

ಸೂಚಿಕೆ

ಅಧ್ಯಾಯ	ವಿಷಯ	ಪುಟ
	ಪೀಠಿಕೆ	1
1	ಜನಜಾಗೃತಿಯ ಅಗತ್ಯ	5
2	ಅಪರಾಧ ಯಾವುದು?	11
3	ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿ	45
4	ಸೈಬರ್ ಸಾಕ್ಷಿ	49
5	ಭಾರತದಲ್ಲಿನ ಸೈಬರ್ ಕಾನೂನು	57
6	ಸೈಬರ್ ಕ್ರಿಮಿನಿಯಂತ್ರಣ	81

ಪೀಠಿಕೆ

“ಕಾನೂನು ಮಾಡುವುದು ಸರ್ಕಾರದ ಕೆಲಸ. ಅದನ್ನು ತಿಳಿದುಕೊಳ್ಳುವುದು ಪ್ರಜೆಯ ಜವಾಬ್ದಾರಿ” ಎಂಬ ಅಭಿಪ್ರಾಯ ಕೆಲವರದು. ಆದರೆ ಈ ರೀತಿಯ ಧೋರಣೆಯಿಂದ ಜನರಲ್ಲಿ ಕಾನೂನಿನ ಬಗ್ಗೆ ಹೆದರಿಕೆ ಬರುತ್ತದೆಯೇ ಹೊರತು ಗೌರವ ಬರುವುದಿಲ್ಲ ಎಂಬುದು ನನ್ನ ಅಭಿಪ್ರಾಯ.

ಕಾನೂನಿನ ಅಜ್ಞಾನದ ಲಾಭ ಜನರ ಅಮಾಯಕತೆಯನ್ನು ದುರುಪಯೋಗ ಮಾಡಿಕೊಳ್ಳುವವರಿಗೆ ಮಾತ್ರ. ಆದ್ದರಿಂದ ಕಾನೂನಿನ ಪರಿಚಯವನ್ನು ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಮಾಡಿಕೊಡಬೇಕಾದುದು ನಮ್ಮ ಕರ್ತವ್ಯ.

ಮಾಹಿತಿ ತಂತ್ರ ಜ್ಞಾನ ಕಾಯಿದೆ (ಮಾತಂಕಾ-2000) ಭಾರತದಲ್ಲಿ ಕಾನೂನಿನ ರೂಪಕ್ಕೆ ಬಂದು 4 ವರ್ಷಗಳು ಕಳೆದಿದ್ದರೂ ಅದರ ಬಗ್ಗೆ ಅರಿವು ಇನ್ನೂ ನಮ್ಮ ಜನಗಳಲ್ಲಿ ಮೂಡಿಲ್ಲ. ಜನ ಸಾಮಾನ್ಯರಲ್ಲದೆ, ವಾಣಿಜ್ಯ ವಲಯದಲ್ಲೂ, ಸರ್ಕಾರಿ ಮತ್ತು ಪ್ರೈವೇಟ್ ವಲಯದಲ್ಲೂ ಈ ಕಾನೂನಿನ ಅರಿವು ಇರಬೇಕಾದಷ್ಟು ಇಲ್ಲ. ವಕೀಲರ ಮತ್ತು ನ್ಯಾಯಾಂಗ ವಲಯದಲ್ಲೂ ಈ ಕಾನೂನಿನ ಬಗ್ಗೆ ಹೆಚ್ಚು ತಿಳುವಳಿಕೆ ಮೂಡಿಲ್ಲ ಎಂಬುದು ಸತ್ಯ.

ಇದಕ್ಕೆ ಮುಖ್ಯ ಕಾರಣ ಮಾತಂಕಾ ಅರ್ಥ ಮಾಡಿಕೊಳ್ಳಬೇಕಿದ್ದರೆ ಸ್ವಲ್ಪ ಮಟ್ಟಿಗೆ ತಾಂತ್ರಿಕ ಜ್ಞಾನ ವನ್ನು ರೂಢಿಸಿಕೊಳ್ಳಬೇಕಾದ ಅವಶ್ಯಕತೆಯಿರುವುದು.

ನಮ್ಮ ನಾಡಿನ ವಕೀಲರಿಗೆ ಇತ್ತೀಚೆಗಷ್ಟೆ ಕಂಪ್ಯೂಟರ್ ಮತ್ತು ಅದರ ಉಪಯೋಗಗಳ ಬಗ್ಗೆ ಆಸಕ್ತಿ ಮೂಡಿದೆ. ಇನ್ನು ಮೇಲೆ ಅವರು ಈ ಕಾನೂನಿನ ಬಗ್ಗೆ ಹೆಚ್ಚಿನ ಗಮನ ಕೊಡುತ್ತಾರೆಂದು ಆಶಿಸುತ್ತೇನೆ.

