SURE PASS | CYBER PATRIOT | Indian Cyber Institute | CYBER JAGRITHI | Supported by ISEA Information Security Education & Awareness

ಸೈಬರ್ ಸೇಫ್ ಗರ್ಲ್ 7.0

ಮಗಳನ್ನು ರಕ್ಷಿಸಿ, ಸೈಬರ್ ಅಪರಾಧದಿಂದ

70 ಕಣ್ಣೆರೆಸುವ
ಮಾಹಿತಿ ಚಿತ್ರಗಳು
ನೆಟ್ಟಿಗರಿಗೆ
ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸುರಕ್ಷಿತ
ವ್ಯವಹರಣೆಗಾಗಿ

ಅನಂತಪ್ರಭು ಜಿ ಪಿಹೆಚ್‌ಡಿ, ಡಾಕ್ಟರೇಟ್ ಪದವೀದರರು

ಸಹಲೇಖಕರು: **ನ್ಯಾ.ಪ್ರಶಾಂತ್ ಝಾಲಾ**

ಲಿಂಗರಾಜು.ಎಸ್ ಕನ್ನಡಾನುವಾದ

ಸೈಬರ್ ಸೇಫ್

ಗರ್ಲ್ 7.0

ಮಗಳನ್ನು ರಕ್ಷಿಸಿ, ಸೈಬರ್ ಅಪರಾಧದಿಂದ .

70 ಕಣ್ತೆರೆಸುವ ಮಾಹಿತಿ ಚಿತ್ರಗಳು
ನೆಟ್ಟಿಗರಿಗೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸುರಕ್ಷಿತ
ವ್ಯವಹರಣೆಗಾಗಿ

ಶೀರ್ಷಿಕೆ: **ಸೈಬರ್ ಸೇಫ್ ಗರ್ಲ್**

ಆವೃತ್ತಿ : 7.0

ಪ್ರಕಾಶಕರು: **ಡಾ॥ ಅನಂತಪ್ರಭು.ಜಿ**

ಸಹ ಲೇಖಕರು: ನ್ಯಾ.ಪ್ರಶಾಂತ್ ಝಾಲಾ

ಅನುವಾದಕರು: **ಲಿಂಗರಾಜು.ಎಸ್**

ಪ್ರಥಮ ಆವೃತ್ತಿ 2018ರಲ್ಲಿ ಭಾರತದಲ್ಲಿ ಬಿಡುಗಡೆಗೊಂಡಿರುತ್ತದೆ

ಕೃತಿಸ್ವಾಮ್ಯ (ಸಿ) ಕ್ಯಾಂಪಸ್ ಸಂದರ್ಶನ ತರಬೇತಿ ಸಲ್ಯೂಷನ್ಸ್ 2025

ಎಲ್ಲಾ ಹಕ್ಕುಗಳನ್ನು ಕಾಯ್ದಿರಿಸಲಾಗಿದೆ. ಮೇಲೆ ಕಾಯ್ದಿರಿಸಿದ ಹಕ್ಕುಸ್ವಾಮ್ಯದ ಅಡಿಯಲ್ಲಿ ಹಕ್ಕುಗಳನ್ನು ಸೀಮಿತಗೊಳಿಸಿದೆ, ಈ ಪ್ರಕಟಣೆಯ ಯಾವುದೇ ಭಾಗವನ್ನು ಯಾವುದೇ ರೂಪದಲ್ಲಿ ಅಥವಾ ಯಾವುದೇ ವಿಧಾನದಿಂದ (ವಿದ್ಯುನ್ಮಾನ, ಮೆಕ್ಯಾನಿಕಲ್, ಫೋಟೋಕಾಪಿಯಿಂಗ್, ರೆಕಾರ್ಡಿಂಗ್ ಅಥವಾ ಇತ್ಯಾದಿ ರೂಪ) ಪುನರುತ್ಪಾದಿಸಲು, ಸಂಗ್ರಹಿಸಲು ಅಥವಾ ಹಿಂಪಡೆಯುವ ಗಣಕಯಂತ್ರ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಕೃತಿಸ್ವಾಮ್ಯ ಮಾಲೀಕರ ಪೂರ್ವ ಲಿಖಿತ ಅನುಮತಿ ಇಲ್ಲದೇ ಪ್ರಕಟಿಸಲು ರವಾನಿಸಲು ಸಾಧ್ಯವಿಲ್ಲ.

ಅನುಮತಿ ಕೋರಿಕೆಗಳನ್ನು ಇಲ್ಲಿಗೆ ನಿರ್ದೇಶಿಸಬೇಕು

educatorananth@gmail.com

ವಿನ್ಯಾಸ ಮತ್ತು ಮುದ್ರಣ

ಟಾರ್ಜನಿ ಕಮ್ಯುನಿಕೇಷನ್ಸ್ ಪ್ರೈ.ಲಿಮಿಟೆಡ್, ಮಂಗಳೂರು

ಇದೊಂದು ಕಾಲ್ಪನಿಕ ಕೃತಿ, ಹೆಸರುಗಳು, ಪಾತ್ರಗಳು, ವ್ಯವಹಾರಗಳು, ಸ್ಥಳಗಳು, ಘಟನೆಗಳು, ಸ್ಥಳ ಮತ್ತು ಘಟನೆಗಳು ಲೇಖಕರ ಕಲ್ಪನೆಯಾಗಿದ್ದು, ಯಾವುದೇ ಜೀವಂತ ಅಥವಾ ಮೃತ ವ್ಯಕ್ತಿಗೆ ಹೋಲಿಕೆಯಾದಲ್ಲಿ ಅದು ಕೇವಲ ಕಾಕತಾಳೀಯವಾಗಿದೆ. ಈ ಪುಸ್ತಕದಲ್ಲಿ ಒದಗಿಸಲಾದ ಮಾಹಿತಿಯ ಬಳಕೆಗೆ ಸಂಬಂಧಿಸಿದಂತೆ ಲೇಖಕರು ಮತ್ತು ಪ್ರಕಾಶಕರು ಯಾವುದೇ ರೀತಿಯಲ್ಲಿ ಹೊಣೆಗಾರರಾಗಿರುವುದಿಲ್ಲ.

9 789334 000849

ಗೌರವಪೂರ್ವಕ ವಂದನೆಗಳು . . .

ಸಂಜಯ್ ಸಹಾಯ್
ಐ.ಪಿ.ಎಸ್ (ನಿ)

ಡಾ॥ ಎಂ.ಎ ಸಲೀಂ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಅಲೋಕ್‌ಕುಮಾರ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಪ್ರನಭ್ ಮೊಹಂತಿ
ಐ.ಪಿ.ಎಸ್

ಡಾ.ಸುಬ್ರಮಣ್ಯ ರಾವ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ರವಿ.ಎಸ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಆರ್.ಹಿತೇಂದ್ರ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಹೇಮಂತ್ ಎನ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಬಿ.ಕೆ. ಸಿಂಗ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಜೆ.ಅರುಣ್ ಚಕ್ರವರ್ತಿ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಕಾರ್ತಿಕ್ ರೆಡ್ಡಿ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಬೋರಲಿಂಗಯ್ಯ. ಎಂ.ಜಿ
ಐ.ಪಿ.ಎಸ್

ಡಾ॥ ಕೆ.ವಂಸಿಕೃಷ್ಣ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಸುಧೀರ್ ಕ. ರೆಡ್ಡಿ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಶೇಖರ್ ಹಚ್ ಟಿ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಅನುಪಂ ಅಗ್ರವಾಲ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಶಶಿಕುಮರ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ರವಿ ಡಿ ಸಿ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ವಿಷ್ಣುವರ್ಧನ್.ಎನ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಆನಂದ್ ಕುಮಾರ್
ಐ.ಪಿ.ಎಸ್

ಅರುಣಾಂಶುಗಿರಿ ಐ.ಪಿ.ಎಸ್

ಪ್ರದೀಪ್ ಗುಂಟಿ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ. ನಿಖಿಲ್ ಬಿ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಪೃಥ್ವಿಕ್ ಶಂಕರ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಮಲ್ಲಿಕಾರ್ಜುನ ಬಾ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಶ್ರೀನಿವಾಸಗೌಡ ಆರ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀಮತಿ ಕ್ಷಮಾ ಮಿಶ್ರ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಯತೀಶ್ ಎನ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಮಿಥುನ್‌ಕುಮಾರ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಅದ್ದೂರು ಶ್ರೀನಿವಾಸ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ಪಿ ಕೃಷ್ಣಕಾಂತ್
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀಮತಿ.ಬಿ.ಎನ್.ನಂದಿನಿ
ಕೆ.ಎಸ್.ಪಿಎಸ್

ಶ್ರೀಮತಿ.ಪಿ.ವಿ.ಸ್ನೇಹ
ಕೆ.ಎಸ್.ಪಿಎಸ್

ಶ್ರೀ.ನರಸಿಂಹ. ಟಿ
ಐ.ಪಿ.ಎಸ್

ಶ್ರೀ.ರಾಮಚಂದ್ರ.ಬಿ
ಎಎಟಿ, ಕೆಎಸ್‌ಪಿ

ಡಾ|| ಅನಂತಪ್ರಭು.ಜಿ, BE, MBA, M.Tech, DCL, PhD, Post Doctoral Fellow

ಓರ್ವ ಲೇಖಕರು, ಸಾಫ್ಟ್‌ವೇರ್ ಇಂಜಿನೀಯರ್, ಪ್ರೇರಣಾ ಭಾಷಣಕಾರರು & ಸೈಬರ್ ಸುರಕ್ಷತಾ ತಜ್ಞರು. ಪ್ರಸ್ತುತ ಸಹ್ಯಾದ್ರಿ ಕಾಲೇಜ್ ಆಫ್ ಇಂಜಿನೀಯರಿಂಗ್ ಮತ್ತು ಮ್ಯಾನೇಜ್‌ಮೆಂಟ್‌ನಲ್ಲಿ ಪ್ರಾಧ್ಯಾಪಕರಾಗಿ ಮತ್ತು ಸುರ್‌ಪಾಸ್ ಅಕಾಡೆಮಿಯಲ್ಲಿ ನಿರ್ದೇಶಕರಾಗಿ ಸೇವೆ ಸಲ್ಲಿಸುತ್ತಿದ್ದಾರೆ. ಇವರು ಕರ್ನಾಟಕ ನ್ಯಾಯಾಂಗ ಅಕಾಡೆಮಿ ಮತ್ತು ಕರ್ನಾಟಕ ಪೊಲೀಸ್ ಅಕಾಡೆಮಿಯಲ್ಲಿ ಸೈಬರ್ ಕಾನೂನು ಮತ್ತು ಭದ್ರತೆಯ ತರಬೇತುದಾರರಾಗಿದ್ದಾರೆ. ಡಾ||ಪ್ರಭು ರವರನ್ನು ಇಂಡಿಯಾ ಟುಡೆ ನಿಯತಕಾಲಿಕೆಯು ೨೦೧೨ರಲ್ಲಿ ನಮ್ಮ ದೇಶದ ೩೦ ವೀರರಲ್ಲಿ ಒಬ್ಬರೆಂದು ಗುರುತಿಸಿದೆ. ಡಾ.ಪ್ರಭು ಅವರು ಸೈಬರ್ ಭದ್ರತೆ ಮತ್ತು ಜಾಗೃತಿ ಕ್ಷೇತ್ರದಲ್ಲಿ ಸಲ್ಲಿಸಿದ ಸೇವೆಗಳಾಗಿ ಕರ್ನಾಟಕ ಜಿಲ್ಲಾ ರಾಜ್ಯೋತ್ಸವ ಪ್ರಶಸ್ತಿ ಮತ್ತು ಆರ್ಯಭಟ ಅಂತರರಾಷ್ಟ್ರೀಯ ಪ್ರಶಸ್ತಿಯನ್ನು ಪಡೆದಿದ್ದಾರೆ.

☎ +91 89515 11111 ✉ info@ananthprabhu.com

ಸಹ-ಲೇಖಕರು

ನ್ಯಾ.ಪ್ರಶಾಂತ್ ಝಾಲ,

ಇವರು ಮುಂಬೈ ಮೂಲದ ಕಾನೂನು ಸಂಘ (www.icladvocates.com) ಐ.ಸಿ.ಎಲ್ ಅಡ್ವೊಕೇಟ್ಸ್‌ನ ಸಂಸ್ಥಾಪಕರು ಮತ್ತು ಸೈಬರ್ ಅಪರಾಧ ತನಿಖೆ, ಗಣಕಯಂತ್ರ ವಿಧಿವಿಜ್ಞಾನ, ಎಥಿಕಲ್ ಹ್ಯಾಕಿಂಗ್ ಮತ್ತು ಮಾಹಿತಿ ಸುರಕ್ಷತೆ, ಸೈಬರ್ ಕಾನೂನು, ಇತ್ಯಾದಿ, ಕ್ಷೇತ್ರದಲ್ಲಿ ಶೈಕ್ಷಣಿಕ ಮತ್ತು ತರಬೇತಿ ಕಾರ್ಯಕ್ರಮ ಗಳನ್ನು ನಡೆಸುವ ಭಾರತೀಯ ಸೈಬರ್ (indiancyberinstitute.com) ಸಹ-ಸಂಸ್ಥಾಪಕರಾಗಿದ್ದಾರೆ. ಇವರು ವಿವಿಧ ಬ್ಯಾಂಕಿಂಗ್ ವೇದಿಕೆಗಳು, ರಕ್ಷಣಾ ಪಡೆಗಳು & ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನದ ಪಾಲುದಾರರು ಆಯೋಜಿಸುವ ಕಾರ್ಯಾಗಾರಗಳು/ ತರಬೇತಿ/ ವಿಚಾರ ಸಂಕೀರ್ಣಗಳಲ್ಲಿ ನಿಯಮಿತ ಗೌರವ ಉಪನ್ಯಾಸಕರು ಮತ್ತು ತರಬೇತುದಾರರಾಗಿದ್ದಾರೆ.

☎ +91 98691 84691 ✉ prashant@icladvocates.com

ಅನುವಾದಕರು

ಅಂಗರಾಜು.ಎಸ್,

ಇವರು ಕರ್ನಾಟಕ ರಾಜ್ಯದ ಪೊಲೀಸ್ ಇಲಾಖೆಯಲ್ಲಿ ೨೭ ವರ್ಷಗಳ ಸೇವೆ ಸಲ್ಲಿಸುತ್ತಿದ್ದು, ಬಹುತೇಕ ೨೨ಕ್ಕೂ ಅಧಿಕ ರಾಷ್ಟ್ರೀಯ ಮತ್ತು ಅಂತರಾಷ್ಟ್ರೀಯ ಸೈಬರ್ ತರಬೇತಿಯನ್ನು ಪಡೆದಿರುತ್ತಾರೆ & ೪೭ ಪುಸ್ತಕಗಳನ್ನು ಹೊರತಂದಿರುತ್ತಾರೆ. ಇವರು ವಿವಿಧ ತರಬೇತಿ ಸಂಸ್ಥೆಗಳಲ್ಲಿ ಅಂದಾಜು ೪೭೦೦ಕ್ಕೂ ಹೆಚ್ಚು ಸೈಬರ್ ತರಗತಿಗಳನ್ನು ನಡೆಸಿರುತ್ತಾರೆ. ಇವರ ಮಹೋನ್ನತ ಸೇವೆಗಾಗಿ ಮುಖ್ಯಮಂತ್ರಿಗಳ ಪದಕವನ್ನು ನೀಡಿ ಗೌರವಿಸಲಾಗಿರುತ್ತದೆ.

☎ +91 94488 44307 ✉ rajuaaryan90@gmail.com

ಡಾ|| ಅನಂತಪ್ರಭು.ಜಿ,

ರವರನ್ನು ನಿಮ್ಮ ಶಾಲಾ/ಕಾಲೇಜಿನ ವಿದ್ಯಾರ್ಥಿಗಳನ್ನು ಅಥವಾ ಸಂಸ್ಥೆ/ಕಛೇರಿ ಉದ್ಯೋಗಿಗಳನ್ನು ಉದ್ದೇಶಿಸಿ ಸಂವಾದ ನಡೆಸಲು ಬಯಸುವಿರಾ..?

ಹಾಗಿದ್ದಲ್ಲಿ ಸಂಪರ್ಕಿಸಿ

+91 89515 11111

info@ananthprabhu.com

ಅವರ ನಿಯಮಿತ ಹೊಸದಿಕೆ ಅನುಸರಿಸಲು ಕೆಳಗಿನ ಪುಟವನ್ನು ಲೈಕ್ ಮಾಡಿ

www.facebook.com/educatorananth

ಸಂಪರ್ಕಿಸಿ

ಅಂಗರಾಜು.ಎಸ್,

+91 94488 44307

rajuaaryan90@gmail.com

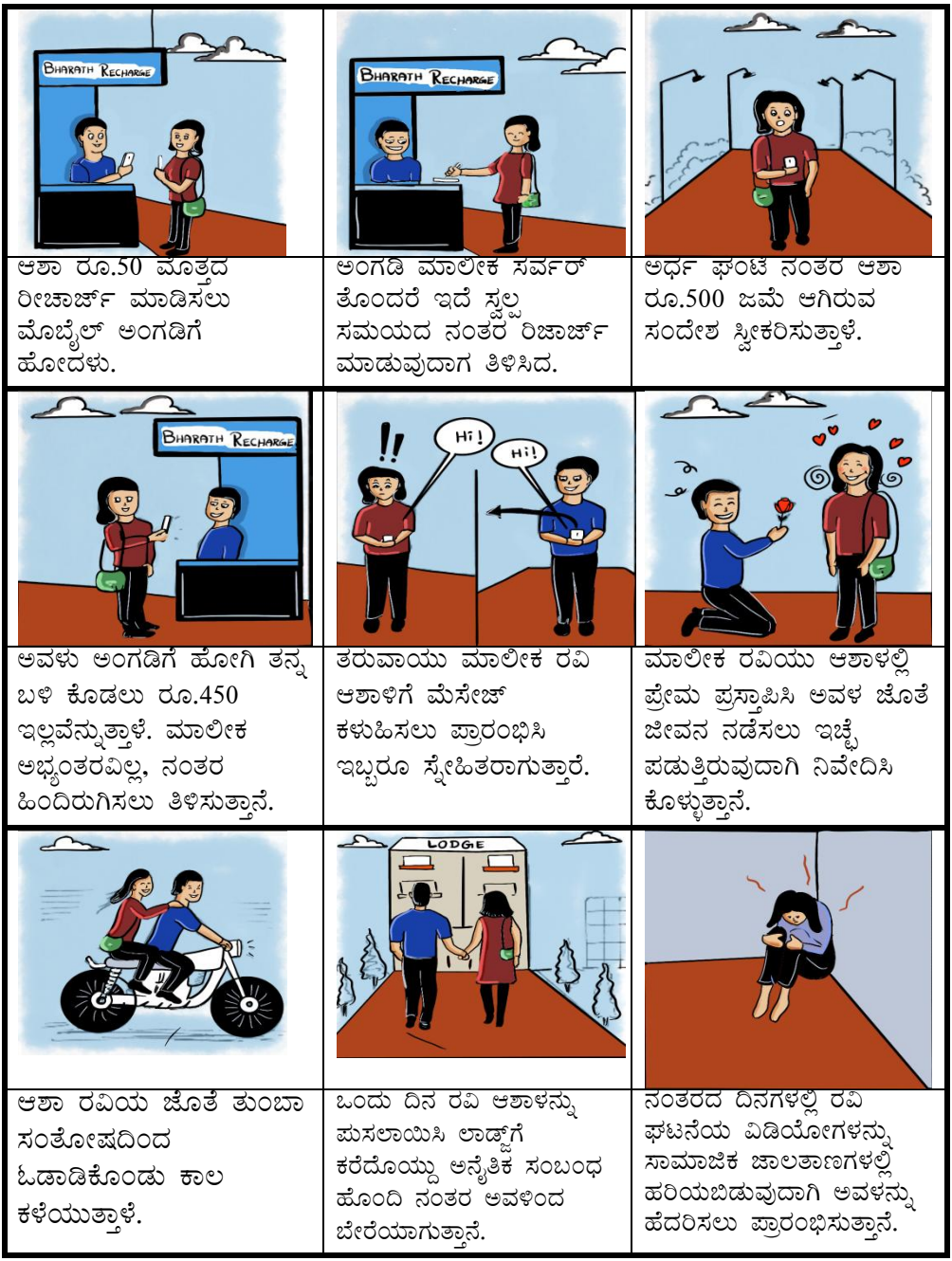
ಅಪರಾಧಗಳು ಮತ್ತು ಅವುಗಳ ಕಾರ್ಯವೈಖರಿ ಲಿಂಗ ನಿರ್ದಿಷ್ಟವಲ್ಲದೆ. ಲಿಂಗ ತಟಸ್ಥವಾಗಿರುತ್ತದೆ.

ವಸ್ತು ವಿಷಯ

ಮೊಬೈಲ್ ರೀಚಾರ್ಜ್ ಮಳಿಗೆ 01
ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಪ್ರತಿರೂಪಿಸುವುದು 03
ಕೀಲಾಗರ್ (ಕೀಲಿ ಭೇದಕಗಳು) 05
ಎಸ್.ಎಂ.ಎಸ್ ಮೋಸದ ಜಾಲ 07
ಮೋಸದ ಕರೆಗಳು 09
ರ್‍ಯಾನ್ಸಮ್‌ವೇರ್ 11
ಸೈಬರ್ ಹಿಂಬಾಲಿಕೆ 13
ಚಿತ್ರ ಆಕೃತಿ ರಚನೆ 15
ವ್ಯಕ್ತಿಚಿತ್ರ ಅತಿಕ್ರಮಣ(ಹ್ಯಾಕಿಂಗ್) 17
ಆನ್‌ಲೈನ್ ಆಟಗಳು 19
ಉದ್ಯೋಗ ಕರೆ ಪತ್ರ 21
ಗಾಢ ವಂಚನೆ (ಡೀಪ್ ಫೇಕ್) 23
ಪ್ರಣಯದ ಭೇಟಿ ಜಾಲತಾಣ 25
ಕ್ಯಾಮರಾ ಹ್ಯಾಕಿಂಗ್ 27
ಸಾಮಾಜಿಕ ಟ್ರೋಲಿಂಗ್ 29
ಪೋಂಝಿ ಯೋಜನೆ 31
ನಕಲಿ ವೈವಾಹಿಕ ವ್ಯಕ್ತಿಚಿತ್ರ(ಮ್ಯಾಟ್ರಿಮೊನಿ) 33
ಮೊಬೈಲ್ ದುರಸ್ತಿ ಮಳಿಗೆ 35
ನಕಲಿ ವಿಮರ್ಶೆ 37
ನಕಲಿ ವ್ಯಕ್ತಿಚಿತ್ರ ದಿಂದ ಸೆಕ್ಸ್‌ಟಾರ್ಷನ್ 39
ಸೈಬರ್ ರಣಹದ್ದುಗಳು (ವಲ್ಚರ್) 41
ಆ್ಯಪ್ ಬಲೆ 43
ಜ್ಯೂಸ್ ಜಾಕಿಂಗ್ 45
ವೈಫೈ ಅತಿಕ್ರಮಣ 47
ಆನ್‌ಲೈನ್ ಆಮೂಲಾಗ್ರೀಕರಣ (ರ್‍ಯಾಡಿಕಲೈಝೇಷನ್) 49
ಜೇನು ಬಲೆ (ಹನಿ ಟ್ರ್ಯಾಪ್) 51
ಕ್ಯೂ.ಆರ್ ಸಂಕೇತ ಹಗರಣ 53
ಆರ್.ಎಫ್.ಐ.ಡಿ ಪ್ರತಿರೂಪಿಸುವುದು 55
ಡ್ರೋನ್ ಕಣ್ಗಾವಲು 57
ಸರ್ಚ್ ಇಂಜಿನ್ ಫಲಿತಾಂಶ ಹಗರಣ 59
ಐ.ಡಿ.ಎನ್ ಹೋಮೋಗ್ರಾಫ್ ಆಕ್ರಮಣ 61
ಸ್ಕ್ರ್ಯಾಚ್ ಕಾರ್ಡ್ ಹಗರಣ 63
ಸಿಮ್ ಮಾರ್ಪಾಡು(ಸ್ವ್ಯಾಪ್) 65
ಕ್ರಿಪ್ಟೋಜಾಕಿಂಗ್ 67
ವಿಡಿಯೋ ಸಮಾವೇಶ ಹಗರಣ 69
ಮಕ್ಕಳ ಮೊಬೈಲ್ ಫೋನ್ 71
ಜಾಣ್ಮೆಯ ಮನೆಗಳು(ಸ್ಮಾರ್ಟ್ ಹೋಂ) 73
ಸಣ್ಣ ಸಾಲಗಳು 75
ಬ್ಲ್ಯೂ ಸ್ನಾರ್ಫಿಂಗ್ 77
ಕಳುವಾದ ಫೋನ್ 79
ಪರೀಕ್ಷೆಯ ದುಷ್ಕೃತ್ಯ 81
ಡ್ರಗ್ಸ್ ಟ್ರಾಫಿಕ್ಕಿಂಗ್ 83
ಅಂತರ್ಜಾಲ ಸಂಪರ್ಕಿತ ಕಾರುಗಳು 85
ಡಾಕ್ಸಿಂಗ್ 87
ಸೈಬರ್ ಗ್ರೂಮಿಂಗ್ 89
ಕ್ರಿಪ್ಟೋ ವಂಚನೆಗಳು 91

ಸೈಬರ್ ಸೆಕ್ಸ್ ಟ್ರಾಫಿಕ್ಕಿಂಗ್ 93
ಸೈಬರ್ ವಾರ್‌ಫೇರ್ 95
ಹ್ಯಾಕ್ಟಿವಿಸಂ 97
ಮೆಟಾವರ್ಸ್ 99
ಅಧಿವೇಶನ ಅಪಹರಣ ದಾಳಿ 101
ಪ್ರಾಂಪ್ಟ್ ಇಂಜೀನಿಯರಿಂಗ್ 103
ಫೈಲ್ ರಹಿತ ದಾಳಿಗಳು 105
ವಿತರಣಾ (ಡೆಲಿವೆರಿ) ಹಗರಣ 107
ವರ್ಚುವಲ್ ಅಪಹರಣ 109
ಫಾರ್ಮ್‌ಜಾಕಿಂಗ್ 111
ಸೈಬರ್ ಸ್ಕ್ವಾಟ್ಟಿಂಗ್ 113
ಡಿ.ಎನ್.ಎಸ್ ಹೈಜಾಕಿಂಗ್ 115
ಸಣ್ಣ ಸಂದೇಶ ಸ್ಫೋಟಗಳು 117
ಒಳಗಿನವರ ಭೀತಿ 119
ನಕಲಿ ಇನ್‌ಫ್ಲೂಯನ್ಸರ್ ಹಗರಣ 121
ಡಿಜಿಟಲ್ ಅರೆಸ್ಟ್ 123
ಜಂಪ್ ಡೆಪಾಸಿಟ್ 125
ಕರೆ ವಿಲೀನ ಹಗರಣ 127
ಮಾಲ್ವೆಟೈಸಿಂಗ್ 129
ವಾಟರಿಂಗ್ ಹೋಲ್ ಆಕ್ರಮಣ 131
ಎಲ್‌ಎಲ್‌ಎಂ ಜೈಲ್‌ಬ್ರೇಕ್ 133
ಸುಳ್ಳು ಸುದ್ದಿ 135
ನಕಲಿ ಉತ್ಪಾದಕಾ ಆ್ಯಪ್ಸ್ 137
ಸ್ಟೆಗ್ನಾಗ್ರಫಿ 139
ಸೈಬರ್ ಸುರಕ್ಷತೆಯಲ್ಲಿ ಮಾಡಬೇಕಾದ್ದು, ಮಾಡಬಾರದ್ದು (ಯಶವಂತ ಕುಮಾರ್.ಎನ್ ರವರ) 141
ಸೈಬರ್ ಅಪರಾಧಗಳ ದೂರು ಸಲ್ಲಿಸುವುದು ಎಲ್ಲಿ 144
ಗೂಗಲ್ ಅಂಡ್ರಾಯ್ಡ್ ಗಟ್ಟಿ ಗೊಳಿಸುವಿಕೆ ಪರಿಶೀಲನಾಪಟ್ಟಿ (ಮಂಜುನಾಥ್ ಆರ್.ಜಿ ರವರ) 145
ಆ್ಯಪಲ್ ಐಓಎಸ್ ಗಟ್ಟಿ ಗೊಳಿಸುವಿಕೆ ಪರಿಶೀಲನಾಪಟ್ಟಿ 147
ಮಾಡಬೇಕಾದ್ದು, ಮಾಡಬಾರದ್ದು (ಶೇಕ್ ಸಲೀಂ ರವರ) 149
ವಿದ್ಯಾರ್ಥಿಗಳಿಗೆ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಪರಿಶೀಲನಾಪಟ್ಟಿ 159
ಪೋಷಕರಿಗೆ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಪರಿಶೀಲನಾಪಟ್ಟಿ 160
ಶಿಕ್ಷಕರಿಗೆ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಪರಿಶೀಲನಾಪಟ್ಟಿ 161
ಡಿಜಿಟಲ್ ಯೋಗಕ್ಷೇಮ & ಆರೋಗ್ಯ ಸಲಹೆಗಳು 162
ಅಪರಾಧಗಳು ಮತ್ತು ಸಂಬಧಿತ ದಂಡನಾ ಕಲಂಗಳು 163
ಆನ್‌ಲೈನ್ ದೂರು ದಾಖಲು & ಸಹಾಯವಾಣಿ ಸಂಖ್ಯೆಗಳು 166
ನಿಮ್ಮ ಹಿನ್ನುಣಿಕೆಯನ್ನು ಹೃದಯ ಪೂರ್ವಕವಾಗಿ ಸ್ವಾಗತಿಸುತ್ತೇವೆ ! 167

ಮೊಬೈಲ್ ರೀಚಾರ್ಜ್ ಮಳಿಗೆ



ಆಶಾ ರೂ.50 ಮೊತ್ತದ ರೀಚಾರ್ಜ್ ಮಾಡಿಸಲು ಮೊಬೈಲ್ ಅಂಗಡಿಗೆ ಹೋದಳು.

ಅಂಗಡಿ ಮಾಲೀಕ ಸರ್ವರ್ ತೊಂದರೆ ಇದೆ ಸ್ವಲ್ಪ ಸಮಯದ ನಂತರ ರಿಚಾರ್ಜ್ ಮಾಡುವುದಾಗ ತಿಳಿಸಿದ.

ಅರ್ಧ ಘಂಟೆ ನಂತರ ಆಶಾ ರೂ.500 ಜಮೆ ಆಗಿರುವ ಸಂದೇಶ ಸ್ವೀಕರಿಸುತ್ತಾಳೆ.

ಅವಳು ಅಂಗಡಿಗೆ ಹೋಗಿ ತನ್ನ ಬಳಿ ಕೊಡಲು ರೂ.450 ಇಲ್ಲವೆನ್ನುತ್ತಾಳೆ. ಮಾಲೀಕ ಅಭ್ಯಂತರವಿಲ್ಲ, ನಂತರ ಹಿಂದಿರುಗಿಸಲು ತಿಳಿಸುತ್ತಾನೆ.

ತರುವಾಯು ಮಾಲೀಕ ರವಿ ಆಶಾಳಿಗೆ ಮೆಸೇಜ್ ಕಳುಹಿಸಲು ಪ್ರಾರಂಭಿಸಿ ಇಬ್ಬರೂ ಸ್ನೇಹಿತರಾಗುತ್ತಾರೆ.

ಮಾಲೀಕ ರವಿಯು ಆಶಾಳಲ್ಲಿ ಪ್ರೇಮ ಪ್ರಸ್ತಾಪಿಸಿ ಅವಳ ಜೊತೆ ಜೀವನ ನಡೆಸಲು ಇಚ್ಛೆ ಪಡುತ್ತಿರುವುದಾಗಿ ನಿವೇದಿಸಿ ಕೊಳ್ಳುತ್ತಾನೆ.

ಆಶಾ ರವಿಯ ಜೊತೆ ತುಂಬಾ ಸಂತೋಷದಿಂದ ಓಡಾಡಿಕೊಂಡು ಕಾಲ ಕಳೆಯುತ್ತಾಳೆ.

ಒಂದು ದಿನ ರವಿ ಆಶಾಳನ್ನು ಪುಸಲಾಯಿಸಿ ಲಾಡ್ಜ್‌ಗೆ ಕರೆದೊಯ್ದು ಅನೈತಿಕ ಸಂಬಂಧ ಹೊಂದಿ ನಂತರ ಅವಳಿಂದ ಬೇರೆಯಾಗುತ್ತಾನೆ.

ನಂತರದ ದಿನಗಳಲ್ಲಿ ರವಿ ಘಟನೆಯ ವಿಡಿಯೋಗಳನ್ನು ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಹರಿಯಬಿಡುವುದಾಗಿ ಅವಳನ್ನು ಹೆದರಿಸಲು ಪ್ರಾರಂಭಿಸುತ್ತಾನೆ.

www.cybersafegirl.com

ಮೊಬೈಲ್ ರಿಚಾರ್ಜ್ ಅಂಗಡಿ/ಮಳಿಗೆಗಳಲ್ಲಿ ಹಗರಣಕೋರರು ನಿಮ್ಮ ಮೊಬೈಲ್‌ಫೋನ್ ಸಂಖ್ಯೆಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ ಪಡೆಯಬಹುದಾಗಿರುತ್ತದೆ.ಏಕೆಂದರೆ ನೀವು ಅವರಿಗೆ ರಿಚಾರ್ಜ್‌ಗಾಗಿ ನಿಮ್ಮ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಯನ್ನು ನೀಡಿರುತ್ತೀರಿ.ಇದರಿಂದ ಅವರು ನಿಮ್ಮ ಸಂಖ್ಯೆಗೆ ಕರೆಮಾಡಲು ಅಥವಾ ಸಂದೇಶ ಕಳುಹಿಸಲು ದುರುಪಯೋಗ ಪಡಿಸಿಕೊಳ್ಳುತ್ತಾರೆ.ಅವರು ನಿಮ್ಮ ಅಜ್ಞಾನವನ್ನು ಬಳಸಿಕೊಳ್ಳುತ್ತಾರೆ ಅಥವಾ ಭಾವನಾತ್ಮಕವಾಗಿ ನಿಮ್ಮನ್ನು ಕುಶಲತೆಯಿಂದ ನಿರ್ವಹಿಸುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂಗಳು(ಅಂಗಡಿ ಮಾಲೀಕನಿಗೆ ಅನ್ವಯವಾಗುವಂತಹವು)

ಐಪಿಸಿ ಕಲಂ 354ಎ/ಬಿಎನ್‌ಎಸ್ 75 –ಲೈಂಗಿಕ ಕಿರುಕುಳ ಮತ್ತು ಲೈಂಗಿಕ ಕಿರುಕುಳಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 354ಸಿ/ಬಿಎನ್‌ಎಸ್ 77 – ಓರ್ವ ಪುರುಷ ಮಹಿಳೆಯು ಲೈಂಗಿಕ ಕೃತ್ಯದಲ್ಲಿ ತೊಡಗಿಸಿಕೊಂಡಿರುವ ಸನ್ನಿವೇಶವನ್ನು ಆಕೆಯ ಅರಿವಿಲ್ಲದೇ ನೋಡುವ ಅಥವಾ ಅವಳು ನಿರೀಕ್ಷಿಸದ ರೀತಿಯಲ್ಲಿ ದೃಶ್ಯ ಸೆರೆಹಿಡಿಯಲು ತೊಡಗಿಸಿಕೊಂಡು ಅದನ್ನು ಪ್ರಸಾರ ಮಾಡುವುದು.

ಐಪಿಸಿ ಕಲಂ 383/384/ಬಿಎನ್‌ಎಸ್ 308– ಸುಲಿಗೆ (ಯಾವುದಾದರೂ ಬೇಡಿಕೆಯಿಂದ)

ಐಪಿಸಿ ಕಲಂ 503/ಬಿಎನ್‌ಎಸ್ 351– ಅಪರಾಧಿ ಬೆದರಿಕೆ

ಐಪಿಸಿ ಕಲಂ 506/ಬಿಎನ್‌ಎಸ್ 351– ಅಪರಾಧಿ ಬೆದರಿಕೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನವಾಗುವ ಉದ್ದೇಶದ ಪದಗಳು, ಸನ್ನೆ ಅಥವಾ ಅಭಿನಯ

ಮಾ.ತ ಕಾಯ್ದೆ:

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಮೊಬೈಲ್ ಸಂಖ್ಯೆಯನ್ನು ಮಳಿಗೆ ಮಾಲೀಕ ಹಿಂಬಾಲಿಕರಿಗೆ ಮಾರಾಟ:

ಐಪಿಸಿ/ಬಿಎನ್‌ಎಸ್ ಕಲಂಗಳು(ಅಂಗಡಿ ಮಾಲೀಕನಿಗೆ ಅನ್ವಯವಾಗುವಂತಹವು)

ಐಪಿಸಿ ಕಲಂ 109/ಬಿಎನ್‌ಎಸ್ 49– ದುಷ್ಪ್ರೇರಣೆಗಾಗಿ ಶಿಕ್ಷೆ

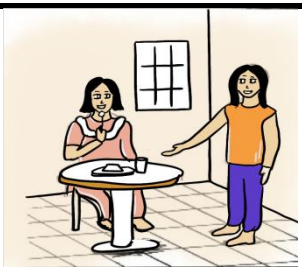
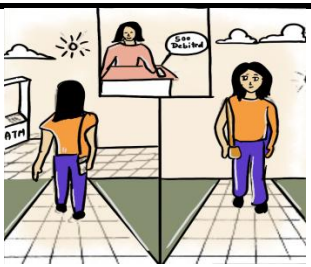
ಐಪಿಸಿ ಕಲಂ 114/ಬಿಎನ್‌ಎಸ್ 54– ಅಪರಾಧ ಜರುಗಿದಾಗ ದುಷ್ಪ್ರೇರಕನ ಹಾಜರು

ಐಪಿಸಿ ಕಲಂ 120ಬಿ/ಬಿಎನ್‌ಎಸ್ 61– ಅಪರಾಧದ ಸಂಚಿಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 406/ಬಿಎನ್‌ಎಸ್ 316– ವಿಶ್ವಾಸ ಭಂಗದ ಅಪರಾಧಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಪ್ರತಿ ವಸ್ತುವಿಗೂ ಬೆಲೆ ಇದೆ, ರಿಚಾರ್ಜ್ ಪ್ರಕರಣದಲ್ಲಾದರೆ, ಯಾವುದೂ ಉಚಿತವಲ್ಲ

ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಪ್ರತಿರೂಪಿಸುವುದು (ನಕಲಿಸುವುದು)

ಮೀನಾ ಮತ್ತು ರೀನಾ ಒಂದೇ ಕಾಲೇಜಿನಲ್ಲಿ ವ್ಯಾಸಾಂಗ ಮಾಡುತ್ತಿರುವ ಗೆಳತಿಯರು.	ಮೀನಾಳ ಗೆಳೆಯ ರಘು ಮಾದಕ ವ್ಯಸನಿಯಾಗಿದ್ದು, ಯಾವಾಗಲೂ ಅವಳನ್ನು ಹಣಕ್ಕಾಗಿ ಪೀಡಿಸುತ್ತಿರುತ್ತಾನೆ.	ಮುಂದೆ ರಘು ಬದಲಾಗ– ಬಹುದೆಂದು ಮೀನಾ ನಂಬಿದ್ದಳು. ಆದರೆ ಅವನು ಅವಳನ್ನು ಬಿಡುವುದಾಗಿ ಹೆದರಿಸಿ ಹಣ ಪಡೆಯುತ್ತಿದ್ದನು.
		
ಮೀನಾ ರೀನಾಳನ್ನು ರೂ.500 ಕೇಳುತ್ತಾಳೆ. ಪ್ರತಿಯಾಗಿ ಮೀನಾಳ ಮೇಲಿನ ನಂಬಿಕೆಯಿಂದ ರೀನಾ ತನ್ನ ATM& ಪಿನ್ ನೀಡಿದಳು.	15 ನಿಮಿಷ ನಂತರ ರೀನಾಳ ಮೊಬೈಲ್‌ಗೆ ರೂ.500 ಮೊತ್ತ ಕಳೆದಿರುವ ಸಂದೇಶ ಬರುತ್ತದೆ. ಕಾರ್ಡ್ ಹಿಂಪಡೆಯುತ್ತಾಳೆ.	ಒಂದು ವಾರದ ನಂತರ ಪುನಃ ರೂ.500 ಮೊತ್ತ ಕಳೆದಿರುವ ಸಂದೇಶವನ್ನು ರೀನಾ ಮೊಬೈಲ್‌ನಲ್ಲಿ ಪಡೆಯುತ್ತಾಳೆ.
ಆ ದಿನ ಮೀನಾ ಕಾರ್ಡ್ ತಂದಾಗ ರಘು ಹೊರಗೆ ಕಾದಿದ್ದು ಅವಳಿಂದ ಕಾರ್ಡ್ ಪಡೆದು ಹೋಗುತ್ತಾನೆ.	ರಘು ಸ್ಕಿಮ್ಮಿಂಗ್ ಸಾಧನ ಬಳಸಿ ಕಾರ್ಡ್‌ನ ನಕಲು ಮಾಡಿ ತನ್ನಲ್ಲಿದ್ದ ಪಿನ್ ಬಳಸಿ 1 ವಾರದ ಬಳಿಕ ಹಣತೆಗೆಯುತ್ತಾನೆ.	ಎಂದಿಗೂ ಸಹ ಯಾರಿಗೂ ಎಷ್ಟೇ ಹತ್ತಿರದವರಿಗೂ ATM & ಪಿನ್ ನೀಡಬಾರದು.

www.cybersafegirl.com

ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಪ್ರತಿರೂಪಿಸುವುದು (ನಕಲಿಸುವುದು)

ಬೇರೊಬ್ಬ ವ್ಯಕ್ತಿಯೊಂದಿಗೆ ಪಿನ್ ಬಹಿರಂಗಪಡಿಸಿದ ಸಂದರ್ಭಗಳಲ್ಲಿ ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಪ್ರತಿರೂಪ ನಡೆಸಲಾಗುವುದು.ಪಿನ್ ತಿಳಿದಿರುವ ಅಥವಾ ಸ್ವಲ್ಪ ಸಮಯದವರೆಗಾದರೂ ಕಾರ್ಡ್ ಸ್ವಾಧೀನ ಹೊಂದಿರುವ ಹಗರಣಕೋರ ಸ್ಕಿಮ್ಮಿಂಗ್/ಸ್ಕಿಮ್ಮಿಂಗ್ ಸಾಧನ ಬಳಸಿ ಕಾರ್ಡನ್ನು ನಕಲು ಮಾಡಿ ಹಣವನ್ನು ಪಡೆಯಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ನಕಲಿಸಿದ್ದಕ್ಕಾಗಿ ಮಾ.ತ ಕಾಯ್ದೆ:

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಪ್ರತಿರೂಪಣ ನಂತರ ಹಣ ವರ್ಗಾವಣೆ :

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಮಾ.ತ. ಕಾಯ್ದೆ

ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

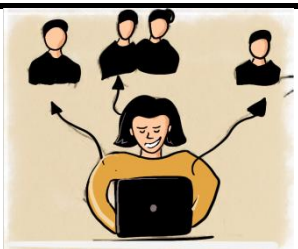
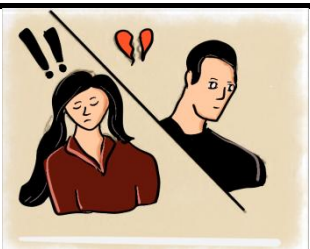
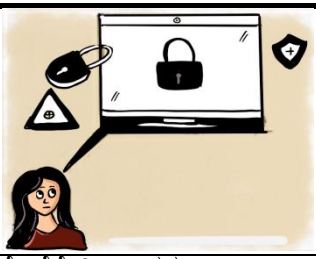
ಕಲಂ 72ಎ– ಕಾನೂನುಬದ್ಧ ಒಪ್ಪಂದದ ಉಲ್ಲಂಘನೆಯಲ್ಲಿ ಮಾಹಿತಿಯ ಬಹಿರಂಗಪಡಿಸುವಿಕೆಗಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 84ಎ– ಗೂಢಲಿಪೀಕರಣಕ್ಕಾಗಿ ಕ್ರಮಗಳು ಅಥವಾ ವಿಧಾನಗಳು.– ವಿದ್ಯುನ್ಮಾನ ಮಾಧ್ಯಮದ ಸುರಕ್ಷಿತ ಬಳಕೆಗಾಗಿ ಮತ್ತು ಇ–ಆಡಳಿತ ಮತ್ತು ಇ–ವಾಣಿಜ್ಯದ ಉತ್ತೇಜನಕ್ಕಾಗಿ ಕೇಂದ್ರ ಸರ್ಕಾರವು ಗೂಢಲಿಪೀಕರಣಕ್ಕಾಗಿ ವಿಧಾನಗಳು ಅಥವಾ ವಿಧಾನಗಳನ್ನು ಸೂಚಿಸಬಹುದು.

ಪ್ರತಿರೂಪಿಸುವುದರ ಮೂಲಕ ಅಪರಾಧಿಗಳು ಆದಾಯ ವೃದ್ಧಿಗೆ ದಾರಿ ಕಂಡುಕೊಳ್ಳಬಹುದು

www.cybersafegirl.com

ಕೀಲಾಗರ್ (ಕೀಲಿ ಭೇದಕಗಳು)

ಸೀತಾ ಮತ್ತು ಗೀತಾ ಪ್ರಾಣ ಸ್ನೇಹಿತರಾಗಿದ್ದು ಒಂದೇ ಕಂಪನಿಯಲ್ಲಿ ಕೆಲಸ ಮಾಡುತ್ತಿದ್ದು, ಪಿ.ಜಿಯಲ್ಲಿ ಒಟ್ಟಿಗೆ ಒಂದೇ ಕೊಠಡಿಯಲ್ಲಿದ್ದರು.	ಆಕಸ್ಮಿಕದಂತೆ, ಇಬ್ಬರಿಗೂ ಸಹ ತಮ್ಮ ಮಾಲೀಕ ರಾಜುವಿನ ಮೇಲೆ ಪ್ರೇಮಾಂಕುರವಾಗುತ್ತದೆ.	ಕೂಡಲೇ ಗೀತಾ ರಾಜುವಿಗೆ ತನ್ನ ಪ್ರೇಮ ಪ್ರಸ್ತಾಪಿಸಿ ಅವನ ಒಪ್ಪಿಗೆ ಪಡೆದು ಅವನೊಂದಿಗೆ ತೀರಾ ವೈಯಕ್ತಿಕವಾಗುತ್ತಾಳೆ.
ಇದರಿಂದ ನೊಂದ ಸೀತಾ, ಗೀತಾಳಿಗೆ ಜೀವನಪರ್ಯಂತ ನೆನೆಸಿಕೊಳ್ಳುವಂತ ಪಾಠ ಕಲಿಸಲು ತೀರ್ಮಾನಿಸುತ್ತಾಳೆ.	ಗೀತಾಳ ನಡೆಗಳ ಬಗ್ಗೆ ತಿಳಿಯಲು ಗೂಢಾಚಾರಿಕೆಗಾಗಿ ಸೀತ ಗೀತಾಳ ಲ್ಯಾಪ್‌ಟಾಪ್‌ನಲ್ಲಿ ಕೀಲಾಗರ್ ತಂತ್ರಾಂಶ ಅಳವಡಿಸುತ್ತಾಳೆ.	ಈಗ ಗೀತಾಳಿಗೆ ತನ್ನ ಮೇಲ್, ಫೋಟೋ, ಗುಪ್ತಪದ, ವೈಯಕ್ತಿಕ ಹರಟೆ, ಅಂತರ್ಜಾಲ ವಿಹಾರದ ವಿವರಗಳು ಸೀತಾಳ ಬಳಿ ಹೋಗಿರುವ ಬಗ್ಗೆ ತಿಳಿದಿರುವುದಿಲ್ಲ.
		
