಿಮ್ಮನ್ನು ಈ ಆ್ಯಪ್‌ಗಳತ್ತ ಕರೆದೊಯ್ಯಬಹುದು. ಈ ಆ್ಯಪ್‌ಗಳು ಸೂಕ್ಷ್ಮ ಸ್ವರೂಪದ ಮಾಹಿತಿ ಅಥವಾ ಅನುಮತಿಗಳನ್ನು ಕೇಳಬಹುದು; ಇವು ವಂಚಕರಿಗೆ ನಿಮ್ಮ ಸಾಧನ ಅಥವಾ ಮಾಹಿತಿಯನ್ನು ಪ್ರವೇಶಿಸಲು ಅವಕಾಶ ಮಾಡಿಕೊಡಬಲ್ಲವು.



ಇ-ಮೇಲ್ ಭದ್ರತೆ

ಇ-ಮೇಲ್ ನಮ್ಮ ದೈನಂದಿನ ಡಿಜಿಟಲ್ ಜೀವನದ ಭಾಗವಾಗಿದೆ ಮತ್ತು ಇದು ಹೆಚ್ಚಾಗಿ ವೈಯಕ್ತಿಕ ಸಂದೇಶಗಳು, ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ ಮತ್ತು ಮಾನ್ಯವಾದ ಸೈನ್ ಅಪ್/ಲಾಗಿನ್ ವಿಧಾನವಾಗಿ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತದೆ.

ಅದಕ್ಕಾಗಿಯೇ ಇ-ಮೇಲ್ ಸುರಕ್ಷತೆ ಮುಖ್ಯವಾಗುತ್ತದೆ: ನಿಮ್ಮ ಇಮೇಲ್ ಖಾತೆಯ ವಿವರ ಬೇರೆಯವರ ಕೈವಶವಾದರೆ,ಅವರು ಈ ಮಾಹಿತಿಯನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳಬಹುದು ಅಥವಾ ನಿಮ್ಮ ಇತರ ಖಾತೆಗಳ ವಿವರವನ್ನು



ಅನುಸರಿಸಬೇಕಾದ ಉತ್ತಮ ಪದ್ಧತಿಗಳು

- ನಿಮ್ಮ ಇ-ಮೇಲ್ ಖಾತೆಯನ್ನು ರಕ್ಷಿಸಲು, ಯಾವಾಗಲೂ ಬಲವಾದ ಮತ್ತು ವಿಶಿಷ್ಟವಾದ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಬಳಸುವ ಹಾಗೂ '2-ಫ್ಯಾಕ್ಟರ್ ಅಥೆಂಟಿಕೇಶನ್' ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುವ ಅಭ್ಯಾಸವನ್ನು ಮಾಡಿಕೊಳ್ಳಿ.

- ಪ್ರತಿಕ್ರಿಯಿಸುವ ಮೊದಲು ಯಾವಾಗಲೂ ಕಳುಹಿಸುವವರ ಇ-ಮೇಲ್ ಐಡಿ ಅನ್ನು ಪರಿಶೀಲಿಸಿ. ಅಂತಹ ಅಡ್ರೆಸ್ ಅನ್ನು ದೃಢೀಕರಿಸಲು ಯಾವುದೇ ಅಸಮಂಜಸತೆಗಳು ಅಥವಾ ಸಣ್ಣ ಕಾಗುಣಿತ ದೋಷಗಳಿವೆಯೇ ಎಂದು ಗಮನಿಸಿ.

- ಲಿಂಕ್‌ಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ಅಪರಿಚಿತ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ, ವಿಶೇಷವಾಗಿ ಪೇಮೆಂಟ್‌ಗಳು, ಪಾಸ್‌ವರ್ಡ್ ರಿಸೆಟ್‌ಗಳು, ರಿಫಂಡ್‌ಗಳು ಅಥವಾ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕೇಳುವ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.

ಲಗತ್ತುಗಳ/ಅಟ್ಯಾಚ್‌ಮೆಂಟ್‌ಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ನಿಮಗೆ ತಿಳಿದಿರುವವರಿಂದ ಬಂದಿದ್ದರೂ ಸಹ, ನಿರೀಕ್ಷಿಸದ ಪಿಡಿಎಫ್‌ಗಳು, ವರ್ಡ್ ಫೈಲ್‌ಗಳು, ಎಕ್ಸೆಲ್ ಶೀಟ್‌ಗಳು ಅಥವಾ ಇತರ ಅಟ್ಯಾಚ್‌ಮೆಂಟ್‌ಗಳನ್ನು / ಲಗತ್ತುಗಳನ್ನು ತೆರೆಯಬೇಡಿ.

ನಿರೀಕ್ಷಿಸದ ವಿನಂತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ. ಒಂದು ವೇಳೆ ಯಾವುದೇ ಇಮೇಲ್ ನಿಮಗೆ ಹಣ ಪಾವತಿಸಲು, ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಅಥವಾ ತುರ್ತು ಕ್ರಮ ತೆಗೆದುಕೊಳ್ಳಲು ಕೇಳಿದರೆ, ಅದನ್ನು ಪ್ರತ್ಯೇಕ, ವಿಶ್ವಾಸಾರ್ಹ ಮಾಧ್ಯಮದ ಮೂಲಕ ಪರಿಶೀಲಿಸಿ.

ಇಮೇಲ್ನಲ್ಲಿ ನಿಮ್ಮ ಐಡಿ ಕಾರ್ಡ್, ಬ್ಯಾಂಕ್ ದಾಖಲೆಗಳು ಅಥವಾ ಯಾವುದೇ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಕಳುಹಿಸಬೇಡಿ. ತುಂಬಾ ತುರ್ತು ಇದ್ದರೆ ಮಾತ್ರ, ನಿಮಗೆ ಚೆನ್ನಾಗಿ ಗೊತ್ತಿರುವ ಮತ್ತು ನಂಬಿಕಸ್ಥರ ಇಮೇಲ್ ಐಡಿಗಳಿಗೆ ಮಾತ್ರ ಕಳುಹಿಸಿ

ನಿಮ್ಮ ಇನ್‌ಬಾಕ್ಸ್ ಅನ್ನು ವ್ಯವಸ್ಥಿತವಾಗಿ ಇಟ್ಟುಕೊಳ್ಳಿ. ನಿಮಗೆ ಇನ್ನು ಮುಂದೆ ಅಗತ್ಯವಿಲ್ಲದ ಸೂಕ್ಷ್ಮ ದಾಖಲೆಗಳು ಮತ್ತು ಫೈಲ್‌ಗಳನ್ನು ತೆಗೆದುಹಾಕಿ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್‌ಗಳು, ಪಿನ್‌ಗಳು ಅಥವಾ ಬ್ಯಾಂಕಿಂಗ್ ವಿವರಗಳನ್ನು ಸ್ಟೋರ್ ಮಾಡಲು ಇ-ಮೇಲ್ ಬಳಸಬೇಡಿ.

ಸ್ಪ್ಯಾಮ್ ಮತ್ತು ಜಂಕ್ ಇ-ಮೇಲ್‌ಗಳನ್ನು ಮ್ಯಾನೇಜ್ ಮಾಡಿ. ಕಳುಹಿಸಿದವರು ಯಾರೆಂದು ನಿಮಗೆ ತಿಳಿಯದಿದ್ದರೆ ಅಥವಾ ನೀವು ಆ ಇ-ಮೇಲ್ ಅನ್ನು ನಿರೀಕ್ಷಿಸದಿದ್ದರೆ, ಅದನ್ನು ಸ್ಪ್ಯಾಮ್ ಎಂದು ಮಾರ್ಕ್ ಮಾಡಿ ಅಥವಾ ಡಿಲೀಟ್ ಮಾಡಿ.

ನಿಮ್ಮ ಇ-ಮೇಲ್ ಡಿಫಾಲ್ಟ್ ಆಗಿ ಲಾಗ್ ಇನ್ ಆಗಿದ್ದರೆ ನಿಮ್ಮ ಡಿವೈಸ್ ಅನ್ನು ಇತರರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ. ಹಂಚಿಕೊಂಡ ಸಾಧನಗಳಿಗಾಗಿ ಆ್ಯಪ್ ಪಾಸ್‌ವರ್ಡ್ಗಳನ್ನು ಬಳಸಿ.

ಸರ್ವಿಸ್ ಪ್ರೊವೈಡರ್‌ಗಳಿಂದ ಆಟೋಜೆನರೇಟ್ ಆಗುವ ಅಪರಿಚಿತ ಲಾಗಿನ್ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್-ರಿಸೆಟ್ ರಿಕ್ವೆಸ್ಟ್ ಇ-ಮೇಲ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ. ಇದು ಅಮಾನ್ಯವಾದ ಲಾಗಿನ್ ಪ್ರಯತ್ನವನ್ನು ಸೂಚಿಸಬಹುದು. ಸಂಬಂಧಿತ ಅಕೌಂಟ್ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ರಿಸೆಟ್ ಮಾಡಿ.



ಸಾಮಾನ್ಯವಾದ ಇ-ಮೇಲ್ ಫಿಶಿಂಗ್ ವಂಚನೆಗಳು

ಫಿಶಿಂಗ್: ಇದು ನಂಬಲರ್ಹ ವ್ಯಕ್ತಿ, ಕಂಪನಿ ಅಥವಾ ಸಂಸ್ಥೆಯಂತೆ ನಟಿಸಿ, ಜನರನ್ನು ಮೋಸಗೊಳಿಸುವ ಮೂಲಕ ಅವರ ವೈಯಕ್ತಿಕ ಅಥವಾ ಆರ್ಥಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವಂತೆ ಮಾಡುವುದು, ಹಾನಿಕಾರಕ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಿಸುವುದು, ಅಸುರಕ್ಷಿತ ಲಗತ್ತುಗಳನ್ನು (ಅಟ್ಯಾಚ್‌ಮೆಂಟ್) ತೆರೆಯುವಂತೆ ಮಾಡುವುದು ಅಥವಾ ಹಣ ಪಾವತಿಸುವಂತೆ ಪ್ರೇರೇಪಿಸುವ ಒಂದು ವಿಧಾನವಾಗಿದೆ.

ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಜನರನ್ನು ಮೋಸಗೊಳಿಸಲು ಇ-ಮೇಲ್ ಅನ್ನು ಬಳಸುವ ಅತ್ಯಂತ ಸಾಮಾನ್ಯ ವಿಧಾನಗಳಲ್ಲಿ ಇದು ಒಂದಾಗಿದೆ. ನಕಲಿ ಇ-ಮೇಲ್ ನಿಮ್ಮ ಬ್ಯಾಂಕ್, ಕೊರಿಯರ್ ಕಂಪನಿ, ಸರ್ಕಾರಿ ಇಲಾಖೆ ಅಥವಾ ಕುಟುಂಬದ ಸದಸ್ಯರಿಂದ ಬಂದಂತೆ ಕಾಣಿಸಬಹುದು; ಅಲ್ಲದೆ, ಯಾವುದೇ ಪರಿಶೀಲನೆ ನಡೆಸದೆಯೇ ನೀವು ತಕ್ಷಣ ಕ್ರಮ ಕೈಗೊಳ್ಳುವಂತೆ ಮಾಡುವ ತುರ್ತು ಪರಿಸ್ಥಿತಿಯ ಭ್ರಮೆಯನ್ನು ಇದು ಸೃಷ್ಟಿಸಬಹುದು.