ಮಾತಂಕಾ ಮೊದಲ ಬಾರಿ ಪ್ರಕಟವಾಗುವ ಮುಂಚೆಯೇ 1999 ನೇ ಇಸವಿಯಲ್ಲಿ ನಾನು ನನ್ನ ಮೊದಲ ಪುಸ್ತಕ “ ಸೈಬರ್ ಲಾಸ್ ಫ್ಲಾರ್ ಎವ್ವೆರಿ ನೆಟಿಜೆನ್” ಪ್ರಕಟ ಮಾಡಿದೆ. ನಂತರ 2003 ರಲ್ಲಿ “ಸೈಬರ್ ಲಾಸ್ ಇನ್ ಇಂಡಿಯಾ..ಐ.ಟಿ.ಎ. 2000 ಎಂಡ್ ಬಿಯಾಂಡ್” ಎಂಬ ಪುಸ್ತಕವನ್ನು ಇ-ಪುಸ್ತಕದ ರೂಪದಲ್ಲಿ ಬಿಡುಗಡೆ ಮಾಡಿದೆ. ಇತ್ತೀಚೆಗಷ್ಟೆ “ಸೈಲಾಕಾಂ... ಕಾರ್ಪೊರೇಟ್ ಮಂತ್ರ ಫ್ಲಾರ್ ದಿ ಡಿಜಿಟಲ್ ಎರಾ” ಎಂಬ ಪುಸ್ತಕವನ್ನೂ ಪ್ರಕಟಿಸಿದೆ.

ಈಗ ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಮತ್ತು ಶಾಲಾ ಕಾಲೇಜು ವಿದ್ಯಾರ್ಥಿಗಳಿಗೆ ಉಪಯೋಗವಾಗುವ ಅಂತರ್ಜಾಲ ಅಪರಾಧ ಹಾಗೂ ಸಾಮಾನ್ಯ ಸೈಬರ್ ಕಾನೂನಿನ ಬಗ್ಗೆ ಕನ್ನಡದಲ್ಲಿ ಪ್ರಕಟಮಾಡಬೇಕೆಂಬ ನನ್ನ ಬಯಕೆ ಈ ಪುಸ್ತಕ ರೂಪದಲ್ಲಿ ಹೊರಬಂದಿದೆ.

ಬಹುಶಃ ಭಾರತದಲ್ಲೇ ಮೊದಲ ಬಾರಿಗೆ ಸೈಬರ್ ಕಾನೂನಿನ ಬಗ್ಗೆ ಪ್ರಾದೇಶಿಕ ಭಾಷೆಯಲ್ಲಿ ಪ್ರಕಟವಾದ ಪುಸ್ತಕ ಇದು ಎಂದು ನನ್ನ ಭಾವನೆ.

ಕರ್ನಾಟಕದಲ್ಲಿ ಸೈಬರ್ ಕೆಫ್ಫೆ ನಿಯಂತ್ರಣ ಜಾರಿಯಾಗಿರುವ ಮೊದಲ ದಿನಗಳಲ್ಲೇ ಈ ಪುಸ್ತಕ ಪ್ರಕಟವಾಗಿರುವುದು ಸೈಬರ್ ಕೆಫ್ಫೆ ಮಾಲೀಕರಿಗೆ ಉಪಯೋಗವಾಗಬಹುದೆಂದು ನನ್ನ ಭಾವನೆ. ಹಾಗೇ ಕಂಪ್ಯೂಟರ್ ಬಗ್ಗೆ ಹಾಗೂ ಅಂತರ್ಜಾಲದ ಬಗ್ಗೆ ವಿದ್ಯೆ ಕಲಿಸುತ್ತಿರುವ ಶಾಲೆಗಳಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ಅಪರಾಧದ ಬಗ್ಗೆಯೂ ಕೂಡ ತಿಳುವಳಿಕೆ ಕೊಡಬೇಕಾದ ಅಗತ್ಯವನ್ನು ಈ ಪುಸ್ತಕ ಪೂರೈಸಬಹುದು.

ಇ-ಆಡಳಿತದ ಮುಂಚೂಣಿಯಲ್ಲಿರುವ ನಮ್ಮ ರಾಜ್ಯದ ಅನೇಕ ಸರ್ಕಾರಿ ಕಾರ್ಯಾಲಯಗಳಲ್ಲೂ ಹಳ್ಳಿ ಪ್ರದೇಶಗಳಲ್ಲಿರುವ ರೆವೆನ್ಯೂ ಕಛೇರಿಗಳಲ್ಲೂ ಸೈಬರ್ ಕಾನೂನಿನ ಅರಿವು ಅಗತ್ಯವಾಗಿದೆ. ಈ ಪುಸ್ತಕ ಸ್ವಲ್ಪ ಮಟ್ಟಿಗಾದರೂ ಇಲ್ಲಿಯ ಅಗತ್ಯಗಳನ್ನು ಪೂರೈಸಬಹುದು.