ಸೀತಾ ಗೀತಾಳ ಪೋಷಕರಿಗೆ ಎಲ್ಲ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಮೇಲ್ ಮಾಡಿ, ಫೋಟೋಗಳನ್ನು ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ನಕಲಿ ಖಾತೆಸೃಷ್ಟಿಸಿ ಅದರಲ್ಲಿ ಅಪ್‌ಲೋಡ್ ಮಾಡುತ್ತಾಳೆ.	ಇದನ್ನು ನೋಡಿ ರಾಜು ಆಘಾತಗೊಳ್ಳುತ್ತಾನೆ. ಗೀತಾಳಿಂದ ದೂರವಾಗುತ್ತಾನೆ. ಗೀತಾ ನೆಮ್ಮದಿ ಕಳೆದು ಕೊಳ್ಳುತ್ತಾಳೆ.	ಕೊನೆಗೆ ಗೀತಾ ತನ್ನ ಲ್ಯಾಪ್‌ಟಾಪ್‌ಗೆ ಗುಪ್ತಪದ ನೀಡದೆ, ಆ್ಯಂಟಿ ವೈರಸ್ ಹಾಕದೇ, ಅಸುರಕ್ಷಿತವಾಗಿ ಇಟ್ಟಿದ್ದರ ಬಗ್ಗೆ ಬೇಸರಗೊಳ್ಳುತ್ತಾಳೆ

ಇದೊಂದು ದುರುದ್ದೇಶಪೂರಕ ತಂತ್ರಾಂಶವಾಗಿದೆ.ಗುಪ್ತಪದ ಮತ್ತು ಇತರೆ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಲು ಗಣಕಯಂತ್ರ ಬಳಕೆದಾರರ ಕೀಲಿಚಲಾವಣೆಗಳನ್ನು ದಾಖಲು ಮಾಡಿಕೊಳ್ಳಬಹುದಾಗಿದೆ.ಕೀಲಾಗರ್‌ಗಳಿಂದ ಅತಿಕ್ರಮಣಕಾರರು ಲಾಗಿನ್ ವಿವರಗಳು ಮತ್ತು ಗಣಕಯಂತ್ರದಲ್ಲಿ ಶೇಖರಿಸಲ್ಪಟ್ಟಿರುವ ಇತರೆ ದತ್ತಾಂಶವನ್ನು ಕಲೆಹಾಕಿಕೊಂಡು ನಿಗದಿಪಡಿಸಿದ ಇ–ಮೇಲ್ ವಿಳಾಸಕ್ಕೆ ಮೇಲ್ ಮುಖೇನ ಕಳುಹಿಸಿಕೊಳ್ಳಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66: ಕೀಲಿ ಬೇಧಕಗಳ ಸ್ಥಾಪನೆ:
– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ : ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಕಳ್ಳತನ
ಕಲಂ 66ಸಿ – ವೈಯಕ್ತಿಕ ಗುರುತು ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ನಕಲಿ ವ್ಯಕ್ತಿಚಿತ್ರ ತಯಾರಿಕೆ ಮತ್ತು ವೈಯಕ್ತಿಕ ಸಂಭಾಷಣೆಯನ್ನು ಪ್ರಸರಿಸುವುದು: ಐ.ಟಿ ಕಾಯ್ದೆ
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ – ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ಮಾಹಿತಿ ಹರಡುವಿಕೆ,

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಎ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ, ಇತ್ಯಾದಿ. ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಬಿ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿರುವ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಲಂಗಳು

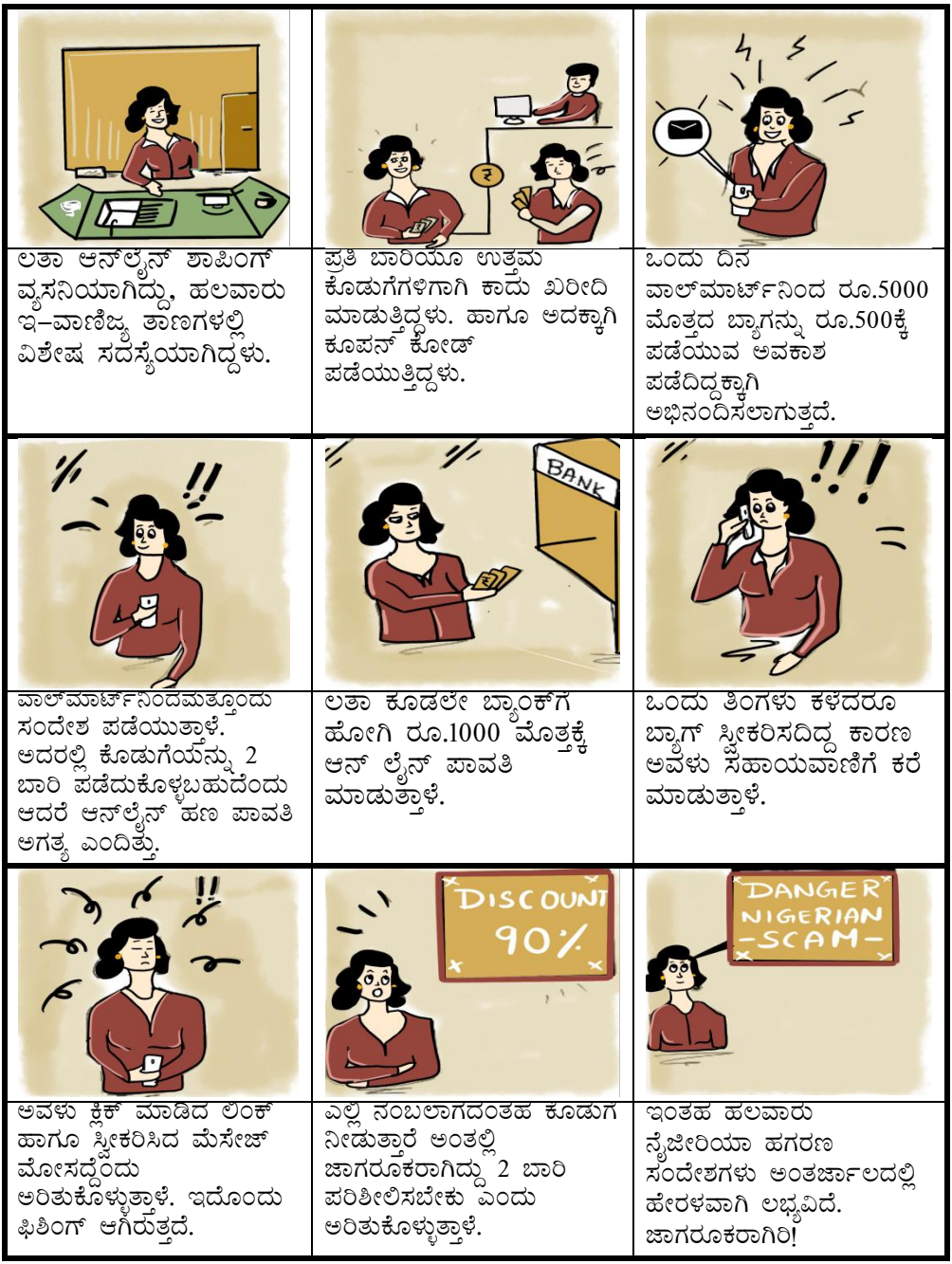
ಕಲಂ 72. ಗೌಪ್ಯತೆ ಮತ್ತು ವೈಯಕ್ತಿಕ ರಹಸ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ದಂಡ

ಐಪಿಸಿ ಕಲಂ 354ಎ/ಬಿಎನ್‌ಎಸ್ 75 –ಲೈಂಗಿಕ ಕಿರುಕುಳ ಮತ್ತು ಲೈಂಗಿಕ ಕಿರುಕುಳಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಕಿರುಕುಳಕ್ಕಾಗಿ ಐಪಿಸಿ ಕಲಂಗಳು:
ಐಪಿಸಿ ಕಲಂ 292/ಬಿಎನ್‌ಎಸ್ 294, 293/ಬಿಎನ್‌ಎಸ್ 295 ಮತ್ತು 294/ಬಿಎನ್‌ಎಸ್ 296

ಕೀಲಿ ಭೇದಕಗಳು ನಿಮ್ಮ ಹಣಪೆಟ್ಟಿಗೆಯನ್ನು ಖಾಲಿ ಮಾಡಬಹುದು.

ಎಸ್.ಎಂ.ಎಸ್ ಮೋಸದ ಜಾಲ


ಲತಾ ಆನ್‌ಲೈನ್ ಶಾಪಿಂಗ್ ವ್ಯಸನಿಯಾಗಿದ್ದು, ಹಲವಾರು ಇ–ವಾಣಿಜ್ಯ ತಾಣಗಳಲ್ಲಿ ವಿಶೇಷ ಸದಸ್ಯೆಯಾಗಿದ್ದಳು.
ಪ್ರತಿ ಬಾರಿಯೂ ಉತ್ತಮ ಕೊಡುಗೆಗಳಿಗಾಗಿ ಕಾದು ಖರೀದಿ ಮಾಡುತ್ತಿದ್ದಳು. ಹಾಗೂ ಅದಕ್ಕಾಗಿ ಕೂಪನ್ ಕೋಡ್ ಪಡೆಯುತ್ತಿದ್ದಳು.
ಒಂದು ದಿನ ವಾಲ್‌ಮಾರ್ಟ್‌ನಿಂದ ರೂ.5000 ಮೊತ್ತದ ಬ್ಯಾಗನ್ನು ರೂ.500ಕ್ಕೆ ಪಡೆಯುವ ಅವಕಾಶ ಪಡೆದಿದ್ದಕ್ಕಾಗಿ ಅಭಿನಂದಿಸಲಾಗುತ್ತದೆ.
ವಾಲ್‌ಮಾರ್ಟ್‌ನಿಂದಮತ್ತೊಂದು ಸಂದೇಶ ಪಡೆಯುತ್ತಾಳೆ. ಅದರಲ್ಲಿ ಕೊಡುಗೆಯನ್ನು 2 ಬಾರಿ ಪಡೆದುಕೊಳ್ಳಬಹುದೆಂದು ಆದರೆ ಆನ್‌ಲೈನ್ ಹಣ ಪಾವತಿ ಅಗತ್ಯ ಎಂದಿತ್ತು.
BANK
ಲತಾ ಕೂಡಲೇ ಬ್ಯಾಂಕ್‌ಗೆ ಹೋಗಿ ರೂ.1000 ಮೊತ್ತಕ್ಕೆ ಆನ್ ಲೈನ್ ಪಾವತಿ ಮಾಡುತ್ತಾಳೆ.
ಒಂದು ತಿಂಗಳು ಕಳೆದರೂ ಬ್ಯಾಗ್ ಸ್ವೀಕರಿಸದಿದ್ದ ಕಾರಣ ಅವಳು ಸಹಾಯವಾಣಿಗೆ ಕರೆ ಮಾಡುತ್ತಾಳೆ.
ಅವಳು ಕ್ಲಿಕ್ ಮಾಡಿದ ಲಿಂಕ್ ಹಾಗೂ ಸ್ವೀಕರಿಸಿದ ಮೆಸೇಜ್ ಮೋಸದ್ದೆಂದು ಅರಿತುಕೊಳ್ಳುತ್ತಾಳೆ. ಇದೊಂದು ಫಿಶಿಂಗ್ ಆಗಿರುತ್ತದೆ.
DISCOUNT 90%
ಎಲ್ಲಿ ನಂಬಲಾಗದಂತಹ ಕೊಡುಗೆ ನೀಡುತ್ತಾರೆ ಅಂತಲ್ಲಿ ಜಾಗರೂಕರಾಗಿದ್ದು 2 ಬಾರಿ ಪರಿಶೀಲಿಸಬೇಕು ಎಂದು ಅರಿತುಕೊಳ್ಳುತ್ತಾಳೆ.
DANGER NIGERIAN -SCAM-
ಇಂತಹ ಹಲವಾರು ನೈಜೀರಿಯಾ ಹಗರಣ ಸಂದೇಶಗಳು ಅಂತರ್ಜಾಲದಲ್ಲಿ ಹೇರಳವಾಗಿ ಲಭ್ಯವಿದೆ. ಜಾಗರೂಕರಾಗಿರಿ!

ಸಾಮಾನ್ಯವಾಗಿ ನಾವು ನಮ್ಮ ಮೊಬೈಲ್/ಇನ್ನಿತರ ಸಾಧನಗಳಿಂದ ಕಳುಹಿಸುವ ಎಸ್.ಎಂ.ಎಸ್. ಸಂದೇಶಗಳ ಜೊತೆಯಲ್ಲಿ ಮೊಬೈಲ್ ಫೋನ್ ಸಂಖ್ಯೆಯು ಯಥಾವತ್ತಾಗಿ ನಮೂದಾಗುವದಾಗಿದ್ದು, ಸಂದೇಶ ರವಾನಿಸುವವರು ಸದರಿ ಸಂಖ್ಯೆಯನ್ನು ಬದಲಾಯಿಸಲು ಅವಕಾಶವಿರುವದಿಲ್ಲ. ಆದರೆಎಸ್.ಎಂ.ಎಸ್. ಸ್ಪೂಫಿಂಗ್ (ವಂಚನೆ) ಮಾಡುವವರು ತಮ್ಮ ಮೊಬೈಲ್ ಸಂಖ್ಯೆ/ಗುರುತನ್ನು ಬದಲಾಯಿಸುವ, ಮರೆಮಾಚುವ ಅಥವಾ ಬೇರಿನ್ಯಾವುದೋ ಗುರುತನ್ನು ಬಳಸುವುದರಿಂದ ಕಾರ್ಯಾಚರಣೆ ಮಾಡುವರು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಒಂದು ಸಂವಹನದ ವಂಚನೆ ಅಥವಾ ತಂತ್ರ ಅಥವಾ ಕೀಟಲೆಯಂತಹ ಕೃತ್ಯಕ್ಕಾಗಿ ಐಪಿಸಿ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 465/ಬಿಎನ್ಎಸ್ 336– ಸುಳ್ಳು ದಾಖಲೆಗಳ ಸೃಷ್ಟಿ(ನಕಲುರುಜು)

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್ಎಸ್ 319–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಮಾ.ತ ಕಾಯ್ದೆ:

ಕಲಂ 43: ಎಸ್ಎಂಎಸ್ ವಂಚನೆಗೆ ನೇರವಾಗಿ ಸಂಬಂಧಿಸದಿದ್ದರೂ, ಈ ಕಲಂ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶಕ್ಕೆ ಸಂಬಂಧಿಸಿದೆ, ಎಸ್ಎಂಎಸ್ ವಂಚನೆ ಮಾಡುವ ಉದ್ದೇಶಕ್ಕಾಗಿ ಯಾರೇ ಸಿಸ್ಟಮ್‌ಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ ಪಡೆದರೆ ಇದು ಅನ್ವಯಿಸಬಹುದು.

ಕಲಂ 43ಎ ಮತ್ತು ಕಲಂ 72ಎ: ಈ ಕಲಂಗಳು ಡೇಟಾ ಮತ್ತು ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆಯನ್ನು ರಕ್ಷಿಸುವಲ್ಲಿ ವಿಫಲವಾದರೆ ಪರಿಹಾರವನ್ನು ವ್ಯವಹರಿಸುತ್ತವೆ. ಎಸ್ಎಂಎಸ್ ವಂಚನೆಯು ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯ ಉಲ್ಲಂಘನೆಗೆ ಕಾರಣವಾದರೆ, ಈ ಕಲಂಗಳು ಕಾರ್ಯರೂಪಕ್ಕೆ ಬರಬಹುದು.

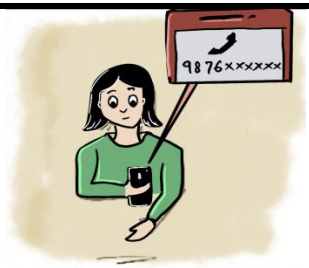
ಕಲಂ 66ಸಿ: ಗುರುತಿನ ಕಳ್ಳತನದ ಬಗ್ಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ. ಬೇರೊಬ್ಬರಂತೆ ನಟಿಸಲು ಮತ್ತು ವಂಚನೆ ಮಾಡಲು ಅಥವಾ ಇತರರನ್ನು ವಂಚಿಸಲು ಎಸ್ಎಂಎಸ್ ವಂಚನೆಯನ್ನು ಬಳಸಿದರೆ, ಅದನ್ನು ಈ ಕಲಂ ಅಡಿಯಲ್ಲಿ ಒಳಗೊಳ್ಳಬಹುದು.

ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 66ಇ: ಈ ಕಲಂ ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಳನ್ನು ಮತ್ತು ಅವರ ಒಪ್ಪಿಗೆಯಿಲ್ಲದೆ ಯಾವುದೇ ವ್ಯಕ್ತಿಯ ಖಾಸಗಿ ಪ್ರದೇಶದ ಚಿತ್ರಗಳನ್ನು ಸೆರೆಹಿಡಿಯುವುದು, ಪ್ರಕಟಿಸುವುದು ಅಥವಾ ರವಾನಿಸುವುದನ್ನು ತಿಳಿಸುತ್ತದೆ. ಈ ರೀತಿಯಲ್ಲಿ ಯಾರೊಬ್ಬರ ಗೌಪ್ಯತೆಯನ್ನು ಆಕ್ರಮಣ ಮಾಡಲು ಎಸ್ಎಂಎಸ್ ವಂಚನೆಯನ್ನು ಬಳಸಿದರೆ, ಈ ವಿಭಾಗವು ಅನ್ವಯಿಸಬಹುದು.

ಸೈಬರ್ ಕಳ್ಳರಿಂದ ಸಣ್ಣ ಸಂದೇಶಗಳ ನಕಲೀಕರಣ ನಡೆಯುತ್ತದೆ.

ಮೋಸದ ಕರೆಗಳು

ನಿಶಾ ವಿಧವೆಯಾಗಿರುತ್ತಾಳೆ. ಅವಳು ತನ್ನ ಸ್ವಂತ ಮನೆಯಲ್ಲಿ ಒಂಟಿಯಾಗಿ ವಾಸಿಸುತ್ತಾಳೆ.	ತಾನು ಬಿಡುವಿಲ್ಲದಂತೆ ಇರಲು ಅಂತರ್ಜಾಲದಲ್ಲಿ ಸಕ್ರಿಯವಾಗಿದ್ದು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಹೆಚ್ಚು ಕ್ರಿಯಾತ್ಮಕವಾಗಿದ್ದಳು.	ಅವಳಿಗೆ ಆನ್‌ಲೈನ್‌ನ ಸಾಮಾಜಿಕ ಕಳಕಳಿ ಬಗ್ಗೆ ಅರಿವು ಇರಲಿಲ್ಲ. ಯಾರೇ ಆನ್‌ಲೈನ್ ಸ್ನೇಹಕ್ಕಾಗಿ ಕೋರಿಕೆ ಸಲ್ಲಿಸಿದರೆ ಯೋಚಿಸದೇ ಅದನ್ನು ಒಪ್ಪಿಕೊಳ್ಳುತ್ತಿದ್ದಳು.
		
ನಿಶಾಳ ಮಗನು ಕರೆಮಾಡಿ ತುರ್ತು ಅಗತ್ಯತೆಗಾಗಿ ರೂ. 1 ಲಕ್ಷವನ್ನು ಸ್ನೇಹಿತನ ಖಾತೆಗೆ ಜಮೆ ಮಾಡಲು ಕೋರುತ್ತಾನೆ.	ನಿಶಾ ಮಗನ ಸಂಖ್ಯೆ ಪರೀಕ್ಷಿಸಿ ದೃಢೀಕರಿಸಿಕೊಂಡು ಮಾನ್ಯವೆಂದು ಅರಿತು, ನಂತರ ಫಲಾನುಭವಿ ಆಗಿ ಖಾತೆಗೆ ಸೇರಿಸಿ ಹಣ ವರ್ಗಾಯಿಸುತ್ತಾಳೆ.	ಹಣ ವರ್ಗಾಯಿಸಿದ ನಂತರ ಮಗನಿಗೆ ಕರೆ ಮಾಡಿ, ಅವನ ಖಾತೆಗೆ ಹಣ ಜಮೆ ಆಗಿರುವ ಬಗ್ಗೆ ಖಾತ್ರಿ ಪಡಿಸಿಕೊಳ್ಳುತ್ತಾಳೆ.
ಅವಳ ಮಗ ಸಂಜು ಆಶ್ಚರ್ಯದಿಂದ ತಾನು ಯಾವುದೇ ರೀತಿ ಹಣ ಕೋರಿ ಕರೆ ಮಾಡಿಲ್ಲ ಎಂದು ಉತ್ತರಿಸುತ್ತಾನೆ.	ನಿಶಾ ಮೋಸದ ಕರೆಗೆ ಬಲಿಯಾಗಿ ಹಣ ಕಳೆದುಕೊಂಡು ಅಪರಿಚಿತ ಹಗರಣಕೋರನಿಂದ ವಂಚಿತಲಾಗಿರುತ್ತಾಳೆ.	ಕೆಲವು ಆ್ಯಪ್ಸ್ ಬಳಸಿ ಯಾವುದೇ ಸಂಖ್ಯೆಯಿಂದ ಸುಳ್ಳು ಕರೆ ಮತ್ತು ಎಸ್‌ಎಂಎಸ್ ಮಾಡಬಹುದಾಗಿರುತ್ತದೆ.

ಅಪರಾಧ ಉದ್ದೇಶ ಹೊಂದಿರುವ ವ್ಯಕ್ತಿಯು ತನ್ನ ಮೊಬೈಲ್ ಸಂಖ್ಯೆ ಮತ್ತು ಧ್ವನಿಯನ್ನು ಬದಲಾಯಿಸಿಕೊಂಡು ಇನ್ನೊಬ್ಬರನ್ನು ವಂಚಿಸಲು ನಿರಾಕಾರವಾಗಿ ಅನುವು ಮಾಡಿಕೊಡುವ ತಂತ್ರಾಂಶಗಳ ಮೂಲಕ ಕರೆ ಮಾಡಿ ವಂಚನೆಗಳು ಸಂಭವಿಸುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಒಂದು ಸಂವಹನದ ವಂಚನೆ ಅಥವಾ ತಂತ್ರ ಅಥವಾ ಕೀಟಲೆಯಂತಹ ಕೃತ್ಯಕ್ಕಾಗಿ ಐಪಿಸಿ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 465/ಬಿಎನ್ಎಸ್ 336– ಸುಳ್ಳು ದಾಖಲೆಗಳ ಸೃಷ್ಟಿ(ನಕಲುರುಜು)

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್ಎಸ್ 319–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಮಾ.ತ ಕಾಯ್ದೆ:

ಕಲಂ 66ಸಿ – ಗುರುತಿನ ಕಳ್ಳತನ: ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯಿದೆಯ ಈ ಕಲಂ ಗುರುತಿನ ಕಳ್ಳತನದ ಬಗ್ಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ, ಇದು ಯಾವುದೇ ಇತರ ವ್ಯಕ್ತಿಯ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಹಿ, ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಯಾವುದೇ ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ. ದುರುದ್ದೇಶದಿಂದ ಯಾರೊಬ್ಬರ ವಿಶಿಷ್ಟ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಕದಿಯುವುದನ್ನು ಒಳಗೊಂಡಿದ್ದರೆ ಸ್ಪೂಫಿಂಗ್ ಕರೆ ಈ ಕಲಂ ವ್ಯಾಪ್ತಿಯ ಅಡಿಯಲ್ಲಿ ಬರಬಹುದು.

ಹೆಚ್ಚುವರಿಯಾಗಿ, ಕಲಂ 66ಡಿ – ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವೈಯಕ್ತಿಕ ಗುರುತು ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಇದನ್ನು ಅನ್ವಯಿಸಬಹುದು. ಈ ವಿಭಾಗವು ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲದ ಬಳಕೆಯ ಮೂಲಕ ವಂಚನೆಯನ್ನು ಪರಿಹರಿಸುತ್ತದೆ. ಯಾರನ್ನಾದರೂ ಮೋಸ ಮಾಡುವ ಅಥವಾ ವಂಚಿಸುವ ಉದ್ದೇಶದಿಂದ ಕರೆ ವಂಚನೆ ಮಾಡಿದರೆ, ಅದು ಈ ವಿಭಾಗದ ಅಡಿಯಲ್ಲಿ ಬರಬಹುದು.

ಕರೆಗಳ ಮರೆಮಾಚುವಿಕೆ ಅಪರಾಧಿಕ ಉದ್ದೇಶಗಳಿಗಾಗಿ ಮಾತ್ರ.

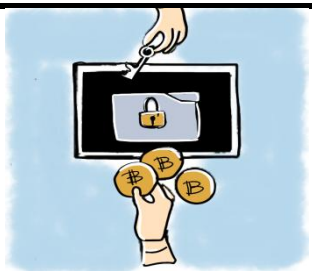
ಬಂಧಿ ವಿಮೋಚನಾ ತಂತ್ರಾಂಶ (ರ್‍ಯಾನ್ಸಮ್‌ವೇರ್)

ಅನು ಒಬ್ಬಳು ಉದ್ಯಮಿ. ಅವಳ ಸಂಸ್ಥೆಯಲ್ಲಿ 50 ನೌಕರರು ಹಾಗೂ 60 ಗಣಕಯಂತ್ರಗಳು ಇರುತ್ತದೆ.

ಒಂದು ದಿನ ತನ್ನ ಮಾರಾಟ ಗಾರರಿಂದ ಒಂದು ಇ-ಮೇಲ್ ಸ್ವೀಕರಿಸುತ್ತಾಳೆ. ಅದು ಒಂದು ಲಗತ್ತನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ.

ಆ ಲಗತ್ತನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುತ್ತಾಳೆ. ಅವಳ ಆ್ಯಂಟಿ ವೈರಸ್ ಪರಿಷ್ಕರಿಸದೇ ಇದ್ದರಿಂದ ಯಾವುದೇ ಎಚ್ಚರಿಕೆ ಸಂದೇಶ ಕಾಣಿಸುವುದಿಲ್ಲ.

ಫೈಲ್ ತೆರೆಯುತ್ತಿದ್ದಂತೆಯೇಗಣಕವು ಬೀಗಮುದ್ರೆಗೊಂಡು ಗಣಕ ಯಂತ್ರದಲ್ಲಿದ್ದ ಇತರೆ ಎಲ್ಲಾ ಫೈಲ್‌ಗಳು ಗೂಢಲಿಪೀಕರಿಸಲಾಗಿರುತ್ತದೆ.



ಪರದೆ ಮೇಲೆ ಎಚ್ಚರಿಕೆ ಸಂದೇಶ ಕಾಣುತ್ತದೆ, ಅದರಲ್ಲಿ 1 ಲಕ್ಷ ಬಿಟ್‌ಕಾಯಿನ್ ಪಾವತಿಸಿ ಕಡತ ಅನ್‌ಲಾಕ್ ಮಾಡಿಕೊಳ್ಳಲು ತಿಳಿಸಲಾಗಿರುತ್ತದೆ.

ಅನು ಬಿಟ್‌ಕಾಯಿನ್ ಚೀಲದ ವಿಳಾಸಕ್ಕೆ ಹಣವನ್ನು ಪಾವತಿ ಮಾಡುತ್ತಾಳೆ.

ಆದರೂ ಹ್ಯಾಕರ್ ಖಾಸಗಿ ಕೀ ಕಳುಹಿಸದೇ ಕಡತಗಳು ಗೂಢ ಲಿಪೀಗ್ರಹಿಸಲಾಗದೇ ಉಪಯೋಗಿಸಲು ಆಗುವುದಿಲ್ಲ.

ಅವಳ ನಿರ್ವಾಹಕನು ತಾನು ಸ್ವೀಕರಿಸಿದ್ದ ಮೇಲ್ ರ್‍ಯಾನ್ಸಮ್‌ವೇರ್ ಹೊಂದಿದ್ದ ಫಿಶಿಂಗ್ ಮೇಲ್ ಎಂದು ಹೇಳುತ್ತಾನೆ.

ಅನು ಕಡತವನ್ನು ತಿಳಿಯದೇ ತೆರೆದಿದ್ದಕ್ಕೆ ಮತ್ತು ಆ್ಯಂಟಿ ವೈರಸ್ ಪರಿಷ್ಕರಿಸದಿದ್ದಕ್ಕೆ ಪಶ್ಚಾತ್ತಾಪಪಡುತ್ತಾಳೆ.

ರ್‍ಯಾನ್ಸಮ್‌ವೇರ್ ಎನ್ನುವುದು ಮಾಲ್ವೇರ್‌ನ ಒಂದು ರೂಪವಾಗಿದ್ದು ಅದು ಅಮಾಯಕರ ಕಡತ ಮತ್ತು ದತ್ತಾಂಶಗಳನ್ನು ಗೂಢಲಿಪೀಕರಿಸುತ್ತದೆ. ನಂತರ ಆಕ್ರಮಣಕಾರನು ಒತ್ತೆಹಣದ ಪಾವತಿಯ ಒಪ್ಪಂದದ ಮೇರೆಗೆ ದತ್ತಾಂಶಗಳಿಗೆ ಮಾಲೀಕನ ಪ್ರವೇಶಾವಕಾಶವನ್ನು ಪುನಃಸ್ಥಾಪಿಸಲಾಗುತ್ತದೆ.ಗೂಢಲಿಪೀಗ್ರಹಣನ ಕೀಲಿಯನ್ನು ಪಡೆಯಲು ಶುಲ್ಕವನ್ನು ಹೇಗೆ ಪಾವತಿಸಬೇಕು ಎಂಬುದರ ಕುರಿತು ಬಳಕೆದಾರರಿಗೆ ಸೂಚನೆಗಳನ್ನು ತೋರಿಸಲಾಗುತ್ತದೆ.ಈ ರೀತಿಯಾದ ಶುಲ್ಕವು ಕೆಲವು ನೂರು ಡಾಲರ್‌ಗಳಿಂದ ಸಾವಿರಾರು ಡಾಲರ್‌ಗಳವರೆಗೆ ಇರಬಹುದು ಹಾಗೂ ಇದನ್ನು ಬಿಟ್‌ಕಾಯಿನ್ ರೂಪದಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧಿಗಳಿಗೆ ಪಾವತಿಸಬೇಕಾಗುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಅನಧಿಕೃತ ಪ್ರವೇಶಾತಿ, ನಿರಾಕರಣೆ, ಗೂಢಲಿಪೀಕರಣ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಕಲಂ 66ಸಿ: ಗುರುತಿನ ಕಳ್ಳತನದ ಬಗ್ಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ. ಬೇರೊಬ್ಬರಂತೆ ನಟಿಸಲು ಮತ್ತು ವಂಚನೆ ಮಾಡಲು ಅಥವಾ ಇತರರನ್ನು ವಂಚಿಸಲು ಎಸ್‌ಎಂಎಸ್ ವಂಚನೆಯನ್ನು ಬಳಸಿದರೆ, ಅದನ್ನು ಈ ಕಲಂ ಅಡಿಯಲ್ಲಿ ಒಳಗೊಳ್ಳಬಹುದು.

ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಪಾವತಿ ಇಲ್ಲದಂತಹ ಬೇಡಿಕೆ

ಐಪಿಸಿ ಕಲಂ384/ಬಿಎನ್‌ಎಸ್ 308– ಸುಲಿಗೆ

ಕಲಂ 386/ಬಿಎನ್‌ಎಸ್ 308: ಈ ಕಲಂ ವ್ಯಕ್ತಿಯನ್ನು ಸಾವಿನ ಭಯ ಅಥವಾ ಘೋರವಾದ ನೋವನ್ನುಂಟು ಮಾಡುವ ಮೂಲಕ ಸುಲಿಗೆಗೆ ಸಂಬಂಧಿಸಿದೆ.

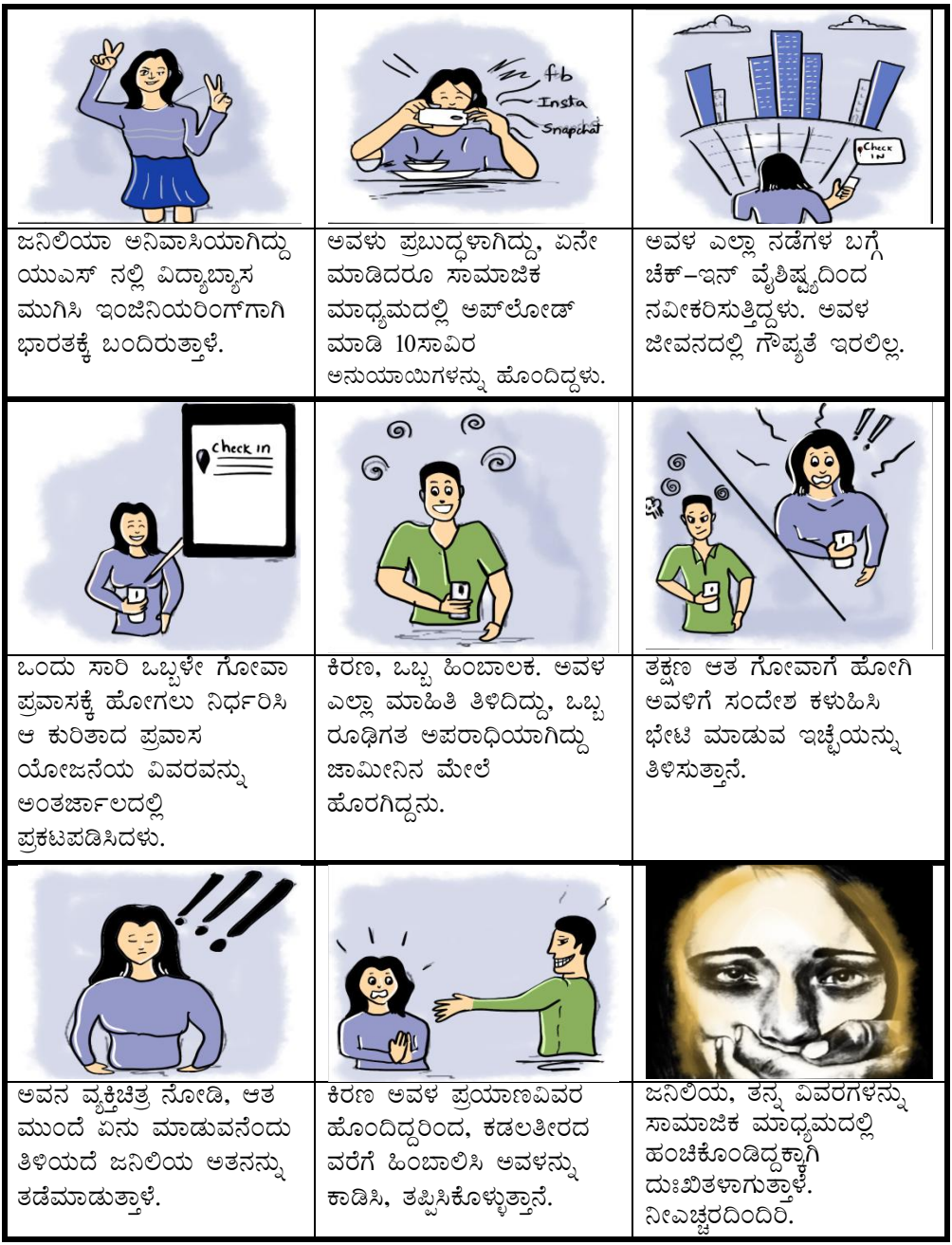
ಐಪಿಸಿ ಕಲಂ 511/ಬಿಎನ್‌ಎಸ್ 62– ಅಪರಾಧ ಎಸಗಲು ಯತ್ನಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಜೀವಾವಧಿ ಶಿಕ್ಷೆ ಅಥವಾ ಇತರೆ ಜೈಲು ಶಿಕ್ಷೆ

ಪಾವತಿ ಮತ್ತು ಬೇಡಿಕೆ

ಐಪಿಸಿ ಕಲಂ384/ಬಿಎನ್‌ಎಸ್ 308– ಸುಲಿಗೆ

ರ್‍ಯಾನ್ಸಮ್‌ವೇರ್‌ಅನ್ನು ನಿಯಂತ್ರಿಸಲು ಆ್ಯಂಟಿ ವೈರಸನ್ನು ಆಗಿಂದಾಗ್ಗೆ ಪರಿಷ್ಕರಿಸಿ.

ಸೈಬರ್ ಹಿಂಬಾಲಿಕೆ



ಜನಿಲಿಯಾ ಅನಿವಾಸಿಯಾಗಿದ್ದು ಯುಎಸ್ ನಲ್ಲಿ ವಿದ್ಯಾಬ್ಯಾಸ ಮುಗಿಸಿ ಇಂಜಿನಿಯರಿಂಗ್‌ಗಾಗಿ ಭಾರತಕ್ಕೆ ಬಂದಿರುತ್ತಾಳೆ.

ಅವಳು ಪ್ರಬುದ್ಧಳಾಗಿದ್ದು, ಏನೇ ಮಾಡಿದರೂ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಅಪ್‌ಲೋಡ್ ಮಾಡಿ 10ಸಾವಿರ ಅನುಯಾಯಿಗಳನ್ನು ಹೊಂದಿದ್ದಳು.

ಅವಳ ಎಲ್ಲಾ ನಡೆಗಳ ಬಗ್ಗೆ ಚೆಕ್–ಇನ್ ವೈಶಿಷ್ಟ್ಯದಿಂದ ನವೀಕರಿಸುತ್ತಿದ್ದಳು. ಅವಳ ಜೀವನದಲ್ಲಿ ಗೌಪ್ಯತೆ ಇರಲಿಲ್ಲ.

ಒಂದು ಸಾರಿ ಒಬ್ಬಳೇ ಗೋವಾ ಪ್ರವಾಸಕ್ಕೆ ಹೋಗಲು ನಿರ್ಧರಿಸಿ ಆ ಕುರಿತಾದ ಪ್ರವಾಸ ಯೋಜನೆಯ ವಿವರವನ್ನು ಅಂತರ್ಜಾಲದಲ್ಲಿ ಪ್ರಕಟಪಡಿಸಿದಳು.

ಕಿರಣ, ಒಬ್ಬ ಹಿಂಬಾಲಕ. ಅವಳ ಎಲ್ಲಾ ಮಾಹಿತಿ ತಿಳಿದಿದ್ದು, ಒಬ್ಬ ರೂಢಿಗತ ಅಪರಾಧಿಯಾಗಿದ್ದು ಜಾಮೀನಿನ ಮೇಲೆ ಹೊರಗಿದ್ದನು.

ತಕ್ಷಣ ಆತ ಗೋವಾಗೆ ಹೋಗಿ ಅವಳಿಗೆ ಸಂದೇಶ ಕಳುಹಿಸಿ ಭೇಟಿ ಮಾಡುವ ಇಚ್ಛೆಯನ್ನು ತಿಳಿಸುತ್ತಾನೆ.

ಅವನ ವ್ಯಕ್ತಿಚಿತ್ರ ನೋಡಿ, ಆತ ಮುಂದೆ ಏನು ಮಾಡುವನೆಂದು ತಿಳಿಯದೆ ಜನಿಲಿಯ ಅತನನ್ನು ತಡೆಮಾಡುತ್ತಾಳೆ.

ಕಿರಣ ಅವಳ ಪ್ರಯಾಣವಿವರ ಹೊಂದಿದ್ದರಿಂದ, ಕಡಲತೀರದ ವರೆಗೆ ಹಿಂಬಾಲಿಸಿ ಅವಳನ್ನು ಕಾಡಿಸಿ, ತಪ್ಪಿಸಿಕೊಳ್ಳುತ್ತಾನೆ.

ಜನಿಲಿಯ, ತನ್ನ ವಿವರಗಳನ್ನು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಹಂಚಿಕೊಂಡಿದ್ದಕ್ಕಾಗಿ ದುಃಖಿತಳಾಗುತ್ತಾಳೆ. ನೀಎಚ್ಚರದಿಂದಿರಿ.

ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಅಪ್‌ಲೋಡ್ ಮಾಡಲಾಗಿರುವ ಮಾಹಿತಿಯನ್ನು ದುರುಪಯೋಗ ಪಡಿಸಿಕೊಂಡು ಮತ್ತೊಬ್ಬರನ್ನು ಹಿಂಬಾಲಿಸಲು ಅಥವಾ ಕಿರುಕುಳ ನೀಡಲು ಅಂತರ್ಜಾಲ ಅಥವಾ ಇನ್ನಿತರೆ ವಿದ್ಯುನ್ಮಾನ ವಿಧಾನಗಳನ್ನು 'ಸೈಬರ್ ಹಿಂಬಾಲಿಕೆ' ಎಂದು ಕರೆಯಲಾಗುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಕಲಂ 66ಎ: ಈ ಕಲಂ ಈ ಹಿಂದೆ ಸಂವಹನ ಸೇವೆಗಳ ಮೂಲಕ ಆಕ್ಷೇಪಾರ್ಹ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸುವ ಅಪರಾಧಗಳಿಗೆ ಸಂಬಂಧಿಸಿದೆ. ಆದಾಗ್ಯೂ, ಅಸ್ಪಷ್ಟ ಮತ್ತು ಮಿತಿಮೀರಿದ ಮತ್ತು ವಾಕ್ ಸ್ವಾತಂತ್ರ್ಯದ ಹಕ್ಕನ್ನು ಉಲ್ಲಂಘಿಸುವ ಆಧಾರದ ಮೇಲೆ 2015 ರಲ್ಲಿ ಭಾರತದ ಸುಪ್ರೀಂ ಕೋರ್ಟ್ ಇದನ್ನು ರದ್ದುಗೊಳಿಸಿತು.

ಆಫ್‌ಲೈನ್:

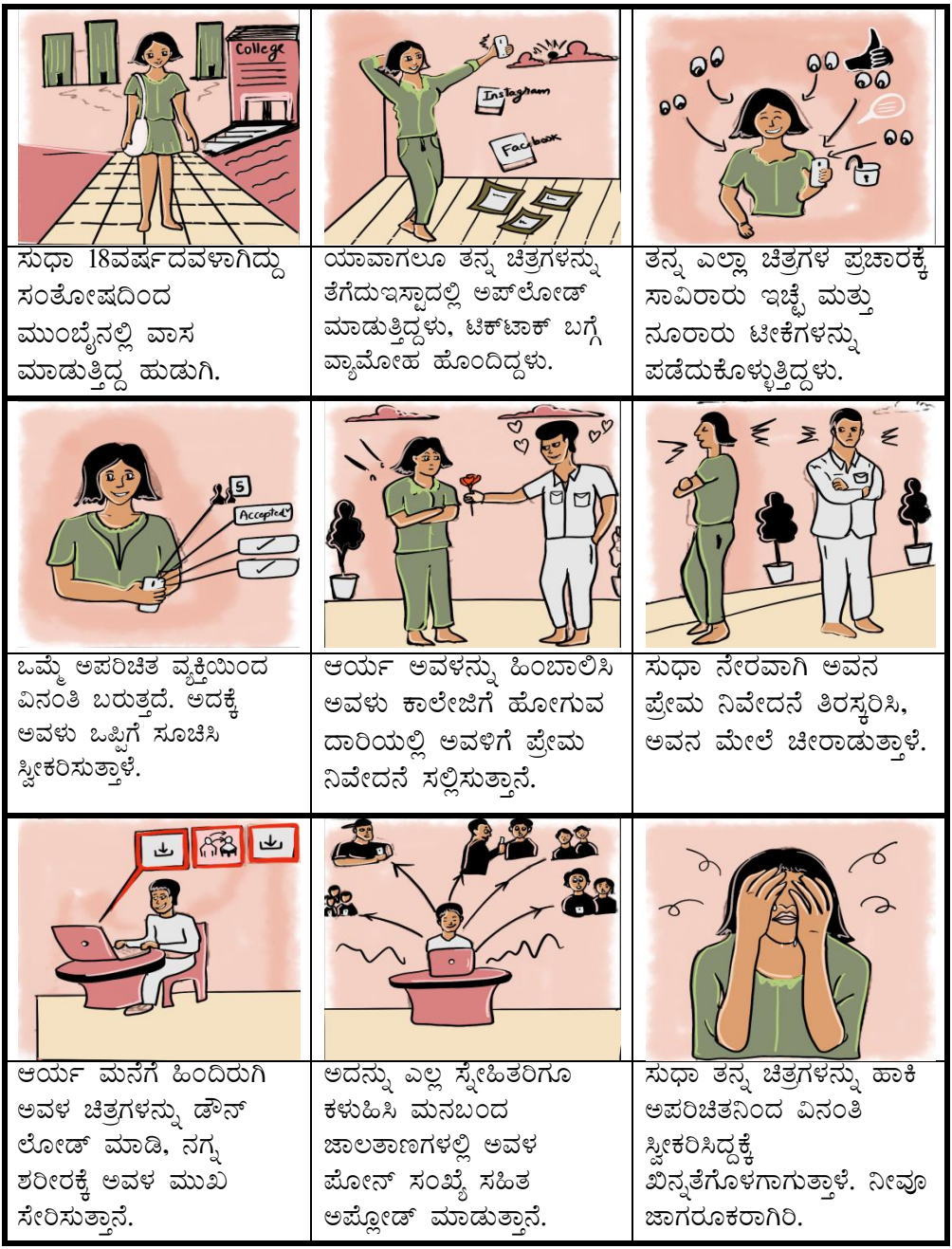
ಐಪಿಸಿ ಸೆಕ್ಷನ್ 354 ಡಿ/ಬಿಎನ್‌ಎಸ್ 78 – ಹಿಂಬಾಲಿಸುವುದು

ಆನ್‌ಲೈನ್:

ಐಪಿಸಿ ಕಲಂ 354 ಡಿ/ಬಿಎನ್‌ಎಸ್ 78 – ಈ ಕಲಂ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ (ತಿದ್ದುಪಡಿ) ಕಾಯಿದೆ, 2013 ಮೂಲಕ ಪರಿಚಯಿಸಲಾಗಿದೆ ಮತ್ತು ನಿರ್ದಿಷ್ಟವಾಗಿ ಸೈಬರ್‌ಸ್ಟಾಕಿಂಗ್ ಅಪರಾಧದ ಬಗ್ಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ. ಇಂಟರ್ನೆಟ್, ಇಮೇಲ್ ಅಥವಾ ಯಾವುದೇ ಇತರ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಂವಹನದಲ್ಲಿ ಮಹಿಳೆಯ ಬಳಕೆಯನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುವ ಯಾವುದೇ ವ್ಯಕ್ತಿ ಸೈಬರ್ ಸ್ಟಾಕಿಂಗ್ ಅಪರಾಧವನ್ನು ಮಾಡುತ್ತಾನೆ ಎಂದು ಅದು ಹೇಳುತ್ತದೆ. ಮಹಿಳೆಯು ತನ್ನ ಸುರಕ್ಷತೆ ಅಥವಾ ತನ್ನ ಸಂಬಂಧಿಕರ ಸುರಕ್ಷತೆಗಾಗಿ ಭಯಪಡುವಂತೆ ಮಾಡುವ ಕ್ರಿಯೆಗಳನ್ನು ಸಹ ಇದು ಅಪರಾಧೀಕರಿಸುತ್ತದೆ. ಈ ಕಲಂಅಡಿಯಲ್ಲಿ ದೋಷಾರೋಪಣೆಯು ಮೂರು ವರ್ಷಗಳವರೆಗೆ ವಿಸ್ತರಿಸಬಹುದಾದ ಅವಧಿಗೆ ಜೈಲು ಶಿಕ್ಷೆ ಮತ್ತು ದಂಡವನ್ನು ಉಂಟುಮಾಡಬಹುದು.

ಮತ್ತೊಬ್ಬರು ನಿಮ್ಮನ್ನು ದೂರದಿಂದ ಗಮನಿಸುತ್ತಿರುವುದನ್ನು ಸೈಬರ್ ಹಿಂಬಾಲಿಕೆ ಎನ್ನಬಹುದು

ಚಿತ್ರ ಆಕೃತಿ ರಚನೆ



ಸುಧಾ 18ವರ್ಷದವಳಾಗಿದ್ದು ಸಂತೋಷದಿಂದ ಮುಂಬೈನಲ್ಲಿ ವಾಸ ಮಾಡುತ್ತಿದ್ದ ಹುಡುಗಿ.

ಯಾವಾಗಲೂ ತನ್ನ ಚಿತ್ರಗಳನ್ನು ತೆಗೆದುಇಸ್ಟಾದಲ್ಲಿ ಅಪ್‌ಲೋಡ್ ಮಾಡುತ್ತಿದ್ದಳು, ಟಿಕ್‌ಟಾಕ್ ಬಗ್ಗೆ ವ್ಯಾಮೋಹ ಹೊಂದಿದ್ದಳು.

ತನ್ನ ಎಲ್ಲಾ ಚಿತ್ರಗಳ ಪ್ರಚಾರಕ್ಕೆ ಸಾವಿರಾರು ಇಚ್ಛೆ ಮತ್ತು ನೂರಾರು ಟೀಕೆಗಳನ್ನು ಪಡೆದುಕೊಳ್ಳುತ್ತಿದ್ದಳು.

ಒಮ್ಮೆ ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಯಿಂದ ವಿನಂತಿ ಬರುತ್ತದೆ. ಅದಕ್ಕೆ ಅವಳು ಒಪ್ಪಿಗೆ ಸೂಚಿಸಿ ಸ್ವೀಕರಿಸುತ್ತಾಳೆ.

ಆರ್ಯ ಅವಳನ್ನು ಹಿಂಬಾಲಿಸಿ ಅವಳು ಕಾಲೇಜಿಗೆ ಹೋಗುವ ದಾರಿಯಲ್ಲಿ ಅವಳಿಗೆ ಪ್ರೇಮ ನಿವೇದನೆ ಸಲ್ಲಿಸುತ್ತಾನೆ.

ಸುಧಾ ನೇರವಾಗಿ ಅವನ ಪ್ರೇಮ ನಿವೇದನೆ ತಿರಸ್ಕರಿಸಿ, ಅವನ ಮೇಲೆ ಚೀರಾಡುತ್ತಾಳೆ.

ಆರ್ಯ ಮನೆಗೆ ಹಿಂದಿರುಗಿ ಅವಳ ಚಿತ್ರಗಳನ್ನು ಡೌನ್ ಲೋಡ್ ಮಾಡಿ, ನಗ್ನ ಶರೀರಕ್ಕೆ ಅವಳ ಮುಖ ಸೇರಿಸುತ್ತಾನೆ.

ಅದನ್ನು ಎಲ್ಲ ಸ್ನೇಹಿತರಿಗೂ ಕಳುಹಿಸಿ ಮನಬಂದ ಜಾಲತಾಣಗಳಲ್ಲಿ ಅವಳ ಫೋನ್ ಸಂಖ್ಯೆ ಸಹಿತ ಅಪ್ಲೋಡ್ ಮಾಡುತ್ತಾನೆ.

ಸುಧಾ ತನ್ನ ಚಿತ್ರಗಳನ್ನು ಹಾಕಿ ಅಪರಿಚಿತನಿಂದ ವಿನಂತಿ ಸ್ವೀಕರಿಸಿದ್ದಕ್ಕೆ ಖಿನ್ನತೆಗೊಳಗಾಗುತ್ತಾಳೆ. ನೀವೂ ಜಾಗರೂಕರಾಗಿರಿ.