ಫಿಶಿಂಗ್' (phishing) ನ ಕೆಲವು ಸಾಮಾನ್ಯ ರೂಪಗಳು ಮತ್ತು ದೈನಂದಿನ ಸನ್ನಿವೇಶಗಳಲ್ಲಿ ಅವು ಹೇಗೆ ಕಾಣಿಸಿಕೊಳ್ಳಬಹುದು



ನಕಲಿ (ಫೇಕ್) ಬ್ಯಾಂಕ್/ ಖಾತೆಯ ಇ-ಮೇಲ್ ಅಪ್‌ಡೇಟ್ ಮಾಡಿ

ಒಂದು ನಕಲಿ ಇ-ಮೇಲ್ ನಿಮ್ಮ ಕೆವೈಸಿ, ಅಕೌಂಟ್, ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಅಥವಾ ಪಾಸ್‌ವರ್ಡ್ ಅಪ್‌ಡೇಟ್ ಮಾಡಬೇಕೆಂದು ಕೇಳುತ್ತದೆ ಮತ್ತು ಹಾಗೆ ಮಾಡದಿದ್ದರೆ ಅಕೌಂಟ್ ಬ್ಲಾಕ್ ಮಾಡುವುದಾಗಿ ಬೆದರಿಕೆ ಹಾಕಬಹುದು.

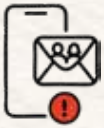
ಅಂತಹ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ ಅಥವಾ ಯಾವುದೇ ಸೂಕ್ಷ್ಮ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ. ನಿಮ್ಮ ಬ್ಯಾಂಕ್‌ನೊಂದಿಗೆ ವೈಯಕ್ತಿಕವಾಗಿ ಪರಿಶೀಲಿಸಿ.



ನಕಲಿ (ಫೇಕ್) ಡೆಲಿವರಿ/ ರಿಫಂಡ್ ಇ-ಮೇಲ್

ನಿಮ್ಮ ಪಾರ್ಸೆಲ್ ತಡವಾಗಿದೆ, ಮರುಪಾವತಿ ಬಾಕಿ ಇದೆ ಅಥವಾ ಪಾವತಿಯ ಅಗತ್ಯವಿದೆ ಎಂದು ನಕಲಿ ಇ-ಮೇಲ್ ನಲ್ಲಿ ಇರುತ್ತದೆ.

ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ ಅಥವಾ ಹಣ ಪಾವತಿಸಬೇಡಿ; ಕಂಪನಿಯ ಅಧಿಕೃತ ಆ್ಯಪ್ ಅಥವಾ ವೆಬ್‌ಸೈಟ್ ಮೂಲಕ ನಿಮ್ಮ ಆರ್ಡರ್ ಅಥವಾ ರಿಫಂಡ್ ಅನ್ನು ಪರಿಶೀಲಿಸಿ.



ನಕಲಿ (ಫೇಕ್) ಕುಟುಂಬದವರ/ಪರಿಚಿತ ವ್ಯಕ್ತಿಯ ಇ-ಮೇಲ್

ಕೆಲವು ಇ-ಮೇಲ್‌ಗಳು ನಿಮ್ಮ ಕುಟುಂಬದ ಸದಸ್ಯರು, ಸ್ನೇಹಿತರು ಅಥವಾ ನಿಮಗೆ ತಿಳಿದಿರುವ ಯಾರೊಬ್ಬರಿಂದ ಬಂದಂತೆ ಕಾಣಿಸಬಹುದು ಮತ್ತು ಹಣ, ಮಾಹಿತಿ ಅಥವಾ ತುರ್ತು ಸಹಾಯಕ್ಕಾಗಿ ಕೇಳಬಹುದು.

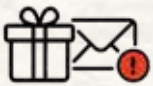
ಅಂತಹ ವಿನಂತಿಗಳ ಬಗ್ಗೆ ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಅವರಿಗೆ ನೇರವಾಗಿ ಕಾಲ್ ಮಾಡಿ.



ನಕಲಿ (ಫೇಕ್) ಸರ್ಕಾರಿ ಇ-ಮೇಲ್

ಕೆಲವು ಇ-ಮೇಲ್‌ಗಳು ಸರ್ಕಾರಿ ಇಲಾಖೆಯಿಂದ ಬಂದಿದೆ ಎಂದು ಹೇಳಿಕೊಳ್ಳಬಹುದು ಮತ್ತು ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಅಪ್‌ಡೇಟ್ ಮಾಡಲು, ದಂಡ/ ಚಲನ್ ಪಾವತಿಸಲು ಅಥವಾ ದಾಖಲೆಗಳನ್ನು ಸಲ್ಲಿಸಲು ಕೇಳಬಹುದು.

ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ ಅಥವಾ ದಾಖಲೆಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ; ಇಲಾಖೆಯ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್ ಮೂಲಕ ಪರಿಶೀಲಿಸಿ.



ನಕಲಿ (ಫೇಕ್) ಕೊಡುಗೆ/ ಬಹುಮಾನಗಳ ಇ-ಮೇಲ್

ಕೆಲವು ಇ-ಮೇಲ್‌ಗಳು ನಿಮಗೆ ಬಹುಮಾನ, ಕ್ಯಾಶ್‌ಬ್ಯಾಕ್, ಗಿಫ್ಟ್ ಅಥವಾ ಡಿಸ್ಕೌಂಟ್ ನೀಡುವ ಭರವಸೆ ನೀಡಬಹುದು ಮತ್ತು ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಲು, ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಅಥವಾ ಶುಲ್ಕ ಪಾವತಿಸಲು ಕೇಳಬಹುದು.

ನಿರೀಕ್ಷಿಸದ ಆಫರ್‌ಗಳ ಮೇಲೆ ಕ್ರಮ ತೆಗೆದುಕೊಳ್ಳಬೇಡಿ; ಕಂಪನಿಯ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್ ಅಥವಾ ಆ್ಯಪ್ ಮೂಲಕ ಅವುಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.





ಯಾವಾಗಲೂ ನೆನಪಿಡಿ

ಒಬ್ಬ ಸ್ಕ್ಯಾಮರ್ ನಿಮ್ಮನ್ನು ಸಂಪರ್ಕಿಸಲು ವಿಭಿನ್ನ ಮಾರ್ಗಗಳನ್ನು ಬಳಸಬಹುದು, ಆದರೆ ಅವರ ತಂತ್ರವು ಹೆಚ್ಚಾಗಿ ಒಂದೇ ಆಗಿರುತ್ತದೆ; ನೀವು ನಂಬುವ ವ್ಯಕ್ತಿಯಂತೆ ನಟಿಸುವುದು ಮತ್ತು ನಿಮ್ಮನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವಂತೆ, ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವಂತೆ ಅಥವಾ ಪಾವತಿ ಮಾಡುವಂತೆ ಮಾಡುವುದು.

ಫಿಶಿಂಗ್

ಇ-ಮೇಲ್ ಮೂಲಕ

"ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅಕೌಂಟ್ ಬ್ಲಾಕ್ ಆಗುತ್ತದೆ. ನಿಮ್ಮ ಕೆವೈಸಿ ಅನ್ನು ಈಗಲೇ ಅಪ್‌ಡೇಟ್ ಮಾಡಿ."

ಸ್ಮಿಶಿಂಗ್

ಎಸ್ಎಮ್ಎಸ್/ವಾಟ್ಸಾಪ್ ಮೂಲಕ

"ನಿಮ್ಮ ಕೆವೈಸಿ ಅವಧಿ ಮುಗಿದಿದೆ. ಅದನ್ನು ಅಪ್‌ಡೇಟ್ ಮಾಡಲು ಇಲ್ಲಿ ಕ್ಲಿಕ್ ಮಾಡಿ."

ವಿಷಿಂಗ್

ಫೋನ್ ಕಾಲ್ ಮೂಲಕ

"ನಾನು ನಿಮ್ಮ ಬ್ಯಾಂಕ್‌ನಿಂದ ಕರೆ ಮಾಡುತ್ತಿದ್ದೇನೆ. ದಯವಿಟ್ಟು ನಿಮ್ಮ ಖಾತೆಯ ವಿವರಗಳನ್ನು ಪರಿಶೀಲಿಸಿ."

ಕ್ವಿಶಿಂಗ್

ಕ್ಯೂಆರ್ ಕೋಡ್ ಮೂಲಕ

"ನಿಮ್ಮ ರಿಫಂಡ್ ಪಡೆಯಲು ಈ ಕ್ಯೂಆರ್ ಕೋಡ್ ಸ್ಕ್ಯಾನ್ ಮಾಡಿ."

ಚಾನೆಲ್ ಬದಲಾಗಬಹುದು, ಆದರೆ ಎಚ್ಚರಿಕೆಯ ಚಿಹ್ನೆಗಳು ಮಾತ್ರ ಹಾಗೆಯೇ ಇರುತ್ತವೆ.



ಸ್ವಲ್ಪ ತಾಳಿ → **ಪರಿಶೀಲಿಸಿ** → **ನಂತರ ಕ್ರಮ ಕೈಗೊಳ್ಳಿ**

ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಸುರಕ್ಷತೆ

ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳು ನಮಗೆ ನಮ್ಮ ಕುಟುಂಬದವರು, ಸಹೋದ್ಯೋಗಿಗಳು, ಸ್ನೇಹಿತರು ಮತ್ತು ಸಮುದಾಯದ ಗುಂಪುಗಳೊಂದಿಗೆ ಸಂಪರ್ಕದಲ್ಲಿರಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ. ನಮಗೆ ತಿಳಿದಿರುವ ಮತ್ತು ನಂಬುವ ಜನರಿಂದ ಫೋಟೋಗಳು, ಸಂದೇಶಗಳು, ವೀಡಿಯೊಗಳು ಮತ್ತು ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಮತ್ತು ಸ್ವೀಕರಿಸಲು ನಾವು ಇದನ್ನು ಬಳಸುತ್ತೇವೆ. ಆದರೆ ಆನ್‌ಲೈನ್ ಕಂಟೆಂಟ್ ಯಾವಾಗಲೂ ಅಸಲಿಯಾಗಿರುವುದಿಲ್ಲ ಮತ್ತು ಪರಿಚಿತ ಅಕೌಂಟ್‌ಗಳು ಕೂಡ ನಕಲಿ ಅಥವಾ ಹ್ಯಾಕ್ ಆಗಿರಬಹುದು. ನಾವು ಹಂಚಿಕೊಳ್ಳುವ ವಿಷಯಗಳು ನಮ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಕೂಡ ಬಹಿರಂಗಪಡಿಸಬಹುದು.