ಮುಖ್ಯವಾಗಿ ಸೈಬರ್ ಅಪರಾಧದ ಅರಿವು ರಾಜ್ಯದ ಎಲ್ಲಾ ಪೊಲೀಸ್ ಸ್ಟೇಷನ್ ಗಳಿಗೂ ತಲುಪುವ ಅಗತ್ಯವಿದೆ. ಬಹುಶಃ ಈ ಪುಸ್ತಕದ ಪ್ರಮುಖ ಉಪಯೋಗ ಇಲ್ಲಿ ಆಗಬಹುದು.

ಕನ್ನಡದಲ್ಲಿ ಕಾನೂನಿನ ಬಗ್ಗೆ, ಅದರಲ್ಲೂ ತಾಂತ್ರಿಕ ಕಾನೂನಿನ ಬಗ್ಗೆ ಪುಸ್ತಕ ಬರೆಯುವುದು ಹೊರನಾಡ ಕನ್ನಡಿಗನಾದವನಿಗೆ ಸುಲಭ ಸಾಧ್ಯವಲ್ಲ. ಆದರೂ ಇರುವ ಅಗತ್ಯವನ್ನು ಮನಗೊಂಡು ನನ್ನ ಅರಿವಿನ ಶಬ್ದ ಸಂಪತ್ತಿನೊಳಗೆ ಈ ಪುಸ್ತಕವನ್ನು ಬರೆಯುವುದಕ್ಕೆ ಪ್ರಯತ್ನ ಸಿದ್ಧೇನೆ. ಇದರಲ್ಲಿ ಕಾಣಬರುವ ಕನ್ನಡ ಪದಗಳ ಕೊರತೆಯನ್ನು ಮುಂದಿನ ಆವೃತ್ತಿಗಳಲ್ಲಿ ನೀಗುವುದಕ್ಕೆ ಪ್ರಯತ್ನ ಮಾಡುತ್ತೇನೆ. ಈ ವಿಚಾರವನ್ನು ಗಮನಿಸಿ ಓದುಗರು ಈ ಪ್ರಯತ್ನಕ್ಕೆ ಪ್ರೋತ್ಸಾಹ ಕೊಡುತ್ತಾರೆಂದು ನಂಬಿದ್ದೇನೆ.

ನಾ.ವಿಜಯಶಂಕರ

[ನಾವಿ]

1. ಸೈಬರ್ ಮೋಸ:

ಮೋಸ ವೆಂದರೆ ಒಬ್ಬರನ್ನು ತಪ್ಪು ಮಾಹಿತಿಯಿಂದ ವಂಚಿಸಿ ಹಣದ ಅಥವಾ ಬೇರಾವುದೇ ರೀತಿಯ ಲಾಭವನ್ನು ಪಡೆದುಕೊಳ್ಳುವುದು ಎನ್ನಬಹುದು.

ಅಂತರ್ಜಾಲ ಇಂದು ಹೊಂದಿರುವ ಲಕ್ಷಾಂತರ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲಿ ಅನೇಕ ರೀತಿಯ ಮಾಹಿತಿ ಇರುವುದರಿಂದ ಜನ ಸಾಮಾನ್ಯರು ಅಗಾಧ ಈ ವೆಬ್ ಸೈಟ್ ಗಳಿಗೆ ಹೋಗಿ ಅಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯುವುದು ಸಹಜ. ಅದೇ ರೀತಿ ಯಾವುದಾದರೂ ಇ-ಮೈಲ್ ಬಂದರೆ ಅದರಲ್ಲಿರುವ ಮಾಹಿತಿ ನಂಬಲರ್ಹವೆಂದುಕೊಳ್ಳುವುದೂ ಸಹಜ. ಅಂತರ್ಜಾಲ ಮೋಸ ಪ್ರಕರಣಗಳಲ್ಲಿ ಮುಖ್ಯವಾಗಿ ವಂಚಕರು ವಂಚನೆಗೆ ಉಪಯೋಗಿಸುವುದು “ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್”ಗಳು.

ಉದಾಹರಣೆಗೆ ಕೆಲವು ವರ್ಷಗಳ ಹಿಂದೆ ಒಂದು ವಂಚನೆ ಪ್ರಕರಣ ಬೆಳಕಿಗೆ ಬಂದಿತು. ಇದರಲ್ಲಿ ಅಂಧದ ಒಬ್ಬ ವ್ಯಾಪಾರಿ ಒಂದು ಅಂತರ ರಾಷ್ಟ್ರೀಯ ಲಾಟರಿಯಲ್ಲಿ ಹಲವು ಕೋಟಿ ರೂಪಾಯಿ ಗೆದ್ದಿರುವುದಾಗಿಯೂ ಅದರ ಆಧಾರದ ಮೇಲೆ ಅವನು ಇಲ್ಲಿಯ ಬ್ಯಾಂಕುಗಳಲ್ಲಿ ಸಾಲ ತೆಗೆದುಕೊಂಡು ವಂಚನೆ ಮಾಡಿರುವುದಾಗಿಯೂ ಆಪಾದಿಸಲಾಗಿತ್ತು. ಈ ಪ್ರಸಂಗದಲ್ಲಿ ತಾನು ಲಾಟರಿಯಲ್ಲಿ ಬಹುಮಾನ ಪಡೆದಿರುವುದಕ್ಕೆ ಒಂದು ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ಆಧಾರವಾಗಿ ಆಪಾದಿತ ತೋರಿಸಿರುವುದಾಗಿಯೂ ಮತ್ತು ಅದು ಸುಳ್ಳಾಗಿತ್ತೆಂದೂ ತಿಳಿಸಲಾಗಿತ್ತು.