ಒಂದು ವ್ಯಕ್ತಿಯ ಮುಖಚಿತ್ರವನ್ನು ಮತ್ತೊಬ್ಬ ವ್ಯಕ್ತಿಯ ದೇಹಕ್ಕೆ ಅಂಟಿಸಿ ಅದನ್ನು ಸುಲಿಗೆ ಮಾಡಲು ಅಥವಾ ವ್ಯಕ್ತಿಯನ್ನು ಬೆದರಿಸುವ ಸಲುವಾಗಿ ಪ್ರಕಟಿಸುವುದು, ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಭಾವಚಿತ್ರಗಳನ್ನು ಅಪ್‌ಲೋಡ್ ಮಾಡುವಂತಹ ಜನರನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳುವ ಒಂದು ಮಾರ್ಗವಾಗಿದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 292/ಬಿಎನ್‌ಎಸ್ 294– ಅಶ್ಲೀಲ ಪುಸ್ತಕಗಳ ಮಾರಾಟ ಇತ್ಯಾದಿ (ಮುದ್ರಣ ಮಾಧ್ಯಮದಲ್ಲಿ)

ಐಪಿಸಿ ಕಲಂ 465/ಬಿಎನ್‌ಎಸ್ 336 –ಭಾವಚಿತ್ರದ ಆಕೃತಿ ರಚಿಸುವುದು ಮತ್ತು ಸುಳ್ಳು ವಿದ್ಯುನ್ಮಾನ ದಾಖಲೆ ಸೃಷ್ಟಿ

ಐಪಿಸಿ ಕಲಂ 469/ಬಿಎನ್‌ಎಸ್ 336– ಮಾನಹಾನಿಯ ಉದ್ದೇಶಕ್ಕಾಗಿ ಸುಳ್ಳು ವಿದ್ಯುನ್ಮಾನ ದಾಖಲೆ ರಚನೆ

ಐಪಿಸಿ ಕಲಂ 507/ಬಿಎನ್‌ಎಸ್ 351– ಅನಾಮಧೇಯ ಸಂವಹನದಿಂದ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ

ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನವಾಗುವ ಉದ್ದೇಶದ ಪದಗಳು, ಸನ್ನೆ ಅಥವಾ ಅಭಿನಯ

ಮಾ.ತ ಕಾಯ್ದೆ:

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

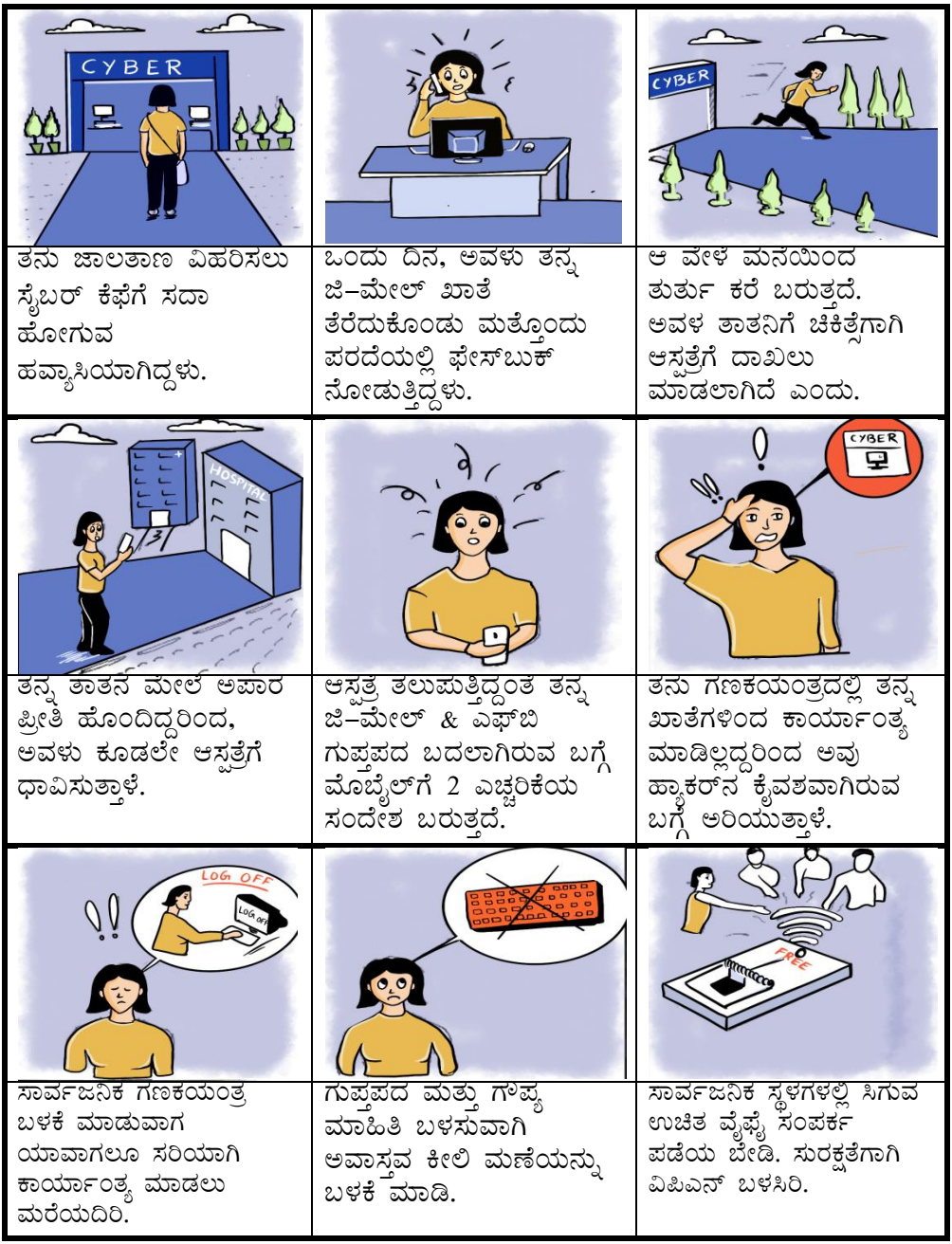
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಎ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಬಿ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವಿನಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿ ವಿದ್ಯುನ್ಮಾನರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಾಯ್ದೆಗಳು

ಮಹಿಳೆಯರ ಅಸಭ್ಯ ಪ್ರಾತಿನಿಧ್ಯವನ್ನು ಹೊಂದಿರುವ ಚಿತ್ರಗಳನ್ನು ಪ್ರಕಟಣೆ ಮಾಡಿದರೆ:
ಕಲಂ 6ರೊಂದಿಗೆ ಓದಲಾದ ಕಲಂ 4ಎ ಮಹಿಳಾ ಅಸಭ್ಯ ಪ್ರಾತಿನಿಧ್ಯ ಕಾಯ್ದೆ, 1986

ನಕಲಿ ಆಕೃತಿ ರಚನೆಯನ್ನು ಮಾನಹಾನಿ ಮಾಡಲು ಬಳಸುತ್ತಾರೆ

ವ್ಯಕ್ತಿಚಿತ್ರ ಅತಿಕ್ರಮಣ(ಹ್ಯಾಕಿಂಗ್)



ತನು ಜಾಲತಾಣ ವಿಹರಿಸಲು ಸೈಬರ್ ಕೆಫೆಗೆ ಸದಾ ಹೋಗುವ ಹವ್ಯಾಸಿಯಾಗಿದ್ದಳು.	ಒಂದು ದಿನ, ಅವಳು ತನ್ನ ಜಿ–ಮೇಲ್ ಖಾತೆ ತೆರೆದುಕೊಂಡು ಮತ್ತೊಂದು ಪರದೆಯಲ್ಲಿ ಫೇಸ್‌ಬುಕ್ ನೋಡುತ್ತಿದ್ದಳು.	ಆ ವೇಳೆ ಮನೆಯಿಂದ ತುರ್ತು ಕರೆ ಬರುತ್ತದೆ. ಅವಳ ತಾತನಿಗೆ ಚಿಕಿತ್ಸೆಗಾಗಿ ಆಸ್ಪತ್ರೆಗೆ ದಾಖಲು ಮಾಡಲಾಗಿದೆ ಎಂದು.
ತನ್ನ ತಾತನ ಮೇಲೆ ಅಪಾರ ಪ್ರೀತಿ ಹೊಂದಿದ್ದರಿಂದ, ಅವಳು ಕೂಡಲೇ ಆಸ್ಪತ್ರೆಗೆ ಧಾವಿಸುತ್ತಾಳೆ.	ಆಸ್ಪತ್ರೆ ತಲುಪುತ್ತಿದ್ದಂತೆ ತನ್ನ ಜಿ–ಮೇಲ್ & ಎಫ್‌ಬಿ ಗುಪ್ತಪದ ಬದಲಾಗಿರುವ ಬಗ್ಗೆ ಮೊಬೈಲ್‌ಗೆ 2 ಎಚ್ಚರಿಕೆಯ ಸಂದೇಶ ಬರುತ್ತದೆ.	ತನು ಗಣಕಯಂತ್ರದಲ್ಲಿ ತನ್ನ ಖಾತೆಗಳಿಂದ ಕಾರ್ಯಾಂತ್ಯ ಮಾಡಿಲ್ಲದ್ದರಿಂದ ಅವು ಹ್ಯಾಕರ್‌ನ ಕೈವಶವಾಗಿರುವ ಬಗ್ಗೆ ಅರಿಯುತ್ತಾಳೆ.
ಸಾರ್ವಜನಿಕ ಗಣಕಯಂತ್ರ ಬಳಕೆ ಮಾಡುವಾಗ ಯಾವಾಗಲೂ ಸರಿಯಾಗಿ ಕಾರ್ಯಾಂತ್ಯ ಮಾಡಲು ಮರೆಯದಿರಿ.	ಗುಪ್ತಪದ ಮತ್ತು ಗೌಪ್ಯ ಮಾಹಿತಿ ಬಳಸುವಾಗಿ ಅವಾಸ್ತವ ಕೀಲಿ ಮಣೆಯನ್ನು ಬಳಕೆ ಮಾಡಿ.	ಸಾರ್ವಜನಿಕ ಸ್ಥಳಗಳಲ್ಲಿ ಸಿಗುವ ಉಚಿತ ವೈಫೈ ಸಂಪರ್ಕ ಪಡೆಯ ಬೇಡಿ. ಸುರಕ್ಷತೆಗಾಗಿ ವಿಪಿಎನ್ ಬಳಸಿರಿ.

ವ್ಯಕ್ತಿಚಿತ್ರ ಅತಿಕ್ರಮಣ(ಹ್ಯಾಕಿಂಗ್)

ಸಂಭವನೀಯ ಹಿಂಬಾಲಕನು ಅವಕಾಶವನ್ನು ಉಪಯೋಗಿಸಿಕೊಂಡು ನಿಮ್ಮ ಇ–ಮೇಲ್ ಅಥವಾ ಸಾಮಾಜಿಕ ಜಾಲತಾಣದ ವ್ಯಕ್ತಿಚಿತ್ರಣವನ್ನು ಅದರ ಗುಪ್ತಪದ ಬದಲಾವಣೆ ಮಾಡುವುದರ ಮೂಲಕ ಅತಿಕ್ರಮಿಸಿ ಕೈವಶ ಮಾಡಿಕೊಳ್ಳುವದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ ಕಾಯ್ದೆ:

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಕಲಂ 66ಸಿ: ಗುರುತಿನ ಕಳ್ಳತನದ ಬಗ್ಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ. ಬೇರೊಬ್ಬರಂತೆ ನಟಿಸಲು ಮತ್ತು ವಂಚನೆ ಮಾಡಲು ಅಥವಾ ಇತರರನ್ನು ವಂಚಿಸಲು ಎಸ್‌ಎಂಎಸ್ ವಂಚನೆಯನ್ನು ಬಳಸಿದರೆ, ಅದನ್ನು ಈ ಕಲಂ ಅಡಿಯಲ್ಲಿ ಒಳಗೊಳ್ಳಬಹುದು.

ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ

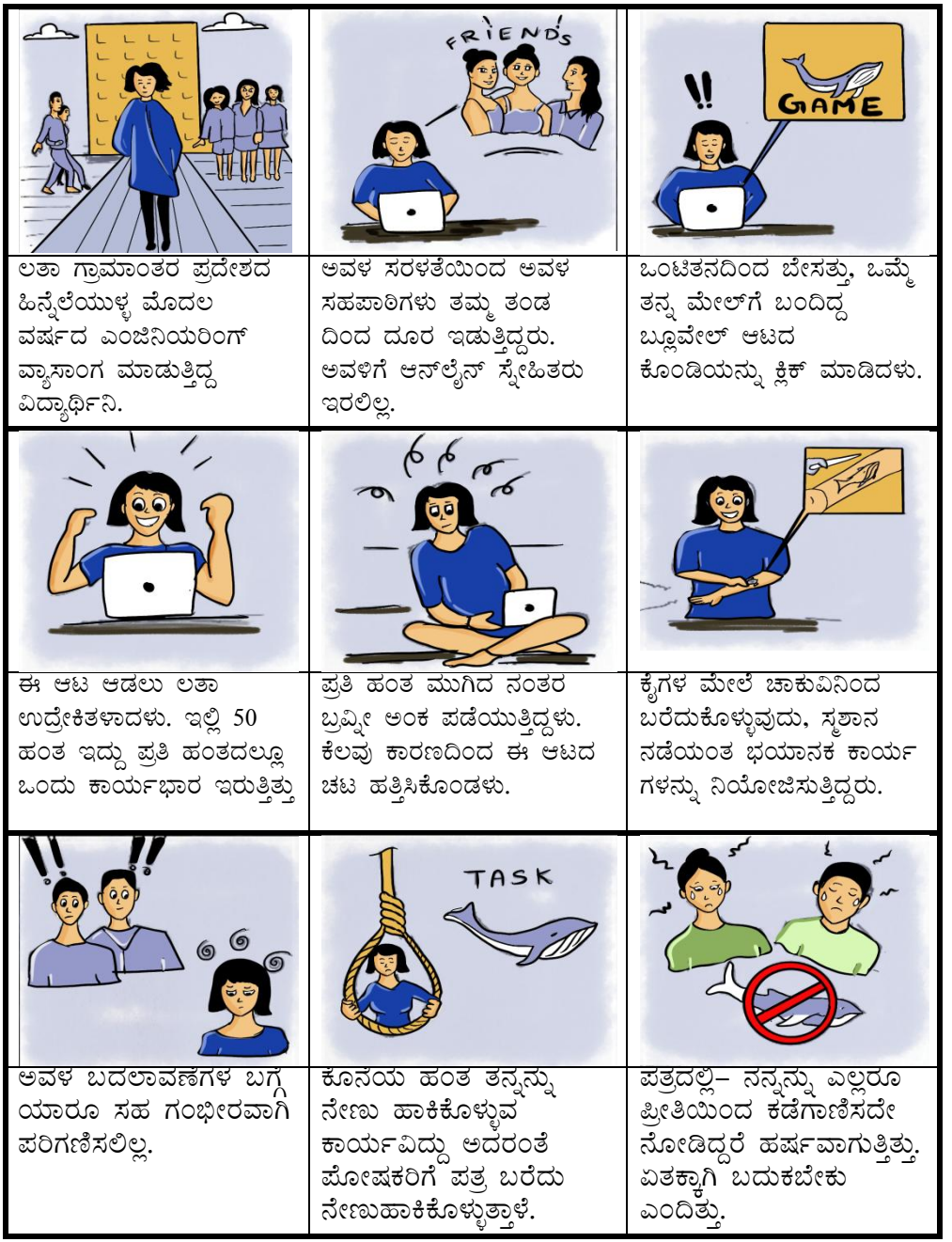
ಕಲಂ 379/ಬಿಎನ್‌ಎಸ್ 303 ಮತ್ತು 380/ಬಿಎನ್‌ಎಸ್ 305 ಐಪಿಸಿ: ಡೇಟಾ ಅಥವಾ ರುಜುವಾತುಗಳ ಕಳ್ಳತನ.

ಕಲಂ 463/ಬಿಎನ್‌ಎಸ್ 336, 464/ಬಿಎನ್‌ಎಸ್ 335, 468/ಬಿಎನ್‌ಎಸ್ 336 ಐಪಿಸಿ: ವಂಚನೆಗಾಗಿ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ದಾಖಲೆಗಳ ಖೋಟಾ/ಫೋರ್ಜರಿ.

ಕಲಂ 507/ಬಿಎನ್‌ಎಸ್ 351 ಐಪಿಸಿ: ಹ್ಯಾಕಿಂಗ್ ಮೂಲಕ ಅಪರಾಧಿ ಬೆದರಿಕೆ.

ಪ್ರತಿ ವಸ್ತುವಿಗೂ ಬೆಲೆ ಇದೆ, ರಿಚಾರ್ಜ್ ಪ್ರಕರಣದಲ್ಲಾದರೆ, ಯಾವುದೂ ಉಚಿತವಿಲ್ಲ

ಆನ್‌ಲೈನ್ ಆಟಗಳು



ಲತಾ ಗ್ರಾಮಾಂತರ ಪ್ರದೇಶದ ಹಿನ್ನೆಲೆಯುಳ್ಳ ಮೊದಲ ವರ್ಷದ ಎಂಜಿನಿಯರಿಂಗ್ ವ್ಯಾಸಾಂಗ ಮಾಡುತ್ತಿದ್ದ ವಿದ್ಯಾರ್ಥಿನಿ.

ಅವಳ ಸರಳತೆಯಿಂದ ಅವಳ ಸಹಪಾಠಿಗಳು ತಮ್ಮ ತಂಡದಿಂದ ದೂರ ಇಡುತ್ತಿದ್ದರು. ಅವಳಿಗೆ ಆನ್‌ಲೈನ್ ಸ್ನೇಹಿತರು ಇರಲಿಲ್ಲ.

ಒಂಟಿತನದಿಂದ ಬೇಸತ್ತು, ಒಮ್ಮೆ ತನ್ನ ಮೇಲ್‌ಗೆ ಬಂದಿದ್ದ ಬ್ಲೂವೇಲ್ ಆಟದ ಕೊಂಡಿಯನ್ನು ಕ್ಲಿಕ್ ಮಾಡಿದಳು.

ಈ ಆಟ ಆಡಲು ಲತಾ ಉದ್ರೇಕಿತಳಾದಳು. ಇಲ್ಲಿ 50 ಹಂತ ಇದ್ದು ಪ್ರತಿ ಹಂತದಲ್ಲೂ ಒಂದು ಕಾರ್ಯಭಾರ ಇರುತ್ತಿತ್ತು

ಪ್ರತಿ ಹಂತ ಮುಗಿದ ನಂತರ ಬ್ರವ್ನೀ ಅಂಕ ಪಡೆಯುತ್ತಿದ್ದಳು. ಕೆಲವು ಕಾರಣದಿಂದ ಈ ಆಟದ ಚಟ ಹತ್ತಿಸಿಕೊಂಡಳು.

ಕೈಗಳ ಮೇಲೆ ಚಾಕುವಿನಿಂದ ಬರೆದುಕೊಳ್ಳುವುದು, ಸ್ಮಶಾನ ನಡೆಯಂತ ಭಯಾನಕ ಕಾರ್ಯಗಳನ್ನು ನಿಯೋಜಿಸುತ್ತಿದ್ದರು.

ಅವಳ ಬದಲಾವಣೆಗಳ ಬಗ್ಗೆ ಯಾರೂ ಸಹ ಗಂಭೀರವಾಗಿ ಪರಿಗಣಿಸಲಿಲ್ಲ.

ಕೊನೆಯ ಹಂತ ತನ್ನನ್ನು ನೇಣು ಹಾಕಿಕೊಳ್ಳುವ ಕಾರ್ಯವಿದ್ದು ಅದರಂತೆ ಪೋಷಕರಿಗೆ ಪತ್ರ ಬರೆದು ನೇಣುಹಾಕಿಕೊಳ್ಳುತ್ತಾಳೆ.

ಪತ್ರದಲ್ಲಿ– ನನ್ನನ್ನು ಎಲ್ಲರೂ ಪ್ರೀತಿಯಿಂದ ಕಡೆಗಾಣಿಸದೇ ನೋಡಿದ್ದರೆ ಹರ್ಷವಾಗುತ್ತಿತ್ತು. ಏತಕ್ಕಾಗಿ ಬದುಕಬೇಕು ಎಂದಿತ್ತು.

ಒಂಟಿತನ, ಕಡಿಮೆ ಸ್ವಾಭಿಮಾನ ಮತ್ತು ವೈದ್ಯಕೀಯ ಖಿನ್ನತೆಗೆ ಒಳಗಾಗಿರುವ ಹುಡುಗಿಯರು ಇಂತಹ ಅಪಾಯಕಾರಿ ಆನ್‌ಲೈನ್ ಆಟಗಳಿಗೆ ಬಲಿಯಾಗಬಹುದು ಮತ್ತು ಇದನ್ನು ಅವರು ಹವ್ಯಾಸವನ್ನಾಗಿ ಮಾಡಿಕೊಂಡು ಇನ್ನಷ್ಟು ಇದರಿಂದ ಹಾನಿಗೊಳಗಾಗಬಹುದು.ಇಂತಹದರಲ್ಲಿ ಕೆಲವು ಕುಖ್ಯಾತ ಬ್ಲ್ಯೂವೇಲ್ ಸವಾಲಿನಂತವು ಬಲಿಪಶುವಿನ ಜೀವ ತೆಗೆದುಕೊಳ್ಳುವುದರಲ್ಲೂ ಯಶಸ್ವಿಯಾಗುತ್ತದೆ.ಇದೊಂದು ವೈಯಕ್ತಿಕವಗಿಯೂ ಸುತ್ತಮುತ್ತಲಿನ ಇತರರಿಗೆ ಸಾಮಾಜಿಕ ಸವಾಲಾಗಿಯೂ ಪರಿಣಮಿಸಿದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮ.ತ.ಕಾಯ್ದೆ

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಎ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಬಿ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವಿನಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿ ವಿದ್ಯುನ್ಮಾನರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಾಯ್ದೆಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 79: ಕೆಲವು ಸಂದರ್ಭಗಳಲ್ಲಿ ಮಧ್ಯವರ್ತಿಗಳನ್ನು ಹೊಣೆಗಾರರನ್ನಾಗಿಸುವುದರಿಂದ ವಿನಾಯಿತಿ

ಐಪಿಸಿ ಕಲಂಗಳು, ಜಾಲತಾಣ

ಐಪಿಸಿ ಕಲಂ 299/ಬಿಎನ್‌ಎಸ್ 100– ದಂಡನೀಯ ನರಹತ್ಯೆ

ಐಪಿಸಿ ಕಲಂ 305/ಬಿಎನ್‌ಎಸ್ 107– ಮಕ್ಕಳ ಅಥವಾ ಮಾನಸಿಕ ದೌರ್ಬಲ್ಯ ವ್ಯಕ್ತಿಯ ಆತ್ಮಹತ್ಯೆಗೆ ಪ್ರಚೋದನೆ

ಐಪಿಸಿ ಕಲಂ 306/ಬಿಎನ್‌ಎಸ್ 108– ಆತ್ಮಹತ್ಯೆಗೆ ಪ್ರಚೋದನೆ

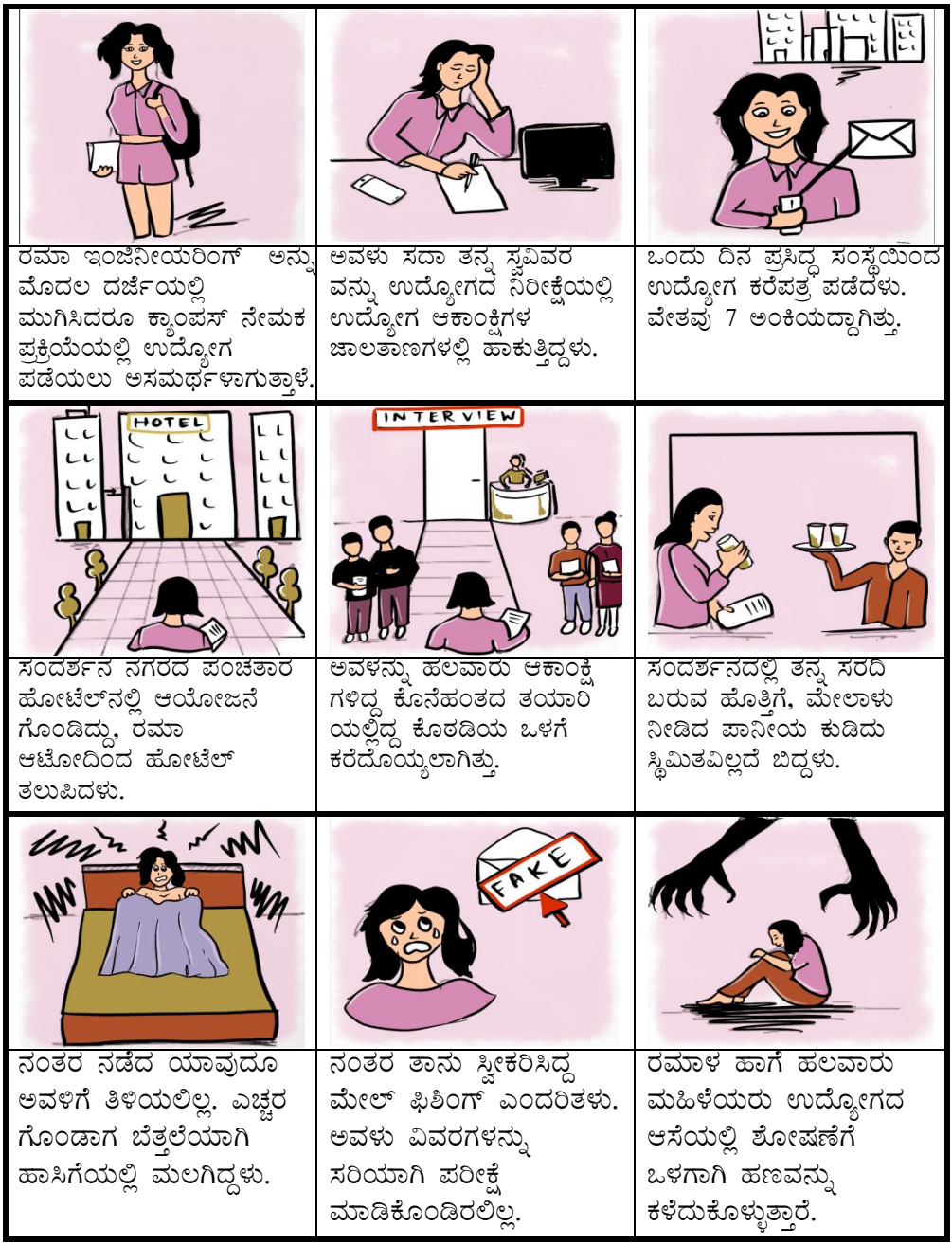
ಐಪಿಸಿ ಕಲಂ 321/ಬಿಎನ್‌ಎಸ್ 115– ಸ್ವಯಂಪ್ರೇರಣೆಯಿಂದ ನೋವುಂಟುಮಾಡಿಕೊಳ್ಳುವುದು

ಐಪಿಸಿ ಕಲಂ 335/ಬಿಎನ್‌ಎಸ್ 122– ಸ್ವಯಂಪ್ರೇರಣೆಯ ಪ್ರಚೋದನೆಯ ಮೇರೆಗೆ ತೀವ್ರವಾದ ನೋವುಂಟುಮಾಡಿಕೊಳ್ಳುವುದು

ಐಪಿಸಿ ಕಲಂ 336/ಬಿಎನ್‌ಎಸ್ 125– ಜೀವಕ್ಕೆ ಅಥವಾ ಇತರೆ ವ್ಯಕ್ತಿಗಳ ಸುರಕ್ಷತೆಗೆ ಅಪಾಯವನ್ನು ಉಂಟುಮಾಡುವ ಕೃತ್ಯ

ನಿಮ್ಮ ಮಗುವಿನ ಭವಿಷ್ಯದ ಮೇಲೆ ಕೆಟ್ಟ ಪರಿಣಾಮವನ್ನು ಬೀರುವುದರಿಂದ, ಅವರ ಗಣಕಯಂತ್ರ ಉಪಕರಣಗಳ ಚಟುವಟಿಕೆಗಳನ್ನು ಗಮನಿಸುತ್ತಿರಿ (ಲ್ಯಾಪ್‌ಟಾಪ್, ಐಪ್ಯಾಡ್, ಮೊಬೈಲ್ ಫೋನ್, ಟ್ಯಾಬ್, ಡೆಸ್ಕ್‌ಟಾಪ್, ಇತ್ಯಾದಿ).

ಉದ್ಯೋಗ ಕರೆ ಪತ್ರ



ರಮಾ ಇಂಜಿನೀಯರಿಂಗ್ ಅನ್ನು ಮೊದಲ ದರ್ಜೆಯಲ್ಲಿ ಮುಗಿಸಿದರೂ ಕ್ಯಾಂಪಸ್ ನೇಮಕ ಪ್ರಕ್ರಿಯೆಯಲ್ಲಿ ಉದ್ಯೋಗ ಪಡೆಯಲು ಅಸಮರ್ಥಳಾಗುತ್ತಾಳೆ.	ಅವಳು ಸದಾ ತನ್ನ ಸ್ವವಿವರ ವನ್ನು ಉದ್ಯೋಗದ ನಿರೀಕ್ಷೆಯಲ್ಲಿ ಉದ್ಯೋಗ ಆಕಾಂಕ್ಷಿಗಳ ಜಾಲತಾಣಗಳಲ್ಲಿ ಹಾಕುತ್ತಿದ್ದಳು.	ಒಂದು ದಿನ ಪ್ರಸಿದ್ಧ ಸಂಸ್ಥೆಯಿಂದ ಉದ್ಯೋಗ ಕರೆಪತ್ರ ಪಡೆದಳು. ವೇತವು 7 ಅಂಕಿಯದ್ದಾಗಿತ್ತು.
ಸಂದರ್ಶನ ನಗರದ ಪಂಚತಾರ ಹೋಟೆಲ್‌ನಲ್ಲಿ ಆಯೋಜನೆ ಗೊಂಡಿದ್ದು, ರಮಾ ಆಟೋದಿಂದ ಹೋಟೆಲ್ ತಲುಪಿದಳು.	ಅವಳನ್ನು ಹಲವಾರು ಆಕಾಂಕ್ಷಿ ಗಳಿದ್ದ ಕೊನೆಹಂತದ ತಯಾರಿ ಯಲ್ಲಿದ್ದ ಕೊಠಡಿಯ ಒಳಗೆ ಕರೆದೊಯ್ಯಲಾಗಿತ್ತು.	ಸಂದರ್ಶನದಲ್ಲಿ ತನ್ನ ಸರದಿ ಬರುವ ಹೊತ್ತಿಗೆ, ಮೇಲಾಳು ನೀಡಿದ ಪಾನೀಯ ಕುಡಿದು ಸ್ಥಿಮಿತವಿಲ್ಲದೆ ಬಿದ್ದಳು.
ನಂತರ ನಡೆದ ಯಾವುದೂ ಅವಳಿಗೆ ತಿಳಿಯಲಿಲ್ಲ. ಎಚ್ಚರ ಗೊಂಡಾಗ ಬೆತ್ತಲೆಯಾಗಿ ಹಾಸಿಗೆಯಲ್ಲಿ ಮಲಗಿದ್ದಳು.	ನಂತರ ತಾನು ಸ್ವೀಕರಿಸಿದ್ದ ಮೇಲ್ ಫಿಶಿಂಗ್ ಎಂದರಿತಳು. ಅವಳು ವಿವರಗಳನ್ನು ಸರಿಯಾಗಿ ಪರೀಕ್ಷೆ ಮಾಡಿಕೊಂಡಿರಲಿಲ್ಲ.	ರಮಾಳ ಹಾಗೆ ಹಲವಾರು ಮಹಿಳೆಯರು ಉದ್ಯೋಗದ ಆಸೆಯಲ್ಲಿ ಶೋಷಣೆಗೆ ಒಳಗಾಗಿ ಹಣವನ್ನು ಕಳೆದುಕೊಳ್ಳುತ್ತಾರೆ.

ಉದ್ಯೋಗಗಳನ್ನು ನೀಡುವಂತಹ ಜಾಲತಾಣಗಳ ನಿಖರತೆ ಮತ್ತು ನೈಜತೆಯನ್ನು ಪರಿಶೀಲಿಸಬೇಕಾಗುತ್ತದೆ. ಇ–ಮೇಲ್‌ಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸುವ ಮೊದಲು ಮತ್ತು ಅವುಗಳ ಸೂಚನೆಗೆ ಸ್ಪಂದಿಸುವ ಮೊದಲು, ಎರಡು ಬಾರಿ ಪರಿಶೀಲಿಸಬೇಕು ಮತ್ತು ಪರೀಕ್ಷಿಸಬೇಕು, ವಿಶೇಷವಾಗಿ ಒಬ್ಬರನ್ನು ವೈಯಕ್ತಿಕವಾಗಿ ಭೇಟಿ ಆಗುವಂತೆ ಆಹ್ವಾನಿಸಿದಾಗ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ನಕಲಿ ಖಾತೆ / ಗುರುತಿನ ಚೀಟಿ:

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮೋಸಕ್ಕಾಗಿ ಪ್ರತಿರೂಪಣ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಐಪಿಸಿ ಕಲಂ 465/ಬಿಎನ್‌ಎಸ್ 336– ಸುಳ್ಳು ಸ್ಪಷ್ಟನೆಗೆ ದಂಡನೆ(ವ್ಯಾಖ್ಯಾನದ ಕಲಂ)

ಐಪಿಸಿ ಕಲಂ 468/ಬಿಎನ್‌ಎಸ್ 336– ಮೋಸಗೊಳಿಸಲು ನಕಲುರುಜು

ಐಪಿಸಿ ಕಲಂ 471/ಬಿಎನ್‌ಎಸ್ 340– ನಕಲುರುಜು ದಾಖಲೆಯನ್ನು ನೈಜವೆಂದು ಉಪಯೋಗಿಸುವುದು

ಐಪಿಸಿ ಕಲಂ 474/ಬಿಎನ್‌ಎಸ್ 339– ನಕಲಿ ದಾಖಲೆಯ ಸ್ವಾಧೀನ

ಐಪಿಸಿ ಕಲಂ 120ಬಿ/ಬಿಎನ್‌ಎಸ್ 61 – ಅಪರಾಧದ ಪಿತೂರಿಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 34/ಬಿಎನ್‌ಎಸ್ 3(5)– ಸಾಮಾನ್ಯ ಉದ್ದೇಶದಿಂದ ಮುಂದುವರೆಯಲು ಹಲವಾರು ವ್ಯಕ್ತಿಗಳಿಂದ ಮಾಡಿದ ಕೃತ್ಯಗಳು

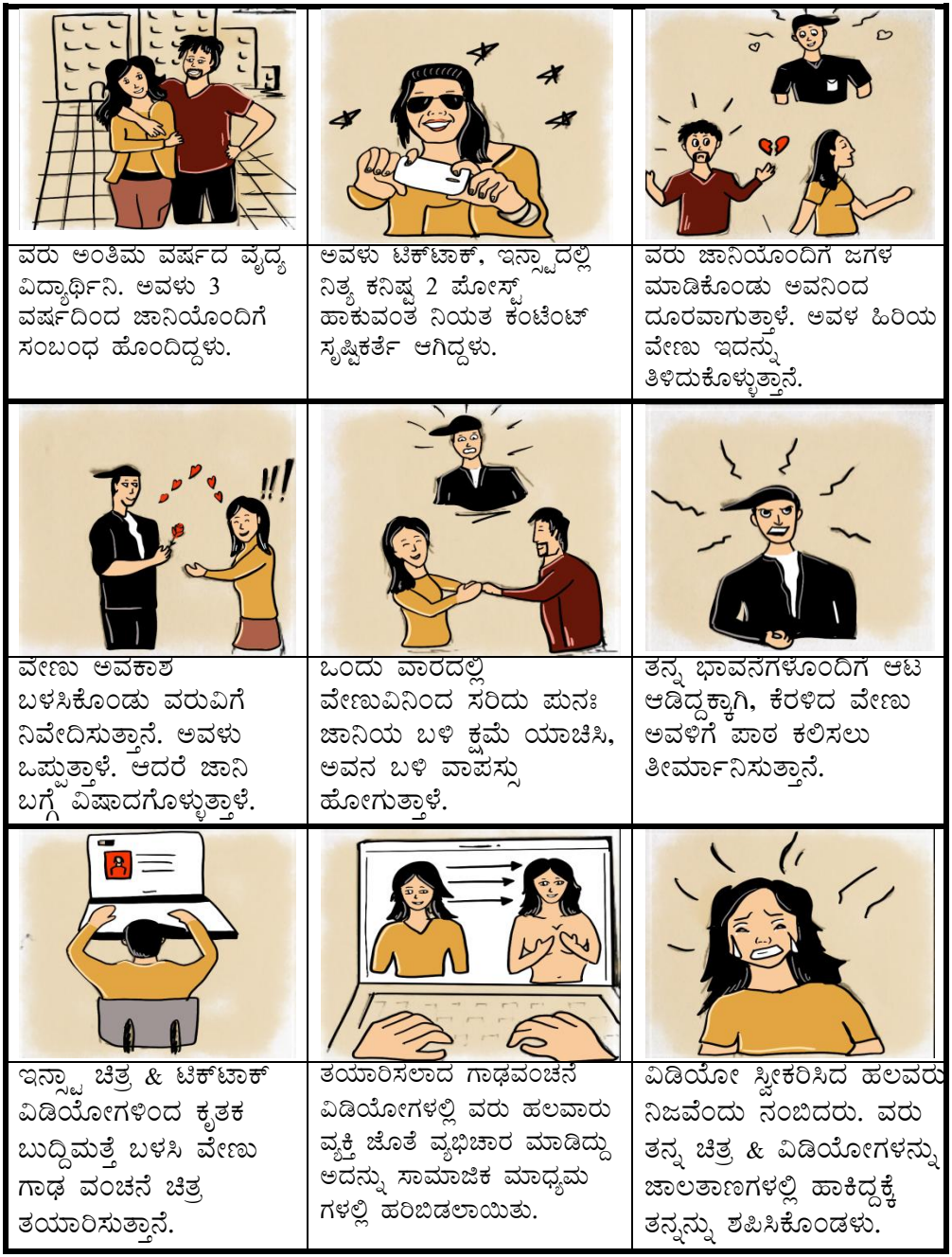
ಅಪರಾಧಕ್ಕೆ ದುಷ್ಪ್ರೇರಣೆ:

ಎ. ಅಪರಾಧ ಸ್ಥಳದಲ್ಲಿ: ಐಪಿಸಿ ಕಲಂ 114/ಬಿಎನ್‌ಎಸ್ 54– ದುಷ್ಪ್ರೇರಕ ಅಪರಾಧ ನಡೆದಾಗ ಹಾಜರಿ

ಬಿ.ದೂರದಿಂದ:ಐಪಿಸಿ ಕಲಂ109/ಬಿಎನ್‌ಎಸ್ 49– ದುಷ್ಪ್ರೇರಣೆಗಾಗಿ ಶಿಕ್ಷೆ

ಈ ತಕ್ಷಣ ಅಥವಾ ಮುಂದೆ ಇಂತಹ ನಕಲಿ ಉದ್ಯೋಗ ಕರೆಪತ್ರವನ್ನು ನೀವು ಸಹ ಪಡೆಯುತ್ತೀರಿ

ತೀಕ್ಷ್ಣ ವಂಚನೆ (ಡೀಪ್ ಫೇಕ್)



ವರು ಅಂತಿಮ ವರ್ಷದ ವೈದ್ಯ ವಿದ್ಯಾರ್ಥಿನಿ. ಅವಳು 3 ವರ್ಷದಿಂದ ಜಾನಿಯೊಂದಿಗೆ ಸಂಬಂಧ ಹೊಂದಿದ್ದಳು.	ಅವಳು ಟಿಕ್‌ಟಾಕ್, ಇನ್ಸ್ಟಾದಲ್ಲಿ ನಿತ್ಯ ಕನಿಷ್ಟ 2 ಪೋಸ್ಟ್ ಹಾಕುವಂತ ನಿಯತ ಕಂಟೆಂಟ್ ಸೃಷ್ಟಿಕರ್ತೆ ಆಗಿದ್ದಳು.	ವರು ಜಾನಿಯೊಂದಿಗೆ ಜಗಳ ಮಾಡಿಕೊಂಡು ಅವನಿಂದ ದೂರವಾಗುತ್ತಾಳೆ. ಅವಳ ಹಿರಿಯ ವೇಣು ಇದನ್ನು ತಿಳಿದುಕೊಳ್ಳುತ್ತಾನೆ.
ವೇಣು ಅವಕಾಶ ಬಳಸಿಕೊಂಡು ವರುವಿಗೆ ನಿವೇದಿಸುತ್ತಾನೆ. ಅವಳು ಒಪ್ಪುತ್ತಾಳೆ. ಆದರೆ ಜಾನಿ ಬಗ್ಗೆ ವಿಷಾದಗೊಳ್ಳುತ್ತಾಳೆ.	ಒಂದು ವಾರದಲ್ಲಿ ವೇಣುವಿನಿಂದ ಸರಿದು ಪುನಃ ಜಾನಿಯ ಬಳಿ ಕ್ಷಮೆ ಯಾಚಿಸಿ, ಅವನ ಬಳಿ ವಾಪಸ್ಸು ಹೋಗುತ್ತಾಳೆ.	ತನ್ನ ಭಾವನೆಗಳೊಂದಿಗೆ ಆಟ ಆಡಿದ್ದಕ್ಕಾಗಿ, ಕೆರಳಿದ ವೇಣು ಅವಳಿಗೆ ಪಾಠ ಕಲಿಸಲು ತೀರ್ಮಾನಿಸುತ್ತಾನೆ.
ಇನ್ಸ್ಟಾ ಚಿತ್ರ & ಟಿಕ್‌ಟಾಕ್ ವಿಡಿಯೋಗಳಿಂದ ಕೃತಕ ಬುದ್ಧಿಮತ್ತೆ ಬಳಸಿ ವೇಣು ಗಾಢ ವಂಚನೆ ಚಿತ್ರ ತಯಾರಿಸುತ್ತಾನೆ.	ತಯಾರಿಸಲಾದ ಗಾಢವಂಚನೆ ವಿಡಿಯೋಗಳಲ್ಲಿ ವರು ಹಲವಾರು ವ್ಯಕ್ತಿ ಜೊತೆ ವ್ಯಭಿಚಾರ ಮಾಡಿದ್ದು ಅದನ್ನು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಗಳಲ್ಲಿ ಹರಿಬಿಡಲಾಯಿತು.	ವಿಡಿಯೋ ಸ್ವೀಕರಿಸಿದ ಹಲವರು ನಿಜವೆಂದು ನಂಬಿದರು. ವರು ತನ್ನ ಚಿತ್ರ & ವಿಡಿಯೋಗಳನ್ನು ಜಾಲತಾಣಗಳಲ್ಲಿ ಹಾಕಿದ್ದಕ್ಕೆ ತನ್ನನ್ನು ಶಪಿಸಿಕೊಂಡಳು.

ತೀಕ್ಷ್ಣ ವಂಚನೆ (ಡೀಪ್ ಫೇಕ್)

ಡೀಪ್ ಫೇಕ್ ಎನ್ನುವುದು ಹೊಸ ಚಿತ್ರಗಳು ಮತ್ತು ವಿಡಿಯೋಗಳನ್ನು ಮೂಲ ಚಿತ್ರಗಳು ಅಥವಾ ವಿಡಿಯೋಗಳಲ್ಲಿ , ಸಂಯೋಜಿಸಲು ಮತ್ತು ಅಧ್ಯಾರೋಪಿಸಲು ಬಳಸುವ ತಂತ್ರವಾಗಿದೆ. ಇದನ್ನು ಮೂಲ ವಿಡಿಯೋಗಳಿಗೆ ಬೇರೆ ಮುಖ ಹಾಗೂ ಧ್ವನಿಗಳನ್ನು ಅಧ್ಯಾರೋಪಿಸುವೆಡೆ ಬಳಸಲಾಗುತ್ತದೆ.ಎಷ್ಟರ ಮಟ್ಟಿಗೆ ಎಂದರೆ ವೀಕ್ಷಕರಿಗೆ ಅಥವಾ ಕೇಳುಗರಿಗೆ ಅಸಲಿ ಮತ್ತು ನಕಲಿಗಳ ನಡುವೆ ವ್ಯತ್ಯಾಸ ತಿಳಿಯಲಾಗದೇ ಅದರ ಸತ್ಯಾಸತ್ಯತೆಯನ್ನು ಪ್ರತ್ಯೇಕಿಸಲು ಅಥವಾ ಅನುಮಾನಿಸಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ನಕಲಿ ಖಾತೆ / ಗುರುತಿನ ಚೀಟಿ: ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮೋಸಕ್ಕಾಗಿ ಪ್ರತಿರೂಪಣ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 43ಎ ಮತ್ತು ಕಲಂ 72ಎ: ಈ ಕಲಂಗಳು ಡೇಟಾ ಮತ್ತು ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆಯನ್ನು ರಕ್ಷಿಸುವಲ್ಲಿ ವಿಫಲವಾದರೆ ಪರಿಹಾರವನ್ನು ವ್ಯವಹರಿಸುತ್ತವೆ.

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್ಎಸ್ 319(2)–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318(4)– ಮೋಸ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಎ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಬಿ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿರುವ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆಮತ್ತು ಪೋಕ್ಸೋ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 354ಎ/ಬಿಎನ್ಎಸ್ 75– ಲೈಂಗಿಕ ಕಿರುಕುಳ ಮತ್ತು ಕಿರುಕುಳಕ್ಕಾಗಿ ಶಿಕ್ಷೆ, **ಕಲಂ–465/ಬಿಎನ್ಎಸ್** 336– ಸುಳ್ಳು ದಾಖಲೆಗಳ ಸೃಷ್ಟಿ(ನಕಲುರುಜು), **ಕಲಂ 499/ಬಿಎನ್ಎಸ್** 356–ಮಾನಹಾನಿ, **ಕಲಂ 500/ಬಿಎನ್ಎಸ್** 356–ಮಾನಹಾನಿಗಾಗಿ ಶಿಕ್ಷೆ, **ಕಲಂ 507/ಬಿಎನ್ಎಸ್** 351– ಅನಾಮಧೇಯ ಸಂವಹನ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ, **ಕಲಂ 509/ಬಿಎನ್ಎಸ್** 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನ

ಹಿಂಬಾಲಿಕೆ: ಐಪಿಸಿ ಕಲಂ 354ಡಿ/ಬಿಎನ್ಎಸ್ 78– ಆಫ್‌ಲೈನ್ ಹಿಂಬಾಲಿಕೆ, **ಐಪಿಸಿ ಕಲಂ 354ಡಿ/ಬಿಎನ್ಎಸ್** 78– ಆನ್‌ಲೈನ್ ಹಿಂಬಾಲಿಕೆ

ಐಪಿಸಿ ಕಲಂ 120ಬಿ/ಬಿಎನ್ಎಸ್ 61– ಅಪರಾಧದ ಸಂಚಿಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 34/ಬಿಎನ್ಎಸ್ 3(5)– ಸಾಮಾನ್ಯ ಉದ್ದೇಶದಿಂದ ಹಲವಾರು ವ್ಯಕ್ತಿಗಳಿಂದ ಮಾಡಿದ ಕೃತ್ಯಗಳು

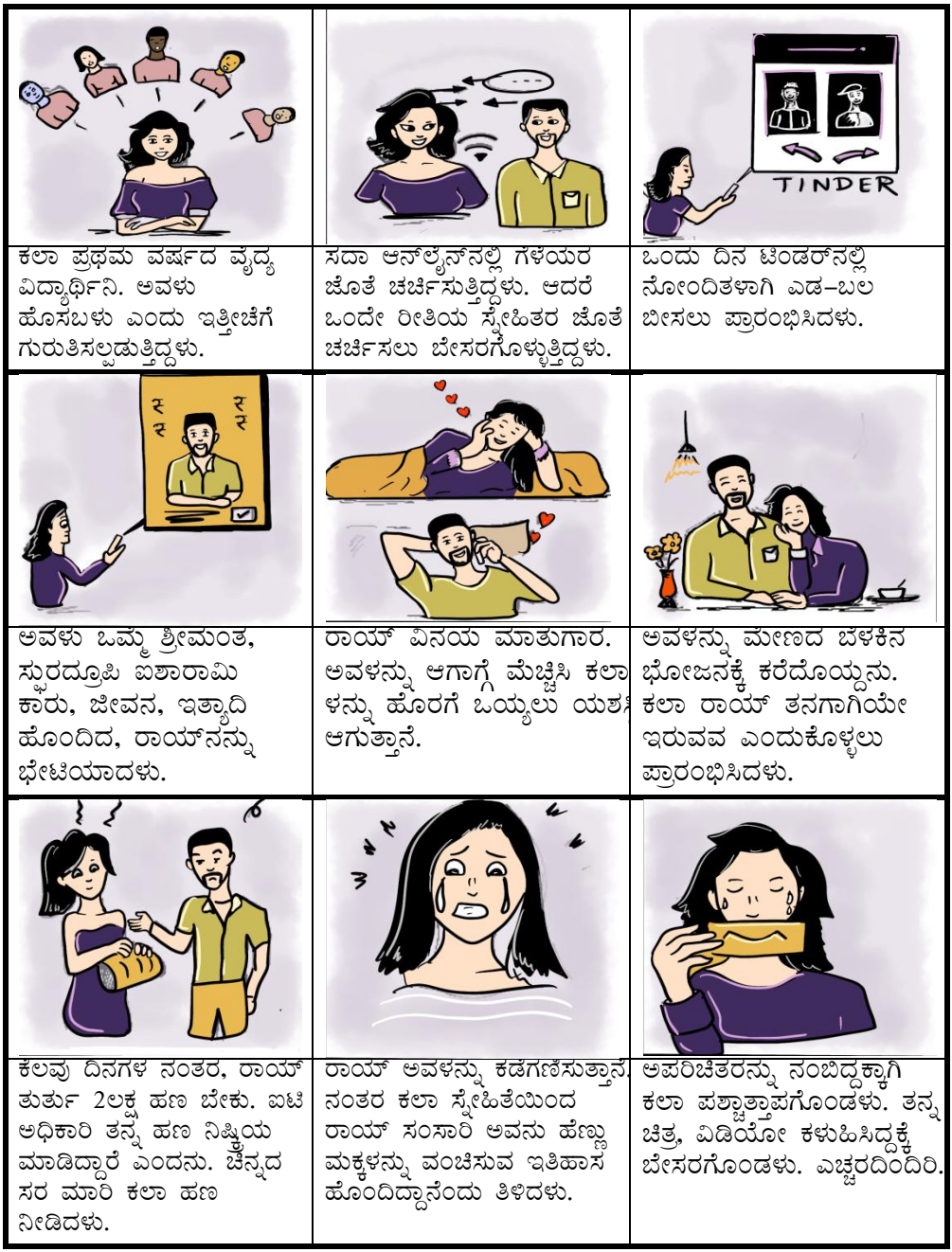
ಅಪರಾಧಕ್ಕೆ ದುಷ್ಪ್ರೇರಣೆ:

ಎ. ಅಪರಾಧ ಸ್ಥಳದಲ್ಲಿ: ಐಪಿಸಿ ಕಲಂ 114/ಬಿಎನ್ಎಸ್ 54– ದುಷ್ಪ್ರೇರಕ ಅಪರಾಧ ನಡೆದಾಗ ಹಾಜರಿ

ಬಿ.ದೂರದಿಂದ:ಐಪಿಸಿ ಕಲಂ 109/ಬಿಎನ್ಎಸ್ 49– ದುಷ್ಪ್ರೇರಣೆಗಾಗಿ ಶಿಕ್ಷೆ

ಡೀಪ್ ಫೇಕ್ ಸುಲಭವಾಗಿ ಪತ್ತೆಹಚ್ಚಲು ಸಾಧ್ಯವಿರುವುದಿಲ್ಲ. ಅದಕ್ಕಾಗಿಯೇ ಅದರಲ್ಲಿ ಹೆಚ್ಚು ಆಸಕ್ತಿ

ಪ್ರಣಯದ ಭೇಟಿ ಜಾಲತಾಣ (ಡೇಟಿಂಗ್)



ಕಲಾ ಪ್ರಥಮ ವರ್ಷದ ವೈದ್ಯ ವಿದ್ಯಾರ್ಥಿನಿ. ಅವಳು ಹೊಸಬಳು ಎಂದು ಇತ್ತೀಚೆಗೆ ಗುರುತಿಸಲ್ಪಡುತ್ತಿದ್ದಳು.

