ಸುರಕ್ಷತೆಗೆ ಕಿವಿಮಾತು

- ಫೋನ್ ಬಳಕೆಯಲ್ಲಿ ಇಲ್ಲದಾಗ ಲಾಕ್ ಮಾಡಿ.
- ಫೋನ್‌ಗಳನ್ನು ಬಳಕೆಯಲ್ಲಿ ಇಲ್ಲದಿದ್ದಾಗ ಲಾಕ್ ಮಾಡುವುದು ಉತ್ತಮ ಅಭ್ಯಾಸ. ಆದರೆ ಹೀಗೆ ಪಿನ್ ಬಳಸುವಾಗ ಅದು ನಿಮ್ಮ ಜನ್ಮದಿನ, ವಿವಾಹ ವಾರ್ಷಿಕೋತ್ಸವ ದಿನ, ಮಕ್ಕಳು ಅಥವಾ ಮಡದಿ ಸೇರಿದಂತೆ ಸಂಬಂಧಿಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ಯಾವುದೇ ದಿನಾಂಕವನ್ನು ಬಳಸದಿರುವುದು ಸೂಕ್ತ. ಇಂಥ ಸಂಖ್ಯೆಗಳನ್ನು ವಂಚಕರು ಸುಲಭವಾಗಿ ಪತ್ತೆ ಹಚ್ಚುವ ಸಾಧ್ಯತೆ ಇದೆ.
- ತಂತ್ರಜ್ಞಾನ ಬೆಳೆದಂತೆ ಬಹುತೇಕ ಕಚೇರಿ ಕೆಲಸಗಳು ಮೊಬೈಲ್ ಮೂಲಕವೇ ಆಗುತ್ತಿವೆ. ಹೀಗಾಗಿ ಎರಡು ಹಂತದ ಭದ್ರತೆ ಹೊಂದುವುದು ತೀರಾ ಮುಖ್ಯ. ಪಿನ್ ಸಂಖ್ಯೆಯೊಂದಿಗೆ, ಮುಖ ನೋಡಿ, ಬೆರಳಚ್ಚು ಪಡೆದು ಫೋನ್ ತೆರೆಯುವ ಅಥವಾ ಯಾವುದೇ ಮೊಬೈಲ್ ಅಪ್ಲಿಕೇಷನ್ ತೆರೆಯುವ ವ್ಯವಸ್ಥೆಯನ್ನು ಮಾಡಬೇಕು.
- ಮೊಬೈಲ್ ತಂತ್ರಾಂಶ ಮತ್ತು ಆ್ಯಪ್‌ಗಳನ್ನು ಕಾಲಕಾಲಕ್ಕೆ ಅಪ್‌ಡೇಟ್ ಮಾಡಿಕೊಳ್ಳುತ್ತಿರಬೇಕು. ಇದರಿಂದ ಕಾಲಕಾಲಕ್ಕೆ ಎದುರಾಗುವ ಕುತಂತ್ರಾಂಶಗಳನ್ನು ತಡೆಯುವ ತಂತ್ರಾಂಶಗಳನ್ನು ಅಳವಡಿಸಲಾಗುತ್ತಿರುತ್ತದೆ.
- ಬ್ಯಾಂಕ್‌ಗಳು ಕಾಲಕಾಲಕ್ಕೆ ಸಂದೇಶ ಮತ್ತು ಇಮೇಲ್ ಮೂಲಕ ಕಳುಹಿಸುವ ಎಚ್ಚರಿಕೆ ಸಂದೇಶಗಳನ್ನು ತಪ್ಪದೇ ಪಾಲಿಸುತ್ತಿರಬೇಕು. ಯುಪಿಐ ಪಿನ್ ಹಾಗೂ ಇನ್ನಿತರ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳದಿರುವುದು ಉತ್ತಮ.

- ಪ್ರಮಾಣೀಕೃತ ಆ್ಯಪ್‌ಗಳನ್ನೇ ಬಳಸುವುದು ಸೂಕ್ತ. ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಅಥವಾ ಐಫೋನ್ ಕಂಪನಿಗಳು ಖಾತ್ರಿಪಡಿಸುವ ಆ್ಯಪ್‌ಗಳನ್ನೇ ಬಳಸುವುದು ಸೂಕ್ತ. ಈ ಆ್ಯಪ್‌ಗಳು ಬಳಕೆದಾರರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಗೋಪ್ಯವಾಗಿಡುವ ಖಾತ್ರಿ ನೀಡುತ್ತವೆ. ಜತೆಗೆ ಅನಧಿಕೃತ ವಹಿವಾಟುಗಳನ್ನು ನಿಯಂತ್ರಿಸುತ್ತವೆ. ಕಳ್ಳತನವನ್ನು ಬೇಗನೆ ಪತ್ತೆ ಮಾಡುತ್ತವೆ.
- ಸ್ಕ್ರೀನ್ ಶೇರಿಂಗ್ ಆ್ಯಪ್ ಬಳಕೆ ಬಗ್ಗೆ ಎಚ್ಚರ ಇರಲಿ.
- ಬಳಸುವ ಮೊಬೈಲ್ ಆ್ಯಪ್‌ಗಳು ಯಾವೆಲ್ಲಾ ಮಾಹಿತಿಗಳನ್ನು ತನ್ನ ಡೆವಲಪರ್‌ನೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುತ್ತಿವೆ ಎಂಬುದರ ಅರಿವೂ ಇರಬೇಕು.