ಮುಖ ನೋಟಕ್ಕೆ ಇದು ತಿಳಿಯಾದ ಮೋಸ ಪ್ರಸಂಗದಂತೆ ಕಾಣಬಹುದು. ಆದರೆ ಇದರ ಹಿಂದೆ ಒಂದು ದೊಡ್ಡ ಅಂತರ್ಜಾಲ ವಂಚನೆಯ ಯೋಜನೆ ಇದ್ದು ಇದರಲ್ಲಿ ಅಂಧದ ಆಪಾದಿತ ಮಹಾಶಯ ಬಹುಶಃ ಒಬ್ಬ ಅಮಾಯಕ ಬಲಿಪಶು (ವಿಕ್ಟಿಮ್) ಆಗಿರಬಹುದು. ಈ ಲಾಟರಿ ಬಹುಮಾನ ವಂಚನೆ ಈಗಲೂ ನಾವು ಕಾಣಬರುವ ಮೋಸ ಪ್ರಸಂಗಗಳಲ್ಲೊಂದು.

ಈ ಮೋಸದ ವೈಖರಿ ಹೀಗಿರುತ್ತದೆ.

ಮೊದಲು ಸಾಮಾನ್ಯವಾಗಿ ಒಬ್ಬರಿಗೆ ಇ-ಮೈಲ್ ಮೂಲಕ ಅವರು ದೊಡ್ಡ (ಸುಮಾರು 5 ಕೋಟಿ ರೂಪಾಯಿ ಇರಬಹುದು) ಲಾಟರಿ ಬಹುಮಾನ ಪಡೆದಿರುವುದಾಗಿಯೂ ಅದನ್ನು

ಪಡೆದುಕೊಳ್ಳಲು ತಮ್ಮ ಇ-ಮೈಲ್ ವಿಳಾಸವನ್ನು ಧೃಢೀಕರಿಸಿದರೆ ಸಾಕೆಂದು ಒಂದು ಇ-ಮೈಲ್ ಬರುತ್ತದೆ. ಇದಕ್ಕೆ ಬದಲು ನೀಡಿದರೆ, ನಂತರ ಮುಂದಿನ ಇ-ಮೈಲ್ ಗಳಲ್ಲಿ, ಇನ್ನೇನು ನಿಮಗೆ ಹಣ ಕಳುಹಿಸಿಬಿಡುತ್ತೇವೆ, ದಯವಿಟ್ಟು ನಮ್ಮ ಕಮಿಶನ್ ನೂರು ಡಾಲರ್ ಕಳುಹಿಸಿ ಎಂದು ನಯವಾದ ಕಾಗದ ಬರುತ್ತದೆ. ಇದನ್ನು ನಂಬಿ ಹಣ ಕಳುಹಿಸಿದರೆ ಅದು ಗೋವಿಂದ.

ಈ ಮೋಸಕ್ಕೆ ಪುಷ್ಟಿ ಕೊಡಲು ಮೋಸಗಾರರ ಕಡೆಯಿಂದ ಫೋನ್ ನಲ್ಲಿ ಮಾತನಾಡಿ ನಾವು ಲಾಟರಿ ಸಂಸ್ಥೆಯ ಆಡಿಟರ್ ಅಥವಾ ಬ್ಯಾಂಕ್ ನವರೆಂದೂ ನಂಬಿಸುವುದೂ ಉಂಟು. ಈ ರೀತಿಯ ಮೋಸದ ಲಾಟರಿ ಬಲೆಯಲ್ಲಿ ಲಕ್ಷಾಂತರ ರೂಪಾಯಿ ಕಳೆದುಕೊಂಡವರ ಉದಾಹರಣೆ ಇದೆ.

ಅಂಧ ಪ್ರಕರಣ ಈ ರೀತಿಯ ಪ್ರಕರಣವೋ ಅಥವಾ ನಿಜವಾಗಿಯೂ ಆಪಾದಿತ ತಾನೇ ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್ ಮಾಡಿ ಮೋಸ ಮಾಡುವುದಕ್ಕೆ ಪ್ರಯತ್ನ ಪಟ್ಟನೋ ನಮಗೆ ತಿಳಿದಿಲ್ಲ. ಆದರೆ ಈ ಲಾಟರಿ ಬಹುಮಾನದ ಇ-ಮೈಲ್ ಬಗ್ಗೆ ಯಾವ ಕಾಳಜಿಯನ್ನೂ ತೋರದಿರುವುದು ಕ್ಷೇಮ.