ಸದಾ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಗೆಳೆಯರ ಜೊತೆ ಚರ್ಚಿಸುತ್ತಿದ್ದಳು. ಆದರೆ ಒಂದೇ ರೀತಿಯ ಸ್ನೇಹಿತರ ಜೊತೆ ಚರ್ಚಿಸಲು ಬೇಸರಗೊಳ್ಳುತ್ತಿದ್ದಳು.

ಒಂದು ದಿನ ಟಿಂಡರ್‌ನಲ್ಲಿ ನೋಂದಿತಳಾಗಿ ಎಡ–ಬಲ ಬೀಸಲು ಪ್ರಾರಂಭಿಸಿದಳು.

ಅವಳು ಒಮ್ಮೆ ಶ್ರೀಮಂತ, ಸ್ಫುರದ್ರೂಪಿ ಐಶಾರಾಮಿ ಕಾರು, ಜೀವನ, ಇತ್ಯಾದಿ ಹೊಂದಿದ, ರಾಯ್‌ನನ್ನು ಭೇಟಿಯಾದಳು.

ರಾಯ್ ವಿನಯ ಮಾತುಗಾರ. ಅವಳನ್ನು ಆಗಾಗ್ಗೆ ಮೆಚ್ಚಿಸಿ ಕಲಾಳನ್ನು ಹೊರಗೆ ಒಯ್ಯಲು ಯಶಸ್ಸಿ ಆಗುತ್ತಾನೆ.

ಅವಳನ್ನು ಮೀಣದ ಬೆಳಕಿನ ಭೋಜನಕ್ಕೆ ಕರೆದೊಯ್ದನು. ಕಲಾ ರಾಯ್ ತನಗಾಗಿಯೇ ಇರುವವ ಎಂದುಕೊಳ್ಳಲು ಪ್ರಾರಂಭಿಸಿದಳು.

ಕೆಲವು ದಿನಗಳ ನಂತರ, ರಾಯ್ ತುರ್ತು 2ಲಕ್ಷ ಹಣ ಬೇಕು. ಐಟಿ ಅಧಿಕಾರಿ ತನ್ನ ಹಣ ನಿಷ್ಕ್ರಿಯ ಮಾಡಿದ್ದಾರೆ ಎಂದನು. ಚೆನ್ನದ ಸರ ಮಾರಿ ಕಲಾ ಹಣ ನೀಡಿದಳು.

ರಾಯ್ ಅವಳನ್ನು ಕಡೆಗಣಿಸುತ್ತಾನೆ. ನಂತರ ಕಲಾ ಸ್ನೇಹಿತೆಯಿಂದ ರಾಯ್ ಸಂಸಾರಿ ಅವನು ಹೆಣ್ಣು ಮಕ್ಕಳನ್ನು ವಂಚಿಸುವ ಇತಿಹಾಸ ಹೊಂದಿದ್ದಾನೆಂದು ತಿಳಿದಳು.

ಅಪರಿಚಿತರನ್ನು ನಂಬಿದ್ದಕ್ಕಾಗಿ ಕಲಾ ಪಶ್ಚಾತ್ತಾಪಗೊಂಡಳು. ತನ್ನ ಚಿತ್ರ, ವಿಡಿಯೋ ಕಳುಹಿಸಿದ್ದಕ್ಕೆ ಬೇಸರಗೊಂಡಳು. ಎಚ್ಚರದಿಂದಿರಿ.

ಡೇಟಿಂಗ್ ಜಾಲತಾಣಗಳಲ್ಲಿ ಸೌಮ್ಯವಾಗಿ ಚಾತುರ್ಯದಿಂದ ಮಾತನಾಡಬಲ್ಲ ವ್ಯಕ್ತಿಗಳು ಹೆಣ್ಣುಮಕ್ಕಳನ್ನು ಭಾವನಾತ್ಮಕವಾಗಿ ಕುಶಲತೆಯಿಂದ ನಿರ್ವಹಿಸಬಹುದು. ಅಂತಹ ಜಾಲತಾಣಗಳಲ್ಲಿ ಸಂಭವನೀಯ ಡೇಟಿಂಗ್ ಸಹಚರರಿಗೆ ಅವರು ಕಳುಹಿಸುವ ಯಾವುದೇ ಖಾಸಗಿ ಚಿತ್ರಗಳು ಅಥವಾ ಪಠ್ಯಗಳು ನಿರ್ಲಜ್ಜ ವ್ಯಕ್ತಿಗಳಿಗೆ ಮುಖ್ಯ ಅಂಶವಾಗಿ ನಂತರ ಅವರನ್ನು ಬೆದರಿಕೆಯಲ್ಲಿಡಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಐಪಿಸಿ ಕಲಂ 354ಎ/ಬಿಎನ್‌ಎಸ್ 75– ಲೈಂಗಿಕ ಕಿರುಕುಳ ಮತ್ತು ಲೈಂಗಿಕ ಕಿರುಕುಳಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 354ಸಿ/ಬಿಎನ್‌ಎಸ್ 77 –ಇತರರ ಲೈಂಗಿಕ ಕೃತ್ಯಗಳನ್ನು ಅನುಕೂಲವಾದ ಸ್ಥಾನದಿಂದ ನೋಡುವ ಪ್ರಯೋಜನ

ಹಿಂಬಾಲಿಕೆ: ಐಪಿಸಿ ಕಲಂ 354 ಡಿ/ಬಿಎನ್‌ಎಸ್ 78– ಆಫ್‌ಲೈನ್ ಹಿಂಬಾಲಿಕೆ, **ಐಪಿಸಿ ಕಲಂ 354 ಡಿ/ಬಿಎನ್‌ಎಸ್ 78**– ಆನ್‌ಲೈನ್ ಹಿಂಬಾಲಿಕೆ

ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪ್ರಕಟಿಸುವುದು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ಹರಡಿ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಎ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಬಿ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿರುವ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ, ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಲಂಗಳು

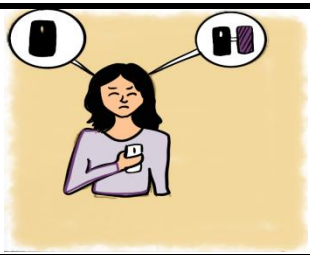
ಐಪಿಸಿ ಕಲಂ 507/ಬಿಎನ್‌ಎಸ್ 351– ಅನಾಮಧೇಯ ಸಂವಹನದಿಂದ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ

ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನ

ಐಪಿಸಿ ಕಲಂ 465/ಬಿಎನ್‌ಎಸ್ 336– ಸುಳ್ಳು ದಾಖಲೆಗಳ ಸೃಷ್ಟಿ

ಪ್ರಣಯ ಭೇಟಿಯ ಕಾತುರದಲ್ಲಿದ್ದೀರಾ, ನಿಮಗೆ ಸರಿಯಾದ ಜೋಡಿ ಸಿಗದಿರಬಹುದು

ಬಿಂಬಗ್ರಾಹಿ ಅತಿಕ್ರಮಣ (ಕ್ಯಾಮರಾ ಹ್ಯಾಕಿಂಗ್)

ಲಿಶಾ ತನ್ನ ಕಾಲೇಜಿನಲ್ಲಿ ಸದಾ ಉತ್ಸಾಹ ಹೊಂದಿದ ವಿದ್ಯಾರ್ಥಿನಿ ಆಗಿದ್ದಳು.	ಮೇಲ್ ನೋಡಲು, ಹಣ ವರ್ಗಾವಣೆ ಮಾಡಲು, ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ನಿರ್ವಹಿಸಲು ತನ್ನ ಮೊಬೈಲ್ ಬಳಕೆ ಮಾಡುತ್ತಿದ್ದಳು	ಶೌಚಾಲಯ ಬಳಸುವಾಗಲೆಲ್ಲಾ ಸದಾ ತನ್ನ ಮೊಬೈಲ್ ಕೊಂಡೊಯ್ಯುತ್ತಿದ್ದಳು.
ಒಮ್ಮೆ ಮೆಸೆಂಜರ್ ಮೂಲಕ ಟ್ರೋಜನ್ ಹೊಂದಿದ ಮಾಲ್ವೇರ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿರುವ ಬಗ್ಗೆ ಅವಳಿಗೆ ಅರಿವಿರಲಿಲ್ಲ.	ದುಷ್ಟ ತಂತ್ರಾಂಶವು ಫೋನ್‌ನ ಹಿಂಬದಿ ಮುಂಬದಿ ಕ್ಯಾಮರವನ್ನು ಅರಿವಿಗೆ ಬಾರದಂತೆ ಪ್ರಾರಂಭಿಸಿ, ಭಿನ್ನವಾದ ವಿಡಿಯೋಗಳನ್ನು ಸೆರೆಹಿಡಿದುಕೊಂಡಿತು.	ಒಮ್ಮೆ ಅರಿವಿಲ್ಲದ ಲಿಶಾ ಫೋನ್ ಬದಿಗಿಟ್ಟು ಶೌಚಾಲಯದಲ್ಲಿ ಸ್ನಾನ ಮಾಡಿದಳು.
		
ಒಂದು ದಿನ, ಅವಳ ಸ್ನೇಹಿತ ಅರಸ್ ಅಶ್ಲೀಲ ಜಾಲತಾಣಗಳಲ್ಲಿ ಅವಳ ವಿಡಿಯೋ ಹರಿದಾಡುತ್ತಿರುವ ಬಗ್ಗೆ ತಿಳಿಸಿದ.	ಲಿಶಾ ಛಿದ್ರಗೊಂಡಳು. ಅವಳ ಫೋನ್ ಆ್ಯಂಟಿ ವೈರಸ್ ಹೊಂದಿರಲಿಲ್ಲ. ಇದ್ದಿದ್ದರೆ ರಕ್ಷಣೆ ಮಾಡುವ ಸಂಭವವಿತ್ತು.	ಮೊಬೈಲ್‌ಗೆ ಫ್ಲಿಪ್ ಕವರ್ ಇರಲಿಲ್ಲ ಮತ್ತು ಕ್ಯಾಮರ ರಕ್ಷಕ ಇರಲಿಲ್ಲವೆಂದು ತೀರಾ ನೊಂದುಕೊಂಡಳು. ನೀವೂ ಜಾಗರೂಕರಾಗಿರಿ.

ಬಿಂಬಗ್ರಾಹಿ ಅತಿಕ್ರಮಣ (ಕ್ಯಾಮರಾ ಹ್ಯಾಕಿಂಗ್)

ಮೊಬೈಲ್ ಫೋನ್‌ಗೆ ಬರುವಂತೆ ಹಲವಾರು ಬಗೆಯ ಲಗತ್ತುಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿದಾಗ ಅರಿವಿಲ್ಲದೆ ಬರುವಂತಹ ಮಾಲ್ವೇರ್‌ಗಳ ಮೂಲಕ ವ್ಯಕ್ತಿಯ ಒಪ್ಪಿಗೆಯಿಲ್ಲದೆ ಛಾಯಾಚಿತ್ರಗಳನ್ನು ತೆಗೆದುಕೊಂಡಾಗ ಕ್ಯಾಮರಾ ಅತಿಕ್ರಮಣ ಸಂಭವಿಸುತ್ತದೆ.ಕ್ಯಾಮರಾ ರಕ್ಷಕಗಳು ಇಲ್ಲದಂತಹ ಫೋನ್‌ಗಳನ್ನು ಇಂತಹ ಅಪರಾಧ ಚಟುವಟಿಕೆಗಳಿಗೆ ಬಳಸಿಕೊಳ್ಳಲಾಗುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಅತಿಕ್ರಮಣ –

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಕಲಂ 66ಬಿ– ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಕಳ್ಳತನ ಗಣಕಯಂತ್ರ ಸ್ವೀಕಾರಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಫೋಟೋ/ವಿಡಿಯೋ ಸೆರೆಹಿಡಿಯುವುದು:

ಐಪಿಸಿ 354(ಸಿ)/ಬಿಎನ್‌ಎಸ್ 77– ಓರ್ವ ಪುರುಷ ಮಹಿಳೆಯು ಲೈಂಗಿಕ ಕೃತ್ಯದಲ್ಲಿ ತೊಡಗಿಸಿಕೊಂಡಿರುವ ಸನ್ನಿವೇಶವನ್ನು ಆಕೆಯ ಅರಿವಿಲ್ಲದೇ ನೋಡುವ ಅಥವಾ ಅವಳು ನಿರೀಕ್ಷಿಸದ ರೀತಿಯಲ್ಲಿ ದೃಶ್ಯ ಸೆರೆಹಿಡಿಯಲು ತೊಡಗಿಸಿಕೊಂಡು ಅದನ್ನು ಪ್ರಸಾರ ಮಾಡುವುದು.

ಮಾ.ತ.ಕಾ ಕಲಂ 66ಡಿ & **66ಇ**– ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ನಕಲಿ ಐಡಿ ಸೃಷ್ಟಿಸಿ ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ 419/ಬಿಎನ್‌ಎಸ್ 319(2)–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಮಹಿಳೆಗೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಲೈಂಗಿಕ ಕಿರುಕುಳ

ಐಪಿಸಿ 354(ಎ)/ಬಿಎನ್‌ಎಸ್ 75– ಲೈಂಗಿಕ ಕಿರುಕುಳ ಮತ್ತು ಲೈಂಗಿಕ ಕಿರುಕುಳಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ 354(ಸಿ)/ಬಿಎನ್‌ಎಸ್ 77 – ಓರ್ವ ಪುರುಷ ಮಹಿಳೆಯು ಲೈಂಗಿಕ ಕೃತ್ಯದಲ್ಲಿ ತೊಡಗಿಸಿಕೊಂಡಿರುವ ಸನ್ನಿವೇಶವನ್ನು ಆಕೆಯ ಅರಿವಿಲ್ಲದೇ ನೋಡುವ ಅಥವಾ ಅವಳು ನಿರೀಕ್ಷಿಸದ ರೀತಿಯಲ್ಲಿ ದೃಶ್ಯ ಸೆರೆಹಿಡಿಯಲು ತೊಡಗಿಸಿಕೊಂಡು ಅದನ್ನು ಪ್ರಸಾರ ಮಾಡುವುದು.

ಹಿಂಬಾಲಿಕೆ: ಐಪಿಸಿ 354(ಡಿ)/ಬಿಎನ್‌ಎಸ್ 78– ಆಫ್‌ಲೈನ್ ಹಿಂಬಾಲಿಕೆ, **ಕಲಂ ಐಪಿಸಿ 354(ಡಿ)/ಬಿಎನ್‌ಎಸ್** 78– ಆನ್‌ಲೈನ್ ಹಿಂಬಾಲಿಕೆ

ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪ್ರಕಟಣೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ಹರಡಿ ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಎ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ, ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಬಿ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿರುವ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ, ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಲಂಗಳು

ಐಪಿಸಿ 507/ಬಿಎನ್‌ಎಸ್ 351(4)– ಅನಾಮಧೇಯ ಸಂವಹನದಿಂದ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ

ಐಪಿಸಿ 509/ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನ

ಶೌಚಾಲಯದಲ್ಲಿ ಮೊಬೈಲ್ ಬಳಸುವ ಹವ್ಯಾಸವಿದ್ದರೆ ಎಚ್ಚರ, ನಿಮ್ಮ ಗೌಪ್ಯತೆ ಬಗ್ಗೆ ಚಿಂತಿಸಿ

ಸಾಮಾಜಿಕ ಟ್ರೋಲಿಂಗ್

ಶೃತಿ ಮಧ್ಯಮ ವರ್ಗದ ಸರಳ ಹುಡುಗಿಯಾಗಿದ್ದು, ನೈತಿಕತೆ ಮತ್ತು ನೀತಿತತ್ವದಲ್ಲಿ ನಂಬಿಕೆ ಹೊಂದಿದ್ದಳು.	ಅವಳು ವಿದ್ಯಾಭ್ಯಾಸ ಮಾಡುತ್ತಿದ್ದ ಕಾಲೇಜಿನ ಸಹಪಾಠಿಗಳೆಲ್ಲ, ಜವಾಬ್ದಾರಿ ಇಲ್ಲದ ಮನೋವಿಕಾರಿಗಳಾಗಿದ್ದರು.	ಪ್ರತಿದಿನ ಅವರೆಲ್ಲ ಶೃತಿಯ ಕಾಲು ಎಳೆಯುತ್ತಿದ್ದರು. ಅವಳನ್ನು ವಿಚಿತ್ರ ಹೆಸರಿಟ್ಟು ಕರೆಯುತ್ತಿದ್ದರು. ಹೀಗೆ ಅವಳನ್ನು ಖಿನ್ನತೆಗೆ ಒಳಗಾಗುವಂತೆ ಮಾಡುತ್ತಿದ್ದರು.
ರಜತ್ ಕಾಲೇಜಿನ ಪ್ರಸಿದ್ದ ಹುಡುಗ. ಅವಳನ್ನು ಅಶಿಕ್ಷಿತೆ ಎಂದು ಕರೆದು ಹಳ್ಳಿಗೆ ವಾಪಸ್ಸು ಹೋಗಲು ಹೇಳಿದನು.	ಶೃತಿ ಇದಕ್ಕೆ ಅಂತ್ಯವಾಡಲು ನಿರ್ಧರಿಸಿ, ಧೈರ್ಯ ತಂದುಕೊಂಡು ಅವನಿಗೆ ತನ್ನ ತಂಟೆಗೆ ಬರದಂತೆ ಇರಲು ಎಚ್ಚರಿಸುತ್ತಾಳೆ.	ರಜತ್ ಮನೆಗೆ ತೆರಳಿ ಶೃತಿ ಹೆಸರಿನಲ್ಲಿ ವಯಸ್ಕರ ಲೇವಡಿ ಸಂದೇಶಗಳನ್ನು ತಯಾರಿಸಿ ಸ್ನೇಹಿತರಿಗೆ ಕಳುಹಿಸುತ್ತಾನೆ.
ಶೃತಿ ಹೆಸರಿನ ಟ್ರೋಲ್ ಪುಟ ತೆರೆದು, ಅಲ್ಲಿ ಅವಳ ಹಾಸ್ಯ ವಿಡಿಯೋ ಮತ್ತು ಮೆಮೆಗಳನ್ನು ಅಪ್‌ಲೋಡ್ ಮಾಡುತ್ತಾನೆ.	ಶೃತಿ ಎಲ್ಲರ ಎದುರು ಹಾಸ್ಯಾಸ್ಪದ ವಾದಳು ಮತ್ತು ತನ್ನ ಶಿಕ್ಷಣವನ್ನು ಮೊಟಕುಗೊಳಿಸುವ ತೀರ್ಮಾನಕ್ಕೆ ಬರುತ್ತಾಳೆ.	ಶೃತಿ ಎಲ್ಲಾ ವಿಚಾರವನ್ನು ಕಾಲೇಜಿನ ಪ್ರಾಧಿಕಾರಕ್ಕೆ ತಿಳಿಸದ್ದಕ್ಕೆ ಚಿಂತಿತಳಾಗಿ ನಂತರ ಕೊನೆಗೆ ಮಹಿಳಾ ಪೊ.ಠಾಣೆಯಲ್ಲಿ ದೂರು ದಾಖಲಿಸುತ್ತಾಳೆ.

ಸಾಮಾಜಿಕ ಟ್ರೋಲಿಂಗ್

ಒಬ್ಬ ವ್ಯಕ್ತಿಗೆ ಅವಮಾನ ಮಾಡುವ ಉದ್ದೇಶದಿಂದ ಅಥವಾ ಉಪದ್ರವ ಉಂಟುಮಾಡುವ ಏಕೈಕ ಉದ್ದೇಶದಿಂದ ಆನ್‌ಲೈನ್ ಮಾಧ್ಯಮದಲ್ಲಿ ಆ ವ್ಯಕ್ತಿಗೆ ಅಥವಾ ಅಂತಹ ಸಂಸ್ಥೆಯ ಬಗ್ಗೆ ಅವಹೇಳನಕಾರಿ ಸಂದೇಶ ಅಥವಾ ದೃಶ್ಯಗಳನ್ನು ಪೋಸ್ಟ್ ಮಾಡುವುದನ್ನು ಸಾಮಾಜಿಕ ಟ್ರೋಲಿಂಗ್ ಎನ್ನಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 507/ಬಿಎನ್‌ಎಸ್ 351– ಅನಾಮಧೇಯ ಸಂವಹನದಿಂದ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ

ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನವಾಗುವ ಉದ್ದೇಶದ ಪದಗಳು, ಸನ್ನೆ ಅಥವಾ ಅಭಿನಯ

ಹಿಂಬಾಲಿಕೆ:

ಐಪಿಸಿ ಕಲಂ 354 ಡಿ/ಬಿಎನ್‌ಎಸ್ 78– ಆಫ್‌ಲೈನ್ ಹಿಂಬಾಲಿಕೆ, **ಕಲಂ 354 ಡಿ/ಬಿಎನ್‌ಎಸ್ 78**– ಆನ್‌ಲೈನ್ ಹಿಂಬಾಲಿಕೆ

ಮ.ತ.ಕಾಯ್ದೆ:

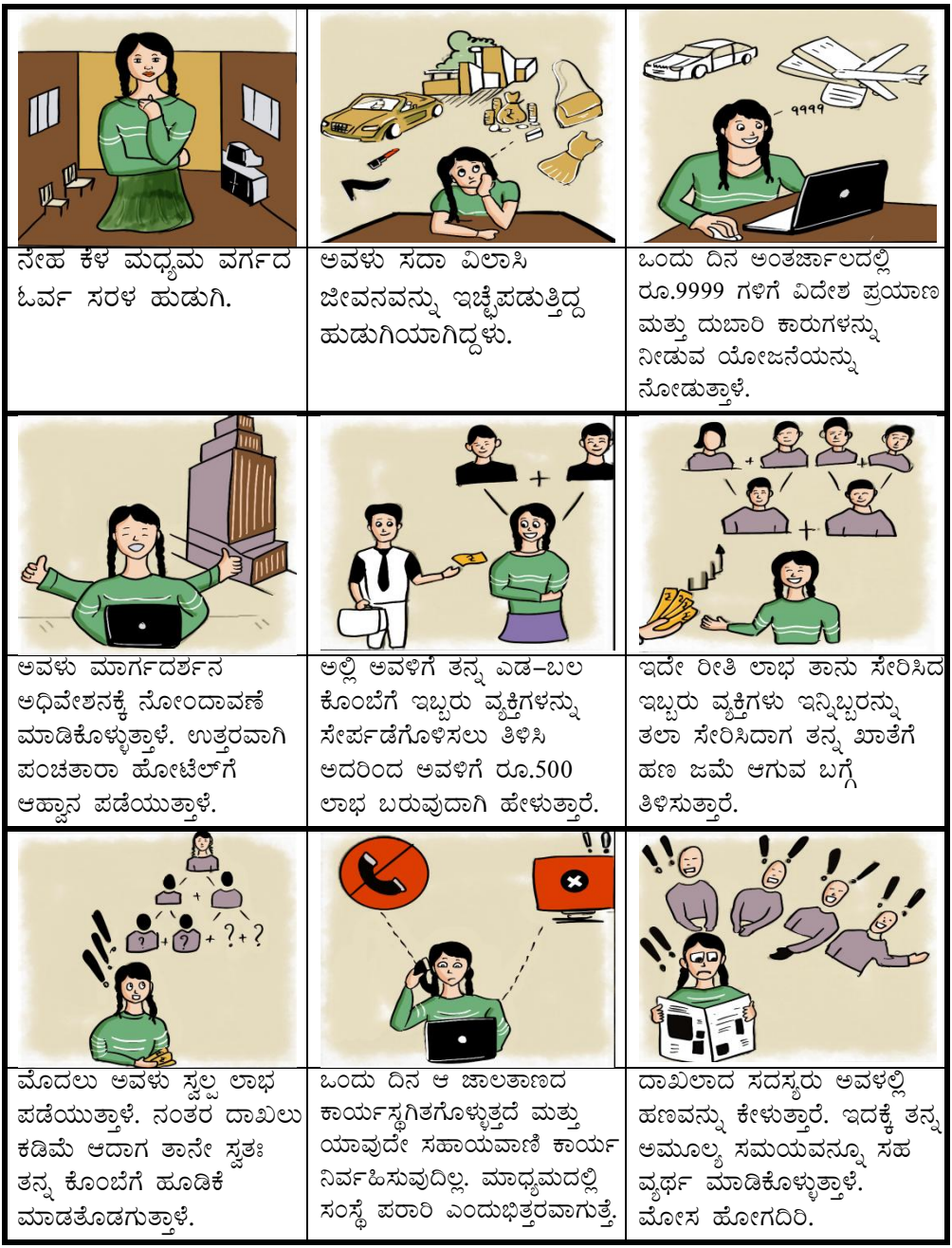
ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಕಲಂ 67 ಎ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ, ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 67 ಬಿ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿರುವ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ, ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಲಂಗಳು

ನೀವು ಸಹ ಟ್ರೋಲ್ ಮಾಡುತ್ತಿರುವಿರಾ, ನಿಮ್ಮನ್ನು ಹಿಂಬಾಲಿಸಲಾಗುತ್ತಿದೆ ಎಚ್ಚರ.

ಪೋಂಝಿ ಯೋಜನೆ



ನೇಹ ಕೆಳ ಮಧ್ಯಮ ವರ್ಗದ ಓರ್ವ ಸರಳ ಹುಡುಗಿ.

ಅವಳು ಸದಾ ವಿಲಾಸಿ ಜೀವನವನ್ನು ಇಚ್ಛೆಪಡುತ್ತಿದ್ದ ಹುಡುಗಿಯಾಗಿದ್ದಳು.

ಒಂದು ದಿನ ಅಂತರ್ಜಾಲದಲ್ಲಿ ರೂ.9999 ಗಳಿಗೆ ವಿದೇಶ ಪ್ರಯಾಣ ಮತ್ತು ದುಬಾರಿ ಕಾರುಗಳನ್ನು ನೀಡುವ ಯೋಜನೆಯನ್ನು ನೋಡುತ್ತಾಳೆ.

ಅವಳು ಮಾರ್ಗದರ್ಶನ ಅಧಿವೇಶನಕ್ಕೆ ನೋಂದಾವಣೆ ಮಾಡಿಕೊಳ್ಳುತ್ತಾಳೆ. ಉತ್ತರವಾಗಿ ಪಂಚತಾರಾ ಹೋಟೆಲ್‌ಗೆ ಆಹ್ವಾನ ಪಡೆಯುತ್ತಾಳೆ.

ಅಲ್ಲಿ ಅವಳಿಗೆ ತನ್ನ ಎಡ–ಬಲ ಕೊಂಬೆಗೆ ಇಬ್ಬರು ವ್ಯಕ್ತಿಗಳನ್ನು ಸೇರ್ಪಡೆಗೊಳಿಸಲು ತಿಳಿಸಿ ಅದರಿಂದ ಅವಳಿಗೆ ರೂ.500 ಲಾಭ ಬರುವುದಾಗಿ ಹೇಳುತ್ತಾರೆ.

ಇದೇ ರೀತಿ ಲಾಭ ತಾನು ಸೇರಿಸಿದ ಇಬ್ಬರು ವ್ಯಕ್ತಿಗಳು ಇನ್ನಿಬ್ಬರನ್ನು ತಲಾ ಸೇರಿಸಿದಾಗ ತನ್ನ ಖಾತೆಗೆ ಹಣ ಜಮೆ ಆಗುವ ಬಗ್ಗೆ ತಿಳಿಸುತ್ತಾರೆ.

ಮೊದಲು ಅವಳು ಸ್ವಲ್ಪ ಲಾಭ ಪಡೆಯುತ್ತಾಳೆ. ನಂತರ ದಾಖಲು ಕಡಿಮೆ ಆದಾಗ ತಾನೇ ಸ್ವತಃ ತನ್ನ ಕೊಂಬೆಗೆ ಹೂಡಿಕೆ ಮಾಡತೊಡಗುತ್ತಾಳೆ.

ಒಂದು ದಿನ ಆ ಜಾಲತಾಣದ ಕಾರ್ಯಸ್ಥಗಿತಗೊಳ್ಳುತ್ತದೆ ಮತ್ತು ಯಾವುದೇ ಸಹಾಯವಾಣಿ ಕಾರ್ಯ ನಿರ್ವಹಿಸುವುದಿಲ್ಲ. ಮಾಧ್ಯಮದಲ್ಲಿ ಸಂಸ್ಥೆ ಪರಾರಿ ಎಂದುಭಿತ್ತರವಾಗುತ್ತೆ.

ದಾಖಲಾದ ಸದಸ್ಯರು ಅವಳಲ್ಲಿ ಹಣವನ್ನು ಕೇಳುತ್ತಾರೆ. ಇದಕ್ಕೆ ತನ್ನ ಅಮೂಲ್ಯ ಸಮಯವನ್ನೂ ಸಹ ವ್ಯರ್ಥ ಮಾಡಿಕೊಳ್ಳುತ್ತಾಳೆ. ಮೋಸ ಹೋಗದಿರಿ.

ಪೋಂಝಿ ಯೋಜನೆಯು ದುರುದ್ದೇಶವುಳ್ಳ ಹಣ ಹೂಡಿಕೆಯ ಹಗರಣವಾಗಿದ್ದು, ಹೂಡಿಕೆದಾರರಿಗೆ ಯಾವುದೇ ಶ್ರಮವಿಲ್ಲದೇ ಕಡಿಮೆ ಹೂಡಿಕೆಗೆ ಅಧಿಕ ಲಾಭವನ್ನು ನೀಡುವಂತಹದ್ದಾಗಿರುತ್ತದೆ.ಅಂತಹ ಯೋಜನೆಯಲ್ಲಿ ಸಿಲುಕುವ ಬಲಿಪಶುಗಳು ದುರುದ್ದೇಶ ಹೊಂದಿರುವ ಆಕ್ರಮಣಕಾರರಿಗೆ ಗುರಿಯಾಗುತ್ತಾರೆ ಮತ್ತು ಅವರುಗಳ ನಷ್ಟವನ್ನು ಮರುಪಡೆಯಬಹುದಾದಂತಹ ಭರವಸೆಗಳಿಗೆ ಬಲಿಯಾಗುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಬಹುಮಾನ ಚೀಟಿ ಮತ್ತು ಹಣ ಚಲಾವಣೆ ಯೋಜನೆಗಳ(ನಿಷೇಧ) ಕಾಯ್ದೆ, 1978 ರ ಕಲಂ 3, 4, 5, 6

ಹಾಗೆಯೇ ರಾಜ್ಯ ಅಧಿನಿಯಮಗಳನ್ನು ಸಹ ಪರಿಗಣಿಸುವುದು. ಉದಾ:

ಹಣಕಾಸು ಪ್ರತಿಷ್ಠಾಪನಾ ಕಾಯ್ದೆ, 2004 ಯಲ್ಲಿ ಕರ್ನಾಟಕ ಠೇವಣಿದಾರರ ಹಿತಾಸಕ್ತಿ ಸಂರಕ್ಷಣೆ ಕಲಂ 9

ಹಣಕಾಸು ಪ್ರತಿಷ್ಠಾಪನಾ ಕಾಯ್ದೆ, 1999 ಇತ್ಯಾದಿಯಲ್ಲಿ ಮಹಾರಾಷ್ಟ್ರ ಠೇವಣಿದಾರರ ಹಿತಾಸಕ್ತಿ ಸಂರಕ್ಷಣೆ ಕಲಂ 3, 4

ಐಪಿಸಿ ಕಲಂ 120ಬಿ/ಬಿಎನ್ಎಸ್ 61– ಅಪರಾಧದ ಸಂಚಿಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 406/ಬಿಎನ್ಎಸ್ 316– ವಿಶ್ವಾಸ ಭಂಗದ ಅಪರಾಧಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

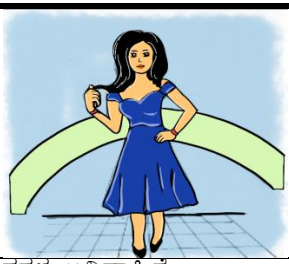
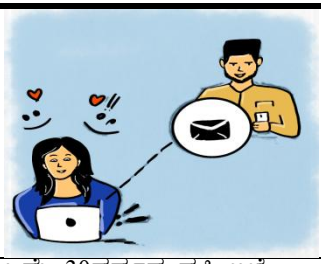
ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318– ಮೋಸ

ಐಪಿಸಿ ಕಲಂ 34/ಬಿಎನ್ಎಸ್ 3(5) ನೊಂದಿಗೆ ಓದಲಾದ– ಸಾಮಾನ್ಯ ಉದ್ದೇಶದಿಂದ ಮುಂದುವರೆಯಲು ಹಲವಾರುವ್ಯಕ್ತಿಗಳಿಂದ ಮಾಡಿದ ಕೃತ್ಯಗಳು

ಕಲಂ 21, 22 & 23 ಬ್ಯಾನಿಂಗ್ ಆಫ್ ಅನ್ ರೆಗ್ಯೂಲೇಟಡ್ ಡೆಪಾಸಿಟ್ ಸ್ಕೀಂ ಕಾಯ್ದೆ 2019

ಪೋಂಝಿ ಯೋಜನೆಯಲ್ಲಿ ತೊಡಗಿದರೆ ಜೀವನದಲ್ಲಿ ನಿಮ್ಮನ್ನು ದಿವಾಳಿಮಾಡುತ್ತದೆ.

ನಕಲಿ ವೈವಾಹಿಕ ವ್ಯಕ್ತಿಚಿತ್ರ (ಮ್ಯಾಟ್ರಿಮೊನಿ)

		
ಸರಳ ಅವಿವಾಹಿತೆ ಇಂಜಿನೀಯರ್ ಆಗಿದ್ದಳು. ಅವಳ ಪೋಷಕರು ಅವಳಿಗಾಗಿ ವರನ ಹುಡುಕಾಟ ನಡೆಸುತ್ತಿದ್ದರು.	ಅವಳು ಹಲವಾರು ವೈವಾಹಿಕ ತಾಣಗಳಲ್ಲಿ ವರನ ಹುಡುಕಾಟದ ನಿರೀಕ್ಷೆಯಲ್ಲಿ ನೋಂದಣಿ ಮಾಡಿಕೊಂಡಿದ್ದಳು.	ಒಮ್ಮೆ 30ವರ್ಷದ ವ್ಯಕ್ತಿ ಇಚ್ಛೆ ವ್ಯಕ್ತಪಡಿಸಿರುವ ಬಗ್ಗೆ ಇನ್‌ಬಾಕ್ಸ್ ಸಂದೇಶ ಸ್ವೀಕರಿಸುತ್ತಾಳೆ.
ಅವಳು ಹುಡುಕಾಟ ನಡೆಸಿ ಅವನೊಬ್ಬ ಭಾರತೀಯ IRS ಅಧಿಕಾರಿ, ಬೆಂಗಳೂರಿನ ಸ್ಥಿತಿವಂತ ಕುಟುಂಬದವನು ಎಂದು ತಿಳಿದಳು.	ಅವನೊಬ್ಬ ಆಕರ್ಷಿತ ವ್ಯಕ್ತಿ ಆದ್ದರಿಂದ ಅವಳು ಅವನಿಗೆ ಸೋತು ಸಂದೇಶ ವಿನಿಮಯ, ಕರೆಗಳ ಸಂವಾದ ಪ್ರಾರಂಭವಾಗುತ್ತದೆ.	ಅವಳನ್ನು ನಂಬಿಸಲು, ತನ್ನ ಖಾತೆ ವಿವರಗಳನ್ನು, ಪೋಷಕರ ವಿವರ, ಸ್ನೇಹಿತರ ವಿವರ, ಫೋಟೋ ಇತ್ಯಾದಿಗಳನ್ನು ಅವಳಿಗೆ ತೋರಿಸುತ್ತಾನೆ.
ಒಂದು ದಿನ ಆತ ರಾಜಕಾರಣಿಗಳ ಹಸ್ತಕ್ಷೇಪದಿಂದ ತನ್ನ ಕೆಲಸವು ಹೋಗಿದ್ದು, ಮರಳಿ ಪಡೆಯಲು ಹಣದ ಅವಶ್ಯಕತೆ ಇರುವುದಾಗಿ ತಿಳಿಸುತ್ತಾನೆ.	ತನ್ನ ಪಾಸ್‌ಪೋರ್ಟ್, ಐಡಿ ಇತರ ದಾಖಲೆಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿಡಲು ಅವಳ ಬಳಿ ನೀಡುತ್ತಾನೆ. ಅವಳು 5 ಲಕ್ಷ ಹಣವನ್ನು ತನ್ನ ಖಾತೆಯಿಂದಅವನ ಖಾತೆಗೆವರ್ಗಾಯಿಸುತ್ತಾಳೆ.	ಒಂದು ವಾರದ ನಂತರ ದಿನಪತ್ರಿಕೆಯಲ್ಲಿ ಆತನನ್ನು ಮಹಿಳೆಯರಿಗೆ ವೈವಾಹಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಮೋಸಮಾಡಿದ ಆರೋಪದಡಿ ಪೊಲೀಸರು ಸೆರೆಹಿಡಿದಿರುವ ವಿಷಯ ಓದುತ್ತಾಳೆ.

ವಂಚಕರು ಮ್ಯಾಟ್ರಿಮೋನಿಯಲ್ ಜಾಲತಾಣಗಳಲ್ಲಿ ನಕಲಿ ವ್ಯಕ್ತಿಚಿತ್ರದೊಂದಿಗೆ ಸಾಮಾನ್ಯವಾಗಿ ನೋಂದಾಯಿಸಿರುತ್ತಾರೆ.ಜಾಲತಾಣದಲ್ಲಿ ಕಾಣಲಾಗುವ ಮಾಹಿತಿಗಳು ಹಾಗೂ ಭಾವಚಿತ್ರಗಳು ಆ ವ್ಯಕ್ತಿಯದ್ದಾಗಿರುವುದಿಲ್ಲ. ಆ ವ್ಯಕ್ತಿ ತನ್ನ ಜಾಣ್ಮೆಯಿಂದ ತನ್ನ ಮೋಡಿಗೆ ಬೀಳುವ ನಿಷ್ಕಲ್ಮಶ ಹುಡುಗಿಯರನ್ನು ಮೋಸಗೊಳಿಸಬಹುದು ಮತ್ತು ತನ್ನ ನಿಜವಾದ ಗುರುತನ್ನು ಮರೆಮಾಚಿ ಸತ್ಯವೆಂಬಂತೆ ನಂಬಿಕೆ ಹುಟ್ಟಿಸುತ್ತಾನೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 415/ಬಿಎನ್ಎಸ್ 318–ವಂಚನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್ಎಸ್ 319–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318– ಮೋಸ

ಐಪಿಸಿ ಕಲಂ 464/ಬಿಎನ್ಎಸ್ 335– ಸುಳ್ಳು ದಾಖಲೆಗಳ ಸೃಷ್ಟಿ

ಐಪಿಸಿ ಕಲಂ 465/ಬಿಎನ್ಎಸ್ 336(2)– ಖೋಟಾ ಸೃಷ್ಟಿಗಾಗಿ ಶಿಕ್ಷೆ

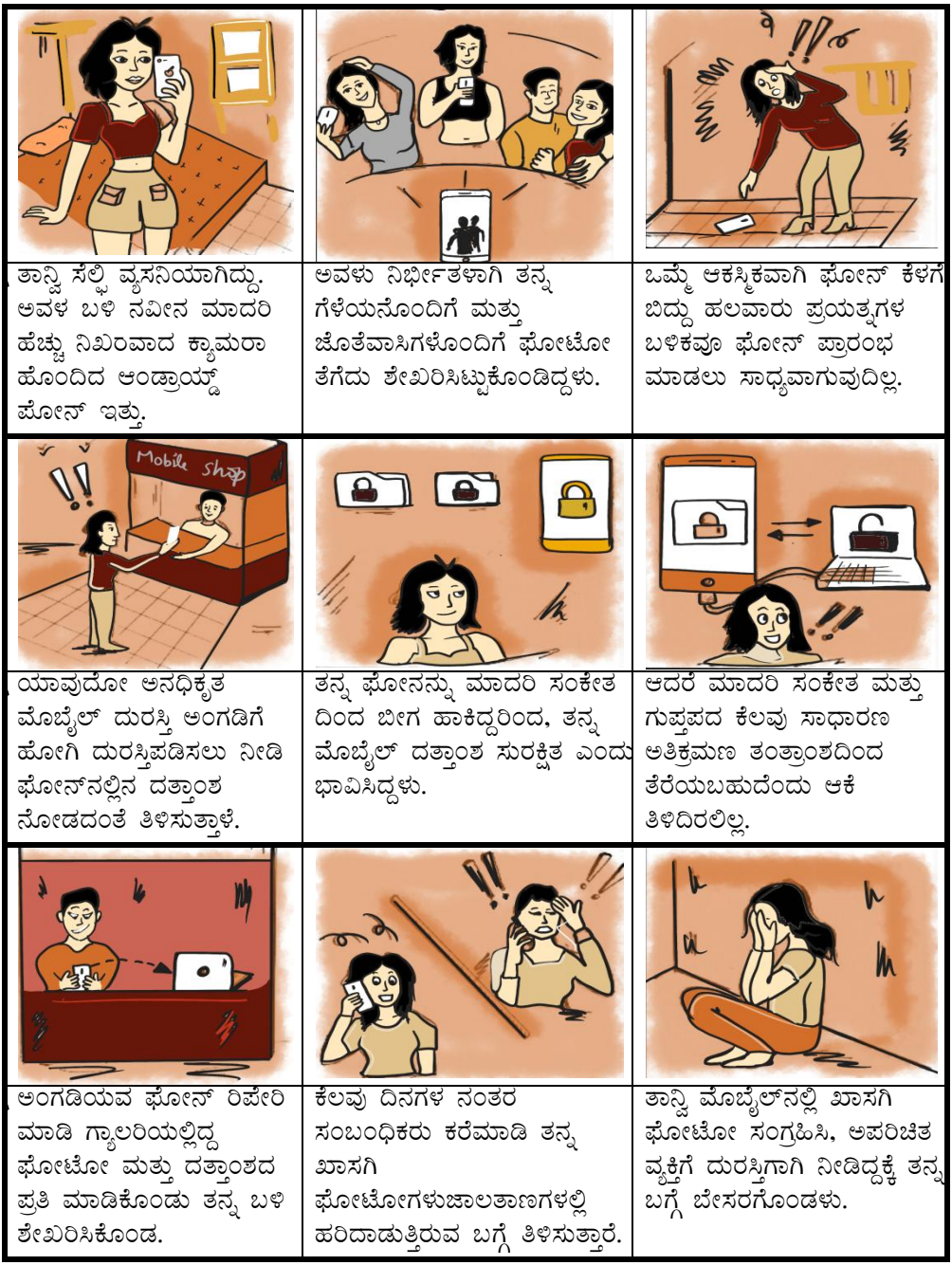
ಐಪಿಸಿ ಕಲಂ 468/ಬಿಎನ್ಎಸ್ 336(3)– ವಂಚನೆಯ ಉದ್ದೇಶಕ್ಕಾಗಿ ಖೋಟಾ ಸೃಷ್ಟಿ

ಐಪಿಸಿ ಕಲಂ 471/ಬಿಎನ್ಎಸ್ 340– ನಕಲಿ ದಾಖಲೆಯನ್ನು ಅಸಲಿಯಾಗಿ ಬಳಸುವುದು

ಐಪಿಸಿ ಕಲಂ 507/ಬಿಎನ್ಎಸ್ 351– ಅನಾಮದೇಯ ಸಂವಹನದಿಂದ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ

ವಿವಾಹಗಳು ಸ್ವರ್ಗದಲ್ಲಿ ನಿಶ್ಚಿತವಾಗಿರುತ್ತದೆ.ಆದರೆ ನಿಜವಾದ ಪ್ರಪಂಚದಲ್ಲಿ ನಮ್ಮ ಜೀವನವನ್ನು ನಾವೇ ನರಕಕ್ಕೆ ಕೊಂಡ್ಯೊಯ್ದುಕೊಳ್ಳುತ್ತೇವೆ.

ಮೊಬೈಲ್ ದುರಸ್ತಿ ಮಳಿಗೆ



ತಾನ್ವಿ ಸೆಲ್ಫಿ ವ್ಯಸನಿಯಾಗಿದ್ದು. ಅವಳ ಬಳಿ ನವೀನ ಮಾದರಿ ಹೆಚ್ಚು ನಿಖರವಾದ ಕ್ಯಾಮರಾ ಹೊಂದಿದ ಆಂಡ್ರಾಯ್ಡ್ ಫೋನ್ ಇತ್ತು.	ಅವಳು ನಿರ್ಭೀತಳಾಗಿ ತನ್ನ ಗೆಳೆಯನೊಂದಿಗೆ ಮತ್ತು ಜೊತೆವಾಸಿಗಳೊಂದಿಗೆ ಫೋಟೋ ತೆಗೆದು ಶೇಖರಿಸಿಟ್ಟುಕೊಂಡಿದ್ದಳು.	ಒಮ್ಮೆ ಆಕಸ್ಮಿಕವಾಗಿ ಫೋನ್ ಕೆಳಗೆ ಬಿದ್ದು ಹಲವಾರು ಪ್ರಯತ್ನಗಳ ಬಳಿಕವೂ ಫೋನ್ ಪ್ರಾರಂಭ ಮಾಡಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲ.
ಯಾವುದೋ ಅನಧಿಕೃತ ಮೊಬೈಲ್ ದುರಸ್ತಿ ಅಂಗಡಿಗೆ ಹೋಗಿ ದುರಸ್ತಿಪಡಿಸಲು ನೀಡಿ ಫೋನ್‌ನಲ್ಲಿನ ದತ್ತಾಂಶ ನೋಡದಂತೆ ತಿಳಿಸುತ್ತಾಳೆ.	ತನ್ನ ಫೋನನ್ನು ಮಾದರಿ ಸಂಕೇತ ದಿಂದ ಬೀಗ ಹಾಕಿದ್ದರಿಂದ, ತನ್ನ ಮೊಬೈಲ್ ದತ್ತಾಂಶ ಸುರಕ್ಷಿತ ಎಂದು ಭಾವಿಸಿದ್ದಳು.	ಆದರೆ ಮಾದರಿ ಸಂಕೇತ ಮತ್ತು ಗುಪ್ತಪದ ಕೆಲವು ಸಾಧಾರಣ ಅತಿಕ್ರಮಣ ತಂತ್ರಾಂಶದಿಂದ ತೆರೆಯಬಹುದೆಂದು ಆಕೆ ತಿಳಿದಿರಲಿಲ್ಲ.
ಅಂಗಡಿಯವ ಫೋನ್ ರಿಪೇರಿ ಮಾಡಿ ಗ್ಯಾಲರಿಯಲ್ಲಿದ್ದ ಫೋಟೋ ಮತ್ತು ದತ್ತಾಂಶದ ಪ್ರತಿ ಮಾಡಿಕೊಂಡು ತನ್ನ ಬಳಿ ಶೇಖರಿಸಿಕೊಂಡ.	ಕೆಲವು ದಿನಗಳ ನಂತರ ಸಂಬಂಧಿಕರು ಕರೆಮಾಡಿ ತನ್ನ ಖಾಸಗಿ ಫೋಟೋಗಳುಜಾಲತಾಣಗಳಲ್ಲಿ ಹರಿದಾಡುತ್ತಿರುವ ಬಗ್ಗೆ ತಿಳಿಸುತ್ತಾರೆ.	ತಾನ್ವಿ ಮೊಬೈಲ್‌ನಲ್ಲಿ ಖಾಸಗಿ ಫೋಟೋ ಸಂಗ್ರಹಿಸಿ, ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಗೆ ದುರಸ್ತಿಗಾಗಿ ನೀಡಿದ್ದಕ್ಕೆ ತನ್ನ ಬಗ್ಗೆ ಬೇಸರಗೊಂಡಳು.

