

ಆನ್‌ಲೈನ್ ಅಪರಾಧ

ಖದೀಮರ ಬಗ್ಗೆ ಇರಲಿ ಎಚ್ಚರ

■ ಸತೀಶ್ ವೆಂಕಟಸುಬ್ಬ

ಇಂದಿನ ಡಿಜಿಟಲ್ ಯುಗದಲ್ಲಿ, ಇಂಟರ್ನೆಟ್ ಮತ್ತು ಸ್ಮಾರ್ಟ್‌ಫೋನ್‌ಗಳು ನಮ್ಮ ಬದುಕಿನ ಭಾಗವಾಗಿವೆ. ಒಂದೆಡೆ, ಇವು ನಮ್ಮ ಕೆಲಸಗಳನ್ನು ಸುಲಭಗೊಳಿಸಿವೆ, ಇನ್ನೊಂದೆಡೆ ಸೈಬರ್ ಅಥವಾ ಆನ್‌ಲೈನ್ ಅಪರಾಧಗಳ ಅಪಾಯವನ್ನು ಹೆಚ್ಚಿಸಿವೆ. ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್‌ನಿಂದ ಹಿಡಿದು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳವರೆಗೆ, ನಾವು ಮಾಡುವ ಪ್ರತಿಯೊಂದು ಕ್ಲಿಕ್‌ನಲ್ಲೂ ಒಂದು ರೀತಿಯ ಅಪಾಯ ಅಡಗಿದೆ.

ಕಳೆದ ವರ್ಷ 2024ರೊಂದರಲ್ಲೇ ವಿಶ್ವಾದ್ಯಂತ ಸೈಬರ್ ಅಪರಾಧಗಳಿಂದ ಆದ ನಷ್ಟ ಏಳು ಲಕ್ಷ ಕೋಟಿ ರೂಪಾಯಿ. ಸಂಸ್ಥೆಗಳಲ್ಲಿ ಪ್ರಸ್ತುತಪಡಿಸಿದ ವರದಿಯ ಪ್ರಕಾರ ಭಾರತದಲ್ಲಿ 36.37 ಲಕ್ಷ ಸೈಬರ್ ಅಪರಾಧಗಳು ವರದಿಯಾಗಿದ್ದು, ಅದರಿಂದ ಆದ ನಷ್ಟ 22,845.73 ಕೋಟಿ ರೂಪಾಯಿಗಳಾಗಿದ್ದು, ಅದು 2023ಕ್ಕೆ ಹೋಲಿಸಿದರೆ ಶೇಕಡ 206ಕ್ಕಿಂತ ಜಾಸ್ತಿಯಾಗಿರುತ್ತದೆ. ಕರ್ನಾಟಕವೊಂದರಲ್ಲೇ 2024ರಲ್ಲಿ 22,415 ಸೈಬರ್ ಅಪರಾಧ ಪ್ರಕರಣಗಳು ವರದಿಯಾಗಿದ್ದು, ಅದರಿಂದ ಆದ ನಷ್ಟ 2,915 ಕೋಟಿ ರೂಪಾಯಿಗಳಾಗಿರುತ್ತದೆ.

ಸರ್ಕಾರ ಮತ್ತು ಕಂಪನಿಗಳು ಸಾಮಾನ್ಯ ಜನರಿಗೆ ಆನ್‌ಲೈನ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಹೇಗೆ ಬಳಸುವುದು ಎಂಬುದರ ಕುರಿತು ತರಬೇತಿ ನೀಡದೆ ಅವುಗಳತ್ತ ನೂಕಿದ್ದು ಇದಕ್ಕೆ ಪ್ರಮುಖ ಕಾರಣಗಳಲ್ಲಿ ಒಂದು. ಈ ನಿಟ್ಟಿನಲ್ಲಿ ಸೈಬರ್ ಅಥವಾ ಆನ್‌ಲೈನ್ ವಂಚನೆ ಎಂದರೆನು, ಪ್ರಮುಖ ಸೈಬರ್ ಅಪರಾಧಗಳ ಸ್ಥೂಲ ಪರಿಚಯ, ಅದರಿಂದ ಪಾರಾಗಲು ಇರುವ ಉಪಾಯಗಳು, ಅದಕ್ಕೆ ನೀವೇನಾದರೂ ಬಲಿಯಾಗಿದ್ದರೆ ಏನು ಮಾಡಬೇಕು ಮತ್ತು ನಿಮ್ಮ ಸಹಾಯಕ್ಕಾಗಿರುವ ಕಾನೂನುಗಳ ಬಗ್ಗೆ ಮಾಹಿತಿ ತಿಳಿದಿರಬೇಕು.

