ಸೋವಾ ವೈರಸ್ ಎಚ್ಚರ ಅತ್ಯಗತ್ಯ

ಬದುಕನ್ನು ಸುಲಭಗೊಳಿಸಿರುವ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಬಗ್ಗೆ ಎಚ್ಚರ ತಪ್ಪಿದರೆ ಬ್ಯಾಂಕ್ ಖಾತೆಯೇ ಬರಿದಾಗುವಂತೆ ಮಾಡುತ್ತದೆ ಸೋವಾ ವೈರಸ್! ಈ ಬಗ್ಗೆ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಸೇವೆಯನ್ನು ಬಳಸುವವರೆಲ್ಲರೂ ಎಚ್ಚರವಹಿಸಲೇಬೇಕು.

■ ಶಶಿಕುಮಾರ್ ಸಿ.

ನಿಮ್ಮ ಅಮೂಲ್ಯವಾದ ಹಕ್ಕನ್ನು ಕದಿಯಲು ಮಾಲ್‌ವೇರ್‌ಗೆ ಅವಕಾಶ ಮಾಡಿಕೊಡಬೇಡಿ. ನಂಬಿಕಸ್ಥ ಆ್ಯಪ್‌ಗಳನ್ನು ಯಾವಾಗಲೂ ನಂಬಿಕಸ್ಥ ಮೂಲಗಳಿಂದಲೇ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ. ಸೋವಾ ವೈರಸ್ ಎಂದರೇನು ಮತ್ತು ಈ ವೈರಸ್‌ಗೆ ಕಡಿವಾಣ ಹಾಕಲು ಏನೆಲ್ಲ ಮುನ್ನೆಚ್ಚರಿಕೆ ಕ್ರಮಗಳನ್ನು ವಹಿಸಬೇಕು ಎಂಬುದನ್ನು ತಿಳಿಯೋಣ.

–ಎಸ್‌ಬಿಐ ಟ್ವೀಟ್

ಸ್ಮಾರ್ಟ್‌ಫೋನ್ ಲೋಕದಲ್ಲಿ ಹೊಸ ಹೊಸ ತಂತ್ರಜ್ಞಾನ ಆವಿಷ್ಕಾರಗೊಂಡಂತೆಲ್ಲ ಸೈಬರ್ ಸಮಸ್ಯೆಗಳು ತಲೆದೋರುತ್ತಲೆ ಇವೆ. ಅದರಲ್ಲೂ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ವ್ಯವಸ್ಥೆಯನ್ನು ಸ್ಮಾರ್ಟ್‌ಫೋನ್‌ಗಳು ಜನರ ಕೈಬೆರಳ ತುದಿಗೆ ತಂದಿಟ್ಟ ಬಳಿಕ ಈ ಸಮಸ್ಯೆಗಳು ಹೆಚ್ಚುತ್ತಲೇ ಇವೆ. ಇವುಗಳ ಸಾಲಿಗೆ ಹೊಸ ಸೇರ್ಪಡೆ 'ಸೋವಾ'.

ಬ್ಯಾಂಕ್ ಖಾತೆಗಳಿಗೆ ಕನ್ನ ಹಾಕಲೆಂದೇ 'ಸೋವಾ' ಎನ್ನುವ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ 'ಟ್ರೋಜನ್' ವೈರಸ್ ಲಗ್ಗೆ ಇಟ್ಟಿದೆ. ಆ್ಯಂಡ್ರಾಯ್ಡ್, ಸ್ಮಾರ್ಟ್‌ಫೋನ್‌ಗಳಲ್ಲಿನ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಗುರಿಯಾಗಿಸಿಕೊಂಡು ಈ ವೈರಸ್ ದಾಳಿ ಮಾಡುತ್ತಿದೆ. ಈ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಲು ಕೇಂದ್ರ ಸರ್ಕಾರದ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಏಜೆನ್ಸಿ ಸಾರ್ವಜನಿಕರಿಗೆ ಸಲಹೆ ನೀಡಿದೆ.

ಏನಿದು ಸೋವಾ ವೈರಸ್?