ಮೊಬೈಲ್ ದುರಸ್ತಿ ಮಳಿಗೆ

ಫೋನ್ ಗ್ಯಾಲರಿಯಲ್ಲಿ ವೈಯಕ್ತಿಕ ಚಿತ್ರಗಳು ಮತ್ತು ವಿಡಿಯೋಗಳ ಸಂಗ್ರಹವಿರುವ ಫೋನನ್ನು ತನ್ನ ವಶಕ್ಕೆ ಪಡೆದ ಯಾವುದೇ ವ್ಯಕ್ತಿಗಳು ಅದಕ್ಕೆ ಪ್ರವೇಶ ಪಡೆಯಬಹುದು.ಮೊಬೈಲ್ ದುರಸ್ತಿ ಮಳಿಗೆಯಲ್ಲಿ ಅಂತಹ ಅಪರಾಧಿಗಳು ಇರಬಹುದು, ಅವರು ಖಾಸಗಿ ಚಿತ್ರಗಳನ್ನು, ವಿಡಿಯೋಗಳನ್ನು ಅಥವಾ ಇತರೆ ದತ್ತಾಂಶಗಳಿಗೆ ಪ್ರವೇಶಾತಿ ಪಡೆಯುತ್ತಾರೆ ಮತ್ತು ಅವುಗಳನ್ನು ವೈರಾಣು ರೀತಿಯಲ್ಲಿ ಹರಡಲು ಕತ್ತಲ ಜಾಲತಾಣಗಳಲ್ಲಿ ಅಪ್‌ಲೋಡ್ ಮಾಡುತ್ತಾರೆ.ಹಾಗೂ ಅವುಗಳನ್ನು ಬೆದರಿಕೆ ಒಡ್ಡಲು ಬಳಸುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಕಲಂ 43ಎ ಮತ್ತು ಕಲಂ 72ಎ: ಈ ಕಲಂಗಳು ಡೇಟಾ ಮತ್ತು ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆಯನ್ನು ರಕ್ಷಿಸುವಲ್ಲಿ ವಿಫಲವಾದರೆ ಪರಿಹಾರವನ್ನು ವ್ಯವಹರಿಸುತ್ತವೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 406– ವಿಶ್ವಾಸ ಭಂಗದ ಅಪರಾಧಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಆನ್‌ಲೈನ್ ಪ್ರಸರಣಕ್ಕಾಗಿ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಎ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಬಿ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವಿನಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿ ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಾಯ್ದೆಗಳು

ಐಪಿಸಿ ಕಲಂ 506/ಬಿಎನ್‌ಎಸ್ 351– ಅಪರಾಧಿ ಬೆದರಿಕೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 507/ಬಿಎನ್‌ಎಸ್ 351(4)– ಅನಾಮಧೇಯ ಸಂವಹನದಿಂದ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ

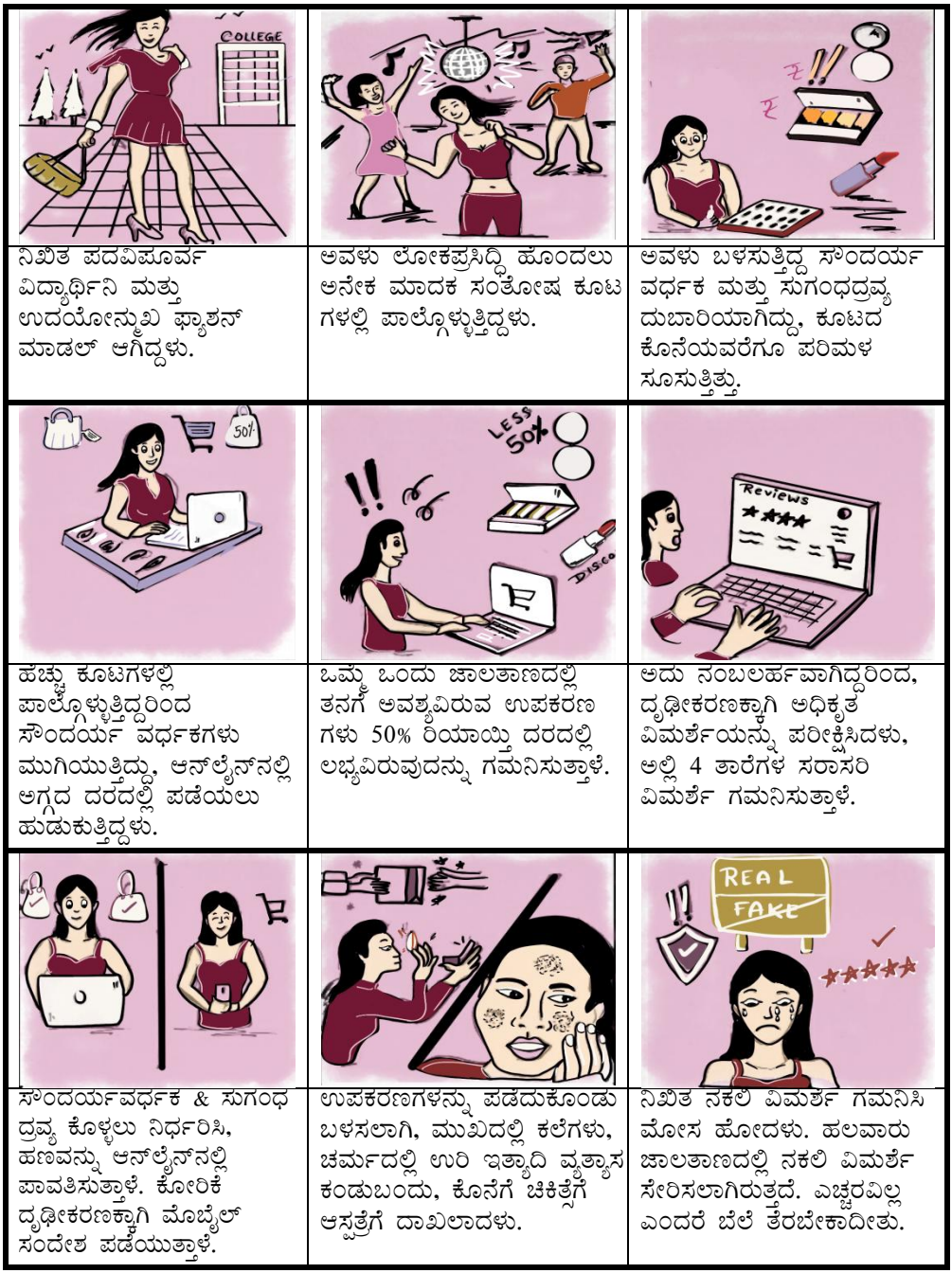
ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನವಾಗುವ ಉದ್ದೇಶದ ಪದಗಳು, ಸನ್ನೆ ಅಥವಾ ಅಭಿನಯ

ಭಾರತೀಯ ಹಕ್ಕುಸ್ವಾಮ್ಯ ಕಾಯಿದೆ, 1957 – ವಿಭಾಗ 63ಬಿ: ಆನ್‌ಲೈನ್ ಹಕ್ಕುಸ್ವಾಮ್ಯ ಉಲ್ಲಂಘನೆ ಹಕ್ಕುಸ್ವಾಮ್ಯವನ್ನು ಉಲ್ಲಂಘಿಸುವ ತಾಂತ್ರಿಕ ಕ್ರಮಗಳನ್ನು ಉದ್ದೇಶಪೂರ್ವಕವಾಗಿ ತಪ್ಪಿಸುವ ಅಪರಾಧದೊಂದಿಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ.

ಇಂತಹ ಮಳಿಗೆಯೊಂದಿಗೆ ಎಚ್ಚರವಿಲ್ಲದಿದ್ದಲ್ಲಿ, ದೊಡ್ಡ ನಷ್ಟಕ್ಕೆ ಬೆಲೆ ತೆರಬೇಕಾದೀತು.

www.cybersafegirl.com

ನಕಲಿ ವಿಮರ್ಶೆ



ನಿಖಿತ ಪದವಿಪೂರ್ವ ವಿದ್ಯಾರ್ಥಿನಿ ಮತ್ತು ಉದಯೋನ್ಮುಖ ಫ್ಯಾಶನ್ ಮಾಡಲ್ ಆಗಿದ್ದಳು.	ಅವಳು ಲೋಕಪ್ರಸಿದ್ಧಿ ಹೊಂದಲು ಅನೇಕ ಮಾದಕ ಸಂತೋಷ ಕೂಟ ಗಳಲ್ಲಿ ಪಾಲ್ಗೊಳ್ಳುತ್ತಿದ್ದಳು.	ಅವಳು ಬಳಸುತ್ತಿದ್ದ ಸೌಂದರ್ಯ ವರ್ಧಕ ಮತ್ತು ಸುಗಂಧದ್ರವ್ಯ ದುಬಾರಿಯಾಗಿದ್ದು, ಕೂಟದ ಕೊನೆಯವರೆಗೂ ಪರಿಮಳ ಸೂಸುತ್ತಿತ್ತು.
ಹೆಚ್ಚು ಕೂಟಗಳಲ್ಲಿ ಪಾಲ್ಗೊಳ್ಳುತ್ತಿದ್ದರಿಂದ ಸೌಂದರ್ಯ ವರ್ಧಕಗಳು ಮುಗಿಯುತ್ತಿದ್ದು, ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಅಗ್ಗದ ದರದಲ್ಲಿ ಪಡೆಯಲು ಹುಡುಕುತ್ತಿದ್ದಳು.	ಒಮ್ಮೆ ಒಂದು ಜಾಲತಾಣದಲ್ಲಿ ತನಗೆ ಅವಶ್ಯವಿರುವ ಉಪಕರಣ ಗಳು 50% ರಿಯಾಯ್ತಿ ದರದಲ್ಲಿ ಲಭ್ಯವಿರುವುದನ್ನು ಗಮನಿಸುತ್ತಾಳೆ.	ಅದು ನಂಬಲರ್ಹವಾಗಿದ್ದರಿಂದ, ದೃಢೀಕರಣಕ್ಕಾಗಿ ಅಧಿಕೃತ ವಿಮರ್ಶೆಯನ್ನು ಪರೀಕ್ಷಿಸಿದಳು, ಅಲ್ಲಿ 4 ತಾರೆಗಳ ಸರಾಸರಿ ವಿಮರ್ಶೆ ಗಮನಿಸುತ್ತಾಳೆ.
ಸೌಂದರ್ಯವರ್ಧಕ & ಸುಗಂಧ ದ್ರವ್ಯ ಕೊಳ್ಳಲು ನಿರ್ಧರಿಸಿ, ಹಣವನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪಾವತಿಸುತ್ತಾಳೆ. ಕೋರಿಕೆ ದೃಢೀಕರಣಕ್ಕಾಗಿ ಮೊಬೈಲ್ ಸಂದೇಶ ಪಡೆಯುತ್ತಾಳೆ.	ಉಪಕರಣಗಳನ್ನು ಪಡೆದುಕೊಂಡು ಬಳಸಲಾಗಿ, ಮುಖದಲ್ಲಿ ಕಲೆಗಳು, ಚರ್ಮದಲ್ಲಿ ಉರಿ ಇತ್ಯಾದಿ ವ್ಯತ್ಯಾಸ ಕಂಡುಬಂದು, ಕೊನೆಗೆ ಚಿಕಿತ್ಸೆಗೆ ಆಸ್ಪತ್ರೆಗೆ ದಾಖಲಾದಳು.	ನಿಖಿತ ನಕಲಿ ವಿಮರ್ಶೆ ಗಮನಿಸಿ ಮೋಸ ಹೋದಳು. ಹಲವಾರು ಜಾಲತಾಣದಲ್ಲಿ ನಕಲಿ ವಿಮರ್ಶೆ ಸೇರಿಸಲಾಗಿರುತ್ತದೆ. ಎಚ್ಚರವಿಲ್ಲ ಎಂದರೆ ಬೆಲೆ ತೆರಬೇಕಾದೀತು.

ಉತ್ಪನ್ನಗಳ ಬಗ್ಗೆ ನಕಲಿ ವಿಮರ್ಶೆಗಳನ್ನು ನೀಡುವ ಮೂಲಕ ಜಾಲತಾಣಗಳು ಗ್ರಾಹಕರನ್ನು ಮೋಸಗೊಳಿಸಬಹುದು.ಅವರು ಗ್ರಾಹಕರನ್ನು ಆಕರ್ಷಿಸಲು ಹಣವನ್ನು ಪಾವತಿಸಿ ಪ್ರಜ್ವಲಿಸುವ ವಿಮರ್ಶೆಗಳನ್ನು ಪಡೆಯುತ್ತಾರೆ, ಇವುಗಳಲ್ಲಿ ವಿಶೇಷವಾಗಿ ರಿಯಾಯಿತಿ ದರಗಳನ್ನು ನೀಡುವುದುಒಂದಾಗಿರುತ್ತದೆ.ಸಂಶಯಾಸ್ಪದ ತಾಣಗಳಲ್ಲಿನ ಈ ಉತ್ಪನ್ನಗಳನ್ನು ಬಳಸಿದರೆ ಹೇಳಲಾಗದ ಹಾನಿಯನ್ನು ಉಂಟುಮಾಡಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 406/ಬಿಎನ್ಎಸ್ 316– ವಿಶ್ವಾಸ ಭಂಗದ ಅಪರಾಧಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318– ಮೋಸ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 43ಎ: ಈ ಕಲಂಗಳು ಡೇಟಾ ಮತ್ತು ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆಯನ್ನು ರಕ್ಷಿಸುವಲ್ಲಿ ವಿಫಲವಾದರೆ ಪರಿಹಾರವನ್ನು ವ್ಯವಹರಿಸುತ್ತವೆ.

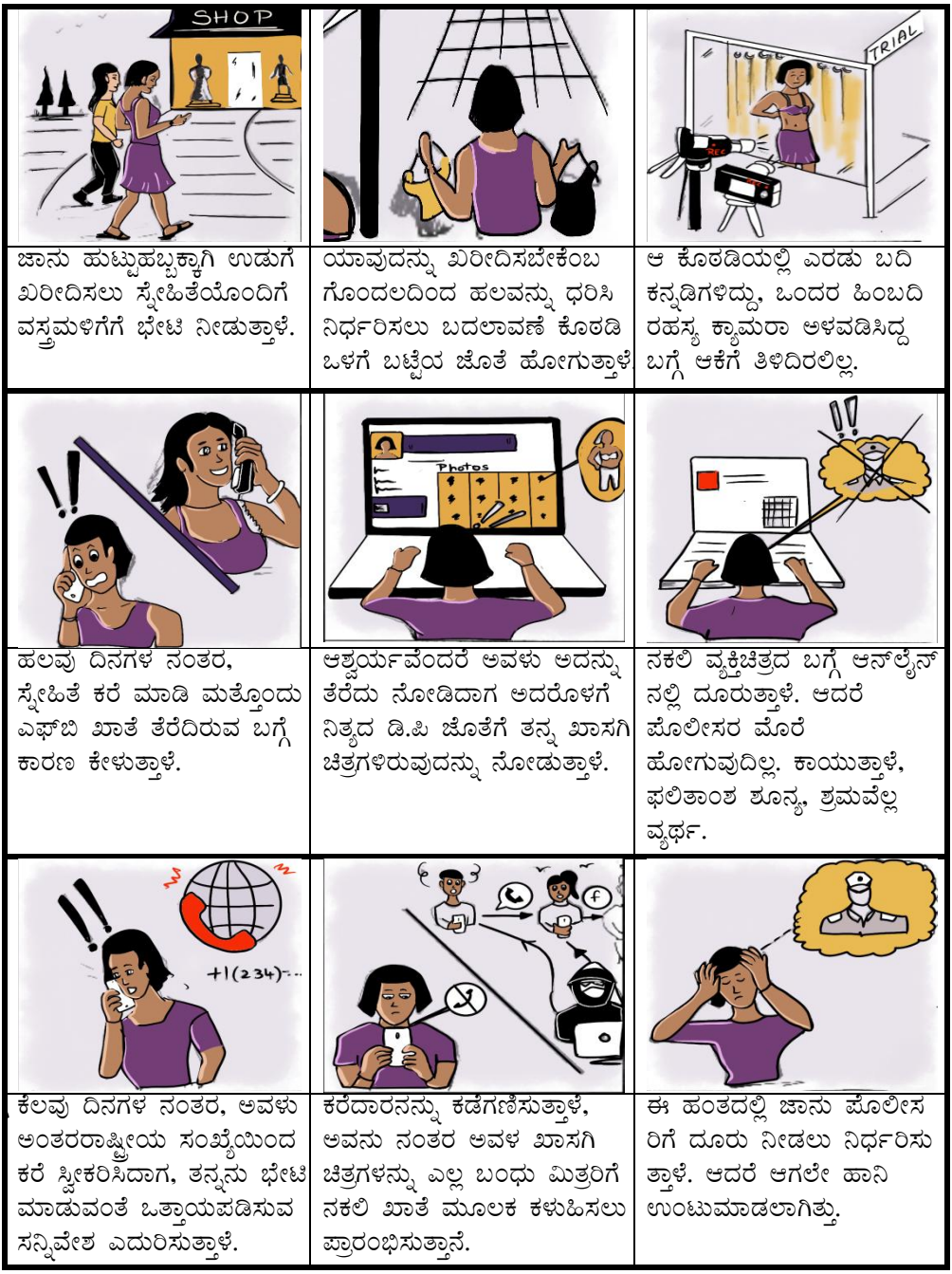
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಎಫ್– ಸೈಬರ್ ಭಯೋತ್ಪಾಚನೆಗಾಗಿ ಶಿಕ್ಷೆ

ನಕಲಿ ವಿಮರ್ಶೆಗಳು ತಪ್ಪು ಆಯ್ಕೆಗೆ ಕಾರಣವಾಗುತ್ತದೆ.

ಲೈಂಗಿಕೋತ್ತಾಯದೊಂದಿಗೆ ನಕಲಿ ವ್ಯಕ್ತಿಚಿತ್ರ (ಸೆಕ್ಸ್‌ಟಾರ್ಷನ್)



ಜಾನು ಹುಟ್ಟುಹಬ್ಬಕ್ಕಾಗಿ ಉಡುಗೆ ಖರೀದಿಸಲು ಸ್ನೇಹಿತೆಯೊಂದಿಗೆ ವಸ್ತ್ರಮಳಿಗೆಗೆ ಭೇಟಿ ನೀಡುತ್ತಾಳೆ.

ಯಾವುದನ್ನು ಖರೀದಿಸಬೇಕೆಂಬ ಗೊಂದಲದಿಂದ ಹಲವನ್ನು ಧರಿಸಿ ನಿರ್ಧರಿಸಲು ಬದಲಾವಣೆ ಕೊಠಡಿ ಒಳಗೆ ಬಟ್ಟೆಯ ಜೊತೆ ಹೋಗುತ್ತಾಳೆ

ಆ ಕೊಠಡಿಯಲ್ಲಿ ಎರಡು ಬದಿ ಕನ್ನಡಿಗಳಿದ್ದು, ಒಂದರ ಹಿಂಬದಿ ರಹಸ್ಯ ಕ್ಯಾಮರಾ ಅಳವಡಿಸಿದ್ದ ಬಗ್ಗೆ ಆಕೆಗೆ ತಿಳಿದಿರಲಿಲ್ಲ.

ಹಲವು ದಿನಗಳ ನಂತರ, ಸ್ನೇಹಿತೆ ಕರೆ ಮಾಡಿ ಮತ್ತೊಂದು ಎಫ್‌ಬಿ ಖಾತೆ ತೆರೆದಿರುವ ಬಗ್ಗೆ ಕಾರಣ ಕೇಳುತ್ತಾಳೆ.

ಆಶ್ಚರ್ಯವೆಂದರೆ ಅವಳು ಅದನ್ನು ತೆರೆದು ನೋಡಿದಾಗ ಅದರೊಳಗೆ ನಿತ್ಯದ ಡಿ.ಪಿ ಜೊತೆಗೆ ತನ್ನ ಖಾಸಗಿ ಚಿತ್ರಗಳಿರುವುದನ್ನು ನೋಡುತ್ತಾಳೆ.

ನಕಲಿ ವ್ಯಕ್ತಿಚಿತ್ರದ ಬಗ್ಗೆ ಆನ್‌ಲೈನ್ ನಲ್ಲಿ ದೂರುತ್ತಾಳೆ. ಆದರೆ ಪೊಲೀಸರ ಮೊರೆ ಹೋಗುವುದಿಲ್ಲ. ಕಾಯುತ್ತಾಳೆ, ಫಲಿತಾಂಶ ಶೂನ್ಯ, ಶ್ರಮವೆಲ್ಲ ವ್ಯರ್ಥ.

ಕೆಲವು ದಿನಗಳ ನಂತರ, ಅವಳು ಅಂತರರಾಷ್ಟ್ರೀಯ ಸಂಖ್ಯೆಯಿಂದ ಕರೆ ಸ್ವೀಕರಿಸಿದಾಗ, ತನ್ನನು ಭೇಟಿ ಮಾಡುವಂತೆ ಒತ್ತಾಯಪಡಿಸುವ ಸನ್ನಿವೇಶ ಎದುರಿಸುತ್ತಾಳೆ.

ಕರೆದಾರನನ್ನು ಕಡೆಗಣಿಸುತ್ತಾಳೆ, ಅವನು ನಂತರ ಅವಳ ಖಾಸಗಿ ಚಿತ್ರಗಳನ್ನು ಎಲ್ಲ ಬಂಧು ಮಿತ್ರರಿಗೆ ನಕಲಿ ಖಾತೆ ಮೂಲಕ ಕಳುಹಿಸಲು ಪ್ರಾರಂಭಿಸುತ್ತಾನೆ.

ಈ ಹಂತದಲ್ಲಿ ಜಾನು ಪೊಲೀಸರಿಗೆ ದೂರು ನೀಡಲು ನಿರ್ಧರಿಸುತ್ತಾಳೆ. ಆದರೆ ಆಗಲೇ ಹಾನಿ ಉಂಟುಮಾಡಲಾಗಿತ್ತು.

ಲೈಂಗಿಕೋತ್ತಾಯದೊಂದಿಗೆ ನಕಲಿ ವ್ಯಕ್ತಿಚಿತ್ರ (ಸೆಕ್ಸ್‌ಟಾರ್ಷನ್)

ಸಾರ್ವಜನಿಕ ವಸ್ತ್ರ ಬದಲಾವಣೆ ಕೋಣೆಗಳಲ್ಲಿ ಆಯಕಟ್ಟಿನ ಜಾಗದಲ್ಲಿ ಕ್ಯಾಮರಾಗಳನ್ನು ಅಳವಡಿಸಿರಬಹುದು.ಅದು ಬಳಕೆದಾರರ ಚಿತ್ರಗಳನ್ನು ಸೆರೆ ಹಿಡಿಯುತ್ತದೆ.ಇಂತಹ ಚಿತ್ರಗಳನ್ನು ನಂತರದಲ್ಲಿ ಸುಲಿಗೆ ಬೆದರಿಕೆ ಮಾಡುವ ದುರುದ್ದೇಶದಿಂದ ನಕಲಿ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಖಾತೆಗಳಲ್ಲಿ ಅಪ್‌ಲೋಡ್ ಮಾಡಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಚಿತ್ರಗಳು/ವಿಡಿಯೋಗಳನ್ನು ಸೆರೆಹಿಡಿಯುವುದು:

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 415/ಬಿಎನ್‌ಎಸ್ 318–ವಂಚನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 416/ಬಿಎನ್‌ಎಸ್ 319– ಗುರುತು ಕಳ್ಳತನದ ವಂಚನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319–ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 354ಎ/ಬಿಎನ್‌ಎಸ್ 75– ಲೈಂಗಿಕ ಕಿರುಕುಳ ಮತ್ತು ಲೈಂಗಿಕ ಕಿರುಕುಳಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 354ಸಿ/ಬಿಎನ್‌ಎಸ್ 77 –ಇತರರ ಲೈಂಗಿಕ ಕೃತ್ಯಗಳನ್ನು ಅನುಕೂಲವಾದ ಸ್ಥಾನದಿಂದ ನೋಡುವ ಪ್ರಯೋಜನ

ಐಪಿಸಿ ಕಲಂ 354 ಡಿ/ಬಿಎನ್‌ಎಸ್ 78–ಹಿಂಬಾಲಿಕೆ

ಐಪಿಸಿ ಕಲಂ 503/ಬಿಎನ್‌ಎಸ್ 351–ಅಪರಾಧಿಕ ಬೆದರಿಕೆ

ಐಪಿಸಿ ಕಲಂ 507/ಬಿಎನ್‌ಎಸ್ 351– ಅನಾಮದೇಯ ಸಂವಹನದಿಂದ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ

ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪ್ರಸರಣ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

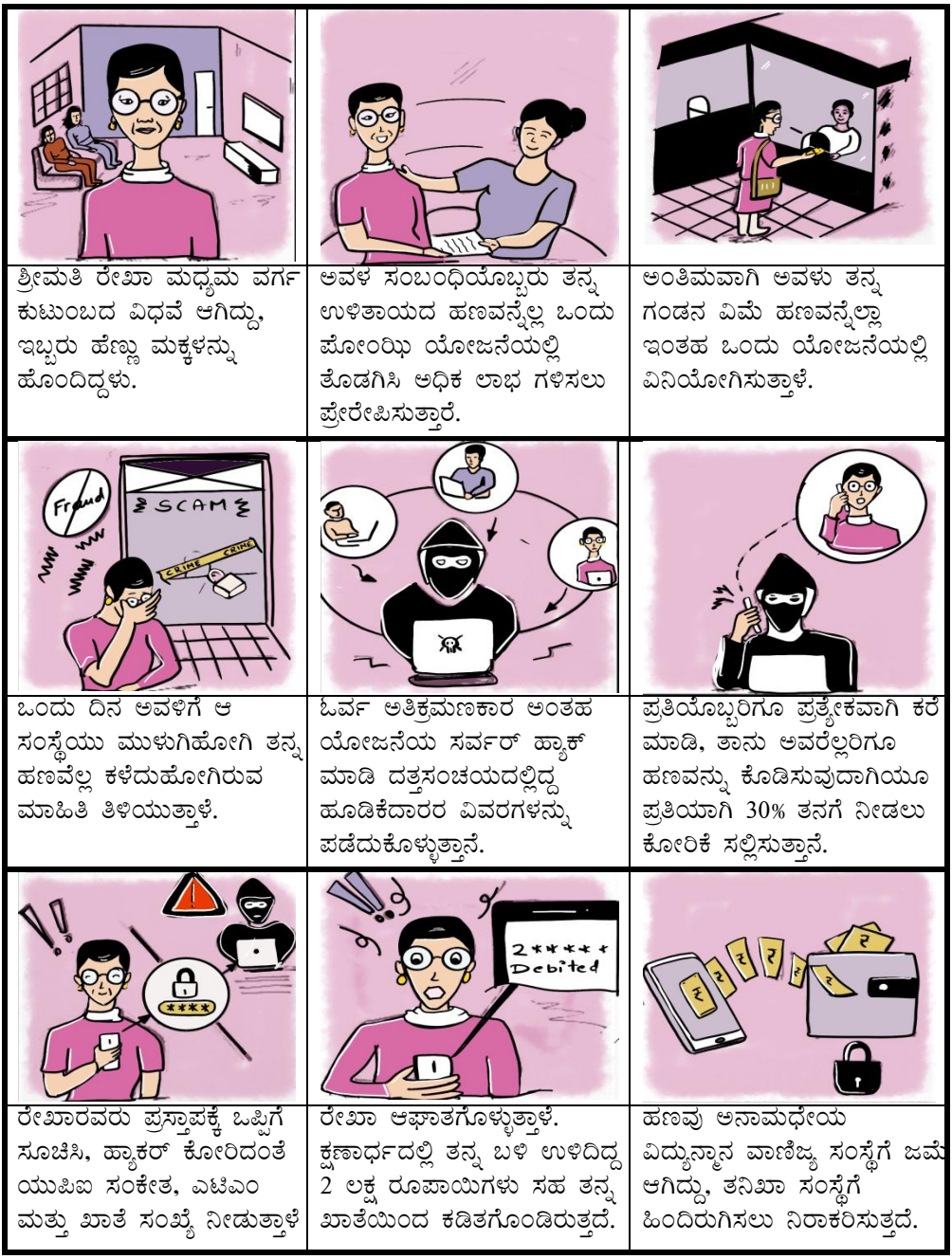
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಎ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಬಿ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವಿನಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿ ವಿದ್ಯುನ್ಮಾನರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಾಯ್ದೆಗಳು

ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನವಾಗುವ ಉದ್ದೇಶದ ಪದಗಳು, ಸನ್ನೆ ಅಥವಾ ಅಭಿನಯ

ಒಬ್ಬ ಮೋಸಗಾರ ಮಾಜಿ ಪ್ರಿಯಕರ ಮರೆಯಲಾರದ ತೊಂದರೆ ನೀಡಬಹುದು

ಸೈಬರ್ ರಣಹದ್ದುಗಳು (ವಲ್ಚರ್)



ಶ್ರೀಮತಿ ರೇಖಾ ಮಧ್ಯಮ ವರ್ಗ ಕುಟುಂಬದ ವಿಧವೆ ಆಗಿದ್ದು, ಇಬ್ಬರು ಹೆಣ್ಣು ಮಕ್ಕಳನ್ನು ಹೊಂದಿದ್ದಳು.	ಅವಳ ಸಂಬಂಧಿಯೊಬ್ಬರು ತನ್ನ ಉಳಿತಾಯದ ಹಣವನ್ನೆಲ್ಲ ಒಂದು ಪೋಂಝಿ ಯೋಜನೆಯಲ್ಲಿ ತೊಡಗಿಸಿ ಅಧಿಕ ಲಾಭ ಗಳಿಸಲು ಪ್ರೇರೇಪಿಸುತ್ತಾರೆ.	ಅಂತಿಮವಾಗಿ ಅವಳು ತನ್ನ ಗಂಡನ ವಿಮೆ ಹಣವನ್ನೆಲ್ಲಾ ಇಂತಹ ಒಂದು ಯೋಜನೆಯಲ್ಲಿ ವಿನಿಯೋಗಿಸುತ್ತಾಳೆ.
ಒಂದು ದಿನ ಅವಳಿಗೆ ಆ ಸಂಸ್ಥೆಯು ಮುಳುಗಿಹೋಗಿ ತನ್ನ ಹಣವೆಲ್ಲ ಕಳೆದುಹೋಗಿರುವ ಮಾಹಿತಿ ತಿಳಿಯುತ್ತಾಳೆ.	ಓರ್ವ ಅತಿಕ್ರಮಣಕಾರ ಅಂತಹ ಯೋಜನೆಯ ಸರ್ವರ್ ಹ್ಯಾಕ್ ಮಾಡಿ ದತ್ತಸಂಚಯದಲ್ಲಿದ್ದ ಹೂಡಿಕೆದಾರರ ವಿವರಗಳನ್ನು ಪಡೆದುಕೊಳ್ಳುತ್ತಾನೆ.	ಪ್ರತಿಯೊಬ್ಬರಿಗೂ ಪ್ರತ್ಯೇಕವಾಗಿ ಕರೆ ಮಾಡಿ, ತಾನು ಅವರೆಲ್ಲರಿಗೂ ಹಣವನ್ನು ಕೊಡಿಸುವುದಾಗಿಯೂ ಪ್ರತಿಯಾಗಿ 30% ತನಗೆ ನೀಡಲು ಕೋರಿಕೆ ಸಲ್ಲಿಸುತ್ತಾನೆ.
ರೇಖಾರವರು ಪ್ರಸ್ತಾಪಕ್ಕೆ ಒಪ್ಪಿಗೆ ಸೂಚಿಸಿ, ಹ್ಯಾಕರ್ ಕೋರಿದಂತೆ ಯುಪಿಐ ಸಂಕೇತ, ಎಟಿಎಂ ಮತ್ತು ಖಾತೆ ಸಂಖ್ಯೆ ನೀಡುತ್ತಾಳೆ	ರೇಖಾ ಆಘಾತಗೊಳ್ಳುತ್ತಾಳೆ. ಕ್ಷಣಾರ್ಧದಲ್ಲಿ ತನ್ನ ಬಳಿ ಉಳಿದಿದ್ದ 2 ಲಕ್ಷ ರೂಪಾಯಿಗಳು ಸಹ ತನ್ನ ಖಾತೆಯಿಂದ ಕಡಿತಗೊಂಡಿರುತ್ತದೆ.	ಹಣವು ಅನಾಮಧೇಯ ವಿದ್ಯುನ್ಮಾನ ವಾಣಿಜ್ಯ ಸಂಸ್ಥೆಗೆ ಜಮೆ ಆಗಿದ್ದು, ತನಿಖಾ ಸಂಸ್ಥೆಗೆ ಹಿಂದಿರುಗಿಸಲು ನಿರಾಕರಿಸುತ್ತದೆ.

ಸೈಬರ್ ರಣಹದ್ದುಗಳು ಸರ್ವರ್‌ಗಳಿಗೆ ಅತಿಕ್ರಮಣ ಪ್ರವೇಶ ಪಡೆಯುವ ಚಾಕಚಕ್ಯತೆ ಹೊಂದಿರುತ್ತಾರೆ.ಅವರುಗಳು ಯಾವುದೇ ರೀತಿಯ ದಾಳಿಯಿಂದ ಬಳಲುತ್ತಿರುವ ಗ್ರಾಹಕರು ಮತ್ತು ವಾಣಿಜ್ಯೋದ್ಯಮದ ದುರ್ಲಾಭ ಪಡೆಯುತ್ತಾರೆ.ಇಂತಹ ಸನ್ನಿವೇಶವನ್ನು ಅವರು ಮೋಸಗೊಳಿಸಲು ಮತ್ತು ಹೆಚ್ಚಿನ ಹಣವನ್ನು ಸುಲಿಗೆ ಮಾಡುವ ಒಂದು ಅವಕಾಶವನ್ನಾಗಿ ಪರಿವರ್ತಿಸಿಕೊಳ್ಳುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಎ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಹಣಕಾಸು ಸಂಸ್ಥೆಗಳಂತೆ ಪ್ರತಿರೂಪಣ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲವನ್ನುಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

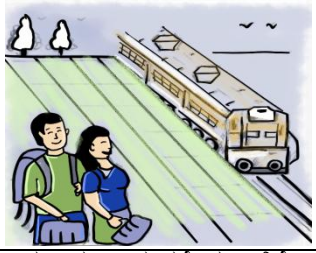
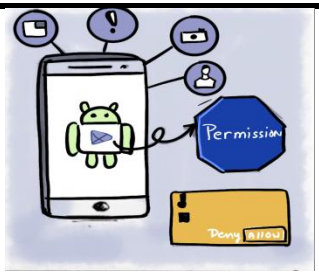
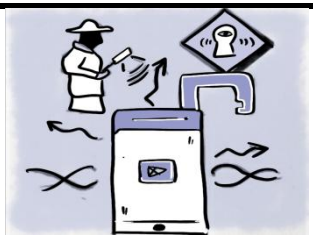
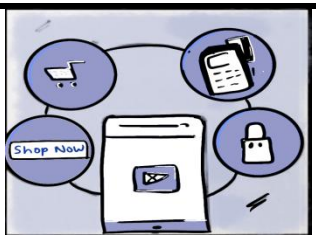
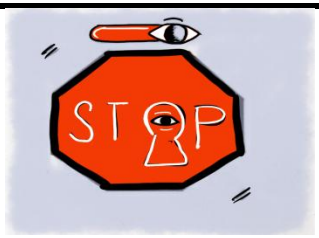
ವೈಯಕ್ತಿಕ/ಬ್ಯಾಂಕಿಂಗ್/ಕ್ರೆಡಿಟ್, ಇತ್ಯಾದಿ ಮಾಹಿತಿಗಳ ಸೆಳೆಯುವಿಕೆ:

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ರಣಹದ್ದುಗಳು ಸತ್ತ ಜೀವಿಗಳನ್ನು ಅವಲಂಬಿಸಿ ಜೀವಿಸುತ್ತವೆ. ಸೈಬರ್ ರಣಹದ್ದುಗಳು ಈಗಾಗಲೇ ಹಣಕಾಸು ನಷ್ಟದಿಂದ ಕುಗ್ಗಿರುವವರನ್ನು ಅವಲಂಬಿಸಿ ಜೀವಿಸುತ್ತಾರೆ

ಅನ್ವಯಿಕೆ(ಆ್ಯಪ್) ಬಲೆ

		
ವಿದ್ಯ ಮತ್ತು ರಾಜು ಪರಸ್ಪರ 5 ವರ್ಷಗಳಿಂದ ಪ್ರಣಯವಿಹಾರ ನಡೆಸುತ್ತಿದ್ದು, ಇಬ್ಬರ ನಡುವೆ ಅವಿನಾಭಾವ ಸಂಬಂಧ ಏರ್ಪಟ್ಟಿತ್ತು.	ಅವರಿಬ್ಬರು ವಾರಂತ್ಯಕ್ಕೆ ಮನಾಲಿಗೆ ಭೇಟಿ ನೀಡಲು ನಿರ್ಧರಿಸಿ, ಬಟ್ಟೆಗಳನ್ನು ಹೊಂದಿಸಿಕೊಂಡು ಲಗೇಜಿನೊಂದಿಗೆ ರೈಲ್ವೆ ನಿಲ್ದಾಣಕ್ಕೆ ತೆರಳುತ್ತಾರೆ.	ಮನಾಲಿಯಲ್ಲಿ 3 ದಿನಗಳನ್ನು ಸಂತಸದಿಂದ ಕಳೆದು ಮಧುರ ನೆನಪುಗಳೊಂದಿಗೆ ಮನೆಗೆ ಹಿಂದಿರುಗುತ್ತಾರೆ.
		
ವಿದ್ಯ ತನ್ನ ಋತುಚಕ್ರ ಮತ್ತು ಇತರೆ ಆರೋಗ್ಯ ವಿಚಾರಗಳ ಬಗ್ಗೆ ಮೊಬೈಲ್ ಆ್ಯಪ್ ಒಂದನ್ನು ಬಳಸುತ್ತಿದ್ದಳು.	ಆದರೆ ಈ ತಿಂಗಳು, ಆ್ಯಪ್‌ನಲ್ಲಿ ಏರಿಳಿತವಾಗಿತ್ತು, ಅವಳು ಗರ್ಭಿಣಿ ಆಗಿರುವ ಬಗ್ಗೆ ಗಾಬರಿಯಾದಳು. ಆ್ಯಪ್‌ನಲ್ಲಿ ಇತರೆ ವೈಶಿಷ್ಟಗಳನ್ನು ಖಾತರಿಗಾಗಿ ಪರೀಕ್ಷಿಸಿದಳು.	ಆ್ಯಪ್ ಮೊಬೈಲ್‌ನ ಇತರೆ ಆಪ್ ನಂತೆಯೇ ಅನುಮತಿ ಪಡೆದು ಮೊಬೈಲ್‌ನ ಕ್ಯಾಮರ, ಸಂಗ್ರಹ, ಸಂಪರ್ಕ ಇತರೆ ವೈಶಿಷ್ಟ್ಯಗಳಿಗೆ ಪ್ರವೇಶಾನುಮತಿ ಪಡೆದಿತ್ತು.
		
ಈ ದತ್ತಾಂಶವನ್ನು ಗರ್ಭನಿರೋಧಕ ಸಂಸ್ಥೆಗಳಿಗೆ ರವಾನಿಸಿದ್ದವು. ಇದರಿಂದ ಅವಳ ಖಾಸಗೀತನ ಧಕ್ಕೆ ಉಂಟಾಯಿತು.	ಪರಿಸ್ಥಿತಿಯನ್ನು ದುರುಪಯೋಗ ಪಡಿಸಿಕೊಂಡು, ಆ್ಯಪ್‌ನವರು ಕೆಲವು ಪರೀಕ್ಷಣಾ ಕಿಟ್ ರಿಯಾಯಿತಿ ದರದಲ್ಲಿ ಖರೀದಿಸಲು ಸೂಚಿಸುತ್ತಿದ್ದಿತು.	ಒಮ್ಮೆ ಆ್ಯಪ್‌ಗೆ ಅನುಮತಿ ನೀಡುವುದರಿಂದ, ಆ್ಯಪ್‌ನವರು ಮೊಬೈಲ್‌ನ ಎಲ್ಲಾ ಸಂಗ್ರಹ, ವಿವರಗಳನ್ನು ನಕಲಿಸಿಟ್ಟುಕೊಳ್ಳಲು ಸಾಧ್ಯವಾಗುತ್ತದೆ.

ಅಂತರ್ಜಾಲದ ಸೇವೆಯು ಗುಪ್ತ ವೆಚ್ಚಗಳನ್ನೂ ಸಹ ಒಳಗೊಂಡಿರುತ್ತದೆ.ಇವುಗಳಲ್ಲಿ ಬಳಕೆದಾರರ ದತ್ತಾಂಶವನ್ನು ಅವರಿಗೆ ತಿಳಿಯದೆಯೇ ಕಳ್ಳತನ ಮಾಡಿಕೊಳ್ಳುವಂತಹ ಪೂರ್ವ ಸ್ಥಾಪಿಸಲಾದ ಆ್ಯಪ್‌ಗಳು ಸಹ ಒಂದು.ಇಂತಹ ಅನ್ವಯಿಕೆಗಳು ಫೋನ್‌ನಲ್ಲಿರುವ ಸಂಗ್ರಹವನ್ನು ಪ್ರವೇಶಿಸಲು ಅನುಮತಿ ಕೇಳುತ್ತವೆ ಮತ್ತು ಒಮ್ಮೆ ಅನುಮತಿ ನೀಡಿದರೆ, ಅವರು ಫೋಟೋ, ವಿಡಿಯೋ ಮತ್ತು ಸಂಗ್ರಹಣೆಯನ್ನು ಬಳಸಿಕೊಳ್ಳಬಹುದು.ಇದು ಮಾತ್ರವಲ್ಲದೆ ಬಿಟ್‌ಕಾಯಿನ್ ಮೈನ್ ಮಾಡಲು ಅಂತರ್ಜಾಲದದತ್ತಾಂಶವನ್ನು ಬಳಸುತ್ತಾರೆ. ಜೊತೆಗೆ ಇತರೆ ದುರುದ್ದೇಶಪೂರಿತ ಕಾರ್ಯಗಳಿಗೂ ಬಳಸಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 406/ಬಿಎನ್‌ಎಸ್ 316– ವಿಶ್ವಾಸ ಭಂಗದ ಅಪರಾಧಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

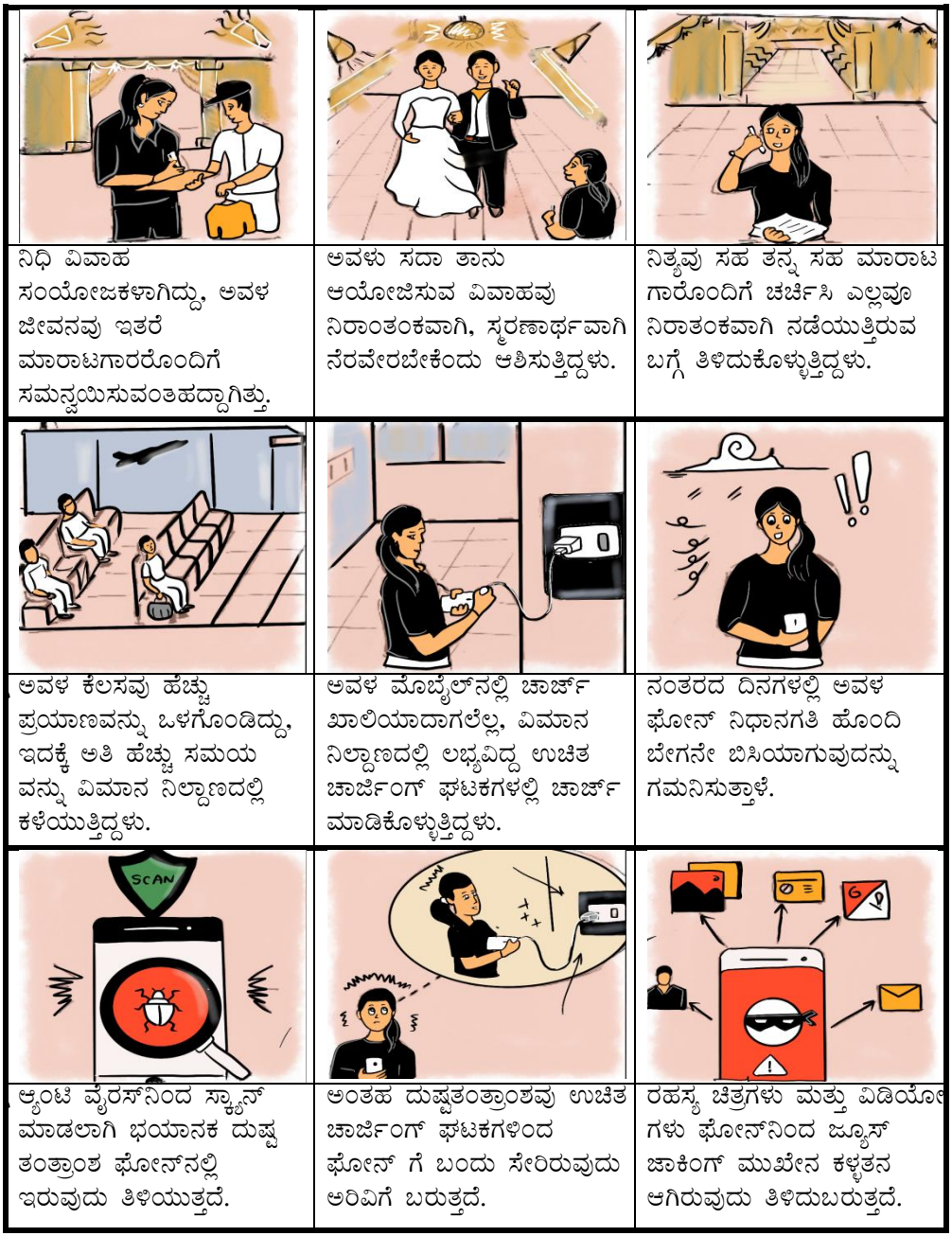
ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಮ.ತ.ಕಾಯ್ದೆ ಕಲಂ 43ಎ: ಈ ಕಲಂ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸುವಲ್ಲಿ ವಿಫಲತೆಯ ಪರಿಹಾರದೊಂದಿಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ. ಸೂಕ್ಷ್ಮವಾದ ವೈಯಕ್ತಿಕ ಡೇಟಾವನ್ನು ನಿರ್ವಹಿಸುವ ಸಂಸ್ಥೆಗಳು ಅಂತಹ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸಲು ಸಮಂಜಸವಾದ ಭದ್ರತಾ ಅಭ್ಯಾಸಗಳನ್ನು ಅಳವಡಿಸಿಕೊಳ್ಳಬೇಕಾಗುತ್ತದೆ. ಅವರು ಹಾಗೆ ಮಾಡಲು ವಿಫಲವಾದರೆ ಮತ್ತು ಅದರ ಪರಿಣಾಮವಾಗಿ ವ್ಯಕ್ತಿಯು ಹಾನಿಯನ್ನು ಅನುಭವಿಸಿದರೆ, ಸಂಸ್ಥೆಯು ಪರಿಹಾರವನ್ನು ಪಾವತಿಸಲು ಹೊಣೆಗಾರನಾಗಬಹುದು.

ಕಲಂ 66: ಈ ಕಲಂ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಕಳ್ಳತನ ಮತ್ತು ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಹಾನಿ ಸೇರಿದಂತೆ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳೊಂದಿಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ.

ಇಂತಹ ಬಲೆಗಳನ್ನು ಸದ್ದಿಲ್ಲದೇ ಬೀಸಲಾಗಿ ಅದು ನಿಮ್ಮ ಅತ್ಯಮೂಲ್ಯ ವೈಯಕ್ತಿಕ ದತ್ತಾಂಶವನ್ನು ಕದಿಯುತ್ತದೆ.

ಜ್ಯೂಸ್ ಜಾಕಿಂಗ್


ನಿಧಿ ವಿವಾಹ ಸಂಯೋಜಕಳಾಗಿದ್ದು, ಅವಳ ಜೀವನವು ಇತರೆ ಮಾರಾಟಗಾರರೊಂದಿಗೆ ಸಮನ್ವಯಿಸುವಂತಹದ್ದಾಗಿತ್ತು.
ಅವಳು ಸದಾ ತಾನು ಆಯೋಜಿಸುವ ವಿವಾಹವು ನಿರಾಂತಂಕವಾಗಿ, ಸ್ಮರಣಾರ್ಥವಾಗಿ ನೆರವೇರಬೇಕೆಂದು ಆಶಿಸುತ್ತಿದ್ದಳು.
ನಿತ್ಯವು ಸಹ ತನ್ನ ಸಹ ಮಾರಾಟ ಗಾರೊಂದಿಗೆ ಚರ್ಚಿಸಿ ಎಲ್ಲವೂ ನಿರಾತಂಕವಾಗಿ ನಡೆಯುತ್ತಿರುವ ಬಗ್ಗೆ ತಿಳಿದುಕೊಳ್ಳುತ್ತಿದ್ದಳು.
ಅವಳ ಕೆಲಸವು ಹೆಚ್ಚು ಪ್ರಯಾಣವನ್ನು ಒಳಗೊಂಡಿದ್ದು, ಇದಕ್ಕೆ ಅತಿ ಹೆಚ್ಚು ಸಮಯ ವನ್ನು ವಿಮಾನ ನಿಲ್ದಾಣದಲ್ಲಿ ಕಳೆಯುತ್ತಿದ್ದಳು.
ಅವಳ ಮೊಬೈಲ್‌ನಲ್ಲಿ ಚಾರ್ಜ್ ಖಾಲಿಯಾದಾಗಲೆಲ್ಲ, ವಿಮಾನ ನಿಲ್ದಾಣದಲ್ಲಿ ಲಭ್ಯವಿದ್ದ ಉಚಿತ ಚಾರ್ಜಿಂಗ್ ಘಟಕಗಳಲ್ಲಿ ಚಾರ್ಜ್ ಮಾಡಿಕೊಳ್ಳುತ್ತಿದ್ದಳು.
ನಂತರದ ದಿನಗಳಲ್ಲಿ ಅವಳ ಫೋನ್ ನಿಧಾನಗತಿ ಹೊಂದಿ ಬೇಗನೇ ಬಿಸಿಯಾಗುವುದನ್ನು ಗಮನಿಸುತ್ತಾಳೆ.
SCAN
ಆ್ಯಂಟಿ ವೈರಸ್‌ನಿಂದ ಸ್ಕ್ಯಾನ್ ಮಾಡಲಾಗಿ ಭಯಾನಕ ದುಷ್ಟ ತಂತ್ರಾಂಶ ಫೋನ್‌ನಲ್ಲಿ ಇರುವುದು ತಿಳಿಯುತ್ತದೆ.
ಅಂತಹ ದುಷ್ಟತಂತ್ರಾಂಶವು ಉಚಿತ ಚಾರ್ಜಿಂಗ್ ಘಟಕಗಳಿಂದ ಫೋನ್ ಗೆ ಬಂದು ಸೇರಿರುವುದು ಅರಿವಿಗೆ ಬರುತ್ತದೆ.
ರಹಸ್ಯ ಚಿತ್ರಗಳು ಮತ್ತು ವಿಡಿಯೋ ಗಳು ಫೋನ್‌ನಿಂದ ಜ್ಯೂಸ್ ಜಾಕಿಂಗ್ ಮುಖೇನ ಕಳ್ಳತನ ಆಗಿರುವುದು ತಿಳಿದುಬರುತ್ತದೆ.