ಅದಕ್ಕಾಗಿಯೇ ಸಾಮಾಜಿಕ ಜಾಲತಾಣದ ಸುರಕ್ಷತೆ ಮುಖ್ಯವಾಗುತ್ತದೆ: ಯಾವುದನ್ನು ನಂಬಬೇಕು, ಯಾವುದನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಕು, ಯಾವುದನ್ನು ಫಾರ್ವರ್ಡ್ ಮಾಡಬೇಕು ಮತ್ತು ನಮ್ಮ ಮಾಹಿತಿಯನ್ನು ಯಾರು ನೋಡಬಹುದು ಎಂದು ತಿಳಿಯಲು ಇದು ನಮಗೆ ಸಹಾಯ ಮಾಡುತ್ತದೆ.

ಅನುಸರಿಸಬೇಕಾದ ಅತ್ಯುತ್ತಮ ಅಭ್ಯಾಸಗಳು

- ನಿಮ್ಮ ಪ್ರೈವೆಸಿ ಸೆಟ್ಟಿಂಗ್ಸ್ ಅನ್ನು ನಿಯಮಿತವಾಗಿ ಚೆಕ್ ಮಾಡಿ ಮತ್ತು ನಿಮ್ಮ ಪ್ರೊಫೈಲ್, ಪೋಸ್ಟ್‌ಗಳು, ಫೋಟೋಗಳು ಮತ್ತು ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಯಾರು ನೋಡಬಹುದು ಎಂಬುದನ್ನು ಆಯ್ಕೆ ಮಾಡಿ.

- ಪೋಸ್ಟ್ ಮಾಡುವ ಮೊದಲು ಯೋಚಿಸಿ ಮತ್ತು ಫೋಟೋ ಅಥವಾ ಪೋಸ್ಟ್ ನಿಮ್ಮ ಮನೆಯ ವಿಳಾಸ, ಲೊಕೇಶನ್, ಫೋನ್ ನಂಬರ್, ಟ್ರಾವೆಲ್ ಪ್ಲಾನ್ ಗಳು, ಡಾಕ್ಯುಮೆಂಟ್ ಗಳು ಅಥವಾ ಇತರ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಬಹಿರಂಗಪಡಿಸುತ್ತದೆಯೇ ಎಂದು ಪರಿಶೀಲಿಸಿ.

- ನಂಬುವ ಅಥವಾ ಫಾರ್ವರ್ಡ್ ಮಾಡುವ ಮೊದಲು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಆಶ್ಚರ್ಯಕರವಾದ ವಿಷಯಗಳನ್ನು ವಿಶ್ವಾಸಾರ್ಹ ಅಥವಾ ಅಧಿಕೃತ ಮೂಲದ ಮೂಲಕ ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

- ಫ್ರೆಂಡ್ ರಿಕ್ವೆಸ್ಟ್‌ಗಳನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಅಕ್ಸೆಪ್ಟ್ ಮಾಡಿ ಮತ್ತು ನಿಮಗೆ ತಿಳಿದಿರುವ ಅಥವಾ ನೀವು ವೆರಿಫೈ ಮಾಡಬಹುದಾದ ಜನರೊಂದಿಗೆ ಮಾತ್ರ ಕನೆಕ್ಟ್ ಆಗಿ.

- ನಿಮಗೆ ಪರಿಚಯವಿರುವವರಿಂದ ಬರುವ ಅಸಾಮಾನ್ಯ ಸಹಾಯ ಅಥವಾ ಹಣದ ವಿನಂತಿಗಳನ್ನು, ನಿಮ್ಮ ಬಳಿ ಈಗಾಗಲೇ ಇರುವ ಅವರ ನಂಬರ್‌ಗೆ ನೇರವಾಗಿ ಕರೆ ಮಾಡುವ ಮೂಲಕ ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ

- ನೀವು ಅವುಗಳನ್ನು ಪರಿಶೀಲಿಸದ ಹೊರತು ಬಹುಮಾನಗಳು, ಉಚಿತ ಉಡುಗೊರೆಗಳು, ನಂಬಲಾಗದ ರಿಯಾಯಿತಿಗಳು ಅಥವಾ ಹೂಡಿಕೆಯ ಅವಕಾಶಗಳನ್ನು ನೀಡುವ ಲಿಂಕ್‌ಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ.

- ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಗೌಪ್ಯವಾಗಿಡಿ ಮತ್ತು ಒಟಿಪಿಗಳು, ಪಿನ್‌ಗಳು, ಪಾಸ್‌ವರ್ಡ್‌ಗಳು, ಬ್ಯಾಂಕಿಂಗ್ ವಿವರಗಳು, ಐಡಿಗಳು ಅಥವಾ ಪ್ರಮುಖ ದಾಖಲೆಗಳನ್ನು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದ ಮೂಲಕ ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

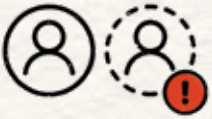
- ಗೆಳೆಯನ ಗೆಳೆಯ, ದೂರದ ಸಂಬಂಧಿ ಅಥವಾ ಕುಟುಂಬದ ಸ್ನೇಹಿತರಂತೆ ನಟಿಸುವ ಅಕೌಂಟ್‌ಗಳಿಂದ ಬರುವ ಡೈರೆಕ್ಟ್ ಮೆಸೇಜ್‌ಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ. ಯಾವಾಗಲೂ ಸಂಬಂಧಪಟ್ಟ ಸ್ನೇಹಿತ ಅಥವಾ ಕುಟುಂಬದ ಸದಸ್ಯರಿಂದ ಇದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

- ಒತ್ತಡ ಹೇರುವ, ಬೆದರಿಕೆ ಹಾಕುವ ಅಥವಾ ನಿಮಗೆ ಅಸಮಾಧಾನ ಉಂಟುಮಾಡುವ ಸಂಭಾಷಣೆಗಳನ್ನು ಮುಂದುವರಿಸುವ ಬದಲು ಅನುಮಾನಾಸ್ಪದ ಅಕೌಂಟ್‌ಗಳನ್ನು ಬ್ಲಾಕ್ ಮಾಡಿ ಮತ್ತು ರಿಪೋರ್ಟ್ ಮಾಡಿ.

- ನೆನಪಿಡಿ, ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಶೇರಿಂಗ್ ಖಾಸಗಿಯಾಗಿರುವುದಿಲ್ಲ, ಏಕೆಂದರೆ ಖಾಸಗಿ ಮೆಸೇಜ್‌ಗಳು, ಫೋಟೋಗಳು ಮತ್ತು ಪೋಸ್ಟ್‌ಗಳನ್ನು ಸೇವ್ ಮಾಡಬಹುದು ಅಥವಾ ಫಾರ್ವರ್ಡ್ ಮಾಡಬಹುದು.



ಸಾಮಾಜಿಕ ಜಾಲತಾಣ-ಸಂಬಂಧಿತ ವಂಚನೆಗಳು ಸಾಮಾನ್ಯವಾಗಿ ಹೇಗೆ ನಡೆಯುತ್ತವೆ



ನಕಲಿ (ಫೇಕ್) ಫ್ಯಾಮಿಲಿ/ಫ್ರೆಂಡ್ ಅಕೌಂಟ್

ವಂಚಕರು, ನಿಮ್ಮ ಕುಟುಂಬದ ಸದಸ್ಯರು ಅಥವಾ ಸ್ನೇಹಿತರ ಹೆಸರು ಮತ್ತು ಫೋಟೋ ಬಳಸಿ ನಕಲಿ ಖಾತೆಯನ್ನು ತೆರೆದು, ಅದರ ಮೂಲಕ ಹಣ ಅಥವಾ ಇನ್ಯಾವುದೇ ತುರ್ತು ಸಹಾಯ ಕೇಳಿ ಸಂದೇಶ ಕಳುಹಿಸಬಹುದು. ಈ ರೀತಿಯ ವಿನಂತಿಯು ಅಸಾಮಾನ್ಯ ಅಥವಾ ತುರ್ತು ಎಂದು ನಿಮಗೆ ಅನಿಸಿದರೆ, ಯಾವುದೇ ಕ್ರಮ ತೆಗೆದುಕೊಳ್ಳುವ ಮುನ್ನ, ನಿಮ್ಮ ಬಳಿ ಮೊದಲೇ ಇರುವ ಅವರ ಅಧಿಕೃತ ಸಂಖ್ಯೆಗೆ ನೇರವಾಗಿ ಕರೆ ಮಾಡಿ ವಿಷಯವನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

ತಪ್ಪು ಅಥವಾ ದಾರಿತಪ್ಪಿಸುವ ಮಾಹಿತಿ



ಸರ್ಕಾರಿ ಆದೇಶ, ಹೊಸ ಆರೋಗ್ಯ ಸಲಹೆ, ಹಣಕಾಸಿನ ಅವಕಾಶ, ಅಥವಾ ತುರ್ತು ಪರಿಸ್ಥಿತಿಯ ಕುರಿತಂತೆ ಕೆಲವು ಪೋಸ್ಟ್‌ಗಳು, ಸಂದೇಶಗಳು ಅಥವಾ ವೀಡಿಯೊಗಳು ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಹರಿದಾಡುತ್ತಿರುತ್ತವೆ. ಇವುಗಳನ್ನು ಆದಷ್ಟು ಬೇಗ ಎಲ್ಲರಿಗೂ ಹಂಚಿಕೊಳ್ಳಿ (ಫಾರ್ವರ್ಡ್ ಮಾಡಿ) ಎಂದು ನಿಮ್ಮನ್ನು ಕೇಳಿಕೊಳ್ಳಬಹುದು ಅಥವಾ ಕೆಲವೊಮ್ಮೆ ಶುಲ್ಕ ಪಾವತಿಸಲು ಸಹ ಸೂಚಿಸಬಹುದು. ನೆನಪಿಡಿ: ಒಂದು ಸುದ್ದಿ ಹೆಚ್ಚು ಜನರ ನಡುವೆ ಹರಿದಾಡುತ್ತಿದೆ (ವೈರಲ್ ಆಗಿದೆ) ಎಂದ ಮಾತ್ರಕ್ಕೆ ಅದು ಸತ್ಯವಾಗಿರುವುದಿಲ್ಲ. ಆದ್ದರಿಂದ, ಯಾವುದೇ ಮಾಹಿತಿಯನ್ನು ನಂಬುವ ಅಥವಾ ಬೇರೆಯವರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವ ಮುನ್ನ, ಅದರ ನಿಜಾಂಶವನ್ನು ಅಧಿಕೃತ ಮೂಲಗಳಿಂದ (ಉದಾ: ಸರ್ಕಾರಿ ವೆಬ್‌ಸೈಟ್‌ಗಳು, ವಿಶ್ವಾಸಾರ್ಹ ಮಾಧ್ಯಮಗಳು) ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.