ಎಸ್‌ಬಿಐ (ಸ್ಟೇಟ್ ಬ್ಯಾಂಕ್ ಆಫ್ ಇಂಡಿಯಾ) ಪ್ರಕಾರ 'ಸೋವಾ' ಎನ್ನುವುದು ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಆಧಾರಿತ ಟ್ರೋಜನ್ ಮಾಲ್‌ವೇರ್ ಆಗಿದೆ. ನಕಲಿ ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಆ್ಯಪ್‌ಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಗ್ರಾಹಕರ ಬ್ಯಾಂಕಿಂಗ್ ಕುರಿತಾದ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಕದಿಯುವ ಚಾಳಿ ಇದರದ್ದು. ಗ್ರಾಹಕರು ಡಿಜಿಟಲ್ ಬ್ಯಾಂಕಿಂಗ್ ವ್ಯವಸ್ಥೆಯ ಮೇಲಿಟ್ಟಿರುವ ವಿಶ್ವಾಸವನ್ನು ಹುಸಿಗೊಳಿಸುವ ಕಾರ್ಯದಲ್ಲಿ ಈ ಟ್ರೋಜನ್ ಮಾಲ್‌ವೇರ್ ತೊಡಗಿಕೊಂಡಿದೆ.

ಸಾರ್ವಜನಿಕರು ನಕಲಿ ಬ್ಯಾಂಕಿಂಗ್ ಆ್ಯಪ್‌ಗಳನ್ನು ಅಚಾನಕ್ಕಾಗಿ ಕ್ಲಿಕ್ಕಿಸಿ ಲಾಗಿನ್ ಆಗುವಾಗ ಒದಗಿಸುವ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಈ ಮಾಲ್‌ವೇರ್ ಸಂಗ್ರಹಿಸುತ್ತದೆ. ಅದನ್ನು ಬಳಸಿಕೊಂಡು ಹ್ಯಾಕರ್‌ಗಳು ಸಾರ್ವಜನಿಕರ ಬ್ಯಾಂಕ್ ಖಾತೆಯಲ್ಲಿನ ಹಣವನ್ನು ಕ್ಷಣಾರ್ಧದಲ್ಲಿ ಗುಳುಂ ಮಾಡುತ್ತಾರೆ.

ಈ ಮಾಲ್‌ವೇರ್ ಒಮ್ಮೆ ನಿಮ್ಮ ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಆಧಾರಿತ ಸ್ಮಾರ್ಟ್‌ಫೋನ್‌ಗಳ ಒಳಹೊಕ್ಕರೆ (ಇನ್‌ಸ್ಟಾಲ್ ಆದರೆ) ಮುಗೀತು ಯಾವುದೇ ಕಾರಣಕ್ಕೂ ಅದನ್ನು ತೆಗೆಯಲು ಸಾಧ್ಯವಿಲ್ಲ. ಕಾರಣ ಇದು ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಆ್ಯಪ್‌ಗಳ ಜೊತೆಯೇ ಸ್ಮಾರ್ಟ್‌ಫೋನ್‌ನಲ್ಲಿ ಅಡಗಿಕೊಳ್ಳುತ್ತದೆ. ಈ ಸೋವಾ ವೈರಸ್ ಅಮೆರಿಕ, ರಷ್ಯಾ, ಸ್ಪೇನ್ ಮತ್ತು ಭಾರತೀಯ ಬ್ಯಾಂಕಿಂಗ್ ಬಳಕೆದಾರರನ್ನು ಗುರಿಯಾಗಿಸಿಕೊಂಡಿರುವುದು ಕಳವಳಕಾರಿ ವಿಚಾರ. ಭಾರತದಲ್ಲಿ ಈ ವೈರಸ್ ಇದೇ ವರ್ಷದ ಜುಲೈ ಆಸುಪಾಸಿನಲ್ಲಿ ಕಂಡುಬಂತಾದರೂ ಅದರ ತೀವ್ರತೆ ಈಗ ಹೆಚ್ಚಾಗಿದೆ.

ಮುನ್ನೆಚ್ಚರಿಕಾ ಕ್ರಮಗಳು

- ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಖಾತೆಗೆ ಎರಡು ಹಂತದ ದೃಢೀಕರಣ (ಅಥೆಂಟಿಕೇಶನ್) ವ್ಯವಸ್ಥೆ ಅಳವಡಿಸಿ.
- ಆ್ಯಪ್‌ಗಳನ್ನು ಟೈಮ್ ಟು ಟೈಮ್ ಅಪ್‌ಡೇಟ್ ಮಾಡಿ.
- ಗುಣಮಟ್ಟದ ಆ್ಯಂಟಿ ವೈರಸ್ ಬಳಸಿ.
- ಅನಾಮಿಕ, ಅನಧಿಕೃತ ಆ್ಯಪ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡದಿರಿ ಮತ್ತು ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ಕಿಸದಿರಿ.
- ಮೊಬೈಲ್ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಂ ಅನ್ನು ಅಪ್‌ಡೇಟ್ ಮಾಡಿ. ಬ್ರೌಸರ್‌ಗಳನ್ನು ಅಪ್‌ಡೇಟ್ ಮಾಡಿ.