ಸೈಬರ್ ಕೈ ಎಂದರೇನು?

ಸರಳವಾಗಿ ಹೇಳುವುದಾದರೆ, ಸೈಬರ್ ಕ್ರೈಮ್ ಅಥವಾ ಆನ್‌ಲೈನ್ ಅಪರಾಧಗಳು ಎನ್ನುವುದು ಕಂಪ್ಯೂಟರ್/ಕಂಪ್ಯೂಟಿಂಗ್ ಸಾಧನ ಅಥವಾ ಇಂಟರ್ನೆಟ್‌ಗೆ ಸಂಪರ್ಕಗೊಂಡಿರುವ ಇತರ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಉಪಕರಣಗಳ ಸಹಾಯದಿಂದ ಮಾಡಿದ ಅಪರಾಧ ಕೃತ್ಯವನ್ನು ಸೂಚಿಸುತ್ತದೆ. ಇಲ್ಲಿ ಕಂಪ್ಯೂಟಿಂಗ್ ಸಾಧನ (ಕಂಪ್ಯೂಟರ್, ಸ್ಮಾರ್ಟ್‌ಫೋನ್, ಟ್ಯಾಬ್ಲೆಟ್ ಇತ್ಯಾದಿ) ಅಥವಾ ನೆಟ್‌ವರ್ಕ್ (ಇಂಟ್ರಾನೆಟ್/ಅಂತರಿಕ ಜಾಲ ಅಥವಾ ಜಾಗತಿಕ ಇಂಟರ್ನೆಟ್/ಅಂತರ್ಜಾಲ) ಅನ್ನು ಸೈಬರ್ ಅಪರಾಧಕ್ಕೆ ಬಳಸಿರಬಹುದು ಅಥವಾ ಅದು ಅಪರಾಧದ ಮೂಲ ಪರಿಕರವಾಗಿರಬಹುದು ಅಥವಾ ಗುರಿ/ಟಾರ್ಗಟ್ ಆಗಿರಬಹುದು. ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು, ವ್ಯಕ್ತಿಗಳ ವಿರುದ್ಧ ನಡೆಸುವ ಸೈಬರ್ ಅಪರಾಧಗಳು (ಸೈಬರ್ ಸ್ಟಾಕಿಂಗ್, ಸಿಮ್‌ಸ್ವಾಪ್ ಹಗರಣ ಇತ್ಯಾದಿ) ಅಥವಾ ಸಂಸ್ಥೆಗಳ ವಿರುದ್ಧ ನಡೆಸುವ ಸೈಬರ್ ಅಪರಾಧಗಳು (ರಾನ್ಸಮ್‌ವೇರ್ ದಾಳಿ, DDoS ದಾಳಿ ಇತ್ಯಾದಿ) ಅಥವಾ ಸರ್ಕಾರ ಅಥವಾ ಸಮಾಜದ ವಿರುದ್ಧ ನಡೆಸುವ ಸೈಬರ್ ಅಪರಾಧಗಳು (ಸೈಬರ್ ಭಯೋತ್ಪಾದನೆ, ಸೈಬರ್ ಅಶ್ಲೀಲತೆ ಇತ್ಯಾದಿ) ಎಂಬ ಆಧಾರದ ಮೇಲೆ ಕೂಡ ವರ್ಗೀಕರಿಸಬಹುದು.