ನೈಜೀರಿಯನ್ ವಂಚನೆ ಎಂಬ ಮತ್ತೊಂದು ವಂಚನೆ ಜಾಲ ದಲ್ಲಿ ಇನ್ನೊಂದು ಬಗೆಯ ಇ-ಮೈಲ್ ಬರುತ್ತದೆ. ಇದರಲ್ಲಿ ನಾನು ನೈಜೀರಿಯ ಮಾಜಿ ಅಧ್ಯಕ್ಷರ ವಿಧವೆಯೆಂದೂ, ತನ್ನ ಬಳಿ ಸುಮಾರು 100 ಕೋಟಿ ರೂಪಾಯಿ ಬ್ಯಾಂಕ್ ಖಾತೆಯಲ್ಲಿರುವುದಾಗಿಯೂ, ಅದನ್ನು ದೇಶದಿಂದ ಹೊರಗೆ ಸಾಗಿಸಲು ಸಹಾಯ ಮಾಡಿದರೆ ನಿಮಗೆ 5 % ಕಮಿಶನ್ ನೀಡುವುದಾಗಿಯೂ ತಿಳಿಸಲಾಗುತ್ತದೆ. ಇದಕ್ಕೆ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ವಿವರ ಕೊಟ್ಟರೆ ಸಾಕು ಅದಕ್ಕೆ ಹಣ ವರ್ಗಾವಣೆ ಮಾಡುವುದಾಗಿಯೂ ತಿಳಿಸಿರುತ್ತೆ. ಕೆಲವು ಬಾರಿ ಇದೇ ರೀತಿಯ ಇ-ಮೈಲ್, ಸದ್ವಾಮ್ ಹುಸೈನ್ ನ ನೆಂಟರಂತೆಯೂ, ನೇಪಾಳದ ಮಾಜಿ ರಾಜ ಬಿರೇಂದ್ರ ವಿಕ್ರಂ ನ ನೆಂಟರಂತೆಯೂ ಅಥವಾ ಒಂದು ಪೆಟ್ರೋಲಿಯಂ ಕಂಪನಿಯ ಮಾಲೀಕನ ಹೆಸರಿನಲ್ಲೂ ಬಂದದ್ದಿದೆ. ಈ ಎಲ್ಲಾ ವಂಚನೆಗಳ ಉದ್ದೇಶ ನಿಮ್ಮಿಂದ ಕಮಿಶನ್ ರೂಪದಲ್ಲಿ ಸುಮಾರು 1000 ದಿಂದ 5000 ಡಾಲರ್ ಹೊಡೆಯುವುದು. ಕೆಲವು ಪ್ರಸಂಗಗಳಲ್ಲಿ ಜನಗಳನ್ನು ನೈಜೀರಿಯ ಅಥವಾ ಲಂಡನ್ ಗೆ ಹೆಚ್ಚಿನ ಮಾತುಕತೆಗೆ ಆಹ್ವಾನಿಸಿ ಅಪಹರಣ ಮಾಡಿ ಕೊಲೆ ಮಾಡಿರುವ ಸಾಧ್ಯತೆಗಳೂ ಇವೆ ಎಂದು ಎಫ್ ಬಿ ಐ ತಿಳಿಸಿದೆ.

ಇದೇ ರೀತಿ ಸಂಭಾಷಣೆ ಆರಂಭಿಸಿ ನಂಬಿದ ಜನರನ್ನು ಹವಾಲ (ವಿದೇಶಿ ಹಣ ಬದಲಾವಣೆ) ವ್ಯವಹಾರಕ್ಕೆ ಬಳಸಿಕೊಳ್ಳುವ ಪ್ರಯತ್ನಗಳೂ ಭಾರತದಲ್ಲಿಯೇ ಬೆಳಕಿಗೆ ಬಂದಿದೆ.

ಬೇರೊಂದು ಬಗೆಯ ಮೋಸದಲ್ಲಿ ಕಿಡಿಗೇಡಿಗಳು ಏನು ಮಾಡುತ್ತಾರೆಂದರೆ, ನಮಗೆಲ್ಲಾ ತಿಳಿದಿರುವ ಸಿಟಿ ಬ್ಯಾಂಕ್ ಅಥವಾ ಹಾಂಕಾಂಗ್ ಬ್ಯಾಂಕ್ ತರಹದ ಬ್ಯಾಂಕ್ ಹೆಸರಿನಲ್ಲಿ ಒಂದು ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್ ಸೃಷ್ಟಿಮಾಡಿ “ನೀವು ಬ್ಯಾಂಕ್ ಗ್ರಾಹಕರಾಗಿದ್ದರೆ ಒಡನೆಯೇ ಈ ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋಗಿ ಖಾತೆ ಸರಿಯಾಗಿದೆಯೇ ಎಂದು ಪರೀಕ್ಷಿಸಿ” ಎಂದು ಇ-

