ನಿರ್ವಹಣೆ, ಸವಾಲು ಮತ್ತು ಸಾಧ್ಯತೆಗಳು

ಸೈಬರ್ ದಾಳಿ ನಿಯಂತ್ರಿಸುವ ನಿಟ್ಟಿನಲ್ಲಿ ಜಗತ್ತಿನಲ್ಲಿ ಬಹಳಷ್ಟು ಪ್ರಯೋಗಗಳು ನಡೆಯುತ್ತಲೇ ಇವೆ. ಆದರೆ ತಂತ್ರಜ್ಞಾನ ಬೆಳೆದಷ್ಟೇ ವೇಗದಲ್ಲಿ ಸೈಬರ್ ದಾಳಿ ನಿಯಂತ್ರಣ ನಡೆಯುತ್ತಿದ್ದರೂ, ದಾಳಿಕೋರರು ಒಂದು ಹೆಜ್ಜೆ ಮುಂದೆಯೇ ಇರುವುದು ಆಘಾತಕಾರಿ. ಇಂಥ ಕೆಲವೊಂದು ಆಂಶಗಳ ಕುರಿತು 'ಎಫ್‌ಐಸಿಐ' ವರದಿಯೊಂದನ್ನು ಸಿದ್ಧಪಡಿಸಿತ್ತು. ಅದರಲ್ಲಿ ಸೈಬರ್ ದಾಳಿಯ ಬಗೆ, ನಿರ್ವಹಣೆ ಹಾಗೂ ಇರುವ ಸವಾಲುಗಳು ಮತ್ತು ಪರಿಹಾರಗಳನ್ನು ವರದಿಯಲ್ಲಿ ಉಲ್ಲೇಖಿಸಿ ಸರ್ಕಾರಕ್ಕೆ ನೀಡಿತ್ತು. ಅದರ ಮುಖ್ಯಾಂಶಗಳು ಕೆಳಕಂಡಂತಿವೆ.

