



4. ಡಿಜಿಟಲ್ ಅರೆಸ್ಟ್: ನಿಮ್ಮ ಕೊರಿಯರ್‌ನಲ್ಲಿ ಮಾದಕ ವಸ್ತುವೋ ಅಥವಾ ನಿಷೇಧಿತ ವಸ್ತುವೋ ಸಿಕ್ಕಿದ ಅಥವಾ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಯಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧದಿಂದ ಬಂದ ಹಣಪತ್ರ ಯಾಗಿದೆ ಎಂದೋ ತಮ್ಮನ್ನು ಪೊಲೀಸ್ ಅಥವಾ ಕಸ್ಟಮ್ಸ್ ಅಥವಾ ಸಿಬಿಐ ಅಧಿಕಾರಿಯೆಂದು ಗುರುತಿಸಿಕೊಳ್ಳುವ ವ್ಯಕ್ತಿಯಿಂದ ಕರೆ ಬರುತ್ತದೆ. ಅವರು ನಿಮ್ಮನ್ನು ಈ ಕೂಡಲೇ ಡಿಜಿಟಲ್ ಅರೆಸ್ಟ್ ಮಾಡಿದ್ದೇವೆ ಎಂದು ಹೆದರಿಸಿ, ನಿಮ್ಮ ಹಣವನ್ನೆಲ್ಲಾ ತನಿಖೆಯ ನೆಪದಲ್ಲಿ ಅವರ ಖಾತೆಗೆ ವರ್ಗಾವಣೆ ಮಾಡುವಂತೆ ಮಾಡಿ ನಿಮ್ಮನ್ನು ವಂಚಿಸುತ್ತಾರೆ.

5. ರಾನ್ಸಮ್ ವೇರ್: ಇಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧಿಗಳು ನಿಮ್ಮ ಕಂಪ್ಯೂಟಿಂಗ್ ಸಾಧನದಲ್ಲಿರುವ ಪ್ರಮುಖ ಫೈಲ್‌ಗಳನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ (ಓದಲು ಬಳಸಲಾಗದಂತೆ) ಮಾಡಿ, ಅವುಗಳನ್ನು ಡಿಕ್ರಿಪ್ಟ್ (ಮೊದಲಿನ ಸ್ಥಿತಿಗೆ ತರಲು) ಮಾಡಲು ಹಣ ಕೇಳುತ್ತಾರೆ. ಬೆದರಿಕೆ ಹಾಕುವವರು ಸಾಮಾನ್ಯವಾಗಿ ಬಿಟ್‌ಕಾಯಿನ್‌ನಂತಹ ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಯಲ್ಲಿ ಸುಲಿಗೆಯನ್ನು

ಬಯಸುತ್ತಾರೆ ಮತ್ತು ಪಾವತಿಸದಿದ್ದರೆ ಡೇಟಾವನ್ನು ಬಹಿರಂಗಪಡಿಸುವುದಾಗಿ ಬೆದರಿಕೆ ಹಾಕುತ್ತಾರೆ. ಇದು ಸಂಸ್ಥೆಗಳನ್ನು ಬಾಧಿಸುವ ಅತ್ಯಂತ ಪ್ರಮುಖ ಸೈಬರ್ ಅಪರಾಧ ಆಗಿರುತ್ತದೆ.

ಸೈಬರ್ ವಂಚನೆಯಿಂದ ರಕ್ಷಿಸಿಕೊಳ್ಳಲು...

1. ಎಲ್ಲಾ ಡಿಜಿಟಲ್ ವಹಿವಾಟುಗಳಿಗೆ 'ಶೂನ್ಯ ಟ್ರಸ್ಟ್', ತಾಳ್ಮೆ ಮತ್ತು ದೃಢೀಕರಣ' ತತ್ವವನ್ನು ಯಾವಾಗಲೂ ಅನುಸರಿಸಿ, ಮೂಲಭೂತವಾಗಿ ಪರಿಶೀಲನೆಯ ನಂತರವೇ ಪ್ರತಿಕ್ರಿಯಿಸಿ.
2. ಅಪರಿಚಿತರು ಕಳುಹಿಸಿದ ಯಾವುದೇ ಲಿಂಕ್ ಅನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ ಅಥವಾ ಕ್ಯೂಆರ್ ಕೋಡ್ ಅನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ ಅಥವಾ ಯಾವುದೇ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಸ್ಥಾಪಿಸಬೇಡಿ.
3. ಯಾವುದೇ ಸಾರ್ವಜನಿಕ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಅಥವಾ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ವೇದಿಕೆಗಳಲ್ಲಿ ನಿಮ್ಮ ಫೋನ್ ಸಂಖ್ಯೆ ಸೇರಿದಂತೆ ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಅಥವಾ ಆರ್ಥಿಕ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

4. ನಿಮ್ಮ ಸಂದೇಶಕ್ಕೆ ಪ್ರತ್ಯುತ್ತರ ಅಥವಾ ಕಾಮೆಂಟ್ ಮೂಲಕ ನಿಮ್ಮನ್ನು ಸಂಪರ್ಕಿಸುವ ಮತ್ತು ಸಹಾಯವನ್ನು ನೀಡುವ ಯಾವುದೇ ವ್ಯಕ್ತಿಯ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ, ನೀವು ಅವರೊಂದಿಗೆ ಮಾತನಾಡುವ ಅಥವಾ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವ ಮೊದಲು ಅವರು ಅಸಲಿಯೇ ಎಂಬುದನ್ನು ಪರಿಶೀಲಿಸಿ ದೃಢೀಕರಿಸಿದ ನಂತರವೇ ಅವರೊಂದಿಗೆ ಮಾಹಿತಿ ಹಂಚಿಕೊಳ್ಳಿ.

5. ಅಪರಿಚಿತರಿಗೆ ಒಟ್ಟಿಗಳನ್ನು ನೀಡುವ ಮೊದಲು, ಆ ಒಟ್ಟಿ ಯಾವುದಕ್ಕೇಂದು ಖಚಿತಪಡಿಸಿಕೊಂಡು ನಂತರ ಹಂಚಿಕೊಳ್ಳಿ.

6. ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆ, ಸೋಷಿಯಲ್ ಮೀಡಿಯಾ, ವಾಟ್ಸಾಪ್ ಅಕೌಂಟ್‌ಗೆ ಕೂಡಲೇ ಓಂ/ಮಲ್ಟಿ ಫ್ಯಾಕ್ಟರ್ ಆಥೆಂಟಿಕೇಷನ್ ಅಳವಡಿಸಿ.

7. ಆದಾರ್ ಅಥವಾ ಪ್ಯಾನ್ ವಿವರಗಳು ಅಥವಾ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆ ಅಥವಾ ಕ್ರೆಡಿಟ್/ಡೆಬಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳಂತಹ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಎಂದಿಗೂ ಅಪರಿಚಿತರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ. ಹೆಸರು, ವಿಳಾಸ ಅಥವಾ ಹುಟ್ಟಿದ ದಿನಾಂಕದ ಪ್ರಮಾಣ ನೀಡಬೇಕಾದರೆ ಡ್ರೈವಿಂಗ್ ಲೈಸೆನ್ಸ್, ವೋಟರ್ ಐಡಿ ನೀಡಿ.