ನಕಲಿ ಬಹುಮಾನ/ ಕೊಡುಗೆಗಳು (ಫೇಕ್ ಪ್ರೈಜ್/ಗಿವ್ ಅವೇ/ಆಫರ್)

ನೀವು ಬಹುಮಾನ ಗೆದ್ದಿದ್ದೀರಿ," "ನಿಮಗೊಂದು ವಿಶೇಷ ಕೊಡುಗೆ ಲಭ್ಯವಿದೆ," ಅಥವಾ "ನೀವು ಉಡುಗೊರೆಗೆ ಆಯ್ಕೆಯಾಗಿದ್ದೀರಿ" ಎಂಬಂತಹ ಆಕರ್ಷಕ ಸಂದೇಶಗಳು, ಪೋಸ್ಟ್‌ಗಳು ಅಥವಾ ಪೇಜ್‌ಗಳು ನಿಮಗೆ ಕಾಣಿಸಬಹುದು. ಇವುಗಳು ಸಾಮಾನ್ಯವಾಗಿ ಒಂದು ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಲು, ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಯ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಅಥವಾ ಪ್ರೊಸೆಸಿಂಗ್ ಶುಲ್ಕ ಪಾವತಿಸಲು ನಿಮ್ಮನ್ನು ಪ್ರೇರೇಪಿಸುತ್ತವೆ. ಇಂತಹ ಯಾವುದೇ ಸಂದೇಶಕ್ಕೆ ಪ್ರತಿಕ್ರಿಯಿಸುವ ಮೊದಲು, ಆ ಕೊಡುಗೆಯ ಸತ್ಯಾಸತ್ಯತೆಯನ್ನು ಸಂಬಂಧಪಟ್ಟ ಸಂಸ್ಥೆಯ ಅಧಿಕೃತ ಜಾಲತಾಣ (ವೆಬ್‌ಸೈಟ್) ಅಥವಾ ಆ್ಯಪ್‌ಗೆ ನೇರವಾಗಿ ಭೇಟಿ ನೀಡಿ ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ



ಯಾವಾಗಲೂ ನೆನಪಿಡಿ

ನಿಮ್ಮ ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಪೋಸ್ಟ್‌ಗಳಿಂದ ವಿವರಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಸ್ಕ್ಯಾಮರ್‌ಗಳು ತಮ್ಮ ಮೆಸೇಜ್‌ಗಳು ವೈಯಕ್ತಿಕವಾಗಿ ಮತ್ತು ನಂಬಲರ್ಹವಾಗಿ ಕಾಣುವಂತೆ ಮಾಡಬಹುದು. ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಸಾರ್ವಜನಿಕವಾಗಿ ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ.

ಗೌಪ್ಯತೆಗೆ (ಪ್ರೈವೆಸಿ) ಸಂಬಂಧಿಸಿದ ಉತ್ತಮ ಅಭ್ಯಾಸಗಳು



ನಿಮಗೆ ಇದರ ಅರಿವಿಲ್ಲದಿರಬಹುದು, ಆದರೆ ಆಪ್‌ಗಳನ್ನು ಬಳಸುವಾಗ, ಆನ್‌ಲೈನ್ ಶಾಪಿಂಗ್ ಮಾಡುವಾಗ, ಪೇಮೆಂಟ್‌ಗಳನ್ನು ಮಾಡುವಾಗ, ಟ್ರಾವೆಲ್ ಬುಕಿಂಗ್ ಮಾಡುವಾಗ, ಗ್ರೂಪ್‌ಗಳಿಗೆ ಸೇರುವಾಗ, ಫಾರ್ಮ್‌ಗಳನ್ನು ಭರ್ತಿ ಮಾಡುವಾಗ ಅಥವಾ ಸರ್ವಿಸ್‌ಗಳಿಗೆ ಸೈನ್ ಅಪ್ ಮಾಡುವಾಗ ನಾವು ಪ್ರತಿದಿನ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುತ್ತೇವೆ. ಇದರಲ್ಲಿ ನಮ್ಮ ಹೆಸರು, ಫೋನ್ ನಂಬರ್, ಅಡ್ರೆಸ್, ಫೋಟೋಗಳು, ಐಡಿಗಳು, ಬ್ಯಾಂಕ್ ಖಾತೆಗಳ ಮಾಹಿತಿಗಳು (ಫೈನಾನ್ಶಿಯಲ್ ಇನ್ಫರ್ಮೇಷನ್) ಮತ್ತು ನಮ್ಮ ಕುಟುಂಬದ ವಿವರಗಳು ಇರಬಹುದು. ಮಾಹಿತಿ ಹಂಚಿಕೊಳ್ಳುವುದು ಹಲವು ಬಾರಿ ಅಗತ್ಯವಾಗಿರುತ್ತದೆ, ಆದರೆ ಅಗತ್ಯಕ್ಕಿಂತ ಹೆಚ್ಚು ಹಂಚಿಕೊಳ್ಳುವುದು ಇತರರಿಗೆ ಅವರಿಗೆ ಬೇಡದ ಮಾಹಿತಿಯನ್ನು ನೀಡಬಹುದು.

ಉತ್ತಮ ಪ್ರೈವೆಸಿ ಹವ್ಯಾಸಗಳು ನೀವು ಏನನ್ನು, ಯಾರೊಂದಿಗೆ ಮತ್ತು ಏಕೆ ಹಂಚಿಕೊಳ್ಳುತ್ತೀರಿ ಎಂಬುದರ ಮೇಲೆ ನಿಯಂತ್ರಣ ಹೊಂದಲು ನಿಮಗೆ ಸಹಾಯ ಮಾಡುತ್ತವೆ.



ವೈಯುಕ್ತಿಕ ಮಾಹಿತಿ (ಪರ್ಸನಲ್ ಇನ್ಫರ್ಮೇಷನ್) ಅಂದರೆ ಏನು ಎಂದು ತಿಳಿದುಕೊಳ್ಳಿ

- ಹೆಸರು, ಫೋನ್ ನಂಬರ್ ಮತ್ತು ಇ-ಮೇಲ್
- ಮನೆಯ ವಿಳಾಸ ಮತ್ತು ಜನ್ಮ ದಿನಾಂಕ
- ಆಧಾರ್, ಪ್ಯಾನ್, ಪಾಸ್‌ಪೋರ್ಟ್, ವೋಟರ್ ಐಡಿ ಮತ್ತು ಇತರ ಗುರುತಿನ ದಾಖಲೆಗಳು
- ಬ್ಯಾಂಕ್ ಸ್ಟೇಟ್‌ಮೆಂಟ್‌ಗಳು ಮತ್ತು ಹಣಕಾಸಿನ ಮಾಹಿತಿ
- ಫೋಟೋಗಳು ಮತ್ತು ವೀಡಿಯೊಗಳು
- ಸ್ಥಳದ ಮಾಹಿತಿ
- ಕುಟುಂಬದ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ (ಜೀವನ ಸಂಗಾತಿ, ಮಕ್ಕಳು, ಇತರರು)



ಗೌಪ್ಯತೆಗೆ (ಪ್ರೈವೆಸಿ) ಸಂಬಂಧಿಸಿದ ಉತ್ತಮ ಅಭ್ಯಾಸಗಳು

ಅಗತ್ಯವಿದ್ದಾಗ ಮಾತ್ರ ಐಡಿಗಳು ಮತ್ತು ಪ್ರಮುಖ ದಾಖಲೆಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಿ. ಅವು ಯಾರಿಗೆ ಬೇಕು, ಏಕೆ ಬೇಕು ಎಂದು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಅವುಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ವಿಶ್ವಾಸಾರ್ಹ ಚಾನಲ್ ಬಳಸಿ.

ಪೋಸ್ಟ್ ಮಾಡುವ ಅಥವಾ ಫಾರ್ವರ್ಡ್ ಮಾಡುವ ಮೊದಲು ಫೋಟೋಗಳನ್ನು ಚೆಕ್ ಮಾಡಿ. ಫೋಟೋದಲ್ಲಿ ಕಾಣುವ ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳು, ಅಡ್ರೆಸ್‌ಗಳು, ವೆಹಿಕಲ್ ನಂಬರ್‌ಗಳು, ಬಿಲ್‌ಗಳು, ಲೊಕೇಶನ್‌ಗಳು ಅಥವಾ ಇತರ ಪರ್ಸನಲ್ ಇನ್ಫರ್ಮೇಶನ್ ಅನ್ನು ಶೇರ್ ಮಾಡಬೇಡಿ ಅಥವಾ ಮಾಸ್ಕ್ ಮಾಡಿ.

ಸಮುದಾಯದ ಗುಂಪುಗಳು (ಕಮ್ಯುನಿಟಿ ಗ್ರೂಪ್ಸ್) ಸಾರ್ವಜನಿಕ ವೇದಿಕೆಗಳಿದ್ದಂತೆ; ಅಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳುವ ಯಾವುದೇ ವಿಷಯ ಖಾಸಗಿಯಾಗಿ ಉಳಿಯುವುದಿಲ್ಲ. ಕುಟುಂಬ, ನಿವಾಸಿಗಳ ಸಂಘ (RWA) ಅಥವಾ ಇನ್ಯಾವುದೇ ಗುಂಪಿನಲ್ಲಿ ನೀವು ಹಂಚಿಕೊಳ್ಳುವ ಸಂದೇಶಗಳು, ಫೋಟೋಗಳು ಮತ್ತು ದಾಖಲೆಗಳನ್ನು ಗುಂಪಿನಲ್ಲಿರುವ ಯಾರಾದರೂ ತಮ್ಮ ಬಳಿ ಉಳಿಸಿಕೊಳ್ಳಬಹುದು (ಸೇವ್), ಬೇರೆಯವರಿಗೆ ಕಳುಹಿಸಬಹುದು (ಫಾರ್ವರ್ಡ್) ಅಥವಾ ಸುಳ್ಳು ಸುದ್ದಿಗಳನ್ನು ಹರಡಲು ದುರ್ಬಳಕೆ ಮಾಡಿಕೊಳ್ಳಬಹುದು.

- ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವ ಮೊದಲು ಸ್ವೀಕರಿಸುವವರನ್ನು ವೆರಿಫೈ ಮಾಡಿ. ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳು ಅಥವಾ ಇತರ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕಳುಹಿಸುವ ಮೊದಲು ಹೆಸರು, ಫೋನ್ ನಂಬರ್ ಅಥವಾ ಇ-ಮೇಲ್ ಅಡ್ರೆಸ್ ಅನ್ನು ಚೆಕ್ ಮಾಡಿ.

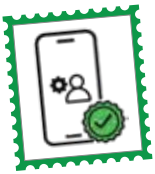
- ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಸಾರ್ವಜನಿಕವಾಗಿ ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ. ನಿಮ್ಮ ಫೋನ್ ನಂಬರ್, ಮನೆಯ ವಿಳಾಸ, ಜನ್ಮ ದಿನಾಂಕ, ಕುಟುಂಬದ ವಿವರಗಳು ಅಥವಾ ದೈನಂದಿನ ದಿನಚರಿಯನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪೋಸ್ಟ್ ಮಾಡಬೇಡಿ.

- ಇತರರ ಗೌಪ್ಯತೆಯನ್ನು ಗೌರವಿಸಿ. ಡಿಜಿಟಲ್ ಮಾಧ್ಯಮದಲ್ಲಿ ಬೇರೊಬ್ಬರ ಫೋಟೋ, ಕಾರ್ಯಕ್ರಮದ ವಿವರ ಅಥವಾ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಪೋಸ್ಟ್ ಮಾಡುವ ಅಥವಾ ಫಾರ್ವರ್ಡ್ ಮಾಡುವ ಮೊದಲು ಅನುಮತಿ ಪಡೆಯಿರಿ.