ಮೈಲ್ ಮೂಲಕ ಎಲ್ಲರಿಗೂ ಸುದ್ದಿ ಕೊಡುತ್ತಾರೆ. ಹಾಗೆ ಯಾರಾದರೂ ಈ ಸುಳ್ಳು ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋಗಿ ತಮ್ಮ ಪಾಸ್ ವರ್ಡ್ ಉಪಯೋಗಿಸಿ (ಖಾತೆಯನ್ನು ಅಂತರ್ಜಾಲದ ಮೂಲಕ ನಿರ್ವಹಿಸುವುದಕ್ಕೆ ಬೇಕಾದ ಗುಟ್ಟಾಗಿಡಬೇಕಾದ ಪ್ರವೇಶ ಪದ) ಪರೀಕ್ಷಿಸಿದರೆ ಒಡನೆಯೇ, ಆ ಪಾಸ್ ವರ್ಡ್ ಕದ್ದು ನಂತರ ತಾವು ನಿಜವಾದ ಬ್ಯಾಂಕ್ ವೆಬ್ ಸೈಟ್ ಗೆ ಹೋಗಿ ಹಣ ದೋಚಿಕೊಂಡು ಪರಾರಿಯಾಗುತ್ತಾರೆ.

ಈ ಪ್ರಕರಣಗಳಲ್ಲಿ ನಾವು ಮುಖ್ಯವಾಗಿ ನೆನಪಿನಲ್ಲಿಡಬೇಕಾದ ಅಂಶ ವೇನೆಂದರೆ, ನಮಗೆ ಬರುವ ಇ-ಮೈಲ್ ಗಳಲ್ಲಿರುವ ವಿಷಯಗಳನ್ನೆಲ್ಲಾ ನಂಬಿ ಮೋಸ ಹೋಗ ಬಾರದು. ಹಾಗೇ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲಿ ಕಳ್ಳ ವೆಬ್ ಸೈಟ್ ಗಳೂ ಇರುತ್ತವೆಂದು ನಾವು ತಿಳಿದಿರಬೇಕು.

ಹಾಗೆಯೇ ಇಂತಹ ಪ್ರಕರಣಗಳು ನಮ್ಮ ಗಮನಕ್ಕೆ ಬಂದರೆ ಅದನ್ನು ಪೊಲೀಸರ ಗಮನಕ್ಕೆ ತರಲು ಪ್ರಯತ್ನ ಪಡಬಹುದು.

ಭಾರತದಲ್ಲಿರುವ ಸೈಬರ್ ಕಾನೂನಿನ ಪ್ರಕಾರ ಸೈಬರ್ ಮೋಸದಿಂದ ವಂಚಿತರಾದವರು ವಿಶೇಷ ಕಾನೂನು ವ್ಯವಸ್ಥೆಯಲ್ಲಿ “ಅಡ್ವಾಡಿಕೇಟರ್” (ಸೈಬರ್ ನಿರ್ಣಯಕಾರ) ಮೂಲಕ ಅಪರಾಧಿಗಳಿಂದ ಒಂದು ಕೋಟಿ ರೂಪಾಯಿವರೆವಿಗೆ ನಷ್ಟ ಪರಿಹಾರ ಕೇಳಬಹುದು.

ಅಂತೆಯೇ, ನಾವು ನ್ಯಾಯವಾಗಿ ಅಂತರ್ಜಾಲದ ಮೂಲಕ ಮಾಡುವ ವ್ಯವಹಾರವನ್ನು ಬೇರೆಯವರು ನಂಬಬೇಕಿದ್ದರೆ ಸೈಬರ್ ಕಾನೂನಿನಲ್ಲಿ ತಿಳಿಸಿರುವ ಡಿಜಿಟಲ್ ಸಿಗ್ನೇಚರ್ ಅಥವಾ “ಡಿಜಿಟಲ್ ಸಹಿ” ಯನ್ನು ನಮ್ಮ ಇ-ಮೈಲ್ ಗಳಲ್ಲೂ ಹಾಗೂ ವೆಬ್ ಸೈಟ್ ಗಳಲ್ಲೂ ಬಳಸಲು ಪರಿಣಿತರ ಸಲಹೆ ಪಡೆಯಬಹುದು.