- ಸದ್ಯ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನೂ ಪೊಲೀಸರೇ ನಿರ್ವಹಿಸುತ್ತಿರುವುದರಿಂದ ಅವರಿಗೆ ಕಾಲಕಾಲಕ್ಕೆ ಆಧುನಿಕಗೊಳ್ಳುತ್ತಿರುವ ಈ ಕ್ಷೇತ್ರದ ಪರಿಚಯ, ಅದರಲ್ಲೂ ಸೈಬರ್ ವಿಧಿವಿಜ್ಞಾನ ಪ್ರಯೋಗಾಲಯ ಕುರಿತು ತರಬೇತಿ ನೀಡುವುದು ಅಗತ್ಯ. ಐಟಿ ತಿದ್ದುಪಡಿ ಕಾಯ್ದೆ 2008ರ ಅನ್ವಯ ತ್ವರಿತ ತನಿಖೆಗೆ ಅಗತ್ಯದಂತೆ ತರಬೇತಿಯನ್ನೂ ನೀಡಬೇಕು.
- ಭಾರತದಲ್ಲಿರುವ ಮತ್ತೊಂದು ಸವಾಲು ಎಂದರೆ, ದಾಳಿಗೊಳಗಾದವರು ದೂರು ನೀಡದಿರುವುದು. ಜಗತ್ತಿನಲ್ಲಿ ಅತಿ ವೇಗವಾಗಿ ಆಂತರ್ಜಾಲ ವ್ಯಾಪ್ತಿಗೆ ಒಳಪಡುತ್ತಿರುವ ಭಾರತದಲ್ಲಿ ನಿತ್ಯ ಬಹಳಷ್ಟು ಸೈಬರ್ ಅಪರಾಧಗಳು ನಡೆಯುತ್ತಲೇ ಇರುತ್ತವೆ. ಆದರೆ ಅವುಗಳಲ್ಲಿ ಬೆರಳೆಣಿಕೆಯಷ್ಟು ಪ್ರಕರಣಗಳು ಮಾತ್ರ ದಾಖಲಾಗುತ್ತಿವೆ.
- ಪ್ರಕರಣಗಳ ಸಂಖ್ಯೆ ಮತ್ತು ಅವುಗಳನ್ನು ಭೇದಿಸಲು ಅಗತ್ಯವಿರುವ ಮಾಹಿತಿ ದೊಡ್ಡಮಟ್ಟದ್ದಾಗಿರುವುದರಿಂದ ಬಹಳಷ್ಟು ಪ್ರಕರಣಗಳು ಕೇಂದ್ರ ಹಾಗೂ ರಾಜ್ಯಗಳ ಪ್ರಯೋಗಾಲಯಗಳಲ್ಲೇ ಬಗೆಹರಿಯದೇ ಕೂತಿವೆ.
- ನಿರ್ದಿಷ್ಟ ಬಳಕೆದಾರರೊಂದಿಗೆ ಮಾತ್ರ ಸಂಪರ್ಕ ಕಲ್ಪಿಸುವ ತಂತ್ರಾಂಶ ಹೊಂದಿರುವ ಡಾರ್ಕ್‌ನೆಟ್ ಬಳಕೆಯಿಂದಾಗಿ ಬಹಳಷ್ಟು ವಂಚಕರು ಮಾದಕವಸ್ತುಗಳು, ಬಾಡಿಗೆ ಹಂತಕರೊಂದಿಗೆ ವ್ಯವಹಾರ, ಮಾಹಿತಿ ಕದಿಯುವುದು, ಮಕ್ಕಳ ಆಶ್ಲೀಲ ಚಿತ್ರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದು ಇತ್ಯಾದಿಗಳನ್ನು ಬಳಕೆ ಮಾಡುತ್ತಿದ್ದಾರೆ. ಇದನ್ನು ಪತ್ತೆ ಮಾಡುವುದು ಕಷ್ಟದ ಕೆಲಸವಾದರೂ ನಿಯಂತ್ರಣ ಅಗತ್ಯ.
- ಸೈಬರ್ ಅಪರಾಧಗಳ ತಡೆಗೆ ಕಾನೂನಿನ ಕೈಗಳು ಕಾಲಕಾಲಕ್ಕೆ ಬಿಗಿಗೊಳ್ಳುತ್ತಲೇ ಇರಬೇಕು. ಸದ್ಯ ಜಗತ್ತಿನ ಬಹುಪಾಲು ರಾಷ್ಟ್ರಗಳಲ್ಲಿ ವ್ಯಾಪಕವಾಗಿರುವ ಕ್ರಿಪ್ಟೊಕರೆನ್ಸಿ ಕುರಿತ ಕಾನೂನು ಭಾರತದಲ್ಲಿ ಈವರೆಗೂ ರಚನೆಯಾಗಿಲ್ಲ. ಅದರಂತೆಯೇ ಸುಳ್ಳು ಸುದ್ದಿ ಹರಡುವವರಿಗೆ ಶಿಕ್ಷೆಯ ಪ್ರಮಾಣವೂ ಸ್ಪಷ್ಟವಿಲ್ಲ. ಆದರೆ ವಂಚಕರು ಬೇರೆ ದೇಶದಲ್ಲಿ ನೆಲೆಸಿದ್ದರೆ ಅವರನ್ನು ಕಾನೂನಿನ ವ್ಯಾಪ್ತಿಗೆ ತರುವ ನಿಟ್ಟಿನಲ್ಲಿ ಇತರ ರಾಷ್ಟ್ರಗಳೊಂದಿಗೆ ಒಡಂಬಡಿಕೆ ಮಾಡಿಕೊಳ್ಳುವುದು ಅಗತ್ಯ. ಸದ್ಯ ಭಾರತವು 39 ರಾಷ್ಟ್ರಗಳೊಂದಿಗೆ ಇಂಥ ಒಡಂಬಡಿಕೆ ಮಾಡಿಕೊಂಡಿದೆ.
- ವೇಗವಾಗಿ ಪ್ರಗತಿ ಹೊಂದುತ್ತಿರುವ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕ್ಷೇತ್ರದಲ್ಲಿ ವಿದೇಶಗಳಲ್ಲಿರುವ ಮಾಹಿತಿಯನ್ನು ಕಲೆಹಾಕುವ ಕೆಲಸ ಕ್ಲಿಷ್ಟಕರವಾದದ್ದು. ಆದರಲ್ಲೂ ಪ್ರಾಕ್ಸಿ, ವರ್ಚುಯಲ್ ಪ್ರೈವೆಟ್ ನೆಟವರ್ಕ್, ಸ್ಟೆಗ್ನೊಗ್ರಫಿ, ಸ್ಪೂಫಿಂಗ್ ಇತ್ಯಾದಿ ವೇದಿಕೆಗಳ ಮೂಲಕ ವಂಚಕರು ದಾಳಿ ನಡೆಸುತ್ತಲೇ ಇದ್ದಾರೆ.

ಅಸಲಿಯತ್ತಿನ ಬಗ್ಗೆ ಎಚ್ಚರಿಕೆ ವಹಿಸಲೇಬೇಕು.