- ಸ್ಥಳ ಮತ್ತು ಪ್ರಯಾಣದ ಮಾಹಿತಿಯ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ನಿಮ್ಮ ಲೈವ್ ಲೊಕೇಶನ್, ನಿಯಮಿತ ದಿನಚರಿ ಅಥವಾ ನೀವು ಮನೆಯಿಂದ ಯಾವಾಗ ಹೊರಗಿರುತ್ತೀರಿ ಎಂದು ತಿಳಿಸುವ ಪ್ಲಾನ್‌ಗಳನ್ನು ಸಾರ್ವಜನಿಕವಾಗಿ ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ.

- ನಿಮಗೆ ಇನ್ನು ಮುಂದೆ ಅಗತ್ಯವಿಲ್ಲದ ಮತ್ತು ಬಳಕೆಯಲ್ಲಿಲ್ಲದ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ನಿಯಮಿತವಾಗಿ ಅಳಿಸಿಹಾಕಿ. ಉದಾಹರಣೆಗೆ, ನಿಮ್ಮ ಫೋನ್, ಚಾಟ್‌ಗಳು ಮತ್ತು ಇ-ಮೇಲ್‌ಗಳಲ್ಲಿರುವ ಹಳೆಯ ದಾಖಲೆಗಳು (ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳು), ಸ್ಕ್ರೀನ್‌ಶಾಟ್‌ಗಳು, ಡೌನ್‌ಲೋಡ್ ಮಾಡಿದ ಗುರುತಿನ ಚೀಟಿಗಳು (ಐಡಿಗಳು) ಹಾಗೂ ಇತರ ಅನಗತ್ಯ ಕಡತಗಳನ್ನು (ಫೈಲ್‌ಗಳನ್ನು) ಹುಡುಕಿ ತೆಗೆದುಹಾಕಿ.

- "ಅಗ್ರೀ (Agree)" ಅಥವಾ "ಅಕ್ಸೆಪ್ಟ್ (Accept)" ಕ್ಲಿಕ್ ಮಾಡುವ ಮೊದಲು ಪರಿಶೀಲಿಸಿ. ಯಾವ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸಲಾಗುತ್ತಿದೆ ಮತ್ತು ಯಾವ ಉದ್ದೇಶಕ್ಕಾಗಿ ಎಂದು ಅರ್ಥಮಾಡಿಕೊಳ್ಳಿ ಮತ್ತು ಕೇವಲ ಸೇವೆಯನ್ನು ಪಡೆಯಲು ಹೆಚ್ಚಿನ ಮಾಹಿತಿಯನ್ನು ನೀಡುವುದನ್ನು ತಪ್ಪಿಸಿ.



ನಿಮ್ಮ ಗೌಪ್ಯತಾ ಅಳವಡಿಕೆಗಳನ್ನು (ಪ್ರೈವೆಸಿ ಸೆಟ್ಟಿಂಗ್ಸ್) ಚೆಕ್ ಮಾಡಿ

ನಿಮ್ಮ ಪ್ರೈವೆಸಿ ಸೆಟ್ಟಿಂಗ್ಸ್ ನಿಮ್ಮ ಮಾಹಿತಿಯನ್ನು ಯಾರು ನೋಡಬಹುದು ಮತ್ತು ಯಾವ ಆಪ್ಸ್ ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಆಕ್ಸೆಸ್ ಮಾಡಬಹುದು ಎಂಬುದನ್ನು ಕಂಟ್ರೋಲ್ ಮಾಡುತ್ತವೆ. ಈ ಸೆಟ್ಟಿಂಗ್ಸ್ ಅನ್ನು ನಿಯಮಿತವಾಗಿ ಚೆಕ್ ಮಾಡಿ ಮತ್ತು ಪರಿಶೀಲಿಸಿ (ರಿವ್ಯೂ) ಮಾಡಿ.

ಸಾಮಾಜಿಕ ಜಾಲತಾಣಕ್ಕಾಗಿ



ಸಾಧ್ಯವಾದಷ್ಟು ನಿಮ್ಮ ಪ್ರೊಫೈಲ್ ಅನ್ನು ಪ್ರೈವೇಟ್ ಆಗಿ ಇರಿಸಿ.



ನಿಮ್ಮ ಬಯೋದಲ್ಲಿ ನಿಮ್ಮ ಪೂರ್ಣ ವಿಳಾಸ, ಫೋನ್ ನಂಬರ್, ಇ-ಮೇಲ್ ಅಥವಾ ಹುಟ್ಟಿದ ದಿನಾಂಕವನ್ನು ಸೇರಿಸಬೇಡಿ.



ನಿಮ್ಮ ಪೋಸ್ಟ್‌ಗಳು, ಫೋಟೋಗಳು ಮತ್ತು ಸ್ಟೋರಿಗಳನ್ನು ಯಾರು ನೋಡಬಹುದು ಎಂಬುದನ್ನು ಲಿಮಿಟ್ ಮಾಡಿ.



ನಿಮ್ಮನ್ನು ಯಾರು ಫಾಲೋ ಮಾಡಬಹುದು ಅಥವಾ ಕಾಂಟ್ಯಾಕ್ಟ್ ಮಾಡಬಹುದು ಎಂಬುದನ್ನು ರಿವ್ಯೂ ಮಾಡಿ ಮತ್ತು ನಿಮಗೆ ಪರಿಚಯವಿಲ್ಲದವರನ್ನು ತೆಗೆಯಿರಿ.



ನಿಮಗೆ ನಿಜವಾಗಿಯೂ ಅಗತ್ಯವಿಲ್ಲದಿದ್ದರೆ ಲೊಕೇಶನ್ ಶೇರಿಂಗ್ ಅನ್ನು ಆಫ್ ಮಾಡಿ.



ಯಾರು ನಿಮ್ಮನ್ನು ಟ್ಯಾಗ್ ಮಾಡಬಹುದು ಅಥವಾ ಮೆನ್ಷನ್ ಮಾಡಬಹುದು ಎಂಬುದನ್ನು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಸಾಧ್ಯವಿರುವ ಕಡೆ ಟ್ಯಾಗ್‌ಗಳನ್ನು ಅಪ್ರೂವ್ ಮಾಡಿ.

ಆಪ್ಸ್‌ಗಳಿಗಾಗಿ



ನಿಮ್ಮ ಲೊಕೇಶನ್, ಕಾಂಟ್ಯಾಕ್ಟ್ಸ್, ಕ್ಯಾಮೆರಾ, ಮೈಕ್ರೋಫೋನ್ ಮತ್ತು ಫೋಟೋಗಳ ಆಕ್ಸೆಸ್ ಅನ್ನು ಚೆಕ್ ಮಾಡಿ.



ಒಂದು ಆಪ್‌ಗೆ ನಿಜವಾಗಿಯೂ ಅಗತ್ಯವಿರುವ ಪರ್ಮಿಷನ್‌ಗಳನ್ನು ಮಾತ್ರ ನೀಡಿ.



ನಿಮ್ಮ ಗೂಗಲ್, ಆಪಲ್, ಇ-ಮೇಲ್ ಅಥವಾ ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಅಕೌಂಟ್‌ಗಳಿಗೆ ಕನೆಕ್ಟ್ ಆಗಿರುವ ಆ್ಯಪ್‌ಗಳನ್ನು ರಿವ್ಯೂ ಮಾಡಿ.



ನಿಮ್ಮ ಫೋನ್‌ನಿಂದ ನೀವು ಇನ್ನು ಮುಂದೆ ಬಳಸದ ಆಪ್‌ಗಳನ್ನು ತೆಗೆದುಹಾಕುವ ಮೊದಲು ಅಕೌಂಟ್ ಡಿಲೀಟ್ ಮಾಡಿ.

ಕ್ವಿಕ್ ಪ್ರೈವೆಸಿ ಚೆಕ್‌ಲಿಸ್ಟ್

ನೀವು ಶೇರ್ ಮಾಡುವ, ಪೋಸ್ಟ್ ಮಾಡುವ,
ಡೌನ್‌ಲೋಡ್ ಮಾಡುವ ಅಥವಾ ಒಪ್ಪುವ ಮೊದಲು,
ನಿಮ್ಮನ್ನು ನೀವೇ ಈ ಮುಂದಿನವುಗಳನ್ನು ಕೇಳಿಕೊಳ್ಳಿ.

- [ ] ನಾನು ಕೇವಲ ಅಗತ್ಯವಿರುವುದನ್ನು ಮಾತ್ರ ಹಂಚಿಕೊಳ್ಳುತ್ತಿದ್ದೀನಾ? ✦
- [ ] ನನ್ನ ವಿವರಗಳನ್ನು ಯಾರು ಕೇಳುತ್ತಿದ್ದಾರೆ ಮತ್ತು ಅವರಿಗೆ ಅದು ಏಕೆ ಬೇಕು ಎಂದು ನನಗೆ ತಿಳಿದಿದೆಯೇ? ✦
- [ ] ನನ್ನ ಗೌಪ್ಯತಾ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ನಾನು ಪರಿಶೀಲಿಸಿದ್ದೇನೆಯೇ? ✦
- [ ] ಆ್ಯಪ್‌ವೊಂದು ಯಾವುದನ್ನೆಲ್ಲಾ ಪ್ರವೇಶಿಸಬಲ್ಲದು ಎಂಬುದನ್ನು ನಾನು ಪರಿಶೀಲಿಸಿದ್ದೇನೆಯೇ? ✦
- [ ] ಫೋಟೋ ಅಥವಾ ದಾಖಲೆಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವ ಮೊದಲು ನಾನು ಅದನ್ನು ಪರಿಶೀಲಿಸಿದ್ದೇನೆಯೇ? ✦
- [ ] ಇದನ್ನು ಸೇವ್ ಮಾಡುವುದು ಅಥವಾ ಫಾರ್ವರ್ಡ್ ಮಾಡುವುದು ನನಗೆ ಸರಿ ಎನ್ನಿಸುತ್ತದೆಯೇ? ✦

ಡಿಜಿಟಲ್ ನೈರ್ಮಲ್ಯ (ಹೈಜೀನ್)



ಡಿಜಿಟಲ್ ನೈರ್ಮಲ್ಯ (ಹೈಜೀನ್) ಎಂದರೆ ನಿಮ್ಮ ಸಾಧನ (ಡಿವೈಸ್) ಗಳು, ಖಾತೆಗಳು, ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಮತ್ತು ಆನ್‌ಲೈನ್ ಚಟುವಟಿಕೆಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ, ವ್ಯವಸ್ಥಿತವಾಗಿ ಮತ್ತು ಸುಲಭವಾಗಿ ನಿರ್ವಹಿಸುವಂತೆ ಇರಿಸಿಕೊಳ್ಳಲು ಸರಳ ಅಭ್ಯಾಸಗಳನ್ನು ಅನುಸರಿಸುವುದು ಎಂದರ್ಥ.