ಇ-ಆಡಳಿತ

ಸರ್ಕಾರಿ ಆಡಳಿತದಲ್ಲಿ ಗಣಕ ದಾಖಲೆಗಳ ಉಪಯೋಗಕ್ಕೆ ಕಾನೂನಿನ ಅಡಚಣೆ ಇರದಂತೆ ಮಾತಂಕಾ 2000 ದಲ್ಲಿ ಸೆಕ್ಷನ್ 6,7,8 ರ ಮೂಲಕ ಸರ್ಕಾರಿ ಘಟಕಗಳಿಗೆ ಹಾಗೂ ಸರ್ಕಾರಿ ಸ್ವಾಮ್ಯದ ಸಂಸ್ಥೆಗಳಿಗೆ ಅನುಮತಿ ನೀಡಲಾಗಿದೆ.

ಇದರ ಪ್ರಕಾರ ಸರ್ಕಾರಕ್ಕೆ ಯಾವುದೇ ಅರ್ಜಿ ಸಲ್ಲಿಸಲು, ಅಥವಾ ಟೆಂಡರ್ ವ್ಯವಹಾರದಲ್ಲೂ ಗಣಕ ಪತ್ರಗಳ ಬಳಕೆಗೆ ಅವಕಾಶ ಮಾಡಬಹುದು. ಹಾಗೆಯೇ, ಹಣ ಪಡೆಯುವುದಕ್ಕೆ ಅಥವಾ ಕೊಡುವುದಕ್ಕೆ ಮತ್ತು ಸರ್ಕಾರಿ ದಾಖಲೆಗಳನ್ನು ಉಳಿಸಿಟ್ಟುಕೊಳ್ಳುವುದಕ್ಕೆ ಕೂಡ ಗಣಕ ದಾಖಲೆಗಳನ್ನು ಉಪಯೋಗಿಸಬಹುದು. ಸರ್ಕಾರಿ ಗೆಜೆಟ್ ಕೂಡಾ ಗಣಕ ಪತ್ರದ ಮೂಲಕ ಹೊರಡಿಸುವುದಕ್ಕೆ ಕೂಡ ಈ ಮೂಲಕ ಅವಕಾಶ ಕೊಡಲಾಗಿದೆ.

ಮೇಲ್ಕಂಡಂತೆ ಸರ್ಕಾರದ ಅನೇಕ ವ್ಯವಹಾರಗಳಲ್ಲಿ ಗಣಕ ಯಂತ್ರದ ಬಳಕೆ ಸಾಧ್ಯವಾದರೂ, ಸೆಕ್ಷನ್ 9 ರ ಪ್ರಕಾರ ಸರ್ಕಾರದಲ್ಲಿ ಗಣಕ ಪತ್ರದ ಬಳಕೆ ಮಾಡುವುದಕ್ಕೆ ಸಾರ್ವಜನಿಕರಿಗೆ ಒತ್ತಾಯ ಮಾಡುವ ಹಕ್ಕು ಇಲ್ಲ ಎಂದು ತಿಳಿಸಲಾಗಿದೆ. ಇದರಿಂದ ಸರ್ಕಾರಿ ಘಟಕಗಳು ತಮ್ಮದೇ ವೇಗದಲ್ಲಿ ಗಣಕ ಯಂತ್ರದ ಬಳಕೆಯನ್ನು ಒಳಗೊಡಿಸಿಕೊಳ್ಳಲು ಅವಕಾಶ ಮಾಡಿಕೊಡಲಾಗಿದೆ.

ಮಾತಂಕಾ-2000 ದ ಅಂಶಗಳನ್ನು ಅನುಷ್ಠಾನಗೊಳಿಸಲು ರಾಜ್ಯ ಸರ್ಕಾರಗಳು ಬೇಕಾದ ನಿಯಮಗಳನ್ನು ಮಾಡಲು ಸೆಕ್ಷನ್ 90 ರ ಪ್ರಕಾರ ಅನುಮತಿ ಕೊಡಲಾಗಿದೆ.

ಸೆಕ್ಷನ್ 66: ಹ್ಯಾಕಿಂಗ್

ಯಾವುದೇ ವ್ಯಕ್ತಿ, ಯಾವುದೇ ವಿಧಾನದಿಂದ, ಉದ್ದೇಶ ಪೂರ್ವಕವಾಗಿ ಅಥವಾ ತಾನು ಬೇರಾರಿಗಾದರೂ ನಷ್ಟವನ್ನುಂಟು ಮಾಡುವ ಸಂಭವವಿದೆಯೆಂಬ ತಿಳುವಳಿಕೆಯಿದ್ದೂ, ಕಂಪ್ಯೂಟರ್‌ನ ಒಳಗಿರುವ ಮಾಹಿತಿಯನ್ನು ನಷ್ಟಗೊಳಿಸುವುದೋ, ಅಳಿಸುವುದೋ, ಪರಿವರ್ತಿಸುವುದೋ, ಅಥವಾ ಬೇರಾವುದೇ ರೀತಿಯಲ್ಲಿ ಅದರ ಬೆಲೆ ಅಥವಾ ಉಪಯುಕ್ತತೆ ಯನ್ನು ಕಡಿತಗೊಳಿಸುವುದೋ ಬಾಧೆಗೊಳಿಸುವುದೋ ಮಾಡಿದಲ್ಲಿ ಅದು “ಹ್ಯಾಕಿಂಗ್” ಎನಿಸುತ್ತದೆ. ಅಂತಹ ಅಪರಾಧಿಗೆ 3 ವರ್ಷ ಸಜೆಯನ್ನೂ ಅಥವಾ ರೂ 2 ಲಕ್ಷದ ವರೆಗೂ ದಂಡವನ್ನೂ ವಿಧಿಸಬಹುದು.