- ನಮ್ಮ ಇಮೇಲ್ ಖಾತೆ, ಸೋಷಿಯಲ್ ಮೀಡಿಯಾ ಖಾತೆಗಳಿಗೆ ಎರಡು ಹಂತದ ದೃಢೀಕರಣ (2 ಸ್ಟೆಪ್ ವೆರಿಫಿಕೇಶನ್) ಸಕ್ರಿಯಗೊಳಿಸಿಕೊಳ್ಳಲೇಬೇಕು.
- ಸೋಷಿಯಲ್ ಮೀಡಿಯಾದಲ್ಲಿ ಎಂದಿಗೂ ಫೋನ್ ನಂಬರ್, ಆಧಾರ್ ನಂಬರ್ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಸೋಷಿಯಲ್ ಮೀಡಿಯಾದಲ್ಲಿ ಖಾಸಗಿತನ ಕಾಪಾಡಿಕೊಂಡಷ್ಟೂ ನಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆ ಭದ್ರವಾಗಿರುತ್ತದೆ.
- ಸೋಷಿಯಲ್ ಮೀಡಿಯಾದಲ್ಲಿ ಸಿಗುವ ಮರುಳು ಮಾತಿನ ವಂಚಕರ ಬಗ್ಗೆ ಮನೆಯ ಮಕ್ಕಳು ಹಾಗೂ ಹಿರಿಯರಲ್ಲಿ ಅರಿವು ಮೂಡಿಸುವುದು ನಮ್ಮ ಕರ್ತವ್ಯವಾಗಲಿ.
- ಫೋನ್ ಮತ್ತು ಕಂಪ್ಯೂಟರ್‌ಗೆ ಪ್ರಬಲವಾದ ಸ್ಕ್ರೀನ್ ಲಾಕ್ ಬಳಸಿ, ಲಾಕ್‌ಸ್ಕ್ರೀನ್ ನೋಟಿಫಿಕೇಶನ್‌ಗಳನ್ನೂ ಡಿಸೇಬಲ್ ಮಾಡಿಬಿಡಿ.
- ಬ್ಯಾಂಕ್ ಖಾತೆಗೆ ಬಳಸುವ ಇ–ಮೇಲ್ ವಿಳಾಸ ಮತ್ತು ಫೋನ್ ನಂಬರು ನಿಮಗೆ ಮತ್ತು ಮನೆಯವರಿಗೆ ಮಾತ್ರವೇ ಗೊತ್ತಿದ್ದರೆ ಸೂಕ್ತ. ಇತರ ಆನ್‌ಲೈನ್ ವ್ಯವಹಾರಗಳಿಗೆ, ಸ್ನೇಹಿತರ ಸಂಪರ್ಕಕ್ಕೆ ಪ್ರತ್ಯೇಕ ಮೊಬೈಲ್ ನಂಬರ್, ಇ–ಮೇಲ್ ವಿಳಾಸ ಇರುವುದು ಒಳಿತು.
- ಕೆಲವು ವೆಬ್ ತಾಣಗಳ ಸವಲತ್ತು ಪಡೆಯಬೇಕಿದ್ದರೆ ಅವುಗಳಿಗೆ ಲಾಗಿನ್ ಆಗಬೇಕಾಗುತ್ತದೆ. ಸರಿಯಾಗಿ ಓದಿಕೊಂಡು, ಕ್ಲಿಕ್ ಮಾಡಿ
- ಮುನ್ನೆಚ್ಚರಿಕೆಯೊಂದೇ ಎಲ್ಲದಕ್ಕೂ ಪರಿಹಾರ.

ಆನ್‌ಲೈನ್ ವ್ಯವಹಾರಕ್ಕೆ ಸರ್ಕಾರವೇ ಪ್ರೋತ್ಸಾಹ ನೀಡುತ್ತಿರುವ ಸಂದರ್ಭದಲ್ಲಿ, ಮೊಬೈಲ್ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಮೂಲಕ ಹಣದ ಕೊಡು–ಕೊಳುವಿಕೆ ಈಗ ಅನಿವಾರ್ಯ ಎನ್ನುವಂತಾಗಿದೆ. ಹಾಗಾಗಿ, ಡಿಜಿಟಲ್ ಜಗತ್ತಿಗೆ ಬೆನ್ನುಹಾಕಿ ಬದುಕುವುದರಲ್ಲಿ ಅರ್ಥವಿಲ್ಲ. ಬೇಕಿರುವುದು ಸಾಮಾನ್ಯಜ್ಞಾನ ಹಾಗೂ ಕೊಂಚ ಸಾವಧಾನ. ಮೊಬೈಲ್ ಅಥವಾ ಇಮೇಲ್‌ಗೆ ರಾಶಿರಾಶಿಯಾಗಿ ಬರುವ ಮಾಹಿತಿಯ ಬಗ್ಗೆ ಮೈಯೆಲ್ಲ ಕಣ್ಣಾಗಿರಬೇಕು. ಅನಗತ್ಯ ಕುತೂಹಲ ಅಪಾಯಕ್ಕೆ ದಾರಿ ಮಾಡಿಕೊಡಬಹುದು ಎನ್ನುವುದನ್ನು ಮರೆಯಬಾರದು. ಯಾವುದೇ ಕೊಂಡಿ ಕ್ಲಿಕ್ಕಿಸುವ ಮುನ್ನ ಅವಸರ ಮಾಡದೆ, ಸಾವಧಾನದ ಮಾರ್ಗ ಅನುಸರಿಸಿದಲ್ಲಿ ಬಹುತೇಕ ಸಮಸ್ಯೆಗಳಿಗೆ ಆಸ್ಪದವೇ ಇರುವುದಿಲ್ಲ.

ಬೆರಳತುದಿಯಲ್ಲಿ ಎಲ್ಲ ವ್ಯವಹಾರ ನಡೆಯುತ್ತಿರುವ ಸಂದರ್ಭದಲ್ಲಿ, ನಮ್ಮ ಬೆರಳಿಗೆ ಕೂಡ ಮೆದುಳಿನ ಸಂವೇದಿಗುಣ ಇರಬೇಕಾದುದು ಈ ಹೊತ್ತಿನ ಅಗತ್ಯ.

ಪ್ರತಿಕ್ರಿಯಿಸಿ: **feedback@sudha.co.in**