ಜ್ಯೂಸ್ ಜಾಕಿಂಗ್ ಎನ್ನುವುದು ಒಂದು ರೀತಿಯ ಸೈಬರ್ ದಾಳಿಯಾಗಿದ್ದು, ಅದು ಚಾರ್ಜಿಂಗ್ ಪೋರ್ಟ್‌ಅನ್ನು ದತ್ತ ಸಂಪರ್ಕವನ್ನಾಗಿ ಬಳಸಿಕೊಳ್ಳುತ್ತದೆ, ಸಾಮಾನ್ಯವಾಗಿ ಯುಎಸ್‌ಬಿ ಮೂಲಕ.ಇದು ಮಾಲ್ವೇರ್ ಅನ್ನು ಸ್ಥಾಪಿಸುವುದು ಅಥವಾ ಸ್ಮಾರ್ಟ್ ಫೋನ್ ಅಥವಾ ಇತರೆ ಗಣಕಯಂತ್ರ ಸಾಧನಗಳಲ್ಲಿನ ಸೂಕ್ಷ್ಮ ದತ್ತಾಂಶವನ್ನು ನಕಲಿಸುವುದನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ.ಸಾರ್ವಜನಿಕ ಸ್ಥಳಗಳಲ್ಲಿ ಚಾರ್ಜಿಂಗ್ ಪೋರ್ಟ್‌ಗಳು ಜ್ಯೂಸ್ ಜಾಕಿಂಗ್‌ಗೆ ಪ್ರಮುಖ ಸ್ಥಳವಾಗಿವೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅಪ್ರಮಾಣಿಕವಾಗಿ ಅಥವಾ ದುರುದ್ದೇಶದಿಂದ ವಿದ್ಯುನ್ಮಾನ ಸಹಿ/ಗುಪ್ತಪದ/ಅನನ್ಯ ಗುರುತು ವೈಶಿಷ್ಟ್ಯವನ್ನು ಬಳಕೆ ಮಾಡಿಕೊಳ್ಳುವುದು.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲವನ್ನುಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 72– ಗೌಪ್ಯತೆ ಮತ್ತು ವೈಯಕ್ತಿಕ ರಹಸ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ದಂಡ

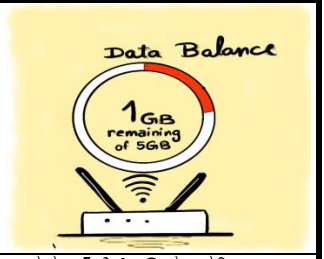
ದತ್ತಾಂಶ ಕಳ್ಳತನ – ಐಪಿಸಿ 379/ಬಿಎನ್‌ಎಸ್ 303

ನಿಮ್ಮ ಅತ್ಯಮೂಲ್ಯ ದತ್ತಾಂಶವನ್ನು ಅಪರಾಧಿಗಳಿಗೆ ಬ್ಯಾಟರಿ ಚಾರ್ಜಿಂಗ್ ನೆಪದಲ್ಲಿ ನೀವೇ ನೀಡಿದಂತಾಗುತ್ತದೆ

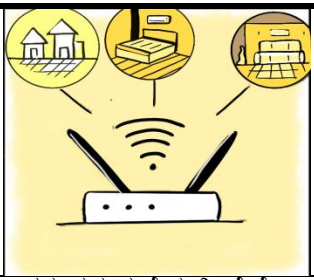
ವೈಫೈ ಅತಿಕ್ರಮಣ

ದಿವ್ಯ ಚಲನಚಿತ್ರಗಳ ವೀಕ್ಷಣೆಯ ಹವ್ಯಾಸಿಯಾಗಿದ್ದು, ಪ್ರತಿದಿನ ಕನಿಷ್ಟ 2 ಚಲನಚಿತ್ರಗಳನ್ನು ನೆಟ್‌ಫ್ಲಿಕ್ಸ್‌ನಲ್ಲಿ ವೀಕ್ಷಿಸುತ್ತಿದ್ದಳು.

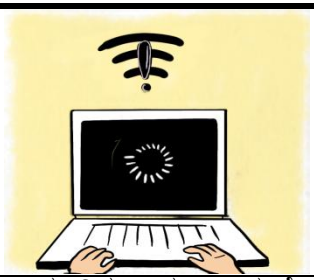
ಚಲನಚಿತ್ರಗಳನ್ನು ಮುಖ್ಯವಾಸ ಕೋಣೆಯ ಸ್ಮಾರ್ಟ್ ಟಿವಿ ಅಥವಾ ಮಲಗುವ ಕೋಣೆಯಲ್ಲಿ ಲ್ಯಾಪ್ ಟಾಪ್‌ನಲ್ಲಿ ವೀಕ್ಷಿಸುತ್ತಿದ್ದಳು.



ಅವಳು 5ಜಿಬಿ ದಿನಂಪ್ರತಿ ಜಾಲ ಯೋಜನೆ ಚಂದಾದಾರಳಾಗಿದ್ದು, ದಿನದ ಕೊನೆಯಲ್ಲಿ 1ಜಿಬಿ ದತ್ತ ಮಾತ್ರ ಉಳಿಕೆಯಾಗುತ್ತಿತ್ತು.



ಅವಳ ನಡುಮನೆಯಲ್ಲಿ ವೈಫೈ ರೌಟರ್ ಹೊಂದಿದ್ದು ಅಲೆಗಳ ಸಾಮರ್ಥ್ಯ ಅತಿಯಾಗಿದ್ದು, ಎಲ್ಲ ಕೊಠಡಿಗೂ ತಲುಪುವ ಸಾಮರ್ಥ್ಯ ಹೊಂದಿತ್ತು.



ಒಂದು ದಿನ ಅಂತರ್ಜಾಲದ ವೇಗ ಕುಗ್ಗಿರುವ ವ್ಯತ್ಯಾಸ ಕಂಡುಬಂದಿದ್ದು ಅದರಿಂದ ಚಲನಚಿತ್ರ ವೀಕ್ಷಣೆ ತುಂಡು–ತುಂಡಾಗಿ ಪ್ರಸಾರ ಆಗುತ್ತಿತ್ತು.

ತಕ್ಷಣ ಅವಳ ಲ್ಯಾಪ್‌ಟಾಪ್‌ನಲ್ಲಿ ಫೈಲ್‌ಗಳು ಹಿಂಬದಿಯಲ್ಲಿ ಡೌನ್‌ಲೋಡ್ ಆಗುತ್ತಿರುವ ಬಗ್ಗೆ ಪರೀಕ್ಷಿಸುತ್ತಾಳೆ.

ತಕ್ಷಣ ಅವಳು ರೌಟರ್‌ನ ನಿರ್ವಾಹಕ ಪರದೆಗೆ ಲಾಗಿನ್ ಆಗುತ್ತಾಳೆ. ಆಶ್ಚರ್ಯಕರವಾಗಿ ಮೂರನೇ ಉಪಕರಣವು ಕೂಡಿ ಕೊಂಡಿರುವುದು ತಿಳಿಯುತ್ತದೆ.

ಅವಳ ನೆರೆಹೊರೆಯವರು ಅವಳ ವೈಫೈ ಸಿಗ್ನಲ್ ಬಳಕೆ ಮಾಡಿ ಉಪಯೋಗಿಸುತ್ತಿರುವುದು ಅರಿವಿಗೆ ಬರುತ್ತದೆ. ಇದು ಸುಲಭ ಗುಪ್ತಪದ ಬಳಕೆಯಿಂದ ಆದ ತಪ್ಪಾಗಿರುತ್ತದೆ.

ಕಡೆಯದಾಗಿ ಅವಳಿಗೆ ತನ್ನ ವೈಫೈ ಬಳಸಿ ಮಾದಕವಸ್ತು ಮಾರಾಟ ಮತ್ತು ಅಶ್ಲೀಲ ವಸ್ತು ವೀಕ್ಷಣೆ ಯನ್ನು ಡಾರ್ಕ್ ವೆಬ್ ಮೂಲಕ ಮಾಡುತ್ತಿದ್ದುದು ಅರಿವಿಗೆ ಬರುತ್ತದೆ

ವೈಫೈ ಆತಿಕ್ರಮಣ ಮೂಲಭೂತವಾಗಿ ವೈರ್‌ಲೆಸ್ ಜಾಲಬಂಧಗಳಲ್ಲಿ, ಆಕ್ರಮಣಕಾರರಿಗೆ ವೀಕ್ಷಿಸಲು, ಸಂಗ್ರಹಿಸಲು, ಡೌನ್‌ಲೋಡ್ ಮಾಡಿಕೊಳ್ಳಲು ಅಥವಾ ದುರುಪಯೋಗ ಪಡಿಸಿಕೊಳ್ಳಲು ಸಂಪೂರ್ಣ ಪ್ರವೇಶಾನುಮತಿಯನ್ನು ನೀಡುವಂತಹದಾಗಿದ್ದು, ಭದ್ರತಾ ಪ್ರೋಟೋಕಾಲ್‌ಗಳನ್ನು ಉಲ್ಲಂಘಿಸುತ್ತವೆ. ವೈಫೈ ಜಾಲಬಂಧಗಳಲ್ಲಿ ಬಳಸಲಾಗುವ ದುರ್ಬಲ ಗುಪ್ತಪದಗಳು ಸುತ್ತಮುತ್ತ ಲಭ್ಯವಿರುವ ವೈಫೈ ಸಂಪರ್ಕದ ಮೂಲಕ ಆತಿಕ್ರಮಣಕಾರರಿಗೆ ಒಳಪ್ರವೇಶಿಸಲು ಅನುವು ಮಾಡಿಕೊಡುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಬಿ– ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಕಳ್ಳತನದ ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಅಥವಾ ಸಂವಹನ ಸಾಧನವನ್ನು ಸ್ವೀಕರಿಸಿದರೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅಪ್ರಮಾಣಿಕವಾಗಿ ಅಥವಾ ದುರುದ್ದೇಶದಿಂದ ವಿದ್ಯುನ್ಮಾನ ಸಹಿ/ಗುಪ್ತಪದ/ಅನನ್ಯ ಗುರುತು ವೈಶಿಷ್ಟ್ಯವನ್ನು ಬಳಕೆ ಮಾಡಿಕೊಳ್ಳುವುದು.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 72. ಗೌಪ್ಯತೆ ಮತ್ತು ವೈಯಕ್ತಿಕ ರಹಸ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ದಂಡ

ಅಂತರ್ಜಾಲ ದತ್ತಾಂಶದ ಅಕ್ರಮ ಲಾಭ ಅಥವ ಅಕ್ರಮ ನಷ್ಟ:

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಅಂತರ್ಜಾಲ ಉಪಯೋಗದ ಕಿರುಕುಳ:

ಐಪಿಸಿ ಕಲಂ 425&426/ಬಿಎನ್‌ಎಸ್ 324 –ಕಿಡಿಗೇಡಿತನ

ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪ್ರಸರಣ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

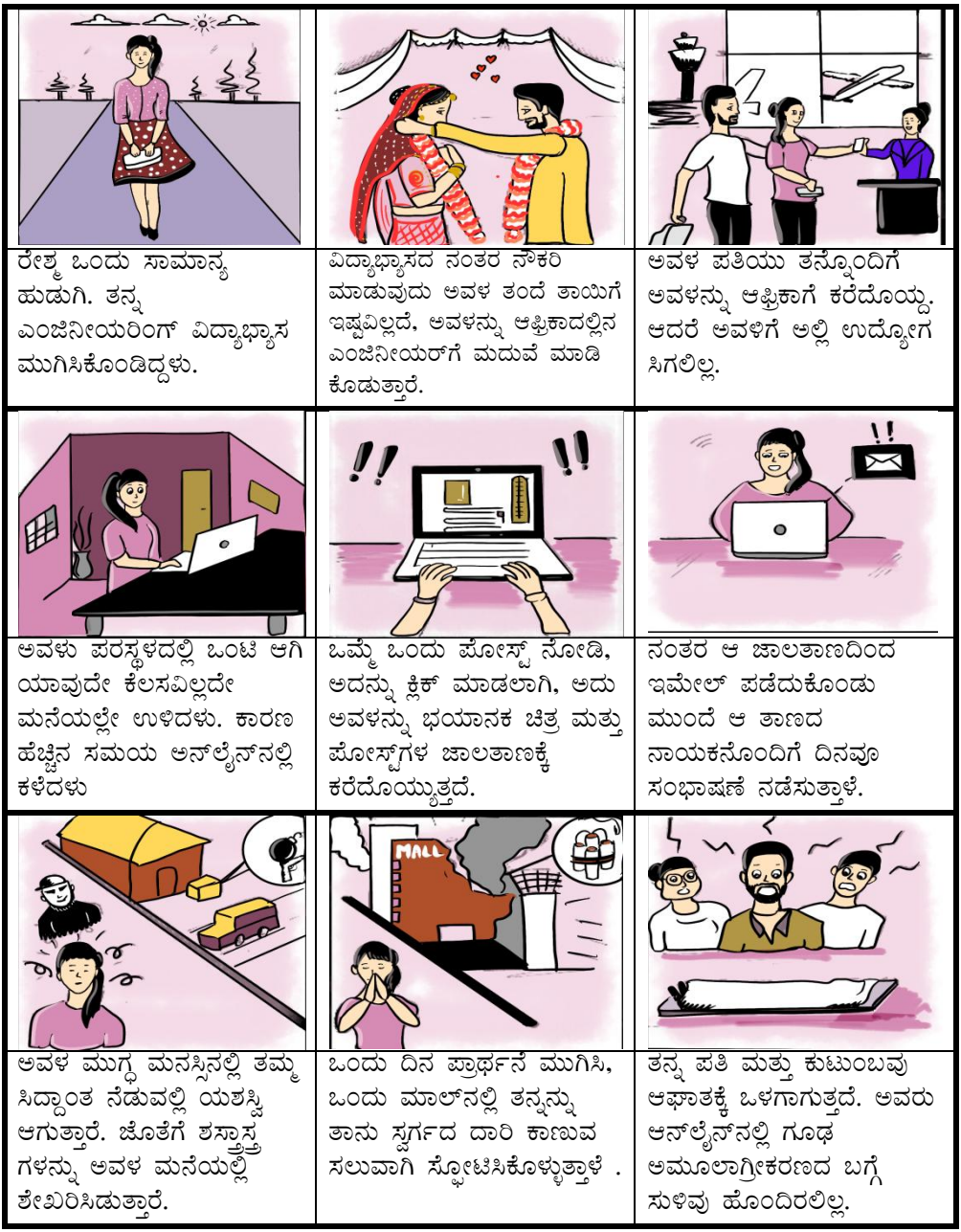
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಎ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಬಿ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವಿನಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿ ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಾಯ್ದೆಗಳು

ಮಾದಕ ದ್ರವ್ಯ ಮತ್ತು ಮಾದಕ ವಸ್ತುಗಳ ಕಾಯ್ದೆ, 1985ರ ಇತರೆ ನಿಬಂಧನೆಗಳು

ಸುರಕ್ಷಿತ ಗೌಪ್ಯ ಜೀವನವನ್ನು ನಡೆಸಲು, ನಿಮ್ಮ ವೈಫೈಅನ್ನು ಸುರಕ್ಷಿತವಾಗಿಡಿ

ಆನ್‌ಲೈನ್ ಆಮೂಲಾಗ್ರೀಕರಣ (ರ್‍ಯಾಡಿಕಲೈಝೇಷನ್)



ರೇಶ್ಮ ಒಂದು ಸಾಮಾನ್ಯ ಹುಡುಗಿ. ತನ್ನ ಎಂಜಿನೀಯರಿಂಗ್ ವಿದ್ಯಾಭ್ಯಾಸ ಮುಗಿಸಿಕೊಂಡಿದ್ದಳು.

ವಿದ್ಯಾಭ್ಯಾಸದ ನಂತರ ನೌಕರಿ ಮಾಡುವುದು ಅವಳ ತಂದೆ ತಾಯಿಗೆ ಇಷ್ಟವಿಲ್ಲದೆ, ಅವಳನ್ನು ಆಫ್ರಿಕಾದಲ್ಲಿನ ಎಂಜಿನೀಯರ್‌ಗೆ ಮದುವೆ ಮಾಡಿ ಕೊಡುತ್ತಾರೆ.

ಅವಳ ಪತಿಯು ತನ್ನೊಂದಿಗೆ ಅವಳನ್ನು ಆಫ್ರಿಕಾಗೆ ಕರೆದೊಯ್ದ. ಆದರೆ ಅವಳಿಗೆ ಅಲ್ಲಿ ಉದ್ಯೋಗ ಸಿಗಲಿಲ್ಲ.

ಅವಳು ಪರಸ್ಥಳದಲ್ಲಿ ಒಂಟಿ ಆಗಿ ಯಾವುದೇ ಕೆಲಸವಿಲ್ಲದೇ ಮನೆಯಲ್ಲೇ ಉಳಿದಳು. ಕಾರಣ ಹೆಚ್ಚಿನ ಸಮಯ ಅನ್‌ಲೈನ್‌ನಲ್ಲಿ ಕಳೆದಳು

ಒಮ್ಮೆ ಒಂದು ಪೋಸ್ಟ್ ನೋಡಿ, ಅದನ್ನು ಕ್ಲಿಕ್ ಮಾಡಲಾಗಿ, ಅದು ಅವಳನ್ನು ಭಯಾನಕ ಚಿತ್ರ ಮತ್ತು ಪೋಸ್ಟ್‌ಗಳ ಜಾಲತಾಣಕ್ಕೆ ಕರೆದೊಯ್ಯುತ್ತದೆ.

ನಂತರ ಆ ಜಾಲತಾಣದಿಂದ ಇಮೇಲ್ ಪಡೆದುಕೊಂಡು ಮುಂದೆ ಆ ತಾಣದ ನಾಯಕನೊಂದಿಗೆ ದಿನವೂ ಸಂಭಾಷಣೆ ನಡೆಸುತ್ತಾಳೆ.

ಅವಳ ಮುಗ್ಧ ಮನಸ್ಸಿನಲ್ಲಿ ತಮ್ಮ ಸಿದ್ಧಾಂತ ನೆಡುವಲ್ಲಿ ಯಶಸ್ವಿ ಆಗುತ್ತಾರೆ. ಜೊತೆಗೆ ಶಸ್ತ್ರಾಸ್ತ್ರ ಗಳನ್ನು ಅವಳ ಮನೆಯಲ್ಲಿ ಶೇಖರಿಸಿಡುತ್ತಾರೆ.

ಒಂದು ದಿನ ಪ್ರಾರ್ಥನೆ ಮುಗಿಸಿ, ಒಂದು ಮಾಲ್‌ನಲ್ಲಿ ತನ್ನನ್ನು ತಾನು ಸ್ವರ್ಗದ ದಾರಿ ಕಾಣುವ ಸಲುವಾಗಿ ಸ್ಫೋಟಿಸಿಕೊಳ್ಳುತ್ತಾಳೆ .

ತನ್ನ ಪತಿ ಮತ್ತು ಕುಟುಂಬವು ಆಘಾತಕ್ಕೆ ಒಳಗಾಗುತ್ತದೆ. ಅವರು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಗೂಢ ಅಮೂಲಾಗ್ರೀಕರಣದ ಬಗ್ಗೆ ಸುಳಿವು ಹೊಂದಿರಲಿಲ್ಲ.

ಯುವಕರು, ದುರ್ಬಲ ವ್ಯಕ್ತಿಗಳು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸಮಯ ಕಳೆಯುವಾಗ ಮತ್ತು ಅಂತರ್ಜಾಲದಲ್ಲಿ ವಿಹರಿಸುವಾಗ ಭಯೋತ್ಪಾದಕರ ಜಾಲಕ್ಕೆ ಬಲಿಯಾಗಬಹುದು.ಅಂತಹ ಉಗ್ರಗಾಮಿಗಳ ಗುರಿಗಳು ಏನೆಂದರೆ ವೈಯಕ್ತಿಕ ವ್ಯಕ್ತಿಗಳು, ಅಥವಾ ಜನಸಮೂಹದ ಮಾನಸಿಕ ಸ್ಥಿತಿ ಅಥವಾ ಕೆಲವೊಮ್ಮೆ ಅವರ ಪಾಲನೆಯಿಂದಾಗಿ, ಅವರುಗಳನ್ನು ಭಯೋತ್ಪಾದಕ ಸಿದ್ಧಾಂತಗಳತ್ತ ಸುಲಭವಾಗಿ ಕರೆದೊಯ್ಯಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಎಫ್–ಸೈಬರ್ ಭಯೋತ್ಪಾದನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 120ಬಿ/ಬಿಎನ್‌ಎಸ್ 61 – ಅಪರಾಧದ ಪಿತೂರಿಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 121/ಬಿಎನ್‌ಎಸ್ 147 – ಭಾರತ ಸರ್ಕಾರದ ವಿರುದ್ಧ ಯುದ್ಧ ಮಾಡುವುದು ಅಥವಾ ಯುದ್ಧ ಮಾಡಲು ಯತ್ನಿಸುವುದು ಅಥವಾ ಯುದ್ಧವನ್ನು ಮಾಡಲು ಸಹಾಯ ಮಾಡುವುದು

ಐಪಿಸಿ ಕಲಂ 121ಎ/ಬಿಎನ್‌ಎಸ್ 148 – ಕಲಂ 121ಎ ಅಡಿಯಲ್ಲಿ ಶಿಕ್ಷಾರ್ಹ ಅಪರಾಧಗಳನ್ನು ಮಾಡಲು ಸಂಚು

ಐಪಿಸಿ ಕಲಂ 122/ಬಿಎನ್‌ಎಸ್ 149 – ಭಾರತ ಸರ್ಕಾರದ ವಿರುದ್ಧ ಯುದ್ಧ ಮಾಡುವ ಉದ್ದೇಶದಿಂದ ಶಸ್ತ್ರಾಸ್ತ್ರ ಸಂಗ್ರಹಿಸುವುದು ಇತ್ಯಾದಿ

ಅಮೂಲಾಗ್ರೀಕರಣಕ್ಕೊಳಗಾಗಬೇಡಿ, ವಿಚಾರವಾದಿಯಾಗಿ ವರ್ತಿಸಿ

ಜೇನು ಬಲೆ (ಹನಿ ಟ್ರ್ಯಾಪ್)

ಶಾಂತ ವಿವಾಹಿತೆಯಾಗಿದ್ದು, ಸುಖರಹಿತ ಸಂಸಾರ ಜೀವನ ನಡೆಸುತ್ತಿದ್ದಳು.

ಹಾಸಿಗೆಗೆ ಹೋಗುವ ಮುನ್ನ ಗೊತ್ತು ಗುರಿ ಇಲ್ಲದ ಗಂಡಸರ ಜೊತೆ ವಿಡಿಯೋ ಸಂಭಾಷಣೆ ನಡೆಸುವ ಚಾಳಿ ಹೊಂದಿದ್ದಳು.

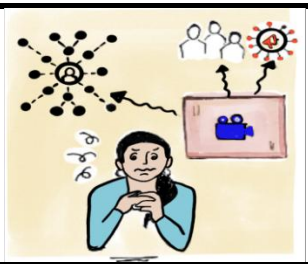
ಒಂದು ರಾತ್ರಿ ಒಬ್ಬ ಸ್ಫುರದ್ರೂಪಿ ಗಂಡಸಿನೊಂದಿಗೆ ಹರಟೆ ಹೊಡೆಯುತ್ತಾಳೆ. ಆತನ ಹೆಸರು ಮೋಹನ.

ಆತ ಅವಳನ್ನು ತನ್ನ ಇನ್ನೂ ಹೆಚ್ಚಿನದನ್ನು ನೋಡುವ ಇಚ್ಛೆ ಇದೆಯೇ ಎಂದಾಗ, ಅವಳು ಪುಳಕಿತಳಾಗಿ ಹೌದೆನ್ನುತ್ತಾಳೆ.

ಒಂದೊಂದಾಗಿ ಬಟ್ಟೆಯನ್ನು ತೆಗೆಯಲು ಪ್ರಾರಂಭಿಸಿ ಮಧ್ಯದಲ್ಲಿ ನಿಲ್ಲಿಸಿ ಅವಳನ್ನು ಸಹ ಹಾಗೆಯೇ ಮಾಡಲು ತಿಳಿಸುತ್ತಾನೆ.

ಅವಳು ಒಪ್ಪಿಗೆ ಸೂಚಿಸಿ ಹಾಗೆಯೇ ನಡೆದುಕೊಳ್ಳುತ್ತಾಳೆ, ಸಂತೋಷದಿಂದ ಕೆಲಸಮಯದ ನಂತರ ಹರಟೆಯನ್ನು ಮುಗಿಸುತ್ತಾರೆ.

5 ನಿಮಿಷದಲ್ಲಿ ಶಾಂತ ತನ್ನ ಮೇಲ್‌ಗೆ ಅವಳ ನಗ್ನ ವಿಡಿಯೋಗಳನ್ನು ಸ್ವೀಕರಿಸುತ್ತಾಳೆ. ಅದರ ಜೊತೆ ಹಣ ಪಾವತಿಗೆ ಬೇಡಿಕೆ ಇಡಲಾಗಿರುತ್ತದೆ.



ಶಾಂತ ಚಿಂತಿತಳಾಗುತ್ತಾಳೆ. ಅವಳು ಹಣ ಪಾವತಿಸದಿದ್ದರೆ ವಿಡಿಯೋ ತನ್ನ ಕುಟುಂಬದ ಸದಸ್ಯರೆಲ್ಲರಿಗೂ ತಿಳಿಯುತ್ತದೆಂದು ಹೆದರುತ್ತಾಳೆ.

ಅವಳಿಗೆ ಇದೊಂದು ಕೃತಕ ಬುದ್ಧಿಮತ್ತೆ ಹೊಂದಿದ ಬಾಟ್ ಹರಟೆ ಎಂದು ತಿಳಿದಿರಲಿಲ್ಲ. ಇದನ್ನು ಅತಿಕ್ರಮಣಕಾರರು ಮೊದಲೇ ರೆಕಾರ್ಡ್ ಮಾಡಿಟ್ಟುಕೊಂಡು ಮೋಸ ಮಾಡಲು ಬಳಸುತ್ತಾರೆ.

ಹನಿ ಬಲೆ ಎನ್ನುವುದು ಒಂದು ತನಿಖಾ ಅಭ್ಯಾಸವಾಗಿದ್ದು, ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಪಡೆದುಕೊಳ್ಳುವ ಉದ್ದೇಶದಿಂದ ಪರಸ್ಪರ, ರಾಜಕೀಯ ಅಥವಾ ವಿತ್ತೀಯ ಉದ್ದೇಶಕ್ಕಾಗಿ ಪ್ರಣಯ ಅಥವಾ ನಿಕಟ ಸಂಬಂಧಗಳ ವಿಧಾನವನ್ನು ಪ್ರಯೋಗಿಸುವುದಾಗಿರುತ್ತದೆ.ಇಂದಿನ ಸೈಬರ್ ಜಗತ್ತಿನಲ್ಲಿ "ಹನಿ ಟ್ರ್ಯಾಪ್" ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ವೇದಿಕೆಗಳಾದ ಫೇಸ್‌ಬುಕ್, ಟ್ವಿಟ್ಟರ್ ಮುಂತಾದವುಗಳಲ್ಲಿ ಅಮಾಯಕರನ್ನು ಬಲೆಗೆ ಬೀಳಿಸಿಕೊಂಡು ಹೊಸ ಆಯಾಮವನ್ನು ಗಳಿಸಿ ಬ್ಲಾಕ್‌ಮೇಲ್ ಮಾಡಲು ಬಳಸಲಾಗುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಚಿತ್ರಗಳು/ವಿಡಿಯೋ ಸೆರೆಹಿಡಿಯುವುದು:

ಐಪಿಸಿ ಕಲಂ 354ಸಿ/ಬಿಎನ್‌ಎಸ್ 77 – ಓರ್ವ ಪುರುಷ ಮಹಿಳೆಯು ಲೈಂಗಿಕ ಕೃತ್ಯದಲ್ಲಿ ತೊಡಗಿಸಿಕೊಂಡಿರುವ ಸನ್ನಿವೇಶವನ್ನು ಆಕೆಯ ಅರಿವಿಲ್ಲದೇ ನೋಡುವ ಅಥವಾ ಅವಳು ನಿರೀಕ್ಷಿಸದ ರೀತಿಯಲ್ಲಿ ದೃಶ್ಯ ಸೆರೆಹಿಡಿಯಲು ತೊಡಗಿಸಿಕೊಂಡು ಅದನ್ನು ಪ್ರಸಾರ ಮಾಡುವುದು.

ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನವಾಗುವ ಉದ್ದೇಶದ ಪದಗಳು, ಸನ್ನೆ ಅಥವಾ ಅಭಿನಯ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ಹರಡಿ ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಎ– ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಬಿ– ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿರುವ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಲಂಗಳು

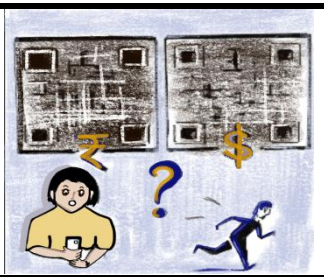
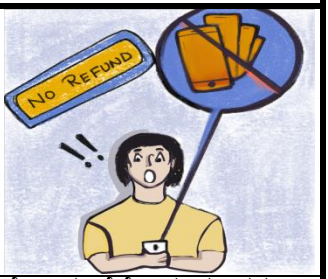
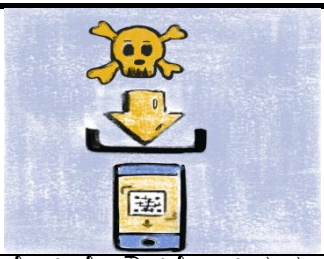
ಒತ್ತೆಹಣಕ್ಕಾಗಿ ಒತ್ತಾಯ (ಪ್ರಯತ್ನ):

ಐಪಿಸಿ ಕಲಂ 385/ಬಿಎನ್‌ಎಸ್ 308–ಸುಲಿಗೆ ಮಾಡುವುದಕ್ಕಾಗಿ ಯಾವನೇ ವ್ಯಕ್ತಿಯನ್ನು ಭಯಪಡಿಸುವುದು

ಐಪಿಸಿ ಕಲಂ 511/ಬಿಎನ್‌ಎಸ್ 62– ಅಪರಾಧ ಎಸಗಲು ಯತ್ನಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಜೀವಾವಧಿ ಶಿಕ್ಷೆ ಅಥವಾ ಇತರೆ ಜೈಲು ಶಿಕ್ಷೆ

ಕೃತಕ ಬುದ್ಧಿಮತ್ತೆಯಿಂದ, ಭ್ರಾಮಕ ಪ್ರಪಂಚಕ್ಕೆ ಕರೆದೊಯ್ದು ಮಾಡಲಾಗುವ ಸುಲಿಗೆ ಯತ್ನಕ್ಕೆ ಬಲಿಯಾಗದಿರಿ.

ಕ್ಷಿಪ್ರ ಪ್ರತಿಕ್ರಿಯೆ(ಕ್ಯೂ.ಆರ್) ಸಂಕೇತ ಹಗರಣ

ಪಾರು ತಂತ್ರಜ್ಞಾನ ನುರಿತೆ ಆಗಿದ್ದು, ಹಣಪಾವತಿಗಾಗಿ ಸದಾ ಡಿಜಿಟಲ್ ಪಾವತಿ ಮಾಧ್ಯಮ ಬಳಸುತ್ತಿದ್ದಳು.	ತನ್ನ ಫೋನ್‌ನಲ್ಲಿ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್, ಕ್ರೆಡಿಟ್– ಡೆಬಿಟ್ ಕಾರ್ಡ್ ವ್ಯವಹಾರ ನಡೆಸುತ್ತಿದ್ದಳು.	ಒಮ್ಮೆ ರೂ.500ಗಳ ಪಾವತಿಗಾಗಿ ಕ್ಯೂಆರ್ ಸಂಕೇತವನ್ನು ತನ್ನ ಫೋನ್‌ನಲ್ಲಿ ಸ್ಕ್ಯಾನ್ ಮಾಡುತ್ತಾಳೆ. ಮೊತ್ತವು ಫೋನ್‌ನಲ್ಲಿ ಗೋಚರವಾಗುತ್ತದೆ.
		
ಕ್ಯೂ.ಆರ್ ಸಂಕೇತ ದುರುದ್ದೇಶ ಪೂರಿತವಾಗಿದ್ದು ರೂಪಾಯಿ ಬದಲು ಡಾಲರ್‌ನಲ್ಲಿ ವರ್ಗೀಕರಣ ಮಾಡಲಾಗಿತ್ತು.	ಪಾರು ನಾಣ್ಯಪದ್ಧತಿ ಮತ್ತು ವಿನಿಮಯ ದರವನ್ನು ಕಡೆಗಣಿಸಿದ್ದಳು.	ಸೇವಾಪೂರೈಕೆದಾರ ಹಣವನ್ನು ಹಿಂದಿರುಗಿಸಲು ಒಪ್ಪಲಿಲ್ಲ. ಕಾರಣ ವ್ಯವಹಾರ ಅವಳ ಸ್ವಇಚ್ಛೆಯಿಂದ ನಡೆದದ್ದು ಆಗಿತ್ತು.
		
ಪಾರು ಸ್ನೇಹಿತೆ ಕೂಡ ಇದೇ ರೀತಿ ಕ್ಯೂಆರ್ ಸಂಕೇತ ಸ್ಕ್ಯಾನ್ ಮಾಡಿ ಫೋನ್‌ಗೆ ಸೋಂಕು ಹತ್ತಿಸಿಕೊಂಡಿದ್ದಳು.	ಡ್ರೈವ್ ಬೈ ಡೌನ್‌ಲೋಡ್ ತಂತ್ರದಿಂದ, ವೈರಾಣು ಡೌನ್‌ಲೋಡ್ ಆಗಿ ಹಿಂಬದಿಯಲ್ಲಿ ಮೊಬೈಲ್‌ನಲ್ಲಿ ಸ್ಥಾಪನೆಗೊಳ್ಳುತ್ತದೆ.	ತಿಳಿಯದ ಕ್ಯೂಆರ್ ಸಂಕೇತ ಸ್ಕ್ಯಾನ್ ಮಾಡುವುದರಿಂದ ನಿಮ್ಮ ಮೊಬೈಲ್ ಆ್ಯಪ್ ನಿಯಂತ್ರಣ ಆಕ್ರಮಣಕಾರರಿಗೆ ನೀಡದಂತೆ ಆಗುತ್ತದೆ.

ಕ್ಷಿಪ್ರ ಪ್ರತಿಕ್ರಿಯೆ(ಕ್ಯೂ.ಆರ್) ಸಂಕೇತಗಳು ದ್ವಿ–ಆಯಾಮದ ಬಾರ್‌ಕೋಡ್‌ಗಳಿಗಿಂತ ವಿಭಿನ್ನವಾದದ್ದಲ್ಲ. ಇಂತಹ ಸಂಕೇತಗಳನ್ನು ಕಾರ್ಖಾನೆಗಳಲ್ಲಿ ಉತ್ಪಾದಿಸುವ ವಸ್ತುಗಳ ಜಾಡನ್ನು ಹಿಡಿಯಲು ರೋಬೋಟ್‌ಗಳಿಂದ ಓದಿಸಬಲ್ಲ ಹಾಗೆ ವಿನ್ಯಾಸಗೊಳಿಸಲಾಗಿರುತ್ತದೆ. ಕ್ಯೂಆರ್ ಸಂಕೇತಗಳು ಪುರಾತನ ಬಾರ್‌ಕೋಡ್‌ಗಳಿಗಿಂತ ಕಡಿಮೆ ಜಾಗವನ್ನು ಬಳಸಿಕೊಳ್ಳುವುದರಿಂದ, ಅದರ ಬಳಕೆ ಶೀಘ್ರಗತಿಯಲ್ಲಿ ಬೆಳೆಯುತ್ತಿದೆ ಹಾಗೂ ಅತಿಕ್ರಮಣಕಾರರು ಅದನ್ನು ತಮ್ಮ ಅನುಕೂಲಕ್ಕೆ ತಕ್ಕಂತೆ ಬಳಸಿಕೊಳ್ಳುತ್ತಾರೆ.ಕ್ಯೂ.ಆರ್ ಸಂಕೇತಗಳನ್ನುಸೃಷ್ಟಿಸುವುದು ಸುಲಭ ಮತ್ತು ಒಂದರಿಂದ ಇನ್ನೊಂದು ಭಿನ್ನವಾಗಿರುತ್ತದೆ.ಆದರೆ ಮಾನವನ ದೃಷ್ಟಿಯಲ್ಲಿ ಬಹುತೇಕ ಎಲ್ಲವೂ ಒಂದೇ ರೀತಿ ಕಾಣುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 406/ಬಿಎನ್‌ಎಸ್ 316– ವಿಶ್ವಾಸ ಭಂಗದ ಅಪರಾಧಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಹಿಂಬದಿಯಲ್ಲಿ ಮಾಲ್ವೇರ್‌ಗಳನ್ನು ಅನುಷ್ಠಾಪಿಸಿ ಅನಧಿಕೃತ ಪ್ರವೇಶಾವಕಾಶ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

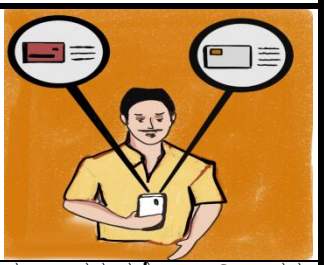
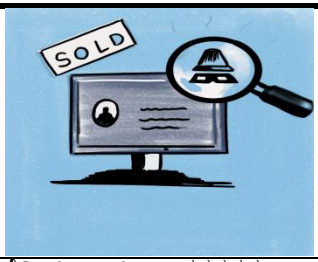
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅಪ್ರಮಾಣಿಕವಾಗಿ ಅಥವಾ ದುರುದ್ದೇಶದಿಂದ ವಿದ್ಯುನ್ಮಾನ ಸಹಿ/ಗುಪ್ತಪದ/ಅನನ್ಯ ಗುರುತು ವೈಶಿಷ್ಟ್ಯವನ್ನು ಬಳಕೆ ಮಾಡಿಕೊಳ್ಳುವುದು.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲವನ್ನುಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ನೀವು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿರುವ ಸಂಕೇತಗಳು ಮತ್ತು ಅನ್ವಯಿಕೆಗಳು ನಕಲಿಯಾಗಿದ್ದರೆ ನಿಮ್ಮ ಹಣವು ಅಪಾಯದಂಚಿನಲ್ಲಿದೆ ಎಂದರ್ಥ.

ಆರ್.ಎಫ್.ಐ.ಡಿ ಪ್ರತಿರೂಪಿಸುವುದು

ಐಶು ಐ.ಟಿ ಉದ್ಯೋಗಿಯಾಗಿದ್ದು ಕಛೇರಿ ಬಾಗಿಲಿನ ನಿಯಂತ್ರಣಕ್ಕಾಗಿ RFID Tag ಬಳಕೆ ಮಾಡುತ್ತಿದ್ದಳು.	ಅವಳು RFID cardಚೀಲದಲ್ಲಿ ಇರಿಸಿ, ನಂತರ ಚೀಲದ ಸಹಿತ ರೀಡರ್ ಎದುರು ಫ್ಲ್ಯಾಶ್ ಮಾಡುತ್ತಿದ್ದಳು.	ಅವಳು ಸದಾ ತನ್ನ ಕೈಚೀಲವನ್ನು ಮೇಜಿನ ಮೇಲೆ ಇಟ್ಟು ಕೆಲಸ ಮಾಡುವ ಹವ್ಯಾಸ ಹೊಂದಿದ್ದಳು.
		
ಒಂದು ದಿನ, ಶೌಚಾಲಯಕ್ಕೆ ಹೋಗುವಾಗ ತನ್ನ ಕೈಚೀಲ ತೆಗೆದುಕೊಂಡು ಹೋಗುವುದನ್ನು ಮರೆತು ಮೇಜಿನ ಮೇಲೆಯೇ ಬಿಟ್ಟು ಹೋಗಿದ್ದಳು.	ಅವಳ ಸಹೋದ್ಯೋಗಿ, ರವಿ ಅವಳ ಯಶಸ್ಸು ಸಹಿಸದೆ ಅಸೂಯೆಯಿಂದ RFID ರೀಡರ್ ಬಳಸಿ ಅವಳ RFID card ಸ್ಕ್ಯಾನ್ ಮಾಡಿಕೊಂಡಿದ್ದನು.	ರವಿ ಅವಳ ಕಛೇರಿ ಐ.ಡಿ ವಿವರ ಮತ್ತು ಸಂಪರ್ಕರಹಿತ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಕಲೆ ಹಾಕಿಕೊಂಡನು.
		
ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಡಾರ್ಕ್ ವೆಬ್‌ನಲ್ಲಿ ಮಾರಾಟ ಮಾಡಿದನು.	ಕಛೇರಿ ಐ.ಡಿ ಪ್ರತಿರೂಪವನ್ನು ರವಿಯು ತಾನು ಕಲೆಹಾಕಿಕೊಂಡ ವಿವರ ಬಳಸಿ ತಯಾರಿಸಿಕೊಂಡನು	ಆ ಐ.ಡಿ ಬಳಸಿ, ಬಾಗಿಲಿನ ಪ್ರವೇಶ ಪಡೆದು ಸರ್ವರ್ ಕೋಣೆ ಪ್ರವೇಶಿಸಿ ಗಣಕಯಂತ್ರಗಳನ್ನು ಅತಿಕ್ರಮಿಸುತ್ತಾನೆ. ತಪ್ಪಿಲ್ಲದೆ ಐಶು ಆಪಾದನೆಗೆ ಒಳಗಾಗುತ್ತಾಳೆ.

ರೇಡಿಯೋ ತರಂಗಗಳನ್ನು ಗುರುತಿಸುವುದು ಅಥವಾ ಆರ್.ಎಫ್.ಐ.ಡಿ ಎನ್ನುವುದು ವಸ್ತುಗಳನ್ನು ಸ್ವಯಂಚಾಲಿತವಾಗಿ ಗುರುತು ಹಿಡಿಯಲು ಬಳಸುವ ವಿಧಾನವಾಗಿದೆ.ಇದರಲ್ಲಿ ವಸ್ತುಗಳ ಐ.ಡಿಗಳು ರೇಡಿಯೋ ತರಂಗಗಳನ್ನು ಬಳಸಿಕೊಂಡು ದತ್ತಾಂಶವನ್ನು ಓದುತ್ತವೆ ಅಥವಾ ಬರೆಯುತ್ತವೆ. ಪ್ರತಿಯೊಂದು ಚಿಪ್‌ನಲ್ಲಿ ಅನನ್ಯ ಸಂಖ್ಯೆಗಳಿದ್ದು ಸ್ಪರ್ಶತಂತುಗಳೊಂದಿಗೆ ಒಳಗಿಂದೊಳಗೆ ಗುರುತಿಸುವಿಕೆಯ ದತ್ತಾಂಶವನ್ನು ಸಂಗ್ರಹಿಸಿಕೊಳ್ಳುತ್ತದೆ. ಈ ಕಾರ್ಡ್‌ಗಳಲ್ಲಿ ಸುಲಭವಾಗಿ ಪ್ರತಿರೂಪಿಸಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಆರ್.ಎಫ್.ಐ.ಡಿ ಪ್ರತಿರೂಪಣ / ಆರ್.ಎಫ್.ಐ.ಡಿ ದತ್ತಾಂಶ ಕಳ್ಳತನ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಕಳ್ಳತನದ ದತ್ತಾಂಶವನ್ನು ಸ್ವಾಧೀನದಲ್ಲಿಟ್ಟುಕೊಳ್ಳುವುದು/ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಮಾರಾಟ ಮಾಡುವುದು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಬಿ– ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಕಳ್ಳತನದ ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಅಥವಾ ಸಂವಹನ ಸಾಧನವನ್ನು ಸ್ವೀಕರಿಸಿದರೆ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಡಿಜಿಟಲ್ ಐಡಿ ಪಡಿಯಚ್ಚು ಮಾಡುವುದು ಮತ್ತು ಪ್ರತಿರೂಪಣದಿಂದ ಸರ್ವರ್ ಪ್ರವೇಶಿಸುವುದು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

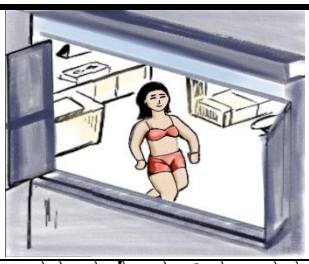
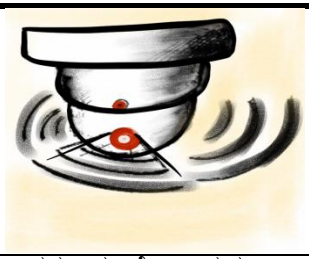
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಸೈಬರ್ ನೈರ್ಮಲ್ಯವನ್ನು ನಿಮ್ಮಿಂದ ನಿಭಾಯಿಸಬಹುದಾದರೆ ಮಾತ್ರ ತಂತ್ರಜ್ಞಾನವನ್ನು ಬಳಸಿ.

ಡ್ರೋನ್ ಕಣ್ಗಾವಲು

		
ರಾಧ ವೈದ್ಯ ವಿದ್ಯಾರ್ಥಿನಿ, ಬಹು ಮಹಡಿ ವಸತಿಮನೆಗಳ 33ನೇ ಮಹಡಿಯಲ್ಲಿ ವಾಸಿಸುತ್ತಿದ್ದಳು.	ಅವಳು ಸದಾ ತನ್ನ ಮನೆಯ ಎಲ್ಲಾ ಕಿಟಕಿಗಳನ್ನು ತೆರೆದಿಟ್ಟುಕೊಳ್ಳುತ್ತಿದ್ದಳು. ಏಕೆಂದರೆ ಹತ್ತಿರ ಯಾವುದೇ ಮನೆ ಇರಲಿಲ್ಲದ್ದರಿಂದ	ಅವಳ ಮನೆ ಯಾರಿಗೂ ಸಹ ತಿಳಿಯದಿದ್ದರಿಂದ ಸಾಮಾನ್ಯವಾಗಿ ಅರೆಬಟ್ಟೆಯಲ್ಲಿ ಮನೆಯಲ್ಲಿ ಇರುತ್ತಿದ್ದಳು.
ರಘು ಅವಳ ಮಾಜಿ ಪ್ರಿಯಕರ ಡ್ರೋನ್ ಬಳಸಿ ಹಲವಾರು ರೀತಿಯಲ್ಲಿ ಅವಳ ಚಟುವಟಿಕೆ ಬಗ್ಗೆ ಗೂಢಾಚಾರಿಕೆ ಮಾಡುತ್ತಿದ್ದನು.	ಒಮ್ಮೆ ಅವಳ ಮಲಗುವಕೋಣೆ ಮತ್ತು ನಡುಕೋಣೆಗೆ ಅವಳ ಚಲನವಲನ ವಿಡಿಯೋ ಮಾಡಲು ಡ್ರೋನ್ ಕಳುಹಿಸುತ್ತಾನೆ.	ಡ್ರೋನ್ ಅವಳ ಎಲ್ಲಾ ಚಟುವಟಿಕೆಗಳನ್ನು ತನ್ನ ಕ್ಯಾಮರದಲ್ಲಿ ಸೆರೆಹಿಡಿದಿಟ್ಟುಕೊಂಡಿತ್ತು.
		
ಅವಳ ಮೇಲಿನ ನಿಗಾವಣೆಗಾಗಿ ಅದರೊಳಗೆ ವೈಫೈ ಕ್ರ್ಯಾಕರ್ ಸಹ ಇದ್ದು, ಅದ್ದರಿಂದ ವೈಫೈ ದತ್ತಾಂಶವನ್ನೆಲ್ಲ ಪ್ರತಿಬಂಧಿಸಬಹುದಿತ್ತು.	ಡ್ರೋನ್ ಬಳಸಿ ಅವಳ ಮನೆ ಒಳಗೆ ಅಪಾಯಕಾರಿ ವಸ್ತು ಮತ್ತು ಶಸ್ತ್ರಾಸ್ತ್ರಗಳನ್ನು ಸಾಗಿಸಬಹುದಾದ ವ್ಯವಸ್ಥೆ ಹೊಂದಿತ್ತು.	ಅವಳು ಚಲನೆ ಅರಿವುಳ್ಳ ಸಿಸಿಟಿವಿ ಕ್ಯಾಮರಾ ಅಳವಡಿಸಿದ್ದಲ್ಲಿ, ಮೊದಲ ಹಂತದಲ್ಲೇ ಡ್ರೋನ್‌ನನ್ನು ಗುರುತಿಸಬಹುದಾಗಿತ್ತು.

ವಾಯುಯಾನದಲ್ಲಿ ಮತ್ತು ಬಾಹ್ಯಾಕಾಶದಲ್ಲಿ ಡ್ರೋನ್‌ನನ್ನು ಒಂದು ಚಾಲಕ ರಹಿತ ವೈಮಾನಿಕ ವಾಹನ ಎನ್ನಲಾಗುತ್ತದೆ.ಡ್ರೋನ್‌ಗಳಲ್ಲಿ ವಿವಿಧ ರೀತಿಯ ಕಣ್ಗಾವಲು ಸಾಧನಗಳನ್ನು ಅಳವಡಿಸಬಹುದಾಗಿದ್ದು, ಅವುಗಳು ಹೆಚ್ಚು ಸಾಮರ್ಥ್ಯದ ವಿಡಿಯೋ ಮತ್ತು ಚಿತ್ರಗಳನ್ನು ರಾತ್ರಿ ಹಾಗೂ ಹಗಲಿನಲ್ಲಿ ಸೆರೆಹಿಡಿಯಬಹುದಾದ ಸಾಧನವಾಗಿದೆ. ಸೆಲ್‌ಫೋನ್ ಕರೆಗಳನ್ನು ಪ್ರತಿಬಂಧಿಸಲು, ಜಿಪಿಎಸ್ ಸ್ಥಳಗಳನ್ನು ನಿರ್ಧರಿಸಲು ಮತ್ತು ಪರವಾನಗಿ ಪ್ಲೇಟ್ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸಲು ಡ್ರೋನ್‌ಗಳಲ್ಲಿ ತಂತ್ರಜ್ಞಾನವನ್ನು ಅಳವಡಿಸಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಹಿಳೆಯರ ಯಾವುದೇ ಖಾಸಗಿ ಅಂಗದ ಚಿತ್ರ/ವಿಡಿಯೋಗಳನ್ನು ಡ್ರೋನ್ ಬಳಸಿ ಅವಳ ಒಪ್ಪಿಗೆ ಇಲ್ಲದೆ ಸೆರೆಹಿಡಿಯುವುದು/ಹಿಂಬಾಲಿಸುವುದು/ಅನುಸರಿಸುವುದು.