ನಿಯಮಿತ ಡಿಜಿಟಲ್ ಚೆಕ್-ಅಪ್‌ಗಳು ನಿಮ್ಮ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸಲು, ಭದ್ರತಾ ಅಪಾಯಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಲು ಮತ್ತು ತಂತ್ರಜ್ಞಾನವನ್ನು ಬಳಸಲು ಸುಲಭವಾಗಿಸಲು ಸಹಾಯ ಮಾಡುತ್ತವೆ.

ಸಾಧನ (ಡಿವೈಸ್) ಮತ್ತು ಖಾತೆಗಳ ನೈರ್ಮಲ್ಯ (ಹೈಜೀನ್)

ನಾವು ಪ್ರತಿದಿನ ಸಂವಹನ, ಮನರಂಜನೆ, ಪಾವತಿಗಳು, ಶಾಪಿಂಗ್ ಮತ್ತು ಕನೆಕ್ಟೆಡ್ ಆಗಿರಲು ನಮ್ಮ ಫೋನ್‌ಗಳನ್ನು ಬಳಸುತ್ತೇವೆ. ಸಮಯ ಕಳೆದಂತೆ, ನಮ್ಮಲ್ಲಿ ಬಳಕೆಯಾಗದ ಆಪ್ಸ್, ಹಳೆಯ ಫೈಲ್ಸ್, ಮರೆತುಹೋದ ಅಕೌಂಟ್ಸ್ ಮತ್ತು ನಾವು ಬದಲಾಯಿಸಿದ್ದನ್ನೇ ಮರೆತಿರುವ ಸೆಟ್ಟಿಂಗ್‌ಗಳು ಉಳಿದುಕೊಳ್ಳಬಹುದು. **ಆಗಾಗ್ಗೆ ನಿಮ್ಮ ಫೋನ್ ಮತ್ತು ಆನ್‌ಲೈನ್ ಅಕೌಂಟ್ಸ್ ಅನ್ನು ಚೆಕ್ ಮಾಡುವುದು ನಿಮ್ಮ ಡಿಜಿಟಲ್ ಲೈಫ್ ಅನ್ನು ವ್ಯವಸ್ಥಿತವಾಗಿ, ಸುಲಭವಾಗಿ ನಿರ್ವಹಿಸಲು ಮತ್ತು ಬಳಸಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ.**

ನೆನಪಿಡಿ

ನನ್ನ ಫೋನ್ ಸ್ವಚ್ಛ ಮತ್ತು ವ್ಯವಸ್ಥಿತವಾಗಿದೆಯೇ?

- **ನಿಮ್ಮ ಆಪ್ಸ್ ಪರಿಶೀಲಿಸಿ:** ನೀವು ಬಳಸದ ಆಪ್ಸ್ ಅನ್ನು ತೆಗೆದುಹಾಕಿ ಮತ್ತು ನಿಮಗೆ ಬೇಕಾದವುಗಳನ್ನು ಮಾತ್ರ ಇರಿಸಿಕೊಳ್ಳಿ.
- **ನಿಮ್ಮ ಸ್ಟೋರೇಜ್ ಪರಿಶೀಲಿಸಿ:** ಅನಗತ್ಯ ಫೋಟೋಗಳು, ವಿಡಿಯೋಗಳು, ಡೌನ್‌ಲೋಡ್‌ಗಳು ಮತ್ತು ಫೈಲ್‌ಗಳನ್ನು ಡಿಲೀಟ್ ಮಾಡಿ.
- **ನಿಮ್ಮ ನೋಟಿಫಿಕೇಶನ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ:** ಬೇಡದ ಅಲರ್ಟ್‌ಗಳನ್ನು ಆಫ್ ಮಾಡಿ, ಇದರಿಂದ ನಿಮ್ಮ ಫೋನ್ ಪದೇ ಪದೇ ನಿಮ್ಮ ಗಮನ ಸೆಳೆಯುವುದಿಲ್ಲ.
- **ನಿಮ್ಮ ಅಕೌಂಟ್‌ಗಳನ್ನು ಚೆಕ್ ಮಾಡಿ:** ನೀವು ಇನ್ನು ಮುಂದೆ ಬಳಸದ ಅಕೌಂಟ್‌ಗಳನ್ನು ರಿವ್ಯೂ ಮಾಡಿ ಮತ್ತು ಅಗತ್ಯವಿದ್ದಲ್ಲಿ ಅವುಗಳನ್ನು ಕ್ಲೋಸ್/ ಡಿಲೀಟ್
- **ನಿಮ್ಮ ಡಿವೈಸ್‌ಗಳನ್ನು ಚೆಕ್ ಮಾಡಿ:** ನೀವು ಇನ್ನು ಮುಂದೆ ಬಳಸದ ಫೋನ್‌ಗಳು, ಟ್ಯಾಬ್ಲೆಟ್‌ಗಳು ಅಥವಾ ಕಂಪ್ಯೂಟರ್‌ಗಳಲ್ಲಿನ ಅಕೌಂಟ್‌ಗಳಿಂದ ಸೈನ್ ಔಟ್ ಮಾಡಿ.

- **ನಿಮ್ಮ ಸೆಟ್ಟಿಂಗ್ಸ್ ಪರೀಕ್ಷಿಸಿ:** ಯಾವ ಆಯ್ಕೆಗಳು ಆನ್ ಆಗಿವೆ ಎಂದು ತಿಳಿಯಲು ಆಗಾಗ್ಗೆ ಪ್ರಮುಖ ಫೋನ್ ಮತ್ತು ಅಕೌಂಟ್ ಸೆಟ್ಟಿಂಗ್ಸ್ ಪರಿಶೀಲಿಸಿ.

- **ಫ್ರೀ ಟ್ರಯಲ್ಸ್ ಮತ್ತು ಸಬ್‌ಸ್ಕ್ರಿಪ್ಷನ್‌ಗಳನ್ನು ಚೆಕ್ ಮಾಡಿ:** ಟ್ರಯಲ್ ಪ್ರಾರಂಭಿಸುವ ಮೊದಲು ಬೆಲೆ, ರಿನ್ಯೂವಲ್ ಡೇಟ್ ಮತ್ತು ಕ್ಯಾನ್ಸಲೇಶನ್ ಟರ್ಮ್ಸ್‌ಗಳನ್ನು ಚೆಕ್ ಮಾಡಿ ಮತ್ತು ನಿಮಗೆ ಇನ್ನು ಮುಂದೆ ಅಗತ್ಯವಿಲ್ಲದ ಸಬ್‌ಸ್ಕ್ರಿಪ್ಷನ್‌ಗಳನ್ನು ಕ್ಯಾನ್ಸಲ್ ಮಾಡಿ.

- **ಡಿಜಿಟಲ್ ಕ್ಲೀನ್-ಅಪ್ ಡೇ ಆಚರಿಸಿ:** ಪ್ರತಿ ತಿಂಗಳು, ನಿಮ್ಮ ಫೋನ್, ಆಪ್ಸ್, ಅಕೌಂಟ್ಸ್, ಸೆಟ್ಟಿಂಗ್ಸ್ ಮತ್ತು ಫೈಲ್ಸ್ ಅನ್ನು ರಿವ್ಯೂ ಮಾಡಲು ಕೆಲವು ಸಮಯ ಮುಡುಪಿಡಿ.



ಒಂದು ಸರಳ ನೆನಪೋಲೆ

ನೀವು ಹೇಗೆ ನಿಮ್ಮ ಮನೆಯನ್ನು ಆಗಾಗ ಅಚ್ಚುಕಟ್ಟಾಗಿ ಇಟ್ಟುಕೊಳ್ಳುತ್ತೀರೋ, ಹಾಗೆಯೇ ನಿಮ್ಮ ಡಿಜಿಟಲ್ ಲೈಫ್ ಅನ್ನು ಕೂಡ ಆಗಾಗ ಕ್ಲೀನ್-ಅಪ್ ಮಾಡಿ.



ಪಾಸ್‌ವರ್ಡ್ ನೈರ್ಮಲ್ಯ (ಹೈಜೀನ್)

ನಮ್ಮಲ್ಲಿ ಇ-ಮೇಲ್, ಬ್ಯಾಂಕಿಂಗ್, ಶಾಪಿಂಗ್, ಸಾಮಾಜಿಕ ಜಾಲತಾಣ, ಟ್ರಾವೆಲ್ ಮತ್ತು ಇತರ ಸೇವೆಗಳಿಗಾಗಿ ಅನೇಕ ಖಾತೆಗಳಿವೆ. ದುರ್ಬಲ ಅಥವಾ ಮರುಬಳಕೆಯ ಪಾಸ್‌ವರ್ಡ್ ಒಂದಕ್ಕಿಂತ ಹೆಚ್ಚು ಖಾತೆಗಳನ್ನು ಅಪಾಯಕ್ಕೆ ಸಿಲುಕಿಸಬಹುದು. **ಉತ್ತಮ ಖಾತೆ ಸುರಕ್ಷತೆಯೆಂದರೆ ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸುವುದು ಮತ್ತು ನಿಮ್ಮ ಲಾಗಿನ್ ವಿವರಗಳನ್ನು ರಕ್ಷಿಸುವುದು.**



ಒಂದು ಸ್ಟ್ರಾಂಗ್ ಪಾಸ್‌ವರ್ಡ್ ಎಂದರೆ ಹೇಗಿರಬೇಕು?

ಒಂದು ಸ್ಟ್ರಾಂಗ್ ಪಾಸ್‌ವರ್ಡ್ ಉದ್ದವಾಗಿರಬೇಕು, ಊಹಿಸಲು ಕಷ್ಟವಾಗಿರಬೇಕು ಮತ್ತು ಪ್ರತಿಯೊಂದು ಪ್ರಮುಖ ಖಾತೆಗೂ ವಿಭಿನ್ನವಾಗಿರಬೇಕು.

ಉದಾಹರಣೆ:

- ✗ charu123
- ✗ password123
- ✗ ಇ-ಮೇಲ್, ಬ್ಯಾಂಕಿಂಗ್ ಮತ್ತು ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಿಗೆ ಒಂದೇ ಪಾಸ್‌ವರ್ಡ್

ಪರಸ್ಪರ ಸಂಬಂಧವಿಲ್ಲದ ಪದಗಳನ್ನು ಬಳಸಿ, ಸೂಕ್ತವೆನಿಸುವ ಕಡೆಗಳಲ್ಲಿ ಸಂಖ್ಯೆಗಳು ಅಥವಾ ಚಿಹ್ನೆಗಳನ್ನು ಸೇರಿಸಿ ರಚಿಸಿದ ದೀರ್ಘವಾದ 'ಪಾಸ್‌ಫ್ರೇಸ್' (passphrase) ಅನ್ನು ಬಳಸುವುದು ಉತ್ತಮ ವಿಧಾನವಾಗಿದೆ.

- ✓ Mango!River7Window

ನೆನಪಿಡಿ

- ಪ್ರಮುಖ ಅಕೌಂಟ್‌ಗಳಿಗೆ ಬೇರೆ ಬೇರೆ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸಿ. ನಿಮ್ಮ ಇ-ಮೇಲ್, ಬ್ಯಾಂಕಿಂಗ್ ಮತ್ತು ಇತರ ಫೈನಾನ್ಶಿಯಲ್ ಅಕೌಂಟ್‌ಗಳಿಗೆ ಪ್ರತ್ಯೇಕ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಇಟ್ಟುಕೊಳ್ಳಿ.