ನಾಮವೊಂದೇ ರೂಪ ಹಲವು!

ಸೋವಾ ನಿರಂತರವಾಗಿ ಅಪ್‌ಡೇಟ್ ಆಗುತ್ತಿರುವ ವೈರಸ್ ಆಗಿದ್ದು, ಇದು ಹಲವು ರೂಪಗಳಲ್ಲಿ ಗ್ರಾಹಕರನ್ನು ಆಕರ್ಷಿಸುತ್ತಿದೆ. ಪೇಮೆಂಟ್ ಆ್ಯಪ್, ಬ್ಯಾಂಕಿಂಗ್ ಮತ್ತು ಇಕಾಮರ್ಸ್ ಆ್ಯಪ್‌ಗಳ ರೂಪದಲ್ಲಿ ಇದು ಇದು ಕಾಣಿಸಿಕೊಳ್ಳುತ್ತಿದೆ. ಕೆಲವೊಮ್ಮೆ ಮೆಸೇಜಿಂಗ್ ಆ್ಯಪ್‌ಗಳಲ್ಲಿ ಲಿಂಕ್‌ಗಳ ಮೂಲಕವೂ ಕಾಣಿಸಿಕೊಳ್ಳುತ್ತಿದೆ. ಗೂಗಲ್ ಕ್ರೋಮ್, ಅಮೆಜಾನ್ ಮತ್ತು ಎನ್‌ಎಫ್‌ಟಿ ರೂಪದಲ್ಲಿ ಸ್ಮಾರ್ಟ್‌ಫೋನ್ ಒಳಗೆ ಕಳ್ಳನಂತೆ ಬಂದು ಕೂರುವ ಸಾಧ್ಯತೆ ಇದೆ. ಇದನ್ನು ಒಮ್ಮೆ ಬಳಸಿದಾಗ ವೈಯಕ್ತಿಕ ವಿವರ, ಬ್ಯಾಂಕಿಂಗ್ ಮತ್ತು ಹಣಕಾಸು ಮಾಹಿತಿಯು ಕಳವಾಗುತ್ತವೆ ಎಂದಿದೆ ಸರ್ಟ್–ಇನ್(ರಾಷ್ಟ್ರೀಯ ಕಂಪ್ಯೂಟರ್ ಭದ್ರತಾ ಮತ್ತು ತುರ್ತು ಪ್ರತಿಕ್ರಿಯೆ ತಂಡ (ಸರ್ಟ್‌ಇನ್).

ಸೋವಾ ಸೇರಿದಂತೆ ಬೇರ್ಯಾವ ವೈರಸ್ ಬಗ್ಗೆಯಾಗಲಿ ಗ್ರಾಹಕರ ಎಚ್ಚರಿಕೆ ಮಹತ್ವದ್ದು. ವಿದೇಶಗಳಲ್ಲಿ ಈಗಾಗಲೇ ಸಾಕಷ್ಟು ಆರ್ಥಿಕ ಹಾನಿ ಮಾಡಿರುವ ಸೋವಾ ಭಾರತದಲ್ಲಿ ಕಾಣಿಸಿಕೊಂಡಿರುವುದು 5ನೇ ಆವೃತ್ತಿಯ ಮೂಲಕ. ಡಿವೈಸ್‌ಗಳಲ್ಲಿ ರ‍್ಯಾಂಡ್‌ಸಂವೇರ್‌ಗಳು ಅಡಗಿ ಗ್ರಾಹಕರ ಬ್ಯಾಂಕ್ ಖಾತೆಗೆ ಬೀಗ ಜಡಿಯುವ ಈ ಸೋವಾ ವೈರಸ್ ನಿರ್ವಾಹಕರು ಅಂದರೆ ಸೈಬರ್ ಖದೀಮರು ಖಾತೆ ಅನ್‌ಬ್ಲಾಕ್ ಮಾಡಲು ಹಣದ ಬೇಡಿಕೆ ಇಡುತ್ತಾರೆ. ■