2012ರಿಂದ ಈಚೆಗೆ ಸಿಮ್ ಕಾರ್ಡ್ ಖರೀದಿ ಮತ್ತು ನಿಷ್ಕ್ರಿಯ ಸಿಮ್ ಕಾರ್ಡ್‌ಗಳ ಬಳಕೆಗೆ ಸರ್ಕಾರ ನಿಯಂತ್ರಣ ಹೇರಿದೆ. ಇತ್ತೀಚೆಗೆ ಗ್ರಾಹಕರ ಪರಿಚಯ ದಾಖಲಿಸುವ ಕೆವೈಸಿ ಕೂಡಾ ಕಡ್ಡಾಯಗೊಳಿಸಲಾಗಿದೆ. ಹೀಗಿದ್ದರೂ ಎಗ್ಗಿಲ್ಲದೆ ವಂಚನೆಗಳೂ ನಡೆಯುತ್ತಿವೆ.

ಕಲ್ಪನೆಗೆ ನಿಲುಕದ ಆಳ-ಗಾಳ

ಫಿಶಿಂಗ್ ಅಥವಾ ಸ್ಮಿಶಿಂಗ್‌ನ ತಂತ್ರಗಾರಿಕೆಯಲ್ಲಿ ಹೆಚ್ಚಾಗಿ ಬೆದರಿಕೆ, ಭಯ ಹುಟ್ಟಿಸುವುದು ಅಥವಾ ಆಮಿಷ ಒಡ್ಡುವುದು ಸೇರಿರುತ್ತದೆ. ಅಂದರೆ, ವಿದ್ಯುತ್ ಸಂಪರ್ಕ ಕಡಿತ, ಬ್ಯಾಂಕ್ ಖಾತೆ ಸ್ಥಗಿತ, ಕೆವೈಸಿ ದಾಖಲಾತಿ ಪೂರ್ಣಗೊಳಿಸಲು ಸೂಚನೆ, ಲಾಟರಿ ಬಂದಿದೆ ಅಥವಾ ಕೆಲಸ ಕರೆ ಬಂದಿದೆ ಎಂಬಿತ್ಯಾದಿ ಆಮಿಷಗಳ ಬಲೆಯನ್ನು ಹೆಣೆಯಲಾಗುತ್ತದೆ. ಕೆಲವು ಪ್ರಕರಣಗಳಲ್ಲಿ ಟೆಲಿಗ್ರಾಂ ಆ್ಯಪ್ ಬಳಸಿ ಕೆಲವೊಂದು ಕೆಲಸಗಳನ್ನು ನೀಡಲಾಗುತ್ತದೆ. ಉದಾಹರಣೆಗೆ, ಸಿನಿಮಾ ವಿಮರ್ಶೆ ಮಾಡುವುದು, ಯೂಟ್ಯೂಬ್ ವಿಡಿಯೊಗೆ ಲೈಕ್ ಕೊಡುವುದು ಇತ್ಯಾದಿ. ಇವುಗಳೊಂದಿಗೆ ಒಂದು ಕೊಂಡಿಯನ್ನೂ ಕೊಟ್ಟಿರಲಾಗುತ್ತದೆ. ಅದನ್ನು ಕ್ಲಿಕ್ ಮಾಡಿದಾಗ ಟ್ರಾಜನ್ ವೈರಸ್ ನೇರವಾಗಿ ನಮ್ಮ ಮೊಬೈಲ್‌ಗೆ ಸೇರುತ್ತದೆ. ಅಲ್ಲಿಂದ ಮುಂದೆ ವಂಚಕರು ನಮ್ಮ ಮೊಬೈಲ್ ಅನ್ನು ಅವರ ಮೊಬೈಲ್‌ನಂತೆಯೇ ಬಳಸುವಂತಾಗುತ್ತದೆ.

ಫಿಶಿಂಗ್ ಮೂಲಕ ವ್ಯಕ್ತಿಯ ಧ್ವನಿ ಹಾಗೂ ದೂರವಾಣಿ ಸಂಭಾಷಣೆಯ ದಾಖಲೆ ಲಭ್ಯವಾಗುತ್ತದೆ. ಇದು ಮುಂದೆ ವಿಶಿಂಗ್