- ದ್ವಿ-ಹಂತದ ದೃಢೀಕರಣವನ್ನು (2-Factor Authentication) ಸಕ್ರಿಯಗೊಳಿಸಿ. ಇದು ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್‌ನ ಜೊತೆಗೆ, ನಿಮ್ಮ ಖಾತೆಗೆ ಒಂದು ಹೆಚ್ಚುವರಿ "ರಕ್ಷಣಾ ಕವಚ"ದಂತೆ ಕೆಲಸ ಮಾಡುತ್ತದೆ.

- ಪಾಸ್‌ವರ್ಡ್‌ಗಳು, ಓಟಿಪಿಗಳು ಅಥವಾ ವೆರಿಫಿಕೇಶನ್ ಅನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ ಕೋಡ್‌ಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

- ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಬೇರೆಯವರಿಗೆ ತಿಳಿದಿದೆ ಎಂದು ನಿಮಗೆ ಅನಿಸಿದರೆ ಅದನ್ನು ಬದಲಾಯಿಸಿ. ನೀವು ಆಕಸ್ಮಿಕವಾಗಿ ಅದನ್ನು ಯಾರಿಗಾದರೂ ಹಂಚಿಕೊಂಡಿದ್ದರೆ ಅಥವಾ ಅನುಮಾನಾಸ್ಪದ ಚಟುವಟಿಕೆಯನ್ನು ಗಮನಿಸಿದರೆ ತಕ್ಷಣವೇ ಅದನ್ನು ಬದಲಾಯಿಸಿ.

- ಹಳೆಯ ಅಕೌಂಟ್‌ಗಳನ್ನು ರಿವ್ಯೂ ಮಾಡಿ. ನೀವು ಇನ್ನು ಮುಂದೆ ಬಳಸದ ಅಕೌಂಟ್‌ಗಳನ್ನು ಕ್ಲೋಸ್ ಮಾಡಿ, ವಿಶೇಷವಾಗಿ ವೈಯಕ್ತಿಕ ಅಥವಾ ಫೈನಾನ್ಶಿಯಲ್ ಇನ್ಫಾರ್ಮೇಶನ್ ಹೊಂದಿರುವ ಅಕೌಂಟ್‌ಗಳನ್ನು.

- ನೀವು ಎಲ್ಲೆಲ್ಲಿ ಲಾಗ್ ಇನ್ ಆಗಿದ್ದೀರಿ ಎಂದು ಚೆಕ್ ಮಾಡಿ. ನಿಮಗೆ ಪರಿಚಯವಿಲ್ಲದ ಅಥವಾ ನೀವು ಬಳಸದ ಡಿವೈಸ್‌ಗಳು ಅಥವಾ ಸೆಷನ್‌ಗಳಿಂದ ಸೈನ್ ಔಟ್ ಮಾಡಿ.

- ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಸ್ಟೋರ್ ಮಾಡಿ. ನಿಮ್ಮ ಫೋನ್ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಹತ್ತಿರ ಅವುಗಳನ್ನು ಬರೆದಿಡುವುದನ್ನು ತಪ್ಪಿಸಿ; ಅಗತ್ಯವಿದ್ದರೆ ಪ್ರತಿಷ್ಠಿತ ಪಾಸ್‌ವರ್ಡ್ ಮ್ಯಾನೇಜರ್ ಬಳಸಿ.

ಡಿಜಿಟಲ್ ಯೋಗಕ್ಷೇಮ

ಡಿಜಿಟಲ್ ಟೆಕ್ನಾಲಜಿ ನಮ್ಮ ಕುಟುಂಬ, ಸ್ನೇಹಿತರು ಮತ್ತು ಸಮುದಾಯಗಳೊಂದಿಗೆ ಸಂಪರ್ಕದಲ್ಲಿರಲು ನಮಗೆ ಸಹಾಯ ಮಾಡುತ್ತದೆ. ಆದರೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಅತಿಯಾದ ಸಮಯ ಕಳೆಯುವುದು, ಸತತವಾಗಿ ನೋಟಿಫಿಕೇಶನ್‌ಗಳನ್ನು ಪಡೆಯುವುದು ಅಥವಾ ಪ್ರತಿಯೊಂದು ಮೆಸೇಜ್‌ಗೆ ಪ್ರತಿಕ್ರಿಯಿಸಲೇಬೇಕು ಎಂಬ ಒತ್ತಡಕ್ಕೆ ಒಳಗಾಗುವುದು ಡಿಜಿಟಲ್ ಜೀವನವನ್ನು ಅತಿಯಾದ ಹೊರೆಯನ್ನಾಗಿಸಬಹುದು. **ಆರೋಗ್ಯಕರ ಡಿಜಿಟಲ್ ಅಭ್ಯಾಸಗಳು ನಿಮ್ಮ ಫೋನ್ ನಿಮ್ಮ ಸಮಯ, ಗಮನ ಅಥವಾ ಮನಸ್ಸಿನ ಶಾಂತಿಯನ್ನು ಕಸಿದುಕೊಳ್ಳದಂತೆ ನೀವು ಸಂಪರ್ಕದಲ್ಲಿರಲು ಸಹಾಯ ಮಾಡುತ್ತವೆ.**

ನಾನು ಟೆಕ್ನಾಲಜಿಯನ್ನು ಆರೋಗ್ಯಕರ ಮತ್ತು ಆರಾಮದಾಯಕ ರೀತಿಯಲ್ಲಿ ಬಳಸುತ್ತಿದ್ದೀರಾ?

ನೆನಪಿಡಿ

- ತಕ್ಷಣವೇ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಕೆಂಬ ಒತ್ತಡಕ್ಕೆ ಒಳಗಾಗಬೇಡಿ. ನಿಧಾನವಾಗಿ ಯೋಚಿಸಿ ನಿರ್ಧರಿಸಿ; ವಿಶೇಷವಾಗಿ ಕರೆ, ಸಂದೇಶ ಅಥವಾ ಮನವಿಯೊಂದು ತುರ್ತಾದದ್ದು ಎಂದು ತೋರಿದಾಗ ಇದು ಮುಖ್ಯ.
- ನಿಮ್ಮ ಫೋನ್‌ನಿಂದ ನಿಯಮಿತವಾಗಿ ವಿರಾಮ ತೆಗೆದುಕೊಳ್ಳಿ. ಊಟ, ಸಂಭಾಷಣೆಗಳು, ನಡಿಗೆ ಮತ್ತು ಮಲಗುವ ಮುನ್ನ ಸ್ವಲ್ಪ ಸಮಯ ಫೋನ್ ಬಳಸದಂತೆ ಸಮಯ ಮೀಸಲಿಡಿ.
- ಆಫ್‌ಲೈನ್‌ನಲ್ಲಿ ಆಫ್‌ಲೈನ್‌ನಲ್ಲೂ ಸಂಪರ್ಕದಲ್ಲಿರಿ. ಕುಟುಂಬ, ಹವ್ಯಾಸಗಳು, ನಡಿಗೆ ಮತ್ತು ಇತರ ಚಟುವಟಿಕೆಗಳೊಂದಿಗೆ ಫೋನ್ ಬಳಸುವ ಸಮಯವನ್ನು ಸಮತೋಲನದಲ್ಲಿಡಿ.
- ನಿಮ್ಮ ಮನಸ್ಸಿನ ಶಾಂತಿಯನ್ನು ಕಾಪಾಡಿಕೊಳ್ಳಿ. ಒತ್ತಡ ಅಥವಾ ಅಸಮಾಧಾನ ಉಂಟುಮಾಡುವ ಗ್ರೂಪ್‌ಗಳು ಮತ್ತು ಸಂಭಾಷಣೆಗಳನ್ನು ಮ್ಯೂಟ್ ಮಾಡಿ, ಅವುಗಳಿಂದ ಹೊರಬನ್ನಿ ಅಥವಾ ಅವುಗಳನ್ನು ನಿರ್ಲಕ್ಷಿಸಿ.
- ಗೊಂದಲವಿದ್ದಾಗ ಸಹಾಯ ಕೇಳಿ. ನಿಮಗೆ ಯಾವುದಾದರೂ ಆ್ಯಪ್, ಮೆಸೇಜ್, ಸೆಟ್ಟಿಂಗ್ ಅಥವಾ ನೋಟಿಫಿಕೇಶನ್ ಅರ್ಥವಾಗದಿದ್ದರೆ, ಮುಂದುವರಿಯುವ ಮೊದಲು ನೀವು ನಂಬುವ ಸಮರ್ಥರಾದವರನ್ನು ಕೇಳಿ.

ಸೈಬರ್ ಅಪರಾಧ ಪರಿಹಾರ





ಸೈಬರ್ ವಂಚನೆ: ಮುಂದೇನು ಮಾಡಬೇಕು?

ಶೀಘ್ರವೇಕಾರ್ಯಪ್ರವೃತ್ತರಾಗಿ (ಆದರೆ ಶಾಂತವಾಗಿರಿ)

ಘಟನೆಯ ಬಗ್ಗೆ ವರದಿ ಮಾಡಲು ಕಾಯಬೇಡಿ ಅಥವಾ ಮುಜುಗರ ಪಡಬೇಡಿ.

ತಕ್ಷಣವೇ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅಥವಾ ಪೇಮೆಂಟ್ ಸರ್ವಿಸ್‌ಗೆ ಮಾಹಿತಿ ನೀಡಿ.

ಅನ್ವಯವಾಗುವಂತೆ, ತೊಂದರೆಗೊಳಗಾದ ಅಕೌಂಟ್, ಕಾರ್ಡ್, ಯುಪಿಐ ಐಡಿ ಅಥವಾ ವಹಿವಾಟನ್ನು ಬ್ಲಾಕ್ ಮಾಡಲು ಅಥವಾ ಸುರಕ್ಷಿತಗೊಳಿಸಲು ಅವರಿಗೆ ತಿಳಿಸಿ.

ಸಾಕ್ಷ್ಯವನ್ನು ಸಂರಕ್ಷಿಸಿ.

ಘಟನೆಗೆ ಸಂಬಂಧಿಸಿದ ಸ್ಕ್ರೀನ್‌ಶಾಟ್‌ಗಳು, ವಹಿವಾಟು (ಟ್ರಾನ್ಸಾಕ್ಷನ್) ಐಡಿಗಳು, ಮೆಸೇಜ್‌ಗಳು, ಫೋನ್ ನಂಬರ್‌ಗಳು, ಇ-ಮೇಲ್ ವಿಳಾಸಗಳು, ಲಿಂಕ್‌ಗಳು ಮತ್ತು ಇತರ ವಿವರಗಳನ್ನು ಸೇವ್ ಮಾಡಿ.

ದುಷ್ಪರಿಣಾಮಕ್ಕೊಳಗಾದ ಅಕೌಂಟ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ.

ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬದಲಾಯಿಸಿ, 2-ಸ್ಟೆಪ್ ವೆರಿಫಿಕೇಶನ್ ಸಕ್ರಿಯಗೊಳಿಸಿ ಮತ್ತು ಅಗತ್ಯವಿದ್ದರೆ ಕಾರ್ಡ್‌ಗಳನ್ನು ಅಥವಾ ಪೇಮೆಂಟ್ ಸರ್ವಿಸ್‌ಗಳನ್ನು ಬ್ಲಾಕ್ ಮಾಡಿ.

ಅನುಮಾನಾಸ್ಪದ ಅಕೌಂಟ್‌ಗಳು ಅಥವಾ ನಂಬರ್‌ಗಳ ಬಗ್ಗೆ ವರದಿ ಮಾಡಿ.

ಸಂಬಂಧಿತ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್ ಅಥವಾ ರಿಪೋರ್ಟಿಂಗ್ ಸರ್ವಿಸ್ ಅನ್ನು ಬಳಸಿ ಮತ್ತು ಸಾಕ್ಷ್ಯವನ್ನು ಸೇವ್ ಮಾಡಿದ ನಂತರ ಅಕೌಂಟ್ ಅನ್ನು ಬ್ಲಾಕ್ ಮಾಡಿ.

ಒಂದು ವೇಳೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ರಿಪೋರ್ಟ್ ಮಾಡಲು ಸಾಧ್ಯವಾಗದಿದ್ದರೆ, ನಿಮ್ಮ ಹತ್ತಿರದ ಪೊಲೀಸ್ ಸ್ಟೇಷನ್ ಅಥವಾ ಸೈಬರ್ ಕ್ರೈಮ್ ಪೊಲೀಸ್ ಸ್ಟೇಷನ್‌ಗೆ ಭೇಟಿ ನೀಡಿ.

ನಿಮ್ಮ ದೂರು/ ರೆಫರೆನ್ಸ್ ವಿವರಗಳನ್ನು ನಿಮ್ಮ ಬಳಿಯೇ ಇಟ್ಟುಕೊಳ್ಳಿ.

ನಿಮ್ಮ ದೂರಿನ ಬಗ್ಗೆ ನಿಗಾ ಇರಿಸಿ.

ಸ್ವೀಕೃತಿ ಸಂಖ್ಯೆ ಅಥವಾ ದೂರಿನ ಸಂಖ್ಯೆಯನ್ನು ಸೇವ್ ಮಾಡಿ ಮತ್ತು ಫಾಲೋ ಅಪ್ ಮಾಡಲು ಅದನ್ನು ಬಳಸಿ.

ಎಲ್ಲಿ ವರದಿ ಮಾಡಬೇಕು?



ನೀವು ಸೈಬರ್ ಕ್ರೈಮ್ ಅಥವಾ ಹಣಕಾಸಿನ ವಂಚನೆಯ ನೀವು ಸೈಬರ್ ಅಪರಾಧ ಅಥವಾ ಆರ್ಥಿಕ ವಂಚನೆಯನ್ನು ಎದುರಿಸಿದ್ದರೆ

ಹಣಕಾಸಿನ ವಂಚನೆಯ ಬಗ್ಗೆ ವರದಿ ಮಾಡಲು ತಕ್ಷಣ **1930 ಗೆ ಕರೆ** ಮಾಡಿ. ನೀವು **ನ್ಯಾಷನಲ್ ಸೈಬರ್ ಕ್ರೈಮ್ ರಿಪೋರ್ಟಿಂಗ್ ಪೋರ್ಟಲ್** ಮೂಲಕ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸೈಬರ್ ಕ್ರೈಮ್ ದೂರನ್ನು ನೋಂದಾಯಿಸಬಹುದು ಮತ್ತು ಟ್ರ್ಯಾಕ್ ಮಾಡಬಹುದು.

ಪೋರ್ಟಲ್: cybercrime.gov.in

ಹೆಲ್ಪ್‌ಲೈನ್: 1930

ನಿಮಗೆ ಅನುಮಾನಾಸ್ಪದ ಕರೆ, ಎಸ್‌ಎಮ್‌ಎಸ್ ಅಥವಾ ಮೆಸೇಜ್ ಬಂದರೆ



ಚಕ್ಷು - ಸಂಚಾರ್ ಸಾಥಿ ಮೂಲಕ ಶಂಕಿತ ವಂಚನೆಯ ಸಂವಹನಗಳನ್ನು ವರದಿ ಮಾಡಿ. ಇದು ಶಂಕಿತ ವಂಚನೆಯ ಕರೆಗಳು, ಎಸ್‌ಎಮ್‌ಎಸ್ ಮತ್ತು ವಾಟ್ಸಾಪ್ ಸಂದೇಶಗಳು ಹಾಗೂ ವೇಷ ಮರೆಸುವ ಪ್ರಯತ್ನಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ.

www.sancharsaathi.gov.in



ನೀವು ಹಿರಿಯ ನಾಗರಿಕರಾಗಿ ಬೆಂಬಲವನ್ನು ಬಯಸಿದರೆ

ಹಿರಿಯ ನಾಗರಿಕರ ಕಾಳಜಿಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ಮಾರ್ಗದರ್ಶನ, ಬೆಂಬಲ ಮತ್ತು ಸಹಾಯಕ್ಕಾಗಿ **ಎಲ್ಡರ್ ಲೈನ್ - 14567** ಗೆ ಕರೆ ಮಾಡಿ.



ನಿಮಗೆ ಸ್ಥಳೀಯ ಪೊಲೀಸ್ ನೆರವು ಬೇಕಾದಲ್ಲಿ

ನಿಮ್ಮ **ಹತ್ತಿರದ ಪೊಲೀಸ್ ಸ್ಟೇಷನ್ ಅಥವಾ ಸೈಬರ್‌ಕ್ರೈಮ್ ಪೊಲೀಸ್ ಸ್ಟೇಷನ್** ಗೆ ಭೇಟಿ ನೀಡಿ. ತುರ್ತು ಸಂದರ್ಭಗಳು ಅಥವಾ ಸೈಬರ್‌ಕ್ರೈಮ್ ಹೊರತುಪಡಿಸಿ ಇತರ ಅಪರಾಧಗಳಿಗಾಗಿ, ಸ್ಥಳೀಯ ಪೊಲೀಸರನ್ನು ಸಂಪರ್ಕಿಸಿ ಸಂಪರ್ಕಿಸಿ.

ನಿಮ್ಮ ಬ್ಯಾಂಕ್, ಕಾರ್ಡ್ ಅಥವಾ ಯುಪಿಐ ಒಳಗೊಂಡಿದ್ದರೆ

ನಿಮ್ಮ ಪಾಸ್‌ಬುಕ್, ಬ್ಯಾಂಕ್ ಸ್ಟೇಟ್‌ಮೆಂಟ್, ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್ ಅಥವಾ ಆ್ಯಪ್‌ನಲ್ಲಿರುವ **ಕಸ್ಟಮರ್ ಕೇರ್ ನಂಬರ್** ಬಳಸಿ ತಕ್ಷಣ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ.





ಅಮೂಲ್ಯ ಸಮಯವನ್ನು (ಗೋಲ್ಡನ್ ಹವರ್) ನೆನಪಿಡಿ

ಹಣಕಾಸಿನ ವಂಚನೆಯಾದ ಮೊದಲ ಒಂದು ಗಂಟೆಯೊಳಗೆ ದೂರು ದಾಖಲಿಸಿ ಮತ್ತು ತಕ್ಷಣ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ, ಇದರಿಂದ ಹಣವನ್ನು ಮರಳಿ ಪಡೆಯುವ ಸಾಧ್ಯತೆಗಳು ಹೆಚ್ಚಿರುತ್ತವೆ.



ವರದಿ ಮಾಡುವಾಗ ಈ ಮಾಹಿತಿಯನ್ನು ಸಿದ್ಧವಾಗಿಟ್ಟುಕೊಳ್ಳಿ

- ಘಟನೆ ನಡೆದ ದಿನಾಂಕ ಮತ್ತು ಸಮಯ
- ಕಳೆದುಕೊಂಡ ಮೊತ್ತ, ಯಾವುದಾದರೂ ಇದ್ದರೆ
- ಟ್ರಾನ್ಸಾಕ್ಷನ್ ಐಡಿ / ಯುಟಿಆರ್ ನಂಬರ್
- ಸಂಬಂದಿತ ಬ್ಯಾಂಕ್ ಅಥವಾ ಯುಪಿಐ ವಿವರಗಳು
- ಫೋನ್ ನಂಬರ್‌ಗಳು ಮತ್ತು ಇ-ಮೇಲ್ ವಿಳಾಸಗಳು
- ಮೆಸೇಜ್‌ಗಳು, ಪ್ರೊಫೈಲ್‌ಗಳು ಅಥವಾ ವೆಬ್‌ಸೈಟ್‌ಗಳ ಸ್ಕ್ರೀನ್‌ಶಾಟ್‌ಗಳು
- ಸಂಬಂಧಿತ ಲಿಂಕ್‌ಗಳು ಮತ್ತು ಅಕೌಂಟ್ ವಿವರಗಳು
- ಈಗಾಗಲೇ ಸ್ವೀಕರಿಸಲಾದ ಯಾವುದೇ ದೂರು/ರೆಫರೆನ್ಸ್ ನಂಬರ್

OPTIV | DSCI
PROMOTING DATA PROTECTION

India
Meri Digital Suraksha
2026

ಮಾಹಿತಿ ಹಂಚಿಕೊಳ್ಳುವುದು, ಇತರರ ಸುರಕ್ಷತೆಯ ಬಗ್ಗೆ ಕಾಳಜಿ ತೋರಿದಂತೆ.

ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆಯ ಮೊದಲ ಹೆಜ್ಜೆ ಜಾಗೃತಿ. ಈ ಮಾರ್ಗದರ್ಶಿಯನ್ನು ನಿಮ್ಮ ಕುಟುಂಬ, ಸ್ನೇಹಿತರು ಮತ್ತು ಅಪ್ತರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವ ಮೂಲಕ, ಅವರು ಡಿಜಿಟಲ್ ಜಗತ್ತಿನಲ್ಲಿ ಆತ್ಮವಿಶ್ವಾಸದಿಂದ ಮುನ್ನಡೆಯಲು ನೆರವಾಗಿ.

ಮಾರ್ಗದರ್ಶಿಯನ್ನು ಹತ್ತಿರ ಇಟ್ಟುಕೊಳ್ಳಲು ಬಯಸುವಿರಾ?
ನಿಮ್ಮ ಪ್ರತಿಯನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ಕ್ಯೂಆರ್ ಕೋಡ್ ಸ್ಕ್ಯಾನ್ ಮಾಡಿ
ಮತ್ತು ನಿಮಗೆ ಅಗತ್ಯವಿರುವಾಗಲೆಲ್ಲಾ ಉತ್ತಮ ಅಭ್ಯಾಸಗಳನ್ನು ಮತ್ತೊಮ್ಮೆ ನೋಡಿ.



DSCI_Connect | dsci.connect | dsci.connect | dscivideo | data-security-council-of-india

Data Security Council of India (DSCI), 4th Floor,
Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303.