ಅಧ್ಯಾಯ 6: ಸೈಬರ್ ಕೆಫ್ಫೆ ನಿಯಂತ್ರಣ

ಅಂತರ್ಜಾಲದ ಉಪಯೋಗಗಳನ್ನು ಸಾಮಾನ್ಯ ಜನಸಮುದಾಯಕ್ಕೆ ತಲುಪಿಸುವುದರಲ್ಲಿ ಸೈಬರ್ ಕೆಫ್ಫೆ ಗಳಿಗೆ ಮಹತ್ತರದ ಪಾತ್ರ ಇದೆ. ಕಂಪ್ಯೂಟರ್ ಬೆಲೆ ಕಡಿಮೆಯಾಗಿ ಬರುತ್ತಿದ್ದರೂ, ಇತ್ತೀಚಿನ ದಿನಗಳಲ್ಲಿ ತಂತ್ರಾಂಶದ ಬೆಲೆ ಹೆಚ್ಚುತ್ತಿರುವುದೇ ಅಲ್ಲದೆ, ರೋಗಾಣು ನಿರೋಧಕ, ಹ್ಯಾಕಿಂಗ್ ನಿರೋಧಕ, ಸ್ಪ್ಯಾಮ್ ನಿರೋಧಕ ಮುಂತಾದ ಉಪ ತಂತ್ರಾಂಶಗಳ ಅವಶ್ಯಕತೆಗಳು ಹೆಚ್ಚುತ್ತಿವೆ. ಅಲ್ಲದೆ, ಟೆಲಿಫೋನ್ ಮೂಲಕ ಅಂತರ್ಜಾಲ ಸೇವೆಯನ್ನು ಪಡೆಯಬೇಕಾದರೆ ಘಂಟೆಗೆ 30 ರೂಪಾಯಿಗೂ ಹೆಚ್ಚು ಖರ್ಚು ಮಾಡಬೇಕಾಗಿರುತ್ತದೆ, ಇದೆಲ್ಲಾ ಕಾರಣದಿಂದ ಜನ ಸಾಮಾನ್ಯರಿಗೆ ಅಂತರ್ಜಾಲ ಇನ್ನೂ ದುಬಾರಿ ಸೇವೆಯಾಗಿಯೇ ಉಳಿದಿದೆ. ಈ ಪರಿಸರದಲ್ಲಿ ಯಾವ ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ತಂತ್ರಾಂಶದ ಖರ್ಚಿಲ್ಲದೆ, ಟೆಲಿಫೋನ್ ಅಥವಾ ಅಂತರ್ಜಾಲ ಸೇವಾ ಖರ್ಚಿಲ್ಲದೆ ಘಂಟೆಗೆ 10-15 ರೂಪಾಯಿಗೂ ಅಂತರ್ಜಾಲ ಸೇವೆ ನಮ್ಮ ಕೈಗೆಟಕುವಂತೆ ಮಾಡಿರುವುದು ಸೈಬರ್ ಕೆಫ್ಫೆಗಳು.

ಈ ಸೈಬರ್ ಕೆಫ್ಫೆಗಳಲ್ಲಿ ಕೆಲವು ಅಶ್ಲೀಲತೆಯ ಪ್ರಚಾರದಿಂದ ಹಣ ಮಾಡುತ್ತಿರುವುದೂ ನಿಜ. ಇದರಿಂದ ಸೈಬರ್ ಕೆಫ್ಫೆಗಳಿಗೆಲ್ಲಾ ಕೆಟ್ಟ ಹೆಸರು ಬಂದು ಬಿಟ್ಟಿದೆ. ಇದಲ್ಲದೆ ಸಾಮಾನ್ಯವಾಗಿಯೇ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ಮಾಡುವ ಅನೇಕರು ಸೈಬರ್ ಕೆಫ್ಫೆಗಳನ್ನು ಉಪಯೋಗಿಸುವುದು ಸಹಜ. ಇದೆಲ್ಲಾ ಕಾರಣಗಳಿಂದ ಸೈಬರ್ ಕೆಫ್ಫೆಗಳ ಮೇಲೆ ನಿಯಂತ್ರಣ ತರಬೇಕೆಂದು ಕೆಲವು ರಾಜ್ಯಗಳಲ್ಲಿ ಕ್ರಮಗಳನ್ನು ಕೈಗೊಳ್ಳಲಾಗಿದೆ.