ಐಪಿಸಿ ಕಲಂ 354ಎ/ಬಿಎನ್‌ಎಸ್ 75 –ಲೈಂಗಿಕ ಕಿರುಕುಳ ಮತ್ತು ಲೈಂಗಿಕ ಕಿರುಕುಳಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಐಪಿಸಿ ಕಲಂ 354ಸಿ/ಬಿಎನ್‌ಎಸ್ 77 – ಓರ್ವ ಪುರುಷ ಮಹಿಳೆಯು ಲೈಂಗಿಕ ಕೃತ್ಯದಲ್ಲಿ ತೊಡಗಿಸಿಕೊಂಡಿರುವ ಸನ್ನಿವೇಶವನ್ನು ಆಕೆಯ ಅರಿವಿಲ್ಲದೇ ನೋಡುವ ಅಥವಾ ಅವಳು ನಿರೀಕ್ಷಿಸದ ರೀತಿಯಲ್ಲಿ ದೃಶ್ಯ ಸೆರೆಹಿಡಿಯಲು ತೊಡಗಿಸಿಕೊಂಡು ಅದನ್ನು ಪ್ರಸಾರ ಮಾಡುವುದು.

ಐಪಿಸಿ ಕಲಂ /ಬಿಎನ್‌ಎಸ್ 78 – ಹಿಂಬಾಲಿಕೆ

ಐಪಿಸಿ ಕಲಂ /ಬಿಎನ್‌ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನವಾಗುವ ಉದ್ದೇಶದ ಪದಗಳು, ಸನ್ನೆ ಅಥವಾ ಅಭಿನಯ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ವೈಫೈ ಕ್ರ್ಯಾಕರ್ ಮೂಲಕ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯ ಕಳ್ಳತನ

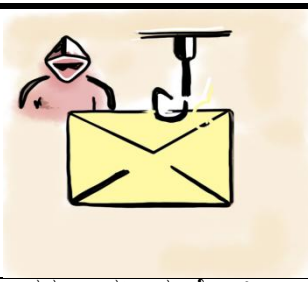
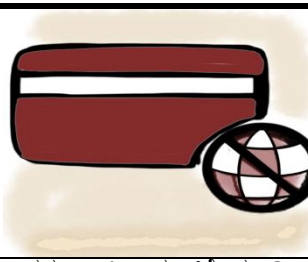
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಡ್ರೋನ್ ಮೂಲಕ ಮನೆಯ ಮೇಲೆ ಅಪಾಯಕಾರಿ ವಸ್ತುವನ್ನು ಎಸೆಯುವುದು:

ಐಪಿಸಿ ಕಲಂ 436/ಬಿಎನ್‌ಎಸ್ 326–ಮನೆ, ಇತ್ಯಾದಿಯನ್ನು ನಾಶಪಡಿಸುವ ಉದ್ದೇಶದಿಂದ ಬೆಂಕಿ ಅಥವಾ ಸ್ಫೋಟಕ ವಸ್ತುಗಳನ್ನು ಬಳಸಿ ಕೇಡು ಮಾಡುವುದು

ನಿಸ್ಸಂದೇಹವಾಗಿ ನೀವು ಪ್ರತಿ ರಾತ್ರಿ ಹಗಲು ಗಮನಿಸಲ್ಪಡುತ್ತಿದ್ದೀರಿ

ಸರ್ಚ್ ಇಂಜಿನ್ ಹಗರಣ

ರಚಿತ ಮಂಗಳೂರಿಗೆ ವಿಮಾನ ಪ್ರಯಾಣದ ಚೀಟಿಯನ್ನು ಕಾಯ್ದಿರಿಸಿದ್ದಳು.	ಎರಡು ದಿನಗಳ ಮೊದಲು ತನ್ನ ಪ್ರಯಾಣದ ಟಿಕೆಟ್ ರದ್ದಾಗಿದೆ ಎಂದು ಇ–ಮೇಲ್ ಮೂಲಕ ಸಂದೇಶ ಸ್ವೀಕರಿಸುತ್ತಾಳೆ.	ಗೂಗಲ್‌ನಲ್ಲಿ ಹುಟುಕಾಟ ನಡೆಸಿ ಫಲಿತಾಂಶದಲ್ಲಿ ಸಿಕ್ಕ ಸಹಾಯ ವಾಣಿ ಸಂಖ್ಯೆಗೆ ಕರೆ ಮಾಡುತ್ತಾಳೆ.
		
ಸಹಾಯವಾಣಿಯು ಪರಿಶೀಲನೆ ನೆಪದಲ್ಲಿ ಅವಳ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಪಡೆಯುತ್ತಾರೆ. ಸಿ.ವಿ.ವಿ ಯನ್ನು ಸಹ ನೀಡುತ್ತಾಳೆ.	ತಕ್ಷಣ ರೂ.10000 ದಂತೆ 5 ಬಾರಿ ಸತತವಾಗಿ ಹಣ ಅವಳ ಖಾತೆಯಿಂದ ಕಡಿತಗೊಳ್ಳುತ್ತದೆ. ಒಟ್ಟಾರೆ ರೂ.50000 ಅವಳ ಖಾತೆಯಿಂದ ಕಡಿತಗೊಂಡಿರುತ್ತದೆ.	ಅವಳು ಸ್ವೀಕರಿಸಿದ್ದ ಮೇಲ್ ವಂಚನೆಯದ್ದಾಗಿದ್ದು, ವಿಮಾನ ಸಂಸ್ಥೆಯಿಂದ ಬಂದದ್ದಾಗಿರಲಿಲ್ಲ.
		
ಅಂತರ್ಜಾಲದಲ್ಲಿ ಸಿಕ್ಕ ಸಂಪರ್ಕ ಕೇಂದ್ರದ ಸಂಖ್ಯೆಯು ಅತಿಕ್ರಮಣ ಮಾಡಿ ಜನರಿಗೆ ಮೋಸ ಮಾಡಲು ನಿರ್ಮಿಸಿದ್ದಂತಹದು.	ಅವಳು ಒಟಿಪಿ ಹಂಚಿಕೆ ಮಾಡಿಲ್ಲ ವಾದರೂ ಅಂತರರಾಷ್ಟ್ರೀಯ ಆನ್‌ಲೈನ್ ವಹಿವಾಟಿಗೆ ಒಟಿಪಿ ಅವಶ್ಯಕತೆ ಇರುವುದಿಲ್ಲ.	ರಚಿತ ತನ್ನ ಡೆಬಿಟ್–ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್‌ಗಳಲ್ಲಿ ಅಂತರರಾಷ್ಟ್ರೀಯ ಹಣಕಾಸು ವಹಿವಾಟು ನಿಷ್ಕ್ರಿಯ ಮಾಡಿರಲಿಲ್ಲ.

ಅತಿಕ್ರಮಣಕಾರರು ಜಾಲತಾಣಗಳನ್ನು ಕಾನೂನುಬದ್ಧವಾಗಿ ಕಾಣುವಂತೆ ರಚಿಸಬಹುದು ಮತ್ತು ಅದನ್ನು ವಿವಿಧ ಸರ್ಚ್ ಇಂಜಿನ್‌ಗಳಿಂದ ಸೂಚಿಕೆ ಪಡೆಯಬಹುದು, ಇದು ನೀವು ಟೈಪ್ ಮಾಡುವ ಕೀಪದಗಳ ಆಧಾರದ ಮೇಲೆ ಹುಡುಕಾಟ ನಡೆಸಿ ಫಲಿತಾಂಶವನ್ನು ನೀಡುತ್ತದೆ.ಈ ರೀತಿಯಾಗಿ ದಾರಿತಪ್ಪಿಸುವ ಫಲಿತಾಂಶಗಳು, ನಕಲಿ ಸಹಾಯವಾಣಿ ಫೋನ್ ಸಂಖ್ಯೆಗಳು ಇತ್ಯಾದಿಗಳನ್ನು ತೋರಿಸುತ್ತವೆ. ಇದರಿಂದಾಗಿ ಬಳಕೆದಾರರು ಅವರನ್ನು ನಂಬುತ್ತಾರೆ ಮತ್ತು ಇಂತಹ ಸರ್ಚ್ ಇಂಜಿನ್ ಆಪ್ಟಿಮೈಷೇಷನ್ (ಎಸ್.ಇ.ಓ) ಹಗರಣಕ್ಕೆ ಬಲಿಯಾಗುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಅಸಲಿ ಸಹಾಯವಾಣಿ ವಿವರಗಳನ್ನು ಅಪರಾಧಿಗಳ ವಿವರಗಳಿಗೆ ಬದಲಾಯಿಸುವುದು:

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

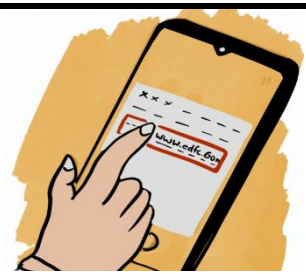
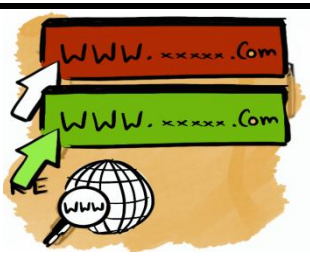
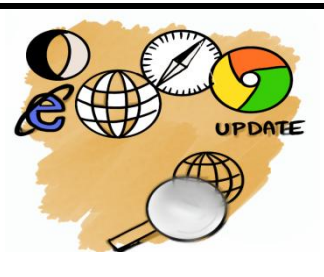
ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಐಪಿಸಿ ಕಲಂ 465/ಬಿಎನ್‌ಎಸ್ 336– ಸುಳ್ಳು ಸ್ವಷ್ಟನೆಗೆ ದಂಡನೆ(ವ್ಯಾಖ್ಯಾನದ ಕಲಂ)

ಐಪಿಸಿ ಕಲಂ 468/ಬಿಎನ್‌ಎಸ್ 336– ಮೋಸಗೊಳಿಸಲು ನಕಲುರುಜು

ಗ್ರಾಹಕರ ನಕಲಿ ಸಹಾಯವಾಣಿ ಸಂಖ್ಯೆಗಳು ನಿಮ್ಮನ್ನು ತೀವ್ರ ನಿಗಾ ಘಟಕಕ್ಕೆ ಕಳುಹಿಸಬಹುದು

ಐ.ಡಿ.ಎನ್ ಹೋಮೋಗ್ರಾಫ್ ಆಕ್ರಮಣ

ಶ್ವೇತ ಬೇರೆ ಊರಿನಲ್ಲಿರುವ ತನ್ನ ತಾಯಿಗೆ ಹಣ ವರ್ಗಾವಣೆ ಮಾಡಬೇಕಾಗಿರುತ್ತದೆ.	ಅವಳು ಬ್ಯಾಂಕಿನ ವತಿಯಿಂದ ಒಂದು ಸಂದೇಶ ಸ್ವೀಕರಿಸುತ್ತಾಳೆ	ಅದರಲ್ಲಿ ಈ ರೀತಿ ವಿಷಯ ಇರುತ್ತದೆ.
		
ಉತ್ಸುಕಳಾಗಿ, ಅವರು ಕಳುಹಿಸಿದ ಕೊಂಡಿಯನ್ನು ಕ್ಲಿಕ್ಕಿಸಿ ತನ್ನ ರುಜುವಾತುಗಳನ್ನು ನೀಡಿ ಲಾಗಿನ್ ಆಗುತ್ತಾಳೆ.	ಸಲ್ಲಿಕೆ ಬಟನ್ ಒತ್ತಿದ ನಂತರ ಜಾಲಪುಟ ಮುಂದುವರೆಯದೇ ಪುನಃ ಅದೇ ಹಳೆಯ ಲಾಗಿನ್ ಪರದೆಗೆ ತೆರಳುತ್ತದೆ.	ಅವಳು ಮತ್ತೊಮ್ಮೆ ಲಾಗಿನ ರುಜುವಾತುಗಳನ್ನು ನೀಡಿ ವ್ಯವಹಾರ ಪೂರ್ಣಗೊಳಿಸುತ್ತಾಳೆ.
		
ಈಗ ಉಡುಗೊರೆ ಚೀಟಿ ಪಡೆಯುವ ಬದಲು ರೂ.10000 ಮೊತ್ತ ಕಡಿತಗೊಂಡಿರುವ ಸಂದೇಶ ನೋಡಿ ಗಾಬರಿ ಆಗುತ್ತಾಳೆ.	ಶ್ವೇತ ಐಡಿಎನ್ ಹೋಮೋಗ್ರಾಫ್ ಆಕ್ರಮಣದ ಬಲಿಪಶು ಆಗಿದ್ದು, ಇಲ್ಲಿ ನಕಲಿ ಜಾಲತಾಣ ಅಸಲಿ ತಾಣಗಳಂತೆ ಅನುಕರಣೆ ಮಾಡಲಾಗಿರುತ್ತದೆ.	ಅವಳು ಜಾಲವಾಹಕವನ್ನು ಅಪ್ ಗ್ರೇಡ್ ಮಾಡಿದ್ದರೆ, ಲ್ಯಾಟಿನ್‌ಪದ ತಾಣವನ್ನು ಅನುಕರಿಸಿದ ಸಿರಿಲಿಕ್ ಪದದ ತಾಣದ ಬಗ್ಗೆ ಎಚ್ಚರಿಕೆ ಸಂದೇಶ ತೋರಿಸಲಾಗುತ್ತಿತ್ತು.

ಐ.ಡಿ.ಎನ್ ಹೋಮೋಗ್ರಾಫ್ ಆಕ್ರಮಣ

ಐಡಿಎನ್ ಹೋಮೋಗ್ರಾಫ್ ದಾಳಿಯು ಟೈಪೊಸ್ಕ್ವಾಟಿಂಗ್ ಎಂದು ಕರೆಯಲ್ಪಡುವ ಮತ್ತೊಂದು ರೀತಿಯ ಡೊಮೇನ್ ಹೆಸರಿನ ವಂಚನೆಯನ್ನು ಹೋಲುತ್ತದೆ.ಎರಡು ತಂತ್ರಗಳಲ್ಲಿಯೂ ಸಹ ಬಳಕೆದಾರರನ್ನು ಒಂದೇ ರೀತಿಯ ಹೋಲಿಕೆ ಇರುವ ಹೊಸ ಡೊಮೇನ್ ಹೆಸರನ್ನು ಬಳಸುವ ಮೂಲಕ ಮೋಸಗೊಳಿಸಲು ಪ್ರಯತ್ನಿಸುತ್ತವೆ, ಆದರೆ ಇಲ್ಲಿ ವಿವಿಧ ರೀತಿಯ ಹೋಲಿಕೆಗಳನ್ನು ಬಳಸಿಕೊಳ್ಳಲಾಗುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

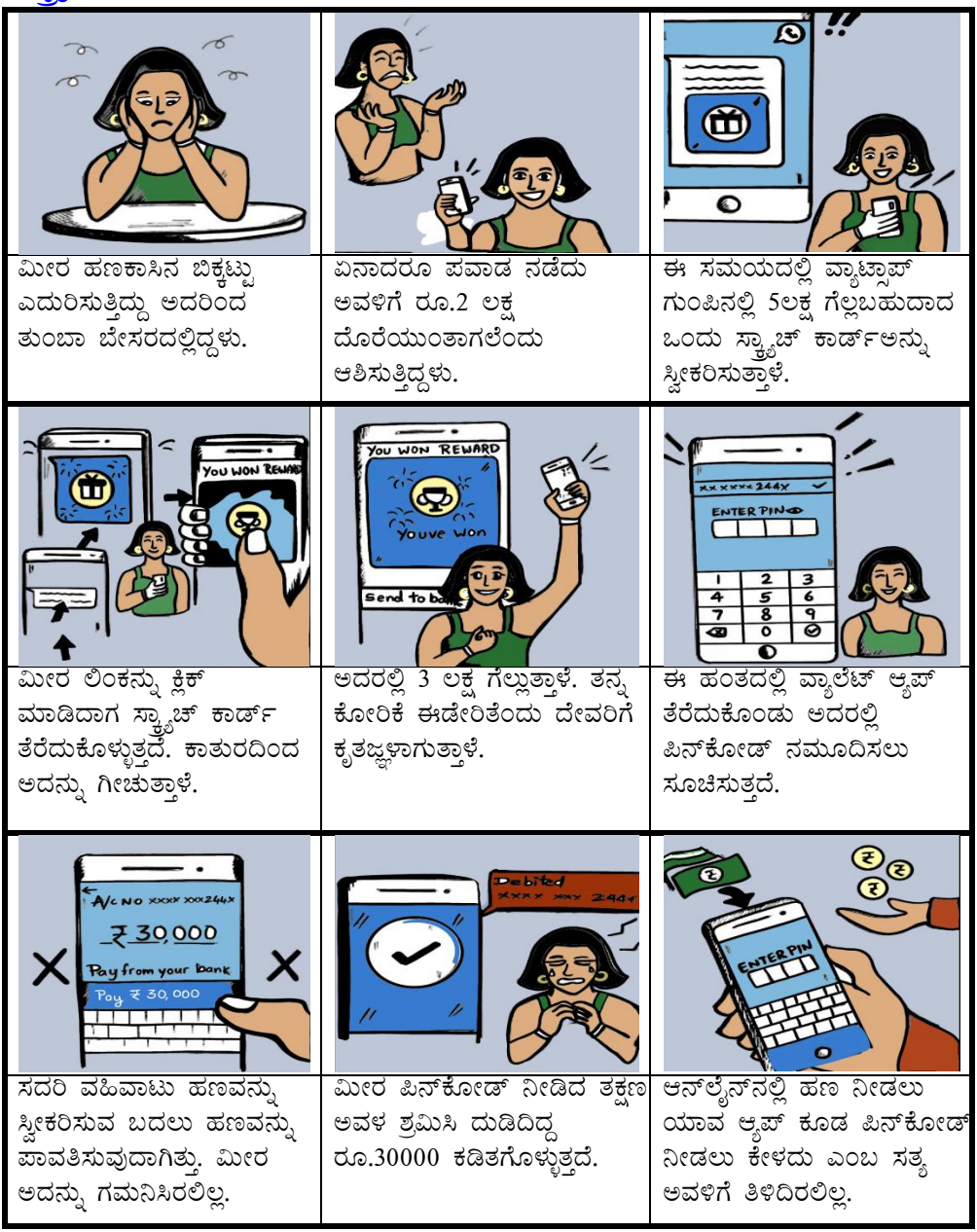
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318– ಮೋಸ

ಖದೀಮರು ಅಕ್ಷರಗಳನ್ನು ಮತ್ತು ಚಿಹ್ನೆಗಳನ್ನು ಬದಲಾಯಿಸಿ ಅಪರಾಧ ಮಾಡುತ್ತಾರೆ.

ಸ್ಕ್ರ್ಯಾಚ್ ಕಾರ್ಡ್ ಹಗರಣ



ಮೀರ ಹಣಕಾಸಿನ ಬಿಕ್ಕಟ್ಟು ಎದುರಿಸುತ್ತಿದ್ದು ಅದರಿಂದ ತುಂಬಾ ಬೇಸರದಲ್ಲಿದ್ದಳು.	ಏನಾದರೂ ಪವಾಡ ನಡೆದು ಅವಳಿಗೆ ರೂ.2 ಲಕ್ಷ ದೊರೆಯುಂತಾಗಲೆಂದು ಆಶಿಸುತ್ತಿದ್ದಳು.	ಈ ಸಮಯದಲ್ಲಿ ವ್ಯಾಟ್ಸಾಪ್ ಗುಂಪಿನಲ್ಲಿ 5ಲಕ್ಷ ಗೆಲ್ಲಬಹುದಾದ ಒಂದು ಸ್ಕ್ರ್ಯಾಚ್ ಕಾರ್ಡ್‌ಅನ್ನು ಸ್ವೀಕರಿಸುತ್ತಾಳೆ.
ಮೀರ ಲಿಂಕನ್ನು ಕ್ಲಿಕ್ ಮಾಡಿದಾಗ ಸ್ಕ್ರ್ಯಾಚ್ ಕಾರ್ಡ್ ತೆರೆದುಕೊಳ್ಳುತ್ತದೆ. ಕಾತುರದಿಂದ ಅದನ್ನು ಗೀಚುತ್ತಾಳೆ.	ಅದರಲ್ಲಿ 3 ಲಕ್ಷ ಗೆಲ್ಲುತ್ತಾಳೆ. ತನ್ನ ಕೋರಿಕೆ ಈಡೇರಿತೆಂದು ದೇವರಿಗೆ ಕೃತಜ್ಞಳಾಗುತ್ತಾಳೆ.	ಈ ಹಂತದಲ್ಲಿ ವ್ಯಾಲೆಟ್ ಆ್ಯಪ್ ತೆರೆದುಕೊಂಡು ಅದರಲ್ಲಿ ಪಿನ್‌ಕೋಡ್ ನಮೂದಿಸಲು ಸೂಚಿಸುತ್ತದೆ.
ಸದರಿ ವಹಿವಾಟು ಹಣವನ್ನು ಸ್ವೀಕರಿಸುವ ಬದಲು ಹಣವನ್ನು ಪಾವತಿಸುವುದಾಗಿತ್ತು. ಮೀರ ಅದನ್ನು ಗಮನಿಸಿರಲಿಲ್ಲ.	ಮೀರ ಪಿನ್‌ಕೋಡ್ ನೀಡಿದ ತಕ್ಷಣ ಅವಳ ಶ್ರಮಿಸಿ ದುಡಿದಿದ್ದ ರೂ.30000 ಕಡಿತಗೊಳ್ಳುತ್ತದೆ.	ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹಣ ನೀಡಲು ಯಾವ ಆ್ಯಪ್ ಕೂಡ ಪಿನ್‌ಕೋಡ್ ನೀಡಲು ಕೇಳದು ಎಂಬ ಸತ್ಯ ಅವಳಿಗೆ ತಿಳಿದಿರಲಿಲ್ಲ.

ಒಂದು ನಿಗಧಿತ ಮೊತ್ತ ಗೆಲ್ಲುವ ಭರವಸೆಯನ್ನು ಬಳಕೆದಾರರಿಗೆ ಒಂದು ಕೊಂಡಿಯನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವ ಮೂಲಕ ಮೂರನೇಯ ಜಾಲತಾಣಕ್ಕೆ ಕರೆದೊಯ್ಯುವ ಸಂದೇಶವನ್ನು ನೀಡುತ್ತದೆ.ಬಳಕೆದಾರರು ಅಂತಹ ಲಿಂಕ್‌ನ್ನು ಕ್ಲಿಕ್ ಮಾಡಿದಾಗ, ಇದೊಂದು ಜನಪ್ರಿಯ ಪೇ ವಾಲೆಟ್ಸ್ ಸ್ಕ್ರ್ಯಾಚ್ ಕಾರ್ಡ್‌ನ ವಿನ್ಯಾಸವನ್ನು ಅನುಕರಿಸುವ ಸ್ಕ್ರ್ಯಾಚ್ ಕಾರ್ಡ್ ಹೊಂದಿರುವ ಜಾಲತಾಣಕ್ಕೆ ಮರುನಿರ್ದೇಶಿಸುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

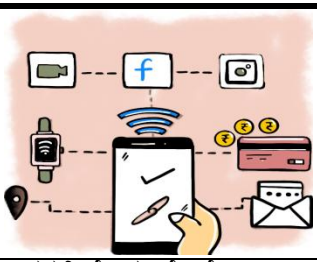
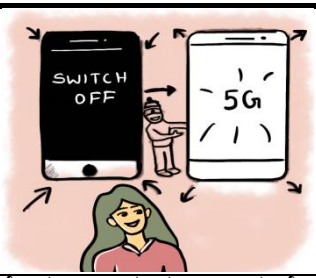
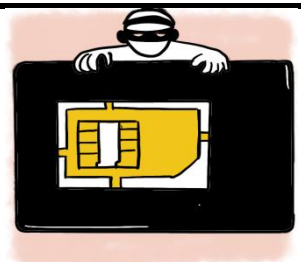
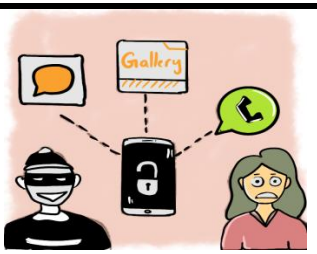
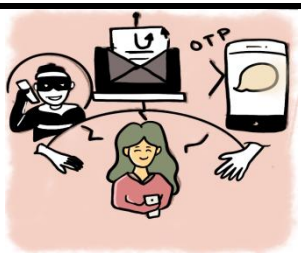
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಸೂಕ್ಷ್ಮ ರುಜುವಾತುಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದರಿಂದ ಗಣನೀಯ ಪ್ರಮಾಣದ ನಷ್ಟವನ್ನು ತರುತ್ತದೆ.

ಸಿಮ್ ಮಾರ್ಪಾಡು(ಸ್ವ್ಯಾಪ್)

		
ತಾನ್ವಿ ತನ್ನ ಮೊಬೈಲ್‌ನಲ್ಲಿ ಹಲವಾರು ಆ್ಯಪ್‌ಗಳ ಖುಜುವಾತಿಗಾಗಿ ತನ್ನ ಫೋನ್ ಸಂಖ್ಯೆ ನೀಡಿದ್ದಳು.	ಅದರಲ್ಲಿ ಕೆಲವು ಮೊಬೈಲ್ ಇ-ವ್ಯಾಲೆಟ್, ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ, ಬ್ಯಾಂಕ್ ಖಾತೆ, ಇ-ಮೇಲ್ ಗಳಿಗೆ**2FA,** ಇತ್ಯಾದಿಗಳು.	ಒಂದು ರಾತ್ರಿ ಒಬ್ಬ ಸೈಬರ್ ಕಳ್ಳ ತಾನು ಸೆಲ್‌ಫೋನ್ ಸಂಸ್ಥೆಯಿಂದ ಕರೆಮಾಡುತ್ತಿರುವುದಾಗಿ ನಂಬುವಂತೆ ಅವಳಿಗೆ ಕರೆ ಮಾಡುತ್ತಾನೆ.
		
ಕೆಲವು ಸೀಮಿತ ಚಂದಾದಾರರಿಗೆ 5ಜಿ ಸಂಪರ್ಕ ಕಲ್ಪಿಸುತ್ತಿದ್ದು ಕ್ರೀಯಾಶೀಲತೆಗಾಗಿ 2 ಗಂಟೆ ಕಾಲ ಫೋನ್ ಸ್ಥಗಿತಗೊಳಿಸಲು ನಂಬಿಸಿ ಯಶಸ್ವಿಯಾಗುತ್ತಾರೆ.	ಅದರಂತೆ ತಾನ್ವಿ ಫೋನ್ ಆಫ್ ಮಾಡಿ ನಿದ್ರೆಗೆ ಜಾರುತ್ತಾಳೆ. ಬೆಳಗ್ಗೆ ಎದ್ದು ನೋಡಿದಾಗ ಫೋನ್‌ನಲ್ಲಿ ನೆಟ್‌ವರ್ಕ್ ಕಾಣುತ್ತಿರಲಿಲ್ಲ.	ಹ್ಯಾಕರ್ ನಕಲಿ ದಾಖಲೆ ನೀಡಿ ಅವರ ಸಂಖ್ಯೆಯ ಮತ್ತೊಂದು ಸಿಮ್ ಖರೀದಿಸಿರುತ್ತಾನೆ. ಕಾರಣ ಅವಳ ಅಸಲಿ ಸಿಮ್ ನಿಷ್ಕ್ರಿಯ ಗೊಂಡಿರುತ್ತದೆ.
		
ಗುಪ್ತಪದ ಮರೆವು ಮತ್ತು ಒಟಿಪಿ ಖುಜುವಾತು ಆಯ್ಕೆ ಬಳಸಿ ಹ್ಯಾಕರ್ ಅವಳ ಎಲ್ಲಾ ಖಾತೆಗೂ ನಿಯಂತ್ರಣ ಸಾಧಿಸುತ್ತಾನೆ.	ಅವಳ ವ್ಯಾಟ್ಸಾಪ್ ಕೂಡ ನಿಯಂತ್ರಣ ಸಿಕ್ಕಿ, ಅವಳ ಖಾಸಗಿ ಹರಟೆ/ಚಿತ್ರಗಳು ಇತ್ಯಾದಿಗಳಿಗೆ ಪ್ರವೇಶಾವಕಾಶವು ದೊರಕುತ್ತದೆ.	ಸಿಮ್ ಸ್ವ್ಯಾಪ್ ಮಾಡದೆಯೂ ಸಹ ಹ್ಯಾಕರ್‌ಗಳು ವಿಶಿಂಗ್/ಫಿಶಿಂಗ್/ ಸ್ಮಿಶಿಂಗ್ ಬಳಸಿ ಒಟಿಪಿ ವಿನಂತಿ ಮಾಡಿ ವ್ಯಾಟ್ಸಾಪ್ ನಿಯಂತ್ರಣ ಪಡೆದುಕೊಳ್ಳುತ್ತಾರೆ.

ಸ್ವಿಮ್ ಸ್ವಾಪ್ ಹಗರಣ (ಪೋರ್ಟ್–ಔಟ್–ಹಗರಣ, ಸಿಮ್ ವಿಭಜನೆ, ಸ್ಮಿಶಿಂಗ್ ಮತ್ತು ಸಿಮ್‌ಜಾಕಿಂಗ್, ಸಿಮ್ ವಿನಿಮಯ ಎಂದೂ ಸಹ ಕರೆಯಲ್ಪಡುವ) ಒಂದು ವಿಧದ ಸ್ವಾಧೀನ ವಂಚನೆ. ವಂಚಕ ಮೊಬೈಲ್ ಫೋನ್ ಸೇವಾಪೂರೈಕೆದಾರರು ಮೊಬೈಲ್ ಸಂಖ್ಯೆಯನ್ನು ಬೇರೆ ಸಿಮ್ ಹೊಂದಿರುವ ಸಾಧನಕ್ಕೆ ಮನಬಂದಂತೆ ಪೋರ್ಟ್ ಮಾಡುವ ಸಾಮರ್ಥ್ಯವನ್ನು ಬಳಸಿಕೊಳುತ್ತಾರೆ. ಈ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಸಾಮಾನ್ಯವಾಗಿ ಫೋನ್ ಕಳುವಾದಾಗ, ಫೋನ್ ಕಳೆದುಕೊಂಡಾಗ ಅಥವಾ ಹೊಸ ಫೋನ್‌ಗೆ ಸೇವೆಯನ್ನು ಬದಲಾಯಿಸುವಾಗ ಬಳಸಲಾಗುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

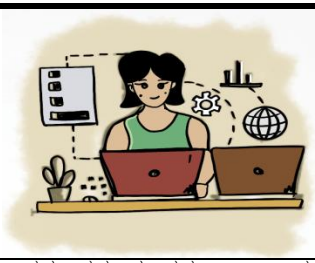
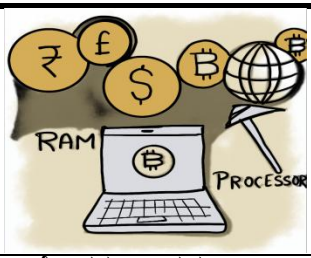
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಸಿಮ್ ಸ್ವ್ಯಾಪ್‌ನಿಂದ ಮಂದ ಸ್ಥಿತಿಗೆ ತಲುಪುತ್ತೀರಿ.

ಕ್ರಿಪ್ಟೋಜಾಕಿಂಗ್

		
ರಾಧ ತಂತ್ರಾಂಶ ಅಭಿವೃದ್ಧಿಗಾರ್ತಿ ಆಗಿದ್ದು, ಮನೆಯಿಂದಲೇ ಕೆಲಸ ನಿರ್ವಹಿಸುತ್ತಿದ್ದಳು	ಅವಳು ತನ್ನ ಸಂಪನ್ಮೂಲ ಸಾಂದ್ರ ಸಂಕೇತಗಳ ಕಾರ್ಯಗತಕ್ಕಾಗಿ 2 ಉನ್ನತ ಸಾಮರ್ಥ್ಯದ ಲ್ಯಾಪ್‌ಟಾಪ್ ಬಳಕೆ ಮಾಡುತ್ತಿದ್ದಳು.	ಕಾಲಕ್ರಮೇಣ ಅವಳ ಲ್ಯಾಪ್ ಟಾಪ್ ವೇಗವು ಮಾಮೂಲಿಗಿಂತ ಕುಂಟಿತವಾಗುತ್ತಿರುವುದನ್ನು ಗಮನಿಸುತ್ತಾಳೆ.
ಜೊತೆಗೆ ವಿದ್ಯುತ್ ಬಳಕೆಯಲ್ಲೂ ಸಹ ಹೇರಳವಾಗಿ ಹೇರಿಕೆಯನ್ನು ಕಾಣುತ್ತಾಳೆ.	ಲ್ಯಾಪ್‌ಟಾಪ್‌ನಲ್ಲಿ ಪ್ರೋಸೆಸ್ ನಿರ್ವಾಹಕ ತೆರೆದಾಗ, ಹಿಂಬದಿ ತಿಳಿಯದ ಆ್ಯಪ್‌ಗಳು ಕಾರ್ಯ ನಿರ್ವಹಿಸುತ್ತಿರುವುದು ತಿಳಿಯುತ್ತದೆ.	ಇಂತಹ ಆ್ಯಪ್‌ಗಳು ಕ್ರಿಪ್ಟೋಜಾಕ್ ಆ್ಯಪ್‌ಗಳಾಗಿದ್ದು ಇವುಗಳು ಬಿಟ್ ಕಾಯಿನ್ ಮೈನ್ ಮಾಡಲು ಅತ್ಯಧಿಕ ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿಕೊಳ್ಳುತ್ತವೆ.
		
ಅವಳು ಎಂದೋ ಯಾವುದೋ ಅಪರಿಚಿತ ಕೊಂಡಿ ಕ್ಲಿಕ್ ಮಾಡಿದ್ದರಿಂದ, ಈ ಆ್ಯಪ್ ಡೌನ್‌ಲೋಡ್ ಆಗಿರುತ್ತದೆ.	ಕಿಡಿಕೇಡಿಗಳು ಅಂತಹ ಗಣಕಯಂತ್ರದ ರ‍್ಯಾಂ & ಸಂಸ್ಕರಕ ಬಳಸಿ ಮೈನಿಂಗ್ ಮಾಡಿ ಲಕ್ಷಾಂತರ ರೂಪಾಯಿ ಸಂಪಾದಿಸುತ್ತಿರುತ್ತಾರೆ.	ಅವಳು ಸುರಕ್ಷತೆಗಾಗಿ ಪಾವತಿಸಿದ ಆ್ಯಂಟಿ ವೈರಸ್ ಬಳಸಿ ಜಾಲವಾಹಕವನ್ನು ಅಪ್‌ಡೇಟ್ ಮಾಡಿದ್ದರೆ, ಅವಳ ಗಣಕಯಂತ್ರವು ಸುರಕ್ಷಿತವಾಗಿ ಇರುತ್ತಿತ್ತು.

ಇದೊಂದು ರೀತಿಯ ಸೈಬರ್ ಆಕ್ರಮಣವಾಗಿದ್ದು, ಇದರಲ್ಲಿ ಆಕ್ರಮಣಕಾರನು ತನ್ನ ಪರವಾಗಿ ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಯನ್ನು ಅಕ್ರಮವಾಗಿ ಮೈನ್ ಮಾಡುವ ಸಲುವಾಗಿ ಬಳಕೆದಾರರ ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಶಕ್ತಿಯನ್ನು ಬಳಸಿಕೊಳ್ಳುತ್ತಾನೆ. ಕ್ರಿಪ್ಟೋಜಾಕಿಂಗ್ ವೈಯಕ್ತಿಕ ಗ್ರಾಹಕರನ್ನು ಅಥವಾ ಬೃಹತ್ ಸಂಸ್ಥೆಗಳನ್ನು ಅಥವಾ ಕೈಗಾರಿಕಾ ನಿಯಂತ್ರಣ ಗಣಕಯಂತ್ರಗಳನ್ನು ಗುರಿಯಾಗಿಸಬಹುದು.ಇದರಿಂದ ಸೊಂಕಿಗೆ ಒಳಪಟ್ಟಿರುವ ಗಣಕಯಂತ್ರವು ನಿಧಾನಗೊಳ್ಳುತ್ತದೆ, ಏಕೆಂದರೆ ಮೈನಿಂಗ್ ಪ್ರಕ್ರಿಯೆಯ ಸಂಸ್ಕರಣಕ್ಕೆ ಗಣಕಯಂತ್ರದ ಇತರೆ ಎಲ್ಲಾ ಅಧಿಕೃತ ಚಟುವಟಿಕೆಗಳನ್ನು ಮೊಟಕುಗೊಳಿಸಿ ಆದ್ಯತೆ ಪಡೆಯುವ ಸಾಮರ್ಥ್ಯವಿರುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

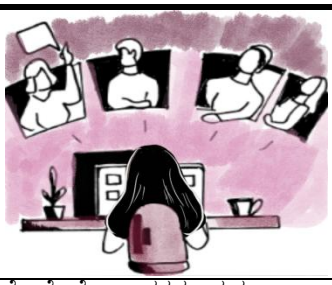
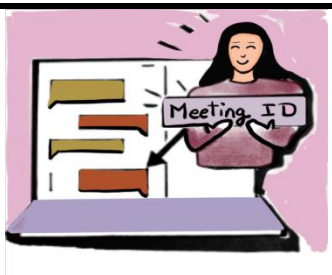
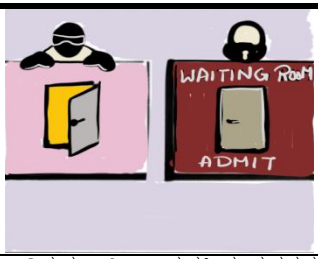
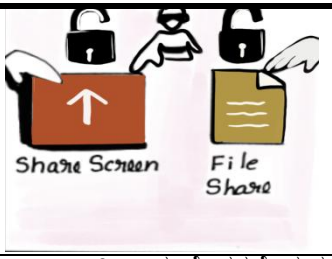
ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ420/ಬಿಎನ್ಎಸ್ 318– ಮೋಸ

ಹಣ ಲಾಂಡರಿಂಗ್ ತಡೆ ಕಾಯ್ದೆ, 2002(ಪಿಎಂಎಲ್ಎ) ಗಳ ಕಲಂಗಳು, ಪ್ರಕರಣದ ಸಂಗತಿಗಳ ಪ್ರಕಾರ ಅನ್ವಯಿಸಬಹುದು

ಆಕ್ರಮಣಕಾರರಿಗೆ ಹಣ ಸಂಪಾದನೆಯಲ್ಲಿ ಕ್ರಿಪ್ಟೋಜಾಕಿಂಗ್ ಸಹಕಾರಿ.

ವಿಡಿಯೋ ಸಮಾವೇಶ ಹಗರಣ

		
ಅಂಕಿತಾ ಬಹುರಾಷ್ಟ್ರೀಯ ಸಂಸ್ಥೆಯಲ್ಲಿ ತಂಡದ ನಾಯಕಿಯಾಗಿ ಕರ್ತವ್ಯ ನಿರ್ವಹಿಸುತ್ತಿದ್ದು, ಪ್ರಸ್ತುತ ಮನೆಯಿಂದ ಕೆಲಸ ಮಾಡುತ್ತಿದ್ದಳು.	ತನ್ನ ತಂಡದ ಸಹಪಾಠಿಯೊಂದಿಗೆ ಸಮನ್ವಯ ಸಾಧಿಸಲು, ಅವಳು ಸದಾ ಆನ್‌ಲೈನ್ ಸಭೆ ನಡೆಸಲು ಆತಿಥ್ಯ ನೀಡುತ್ತಿದ್ದಳು.	ಕೆಲವೊಮ್ಮೆ ಗ್ರಾಹಕರು ಸಹ ವಿಡಿಯೋ ಸಂವಾದದ ಮೂಲಕ ಪ್ರಗತಿ ಮತ್ತು ಬದಲಾವಣೆಯ ಸಲಹೆ, ನೀಡುತ್ತಿದ್ದರು.
		
ಒಂದು ದಿನ, ಗ್ರಾಹಕರ ಆನ್‌ಲೈನ್ ಸಭೆ ನಡೆಯುತ್ತಿದ್ದಾಗ, ಅಪರಿಚಿತ ವ್ಯಕ್ತಿ ಸಭೆಗೆ ಲಾಗಿನ್ ಆಗಿ ಅಶ್ಲೀಲ ವಿಡಿಯೋ ಪೋಸ್ಟ್ ಮಾಡಿದ.	ಈ ಘಟನೆಯಿಂದ ಗಲಿಬಿಲಿಗೊಂಡ ಅಂಕಿತಾ ಸಭೆಯನ್ನು ಮೊಟಕುಗೊಳಿಸಿ ಹೊರನಡೆದಳು.	ಅವಳು ಮಾಡಿದ ತಪ್ಪೆಂದರೆ ಸಭೆಗೆ ಸಂಬಂಧಿಸಿದ ಖುಜುವಾತುಗಳನ್ನು ಸಾಮಾನ್ಯ ವೇದಿಕೆಯಲ್ಲಿ ಸಂದೇಶ ರೂಪದಲ್ಲಿ ಹಂಚಿಕೆ ಮಾಡಿಕೊಂಡಿದ್ದಳು.
		
ಅಸಮಾಧಾನಗೊಂಡ ಅದೇ ಸಂಸ್ಥೆಯ ಉದ್ಯೋಗಿ, ಸುಳ್ಳು ಹೆಸರಿನಿಂದ ಸಭೆಗೆ ಸೇರಿ ಆ ಕೃತ್ಯ ನಡೆಸಿದ್ದನು.	ಅಧಿಕೃತವಾಗಿ ಭಾಗವಹಿಸುವವರನ್ನು ಶೋಧಿಸಲು ವೇಯ್ಟಿಂಗ್ ರೂಂ ಸಕ್ರಿಯೆಗೊಳಿಸಿರಲಿಲ್ಲ.	ಎಲ್ಲಾ ಭಾಗೀದಾರರಿಗೆ ಪರದೆ ಮತ್ತು ಕಡತ ಹಂಚಿಕೆ ಆಯ್ಕೆಯನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿರಲಿಲ್ಲ.

ಆನ್‌ಲೈನ್‌ಗಳಲ್ಲಿ ಸಭೆಗಳು, ತರಗತಿಗಳು, ಸಮ್ಮೇಳನಗಳನ್ನು ನಡೆಸುವಾಗ ಈ ವೇದಿಕೆಗಳಲ್ಲಿ ಸುರಕ್ಷತಾ ನಿಯಮಗಳಿಗೆ ಹೆಚ್ಚು ಪರಿಗಣನೆ ನೀಡದೇ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ವೇದಿಕೆಗಳ ಸಾಮೂಹಿಕ ರೂಪಾಂತರ ಕಂಡುಬಂದಿದೆ.ದುರುದ್ದೇಶಪೂರಿತ ಉದ್ದೇಶಗಳಿಗಾಗಿ ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಲೋಪದೋಷಗಳ ಲಾಭ ಪಡೆಯಲು ಇದು ದಾರಿ ಮಾಡಿಕೊಟ್ಟಿದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಎ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಕಳ್ಳತನ

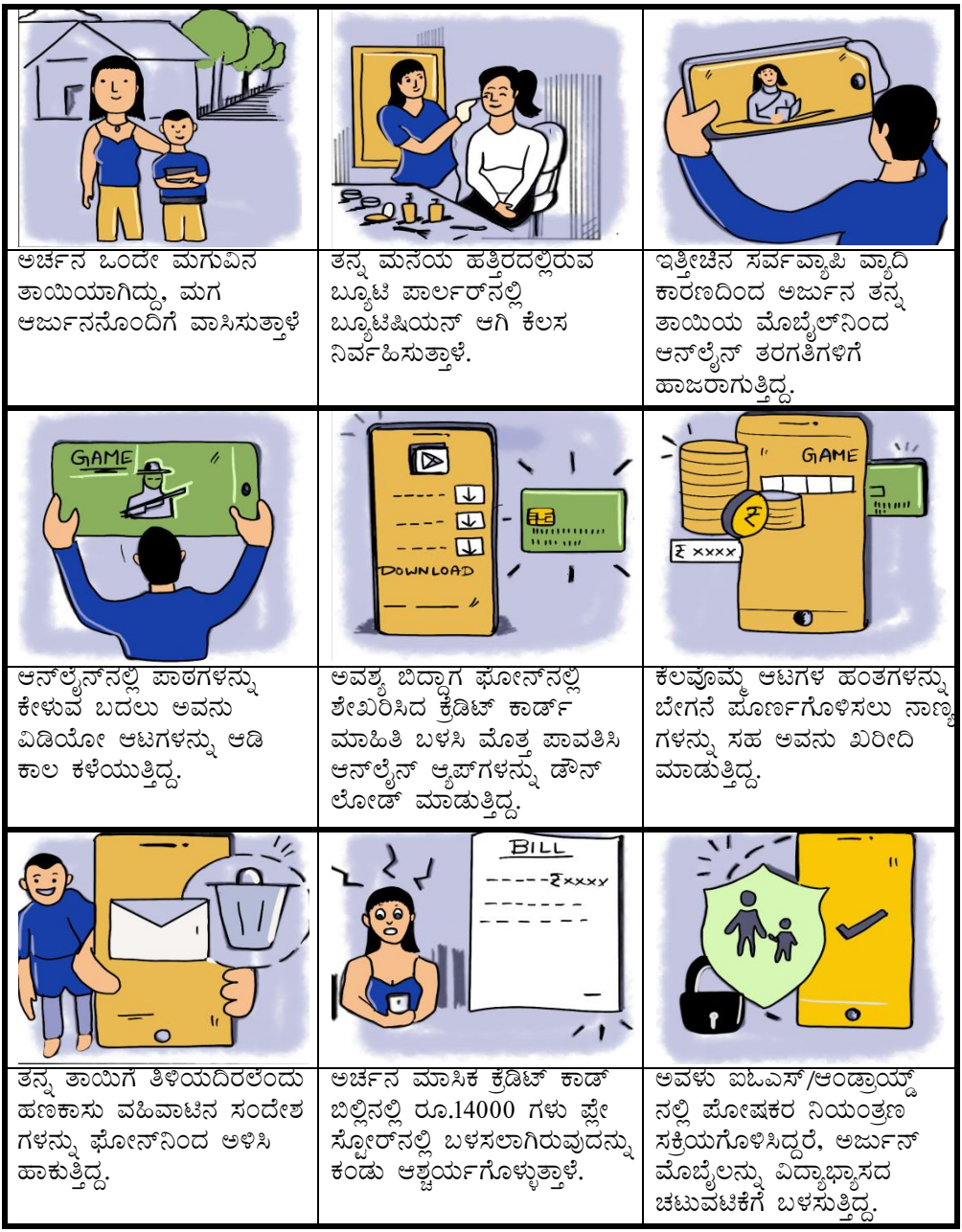
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಪ್ರಕರಣದ ಸಂಗತಿ ಅನುಸಾರ)

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಇಂತಹ ವಾಸ್ತವ ಸಭೆಗಳಲ್ಲಿ ಪಾಲ್ಗೊಳ್ಳುವವರ ಬಗ್ಗೆ ತಿಳಿದಿರಬೇಕು.

ಮಕ್ಕಳ ಮೊಬೈಲ್ ಫೋನ್



ಅರ್ಚನ ಒಂದೇ ಮಗುವಿನ ತಾಯಿಯಾಗಿದ್ದು, ಮಗ ಅರ್ಜುನನೊಂದಿಗೆ ವಾಸಿಸುತ್ತಾಳೆ	ತನ್ನ ಮನೆಯ ಹತ್ತಿರದಲ್ಲಿರುವ ಬ್ಯೂಟಿ ಪಾರ್ಲರ್‌ನಲ್ಲಿ ಬ್ಯೂಟಿಷಿಯನ್ ಆಗಿ ಕೆಲಸ ನಿರ್ವಹಿಸುತ್ತಾಳೆ.	ಇತ್ತೀಚಿನ ಸರ್ವವ್ಯಾಪಿ ವ್ಯಾಧಿ ಕಾರಣದಿಂದ ಅರ್ಜುನ ತನ್ನ ತಾಯಿಯ ಮೊಬೈಲ್‌ನಿಂದ ಆನ್‌ಲೈನ್ ತರಗತಿಗಳಿಗೆ ಹಾಜರಾಗುತ್ತಿದ್ದ.
ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪಾಠಗಳನ್ನು ಕೇಳುವ ಬದಲು ಅವನು ವಿಡಿಯೋ ಆಟಗಳನ್ನು ಆಡಿ ಕಾಲ ಕಳೆಯುತ್ತಿದ್ದ.	ಅವಶ್ಯ ಬಿದ್ದಾಗ ಫೋನ್‌ನಲ್ಲಿ ಶೇಖರಿಸಿದ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಮಾಹಿತಿ ಬಳಸಿ ಮೊತ್ತ ಪಾವತಿಸಿ ಆನ್‌ಲೈನ್ ಆ್ಯಪ್‌ಗಳನ್ನು ಡೌನ್ ಲೋಡ್ ಮಾಡುತ್ತಿದ್ದ.	ಕೆಲವೊಮ್ಮೆ ಆಟಗಳ ಹಂತಗಳನ್ನು ಬೇಗನೆ ಪೂರ್ಣಗೊಳಿಸಲು ನಾಣ್ಯಗಳನ್ನು ಸಹ ಅವನು ಖರೀದಿ ಮಾಡುತ್ತಿದ್ದ.
ತನ್ನ ತಾಯಿಗೆ ತಿಳಿಯದಿರಲೆಂದು ಹಣಕಾಸು ವಹಿವಾಟಿನ ಸಂದೇಶಗಳನ್ನು ಫೋನ್‌ನಿಂದ ಅಳಿಸಿ ಹಾಕುತ್ತಿದ್ದ.	ಅರ್ಚನ ಮಾಸಿಕ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಬಿಲ್ಲಿನಲ್ಲಿ ರೂ.14000 ಗಳು ಪ್ಲೇ ಸ್ಟೋರ್‌ನಲ್ಲಿ ಬಳಸಲಾಗಿರುವುದನ್ನು ಕಂಡು ಆಶ್ಚರ್ಯಗೊಳ್ಳುತ್ತಾಳೆ.	ಅವಳು ಐಓಎಸ್/ಆಂಡ್ರಾಯ್ಡ್‌ನಲ್ಲಿ ಪೋಷಕರ ನಿಯಂತ್ರಣ ಸಕ್ರಿಯಗೊಳಿಸಿದ್ದರೆ, ಅರ್ಜುನ್ ಮೊಬೈಲನ್ನು ವಿದ್ಯಾಭ್ಯಾಸದ ಚಟುವಟಿಕೆಗೆ ಬಳಸುತ್ತಿದ್ದ.

www.cybersafegirl.com

ಇತ್ತೀಚೆಗೆ ಮಕ್ಕಳು ಚಿಕ್ಕ ವಯಸ್ಸಿನಲ್ಲಿಯೇ ಮೊಬೈಲ್‌ಗಳನ್ನು ಬಳಸುವ ಅನಿವಾರ್ಯತೆ ಇರುತ್ತದೆ.ಇಲ್ಲಿ ಪೋಷಕರು ತಮ್ಮ ಮಕ್ಕಳು ಅಂತರ್ಜಾಲದಲ್ಲಿ ವಯಸ್ಕ, ನಿಂದನೀಯ ಅಥವಾ ಹಿಂಸಾತ್ಮಕ ವಿಷಯವನ್ನು ನೋಡುವುದನ್ನು ಬಯಸುವುದಿಲ್ಲವಾದ್ದರಿಂದ ಇದೊಂದು ಸಂದಿಗ್ಧ ಪರಿಸ್ಥಿತಿಯಾಗಿದೆ.ಆದ್ದರಿಂದ ಅವರು ಬಳಸುವ ಸಾಧನಗಳಲ್ಲಿ ನಿಯಂತ್ರಣಗಳನ್ನು ಹೊಂದಿಸುವುದು ಬಹುಮುಖ್ಯ ಜವಾಬ್ದಾರಿಯುತವಾಗಿ ಮೊಬೈಲ್ ಫೋನ್ ಬಳಕೆಯ ವೆಚ್ಚಗಳನ್ನು ನಿರ್ವಹಿಸುವುದು, ಕುಟುಂಬದ ಮೌಲ್ಯಗಳಿಗೆ ಬದ್ಧವಾಗಿರುವುದು, ಫೋನ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿರಿಸುವುದು ಮತ್ತು ಗೌರವಯುತವಾಗಿಟ್ಟುಕೊಳ್ಳುವುದು ಮುಖ್ಯವಾಗಿರುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಜೂಜಾಟದಲ್ಲಿ ಭಾಗಿಯಾಗಿದ್ದರೆ:
ಕೆಳಗಿನ ಕಾಯ್ದೆಗಳು ಅನ್ವಯವಾಗಬಹುದು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 69ಎ– ಅಕ್ರಮ ಜೂಜಾಟದ ಜಾಲತಾಣಗಳನ್ನು ನಿರ್ಬಂಧಿಸುವುದು.

ಸಾರ್ವಜನಿಕ ಜೂಜಾಟ ಕಾಯ್ದೆ, 1867
ವಿದೇಶಿ ವಿನಿಮಯ ನಿರ್ವಹಣಾ ಕಾಯ್ದೆ, 1999(ಫೆಮಾ)
1998ರ ಲಾಟರಿ ನಿಯಂತ್ರಣ ಕಾಯ್ದೆ

ಕೆಲವು ರಾಜ್ಯಗಳು ಜೂಜಾಟಕ್ಕೆ ಅವಕಾಶವನ್ನು ಕಲ್ಪಿಸಿದೆ

ವಿನಾಯಿತಿಗಳು:

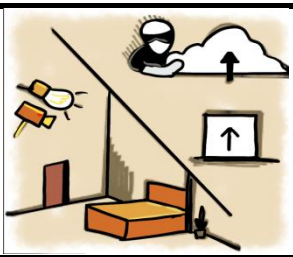
1. ಭಾರತದಲ್ಲಿ ಕುದುರೆ ಓಟದ ಜೂಜು ಕಾನೂನುಬದ್ಧವಾಗಿದೆ.
2. ಲಾಟರಿ ವ್ಯವಸ್ಥೆ (ಕೆಲವು ರಾಜ್ಯಗಳಲ್ಲಿ)
3. 1867ರ ಸಾರ್ವಜನಿಕ ಜೂಜಾಟ ಕಾಯ್ದೆಯು ಕೌಶಲ್ಯ ಆಧಾರಿತ ಆಟಗಳನ್ನು ಜೂಜಿನ ವ್ಯಾಖ್ಯಾನದಿಂದ ವಿನಾಯಿತಿ ನೀಡಲಾಗಿದೆ.

.

ಆನ್‌ಲೈನ್ ಆಟಗಳು ಹಣಕಾಸು ನಷ್ಟ, ಅಪಖ್ಯಾತಿ ಮತ್ತು ಅವಮಾನವನ್ನು ಉಂಟುಮಾಡಬಹುದು.

www.cybersafegirl.com

ಜಾಣ್ಮೆಯಮನೆಗಳು(ಸ್ಮಾರ್ಟ್ ಹೋಂ)

ಚಾರು ತಾಂತ್ರಿಕ ಜ್ಞಾನವುಳ್ಳ ಗೃಹಿಣಿ. ಅವಳು ಆಧುನಿಕ ಉಪಕರಣಗಳನ್ನು ಮನೆಯಲ್ಲಿ ಖರೀದಿಸಿ ಅಳವಡಿಸುವ ಇಚ್ಛೆ ಹೊಂದಿದ್ದಳು.	ಒಮ್ಮೆ ಅಗ್ಗದ ಅಂತರ್ಜಾಲ ವಸ್ತುಗಳ (IoT) ಮೇಳ ನಡೆಯುತ್ತಿದಂತಹ ಮಾರುಕಟ್ಟೆಗೆ ಹೋಗುತ್ತಾಳೆ.	ಅಲ್ಲಿ ಹಲವಾರು ಸಾಧನಗಳು ಶೇಕಡ 60% ರಿಯಾಯ್ತಿ ದರದಲ್ಲಿ ಇದ್ದದ್ದು ಕಂಡು ಸಂತಸಗೊಳ್ಳುತ್ತಾಳೆ.
ಚಾರು ಒಂದು ಜಾಣ್ಮೆಯ ಬಲ್ಬು ಖರೀದಿಸಿ ತನ್ನ ಮಲಗುವ ಕೊಠಡಿಯಲ್ಲಿ ಹಾಕುತ್ತಾಳೆ.	ಸದರಿ ಬಲ್ಬನ್ನು ತನ್ನ ಫೋನ್ ನಿಂದ ನಿಯಂತ್ರಸಬಹುದಾಗಿತ್ತು. ಬಣ್ಣಗಳ ಬದಲಾವಣೆ ಮತ್ತು ಆನ್/ಆಫ್ ಫೋನ್ ಮುಖೇನ ಮಾಡಬಹುದಿತ್ತು.	ಆದರೆ ಆ ಬಲ್ಬಿನಲ್ಲಿ ವೈಫೈ ಸಂಪರ್ಕಿತ ಸೂಕ್ಷ್ಮ ಗುಪ್ತ ಕ್ಯಾಮರಾ ಅಳವಡಿಕೆ ಆಗಿರುವುದು ಅವಳಿಗೆ ತಿಳಿದಿರಲಿಲ್ಲ.
		
ಕ್ಯಾಮರಾ ಕೋಣೆಯಲ್ಲಿ ನಡೆಯುವ ಎಲ್ಲಾ ಚಟುವಟಿಕೆಗಳನ್ನು ಸೆರೆಹಿಡಿದು ತನ್ನ ಸರ್ವರ್‌ಗೆ ರವಾನಿಸುತ್ತಿತ್ತು.	IoT ಉಪಕರಣಗಳನ್ನು ಪ್ರಾಮಾಣಿಕ ಮಾರಾಟಗಾರರಿಂದ ಮಾತ್ರ ಖರೀದಿಸಬೇಕು ಹಾಗೂ ಸುರಕ್ಷಿತ ಆಯ್ಕೆಗಳನ್ನು ಪ್ರತಿಷ್ಠಾಪಿಸಬೇಕು ಎಂಬುದು ಆಕೆಗೆ ತಿಳಿದಿರಲಿಲ್ಲ.	ಅಂತರ್ಜಾಲ ಅವಲಂಬಿತ ಎಲ್ಲಾ ಉಪಕರಣಗಳನ್ನು ಗೂಢಾಚಾರಿಕೆ ಮಾಡಲು ಬಳಸಬಹುದು. ತಂತ್ರಜ್ಞಾನ ಎರಡು ಬದಿಯ ಕತ್ತಿ ಇದ್ದಂತೆ.

ನಿಮ್ಮ ಜನ್ಮ ದಿನಾಂಕದಿಂದ ಹಿಡಿದು ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳವರೆಗೆ ಜಾಣ್ಮೆಯ ಮನೆ ಸಾಧನಗಳು ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯ ನಿಧಿಯನ್ನು ಹೊಂದಿರುತ್ತವೆ, ಇಂತಹ ನಿಧಿಯನ್ನು ಸೈಬರ್ ಅಪರಾಧಿಗಳು ದೃಢವಾದ ರಕ್ಷಣೆಯಿಲ್ಲದಿದ್ದರೆ ಅತಿಕ್ರಮಣ ಪ್ರವೇಶದ ಮೂಲಕ ಕದಿಯಬಹುದು.ನಂತರ ಅವರು ಕದ್ದಂತಹ ದತ್ತಾಂಶವನ್ನು ಬಳಸಿಕೊಂಡು ಮೋಸದ ವ್ಯವಹಾರಗಳಿಗೆ ನಿಮ್ಮನ್ನು ಒಳಪಡಿಸಿ ಉದ್ದೇಶಿತ ದಾಳಿಗಳನ್ನು ನಿಮ್ಮ ಮೇಲೆ ಪ್ರಾರಂಭಿಸಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 354/ಬಿಎನ್ಎಸ್ 74 – ಹೆಂಗಸಿನ ಮಾನಭಂಗ ಮಾಡುವ ಉದ್ದೇಶದಿಂದ ಅವಳ ಮೇಲೆ ಹಲ್ಲೆ ಅಥವಾ ಅಪರಾಧಿಕ ಬಲಪ್ರಯೋಗ

ಐಪಿಸಿ ಕಲಂ 354ಸಿ/ಬಿಎನ್ಎಸ್ 77 – ಓರ್ವ ಪುರುಷ ಮಹಿಳೆಯು ಲೈಂಗಿಕ ಕೃತ್ಯದಲ್ಲಿ ತೊಡಗಿಸಿಕೊಂಡಿರುವ ಸನ್ನಿವೇಶವನ್ನು ಆಕೆಯ ಅರಿವಿಲ್ಲದೇ ನೋಡುವ ಅಥವಾ ಅವಳು ನಿರೀಕ್ಷಿಸದ ರೀತಿಯಲ್ಲಿ ದೃಶ್ಯ ಸೆರೆಹಿಡಿಯಲು ತೊಡಗಿಸಿಕೊಂಡು ಅದನ್ನು ಪ್ರಸಾರ ಮಾಡುವುದು.

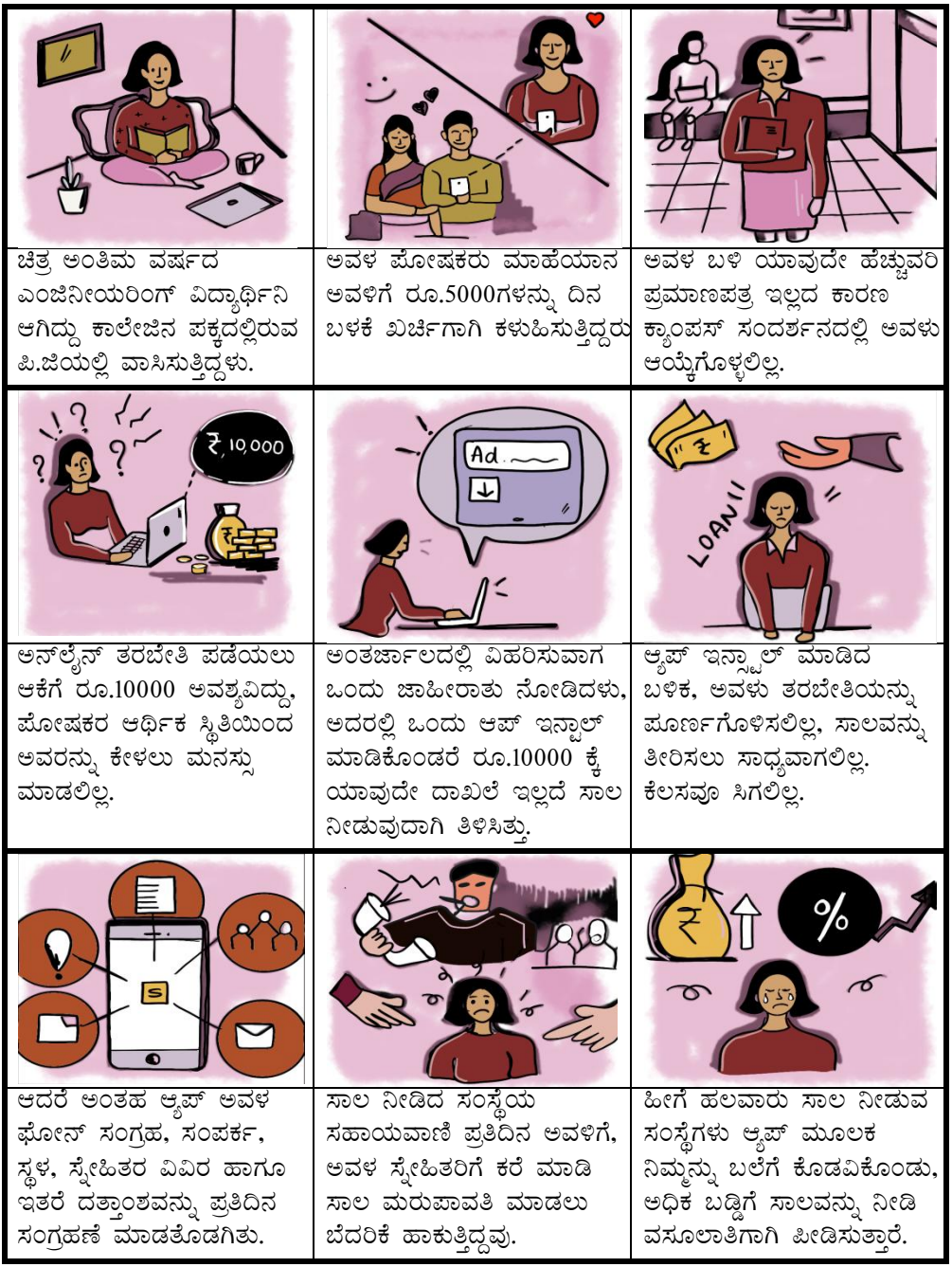
ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ನಕಲಿ ಐಡಿ ಸೃಷ್ಟಿಸಿ ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಡಿಜಿಟಲ್ ವ್ಯಾಮೋಹ ಗೌಪ್ಯತೆ ಉಲ್ಲಂಘನೆಗೆ ಕಾರಣವಾಗಬಹುದು.

ಸಣ್ಣ ಸಾಲಗಳು



ಚಿತ್ರ ಅಂತಿಮ ವರ್ಷದ ಎಂಜಿನೀಯರಿಂಗ್ ವಿದ್ಯಾರ್ಥಿನಿ ಆಗಿದ್ದು ಕಾಲೇಜಿನ ಪಕ್ಕದಲ್ಲಿರುವ ಪಿ.ಜಿಯಲ್ಲಿ ವಾಸಿಸುತ್ತಿದ್ದಳು.	ಅವಳ ಪೋಷಕರು ಮಾಹೆಯಾನ ಅವಳಿಗೆ ರೂ.5000ಗಳನ್ನು ದಿನ ಬಳಕೆ ಖರ್ಚಿಗಾಗಿ ಕಳುಹಿಸುತ್ತಿದ್ದರು	ಅವಳ ಬಳಿ ಯಾವುದೇ ಹೆಚ್ಚುವರಿ ಪ್ರಮಾಣಪತ್ರ ಇಲ್ಲದ ಕಾರಣ ಕ್ಯಾಂಪಸ್ ಸಂದರ್ಶನದಲ್ಲಿ ಅವಳು ಆಯ್ಕೆಗೊಳ್ಳಲಿಲ್ಲ.
ಅನ್‌ಲೈನ್ ತರಬೇತಿ ಪಡೆಯಲು ಆಕೆಗೆ ರೂ.10000 ಅವಶ್ಯವಿದ್ದು, ಪೋಷಕರ ಆರ್ಥಿಕ ಸ್ಥಿತಿಯಿಂದ ಅವರನ್ನು ಕೇಳಲು ಮನಸ್ಸು ಮಾಡಲಿಲ್ಲ.	ಅಂತರ್ಜಾಲದಲ್ಲಿ ವಿಹರಿಸುವಾಗ ಒಂದು ಜಾಹೀರಾತು ನೋಡಿದಳು, ಅದರಲ್ಲಿ ಒಂದು ಆಪ್ ಇನ್ಸ್ಟಾಲ್ ಮಾಡಿಕೊಂಡರೆ ರೂ.10000 ಕ್ಕೆ ಯಾವುದೇ ದಾಖಲೆ ಇಲ್ಲದೆ ಸಾಲ ನೀಡುವುದಾಗಿ ತಿಳಿಸಿತ್ತು.	ಆ್ಯಪ್ ಇನ್ಸ್ಟಾಲ್ ಮಾಡಿದ ಬಳಿಕ, ಅವಳು ತರಬೇತಿಯನ್ನು ಪೂರ್ಣಗೊಳಿಸಲಿಲ್ಲ, ಸಾಲವನ್ನು ತೀರಿಸಲು ಸಾಧ್ಯವಾಗಲಿಲ್ಲ. ಕೆಲಸವೂ ಸಿಗಲಿಲ್ಲ.
ಆದರೆ ಅಂತಹ ಆ್ಯಪ್ ಅವಳ ಫೋನ್ ಸಂಗ್ರಹ, ಸಂಪರ್ಕ, ಸ್ಥಳ, ಸ್ನೇಹಿತರ ವಿವರ ಹಾಗೂ ಇತರೆ ದತ್ತಾಂಶವನ್ನು ಪ್ರತಿದಿನ ಸಂಗ್ರಹಣೆ ಮಾಡತೊಡಗಿತು.	ಸಾಲ ನೀಡಿದ ಸಂಸ್ಥೆಯ ಸಹಾಯವಾಣಿ ಪ್ರತಿದಿನ ಅವಳಿಗೆ, ಅವಳ ಸ್ನೇಹಿತರಿಗೆ ಕರೆ ಮಾಡಿ ಸಾಲ ಮರುಪಾವತಿ ಮಾಡಲು ಬೆದರಿಕೆ ಹಾಕುತ್ತಿದ್ದವು.	ಹೀಗೆ ಹಲವಾರು ಸಾಲ ನೀಡುವ ಸಂಸ್ಥೆಗಳು ಆ್ಯಪ್ ಮೂಲಕ ನಿಮ್ಮನ್ನು ಬಲೆಗೆ ಕೊಡವಿಕೊಂಡು, ಅಧಿಕ ಬಡ್ಡಿಗೆ ಸಾಲವನ್ನು ನೀಡಿ ವಸೂಲಾತಿಗಾಗಿ ಪೀಡಿಸುತ್ತಾರೆ.

ಫ್ಲೈ–ಬೈ–ನೈಟ್ ಮೈಕ್ರೋ ಲೆಂಡಿಂಗ್ ಅಕ್ರಮ ಅನ್ವಯಿಕೆ ಆಧಾರಿತ ಹಣಕಾಸು ವಿತರಕರು ದಿನೇ ದಿನೇ ಅಭಿವೃದ್ಧಿ ಹೊಂದುತ್ತಿದ್ದಾರೆ.ಹಣದ ಅತಿಆಸೆ ಹೊಂದಿದವರ ಉದ್ದೇಶಗಳ ಅನ್ವಯ ತ್ವರಿತ ಸಾಲವನ್ನು ನೀಡುವ ಯೋಜನೆಯಿಂದ ಕಿರಿಯ ಸಾಲಗಾರರನ್ನು ಗುರಿಯಾಗಿಸಿರುತ್ತಾರೆ. ಹಣ ಪಡೆದು ಪಾವತಿಸಲು ವಿಫಲರಾದವರು ತಮ್ಮ ಫೋಟೋಗಳನ್ನು ತಮ್ಮ ಕುಟುಂಬದ ಸದಸ್ಯರಲ್ಲಿ ಮತ್ತು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಗುಂಪುಗಳಲ್ಲಿ ಹರಿಬಿಡಲು ಕಾರಣರಾಗುತ್ತಾರೆ.ಇದು ಅನೇಕರನ್ನು ಹತಾಶೆಗೆ ದೂಡಿದೆ.

.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318– ಮೋಸ

ಐಪಿಸಿ ಕಲಂ 503/ಬಿಎನ್ಎಸ್ 351– ಅಪರಾಧಿ ಬೆದರಿಕೆ

ಐಪಿಸಿ ಕಲಂ 506/ಬಿಎನ್ಎಸ್ 351– ಅಪರಾಧಿ ಬೆದರಿಕೆಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 383/ಬಿಎನ್ಎಸ್ 308– ಸುಲಿಗೆ (ಯಾವುದಾದರೂ ಬೇಡಿಕೆಯಿಂದ)

ಐಪಿಸಿ ಕಲಂ 306/ಬಿಎನ್ಎಸ್ 108– ಆತ್ಮಹತ್ಯೆಗೆ ಪ್ರಚೋದನೆ

ಐಪಿಸಿ ಕಲಂ 499&500/ಬಿಎನ್ಎಸ್ 356– ಮಾನಹಾನಿ ಮತ್ತು ಮಾನಹಾನಿಗೆ ದಂಡನೆ

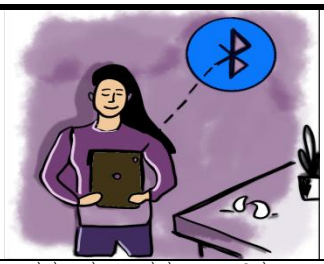
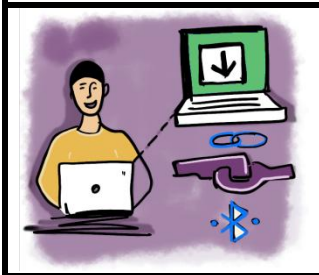
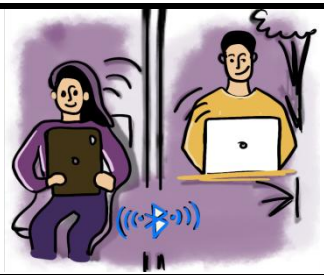
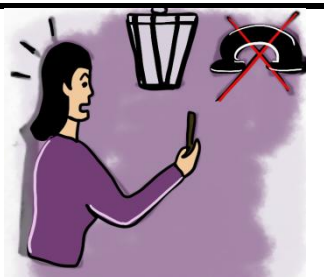
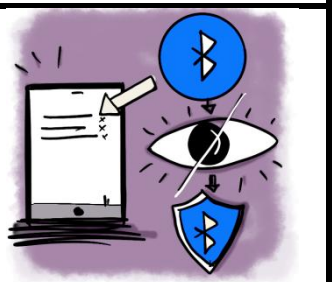
ಐಪಿಸಿ ಕಲಂ 120ಬಿ/ಬಿಎನ್ಎಸ್ 61 – ಅಪರಾಧದ ಪಿತೂರಿಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 34/ಬಿಎನ್ಎಸ್ 3(5) – ಸಾಮಾನ್ಯ ಉದ್ದೇಶಿತ ಕಲಂಗಳಾದ

ಭಾರತೀಯ ರಿಸರ್ವ್ ಬ್ಯಾಂಕ್ ಕಾಯ್ದೆ, 1934 (ಪ್ರಕರಣಕ್ಕನುಗುಣವಾಗಿ)

ಅನ್ವಯಿಕೆ ಆ್ಯಪ್ ಆಧಾರಿತ ಸಾಲಗಳು ಮತ್ತು ಸಾಲಗಾರನು ಅಸುರಕ್ಷಿತನಾಗಿರುತ್ತಾನೆ.

ಬ್ಲೂ ಸ್ನಾರ್ಫಿಂಗ್

		
ಅಶ್ವಿನಿ ಆನ್‌ಲೈನ್ ಉಪನ್ಯಾಸ ಮಾಡಲು, ಕಡಿಮೆ ದರದಲ್ಲಿ ಕಪ್ಪು ಮಾರುಕಟ್ಟೆಯಿಂದ ಒಂದು ಟ್ಯಾಬ್ ಖರೀದಿಸಿ ತಂದಳು.	ಅವಳು ಸದಾ ತನ್ನ ಟ್ಯಾಬ್‌ನ ಬ್ಲೂಟೂಥ್ ಆನ್ ಮಾಡಿಕೊಂಡು ಇಯರ್‌ಪಾಡ್ ಕೂಡಿಸಿಕೊಂಡು ಕಾರ್ಯ ನಿರ್ವಹಿಸುತ್ತಿದ್ದಳು.	ನೆರೆಮನೆಯ ವಾಸು ಕೆಲವು ಹ್ಯಾಕಿಂಗ್ ತಂತ್ರಗಳನ್ನು ಡಾರ್ಕ್ ವೆಬ್ ಮುಖೇನ ತರಬೇತಿ ಪಡೆದು ಕಲಿತುಕೊಂಡಿದ್ದನು.
		
ಅವನು ಒಂದು ಟೂಲ್‌ಕಿಟ್ ಡೌನಲೋಡ್ ಮಾಡಿದ. ಅದು ಯಾವುದೆ ಡಿಜಿಟಲ್ ಸಾಧನದ ನ್ಯೂನ್ಯತೆ ಕಂಡುಹಿಡಿದು ಅದರ ಜೊತೆ ಕೂಡಿಕೊಳ್ಳುತ್ತಿತ್ತು.	ಅಶ್ವಿನಿ ಟ್ಯಾಬ್ ಬ್ಲೂಟೂಥ್ ಸ್ವಲ್ಪ ದೂರದಲ್ಲೇ ಇದ್ದುದರಿಂದ, ಅವಳ ಸಾಧನಕ್ಕೆ ಗುಪ್ತವಾಗಿ ಲಗ್ಗೆ ಹಾಕಿ ಟ್ಯಾಬ್‌ನೊಂದಿಗೆ ಕನೆಕ್ಟ್ ಆಗುತ್ತಾನೆ.	ಯಶಸ್ವಿ ಜೊತೆಗೂಡಿಕೆ ನಂತರ, ಅವಳ ಟ್ಯಾಬ್‌ನಲ್ಲಿ ಫೈಲ್, ಫೋಲ್ಡರ್ ಮತ್ತು ಐಎಂಇಐ ಸಂಖ್ಯೆಗಳಿಗೆ ಪ್ರವೇಶ ಪಡೆಯುತ್ತಾನೆ
		
ನಂತರ ತನ್ನ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಗೆ ಮಾಹಿತಿ ವರ್ಗಾಯಿಸಿ ಅದರ ಮುಖೇನ ಕರೆಗಳು ಮತ್ತು ಸಂದೇಶಗಳನ್ನು ನಿರ್ವಹಿಸುತ್ತಾನೆ.	ಅಶ್ವಿನಿಯ ಟ್ಯಾಬ್‌ನಲ್ಲಿ ಅನೇಕ ಚಿತ್ರ, ಕಡತಗಳು ಕಾಣೆಯಾಗತೊಡಗಿದ್ದು, ಸಿಮ್ ಹೊಂದಿದ ಟ್ಯಾಬ್‌ಗೆ ಯಾವುದೇ ಕರೆಗಳು ಬಾರದಂತೆ ಆಗುತ್ತದೆ.	ಇಂತಹ ಸನ್ನಿವೇಶದಲ್ಲಿ, ಅವಳು ತನ್ನ ಬ್ಲೂಟೂಥ್ ಮ್ಯಾಕ್ ಐಡಿ ತೆರೆದ ರೂಪದಲ್ಲಿ ಬಿಡದೆ ಮರೆಮಾಚಿದ್ದರೆ, ಅವಳು ಸುರಕ್ಷಿತ ವಾಗಿ ಇರುತ್ತಿದ್ದಳು.

ವೈರ್‌ಲೆಸ್, ಬ್ಲೂಟೂಥ್–ಶಕ್ತಗೊಂಡ ಸಾಧನವು ಕಾಣಬಹುದಾದಂತಹ ಸ್ಥಿತಿಯಲ್ಲಿರುವಾಗ ಅವುಗಳನ್ನು ಅತಿಕ್ರಮಿಸುವ ನಿರ್ವಹಣ ಸಾಧನ ಬ್ಲ್ಯೂ ಸ್ನಾರ್ಫಿಂಗ್ ಆಗಿದೆ.ಬಳಕೆದಾರರ ಸಂಪರ್ಕಗಳು, ಕ್ಯಾಲೆಂಡರ್, ಇ–ಮೇಲ್‌ಗಳು ಮತ್ತು ಪಠ್ಯ ಸಂದೇಶಗಳಂತಹ ಬ್ಲೂಟೂಥ್ ಸಾಧನ ದತ್ತಾಂಶಗಳನ್ನು ದೂರದಿಂದಲೇ ಪ್ರವೇಶಿಸಲು ಬ್ಲೂಸ್ನಾರ್ಫಿಂಗ್ ಅತಿಕ್ರಮಣಕಾರರಿಗೆ ಅನುಮತಿಸುತ್ತದೆ.ಅಮಾಯಕರ ಅರಿವಿಗೆ ಬಾರದಂತೆ ಈ ದಾಳಿಯನ್ನು ಮಾಡಲಾಗುವುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ– ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ನಿಮ್ಮ ಮಾಹಿತಿಗಳನ್ನು ಹಿಂಬಾಲಿಸಿ ಪಡೆಯಲು ಹ್ಯಾಕರ್ ಬ್ಲೂಟೂಥ್ ವಿಧಾನ ಅನುಸರಿಸಬಹುದು.

ಕಳುವಾದ ಫೋನ್

ಸ್ಮಿತಾ ಸೆಲ್‌ಫೋನ್ ವ್ಯಸನಿ ಆಗಿದ್ದು. ಸದಾ ಸ್ನ್ಯಾಪ್‌ಚಾಟ್, ವ್ಯಾಟ್ಸಾಪ್, ಇನ್ಸ್ಟಾದಲ್ಲಿ ಸಕ್ರಿಯ ವಾಗಿ ಹರಟೆ ಮಾಡುತ್ತಿದ್ದಳು.

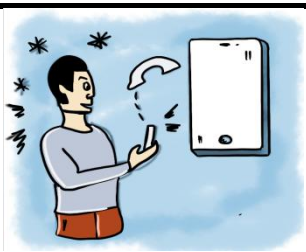
ಅವಳ ಸ್ನೇಹಿತೆ ದಿವ್ಯಾಳೊಂದಿಗೆ ಒಮ್ಮೆ ಸ್ಮಿತಾ ಒಂದು ಉತ್ಸವಕ್ಕೆ ಹೋಗುತ್ತಾಳೆ.

ತಿರುಗುವ ಬಂಡಿ ನೋಡಿ ಪುಳಕಿತರಾಗಿ ಇಬ್ಬರೂ ಸಹ ಅದರಲ್ಲಿ ಕೂರುವ ಇಚ್ಛೆಯಿಂದ ಪ್ರವೇಶ ಚೀಟಿ ಪಡೆದು ಬಂಡಿ ಏರುತ್ತಾರೆ.

ಬಂಡಿ ತಿರುಗುವ ಸಂದರ್ಭದಲ್ಲಿ ಅವಳ ಗಮನಕ್ಕೆ ಬಾರದೇ ಅವಳ ಸೆಲ್‌ಫೋನ್ ಜೇಬಿನಿಂದ ಕೆಳಗೆ ಬೀಳುತ್ತದೆ.

ಬಂಡಿ ಮೇಲೆ ಹೋದಾಗ ಸೆಲ್ಫಿ ತೆಗೆಯುವ ಸಲುವಾಗಿ ಫೋನ್ ಗಾಗಿ ಜೇಬಿಗೆ ಕೈ ಹಾಕಿದಾಗ, ಆಘಾತ ಕಾದಿತ್ತು.

ಅವಳು ತನ್ನ ಮೊಬೈಲ್ ಕಳೆದು ಕೊಂಡಿದ್ದಳು. ಕೂಡಲೇ ದಿವ್ಯಾಳ ಫೋನ್‌ನಿಂದ ತನ್ನ ಮೊಬೈಲ್‌ಗೆ ಕರೆ ಮಾಡಿದಳು.



ಮೊಬೈಲ್ ಕದ್ದಾತ, ಮೊದಲು ಕರೆ ಕಡಿತ ಮಾಡಿ ನಂತರ ಫೋನ್ ಸ್ವಿಚ್ ಆಫ್ ಮಾಡುತ್ತಾನೆ.

ಸ್ಮಿತಾ ಕೂಡಲೇ ತನ್ನ ಫೋನ್‌ನ ಮೈ ಡಿವೈಸ್ ಪೋರ್ಟಲ್‌ಗೆ ಲಾಗಿನ್ ಆಗಿ ತನ್ನ ಫೋನ್ ಜಾಡುಹಿಡಿಯಬಹುದಿತ್ತು.

ಅವಳ ಫೋನಿನ ದತ್ತಾಂಶವನ್ನು ದೂರದಿಂದಲೇ ಸಂಪರ್ಕ ರಹಿತ ವಾಗಿ ಫಾರ್ಮಾಟ್ ಮಾಡಿ ಫೋನ್‌ನಲ್ಲಿನ ದತ್ತಾಂಶದ ರಕ್ಷಣೆಯನ್ನು ಮಾಡಬಹುದಿತ್ತು.

ಕಳುವಾದ ಫೋನ್ ನಿಮಗೆ ಅಸಹಾಯಕ ಮತ್ತು ಹತಾಶೆ ಭಾವನೆಯನ್ನು ನೀಡುತ್ತದೆ.ಮೊಬೈಲ್ ಫೋನ್ ಮತ್ತು ಅದರಲ್ಲಿರುವ ದತ್ತಾಂಶ ಕಳ್ಳರಿಗೆ ಬಹಳ ಮೌಲ್ಯಯುತವಾಗಿದೆ ಮತ್ತು ಇದೇ ರೀತಿಯ ಕಾರಣಗಳಿಗಾಗಿ– ಅವರು ನೈಜ ಮತ್ತು ಭಾವನಾತ್ಮಕ ಮೌಲ್ಯದ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹೊಂದಿರುತ್ತಾರೆ– ಕಳ್ಳತನವು ಮಾಲೀಕರಿಗೆ ಬಹುದೊಡ್ಡ ನಷ್ಟವಾಗಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 378&379/ಬಿಎನ್ಎಸ್ 303–ಕಳ್ಳತನ– ಈ ಕಲಂ ಕಳ್ಳತನದ ಬಗ್ಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ ಮತ್ತು ಕದ್ದ ಫೋನ್‌ಗಳು ಸೇರಿದಂತೆ ಚಲಿಸಬಲ್ಲ ಆಸ್ತಿಯನ್ನು ಕಾನೂನುಬಾಹಿರವಾಗಿ ತೆಗೆದುಕೊಳ್ಳುವುದನ್ನು ಒಳಗೊಂಡಿದೆ.

ಐಪಿಸಿ ಕಲಂ 406/ಬಿಎನ್ಎಸ್ 316– ವಿಶ್ವಾಸ ಭಂಗದ ಅಪರಾಧಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 411/ಬಿಎನ್ಎಸ್ 317– ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಕಳ್ಳತನದ ವಸ್ತುವನ್ನು ಪಡೆದುಕೊಳ್ಳುವುದು.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು ಈ ಕಲಂ ಗುರುತಿನ ಕಳ್ಳತನ ಮತ್ತು ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಹಿಗಳು, ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಅಥವಾ ಯಾವುದೇ ಇತರ ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯಗಳ ಅನಧಿಕೃತ ಬಳಕೆಯನ್ನು ತಿಳಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಡಿ– ಈ ಕಲಂ ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲಗಳನ್ನು ಬಳಸಿಕೊಂಡು ವಂಚನೆಗೆ ಸಂಬಂಧಿಸಿದೆ.

ಕಳುವಾದ ಸೆಲ್‌ಫೋನ್ ನಿಮಗೆ ವೈಯಕ್ತಿಕ ನಷ್ಟವನ್ನುಂಟುಮಾಡಿಬಾಧಿಸುತ್ತದೆ.

ಪರೀಕ್ಷೆಯ ದುಷ್ಕೃತ್ಯ

ಧನ್ಯ ಶೈಕ್ಷಣಿಕವಾಗಿ ಪ್ರವೀಣೆ ವಿದ್ಯಾರ್ಥಿನಿ.	ದುರದೃಷ್ಟವಶಾತ್, ಅವಳು ಕೋವಿಡ್ ಸೋಂಕಿಗೆ ಒಳಗಾಗುತ್ತಾಳೆ ಮತ್ತು ತರಗತಿಗಳಿಗೆ ಹಾಜರಾಗಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲ.	ಧನ್ಯ ಅವಳ ಮುಂಬರುವ ಪರೀಕ್ಷೆಗಳ ಬಗ್ಗೆ ಚಿಂತಿತಳಾಗುತ್ತಾಳೆ.
ಆಕೆಯ ಆತ್ಮೀಯ ಗೆಳತಿ ನಿತ್ಯಾ ಆಕೆಗೆ ಪರೀಕ್ಷೆಗಳಲ್ಲಿ ನಕಲು ಮಾಡಲು ಸಾಧನವೊಂದನ್ನು ಸೂಚಿಸುತ್ತಾಳೆ.	ಸಾಧನವು ದುರ್ಮಾರ್ಗಕ್ಕಾಗಿ ವಿನ್ಯಾಸಗೊಳಿಸಲಾದ ಸ್ಟೆಬ್ಲೂಟೂತ್ ಇಯರ್‌ಪೀಸ್ ಆಗಿರುತ್ತದೆ.	ಧನ್ಯಾ ತನ್ನ ಕಿವಿಯಲ್ಲಿ ಸಾಧನವನ್ನು ಅಳವಡಿಸುತ್ತಾಳೆ. ನಿತ್ಯಾ ಪರೀಕ್ಷೆ ಹಾಲ್‌ನ ಹೊರಗೆ ಕುಳಿತು ಉತ್ತರ ಹೇಳುತ್ತಿರುತ್ತಾಳೆ.
ಧನ್ಯ ಕ್ಯಾಮೆರಾ, ಮೈಕ್ ಮತ್ತು ಇಂಟರ್ನೆಟ್ ಹೊಂದಿರುವ ಸ್ಮಾರ್ಟ್ ಗ್ಲಾಸ್‌ಗಳನ್ನು ಸಹ ಧರಿಸಿರುತ್ತಾಳೆ.	ಧನ್ಯಾಳ ವಿಚಿತ್ರ ನಡವಳಿಕೆಯನ್ನು ಮೇಲ್ವಿಚಾರಕ ಗಮನಿಸುತ್ತಾನೆ ಮತ್ತು ಅವಳನ್ನು ತಪಾಸಣೆಗೆ ಒಳಪಡಿಸುತ್ತಾನೆ.	ಈಗ ಧನ್ಯಾ 3 ವರ್ಷ ಡಿಬಾರ್ ಆಗಿದ್ದಾಳೆ, ಆಕೆಯ ಶೈಕ್ಷಣಿಕ ಭವಿಷ್ಯ ಹಾಳಾಗಿದೆ.

ಪರೀಕ್ಷಾ ದುಷ್ಕೃತ್ಯವನ್ನು ಅಭ್ಯರ್ಥಿಗೆ ಅನಗತ್ಯ ಪ್ರಯೋಜನವನ್ನು ನೀಡಲು ವಿನ್ಯಾಸಗೊಳಿಸಲಾದ ಪರೀಕ್ಷೆಗಳ ನಿಯಮಗಳಿಗೆ ವಿರುದ್ಧವಾಗಿ ಯಾವುದೇ ಉದ್ದೇಶಪೂರ್ವಕ ತಪ್ಪು ಮಾಡುವಿಕೆ ಎಂದು ವ್ಯಾಖ್ಯಾನಿಸಲಾಗಿದೆ. ವಂಚನೆ ಎಂದೂ ಕರೆಯಲ್ಪಡುವ ಈ ದಿನಗಳಲ್ಲಿ ವಿದ್ಯಾರ್ಥಿಗಳು ಶೈಕ್ಷಣಿಕ ವ್ಯವಸ್ಥೆಯ ವಿವಿಧ ಹಂತಗಳಲ್ಲಿ ಹೈಟೆಕ್ ಪರೀಕ್ಷೆಯ ದುಷ್ಕೃತ್ಯವನ್ನು (ಇಲ್ಲದಿದ್ದರೆ ಇ–ಚೀಟಿಂಗ್ ಅಥವಾ ಡಿಜಿಟಲ್ ಚೀಟಿಂಗ್ ಎಂದು ಕರೆಯಲಾಗುತ್ತದೆ) ಆಶ್ರಯಿಸುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318– ಈ ಕಲಂ ವಂಚನೆ ಮತ್ತು ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಆಸ್ತಿಯ ವಿತರಣೆಯನ್ನು ಪ್ರೇರೇಪಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66 R/w 43(c) – ಈ ಕಲಂ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ಒಳಗೊಂಡಂತೆ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳೊಂದಿಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ.
ಕಲಂ 43: ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಹಾನಿ ಮತ್ತು ಡೇಟಾ ಉಲ್ಲಂಘನೆಗಳಿಗೆ ಈ ಕಲಂ ದಂಡವನ್ನು ಒಳಗೊಂಡಿದೆ.

ಪ್ರಿವೆನ್ಷನ್ ಆಫ್ ಅನ್‌ಫೇರ್ ಮೀನ್ಸ್ ಆಕ್ಟ್ (PUMA): ಸೈಬರ್ ಕಾನೂನಲ್ಲದಿದ್ದರೂ, ಪರೀಕ್ಷೆಯ ಸಮಯದಲ್ಲಿ ಮೋಸದ ಅಭ್ಯಾಸಗಳನ್ನು ತಿಳಿಸುವುದರಿಂದ ಈ ಕಾಯಿದೆಯು ಪ್ರಸ್ತುತವಾಗಿದೆ.

ಯುಜಿಸಿ ನಿಯಮಗಳು / ವಿಶ್ವವಿದ್ಯಾನಿಲಯ ನಿಯಮಗಳು: ವಿಶ್ವವಿದ್ಯಾನಿಲಯಗಳು ಮತ್ತು ಶಿಕ್ಷಣ ಸಂಸ್ಥೆಗಳು ಪರೀಕ್ಷೆಯ ದುಷ್ಕೃತ್ಯವನ್ನು ತಡೆಗಟ್ಟಲು ತಮ್ಮದೇ ಆದ ನಿಯಮಗಳು ಮತ್ತು ನಿಬಂಧನೆಗಳನ್ನು ಹೊಂದಿವೆ.

ಶಾರ್ಟ್‌ಕಟ್ ನಿಮ್ಮ ವೃತ್ತಿಜೀವನವನ್ನು ಮೊಟಕುಗೊಳಿಸಬಹುದು.

ಅಂತರ್ಜಾಲ ಸಂಪರ್ಕಿತ ಕಾರುಗಳು

ಮಾಲಾ ತನ್ನ ಮೊದಲನೆ ಕಾರನ್ನು ಖರೀದಿಸಲು ಕಾರ್ ಶೋರೂಮ್‌ಗೆ ಭೇಟಿ ನೀಡುತ್ತಾಳೆ.	ಅಂತರ್ಜಾಲ ಸಂಪರ್ಕಿತ ಕಾರಿನ ವೈಶಿಷ್ಟ್ಯ ಕಂಡು ಅವಳು ಪ್ರಭಾವಿತಳಾಗುತ್ತಾಳೆ.	ಆ ಕಾರಿನ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ಮೊಬೈಲ್ ಫೋನ್‌ನಿಂದ ಸಹ ನಿಯಂತ್ರಿಸಬಹುದಾಗಿರುತ್ತದೆ.
ಆಕೆಯ ಮಾಜಿ ಗೆಳೆಯ ಅರುಣ್ ಯಾವಾಗಲೂ ಅವಳ ಮೇಲೆ ಕಣ್ಣಿಡಲು ಅವಳನ್ನು ಸ್ನೂಪ್ ಮಾಡುತ್ತಿದ್ದನು.	ಅವಳ ಸಂಪರ್ಕಿತ ಕಾರಿನಲ್ಲಿರುವ ಭದ್ರತಾ ಲೋಪದೋಷಗಳನ್ನು ಅವನು ಅರಿತು ಅದನ್ನು ಹ್ಯಾಕ್ ಮಾಡುತ್ತಾನೆ.	ಅರುಣ್ ಅವಳ ಸ್ಥಳ ಮತ್ತು ಅವಳ ಪ್ರಯಾಣದ ಇತರ ವಿವರಗಳಿಗೆ ಪ್ರವೇಶವನ್ನು ಪಡೆಯುತ್ತಾನೆ.
ಮಾಲಾ ತನ್ನ ಕಾರಿನ ಫರ್ಮ್‌ವೇರ್ & ಸಾಫ್ಟ್‌ವೇರ್ ಪ್ಯಾಚ್‌ಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ನವೀಕರಿಸಿರಲಿಲ್ಲ.	ಅವುಗಳಲ್ಲಿ ವಾಹನ ಕಳ್ಳತನ, ಸುರಕ್ಷತಾ ನಿರ್ಣಾಯಕ ವ್ಯವಸ್ಥೆಗಳ ಕುಶಲತೆ, ವೈಯಕ್ತಿಕ ಡೇಟಾದ ಪರೀಕ್ಷೆ, ಆಯ್ಕೆಗಳು ಸೇರಿರುತ್ತವೆ.	ಮಿಸ್ ಕಾನ್ಫಿಗರೇಶನ್ ಸಮಸ್ಯೆಗಳು ಮತ್ತು ಸೇವೆಯ ನಿರಾಕರಣೆಯು ಸಂಪರ್ಕಿತ ಕಾರುಗಳಲ್ಲಿ ಒಳಗೊಂಡಿರುವ ಕೆಲವು ಭದ್ರತಾ ಅಪಾಯಗಳಾಗಿವೆ.

ಸಂಪರ್ಕಿತ ಕಾರುಗಳು 'ಇಂಟರ್ನೆಟ್ ಆಫ್ ಥಿಂಗ್ಸ್' ನ ಒಂದು ಭಾಗವಾಗಿದ್ದು, ಇದು ನಮ್ಮ ಜೀವನವನ್ನು ಸುಲಭಗೊಳಿಸುವ ಉದ್ದೇಶದಿಂದ ದೈನಂದಿನ ವಸ್ತುಗಳನ್ನು ಇಂಟರ್ನೆಟ್‌ಗೆ ಸಂಪರ್ಕಿಸುವುದನ್ನು ಸೂಚಿಸುತ್ತದೆ. ಸಂಪರ್ಕಿತ ಕಾರು ದಿನೇ ದಿನೇ ಸಾಫ್ಟ್‌ವೇರ್–ನಿಯಂತ್ರಿತ, ನೆಟ್‌ವರ್ಕ್–ಅರಿತ ಮತ್ತು ಅಲ್ಟ್ರಾ–ಕನೆಕ್ಟ್ ಸೌಲಭ್ಯ ಹೊಂದುತ್ತಿದೆ, ಇದು ಡೇಟಾವನ್ನು ರವಾನಿಸುತ್ತದೆ ಮತ್ತು ರಸ್ತೆ ಮತ್ತು ಅದರ ಸುತ್ತಲಿನ ಪ್ರತಿಯೊಂದು ವಾಹನದೊಂದಿಗೆ "ಸಂವಾದಿಸುತ್ತಿದೆ", ಇದರಿಂದ ಹ್ಯಾಕ್ ಆಗುವ ಸಾಧ್ಯತೆಗಳನ್ನು ಹೆಚ್ಚಿಸುತ್ತದೆ!

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಐಪಿಸಿ ಕಲಂ 354 ಡಿ/ಬಿಎನ್‌ಎಸ್ 78 – ಈ ಕಲಂ ಆನ್‌ಲೈನ್ ಸ್ಟಾಕಿಂಗ್ ಅನ್ನು ಸಹ ಒಳಗೊಳ್ಳುತ್ತದೆ. ಇಂಟರ್ನೆಟ್, ಇಮೇಲ್ ಅಥವಾ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಂವಹನಗಳ ಇತರ ರೂಪಗಳ ಬಳಕೆಯನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುವುದನ್ನು ಹೇಳಲು 66 R/W 43 (a), ಮತ್ತು DOS ಅನ್ನು ಉಂಟುಮಾಡಿದರೆ 43(f) ಅನ್ವಯವಾಗುತ್ತದೆ.

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ.

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66– ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಬಿ– ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಕಳ್ಳತನದ ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಅಥವಾ ಸಂವಹನ ಸಾಧನವನ್ನು ಸ್ವೀಕರಿಸಿದರೆ ಶಿಕ್ಷೆ

ಮೋಟಾರು ವಾಹನಗಳ ಕಾಯಿದೆ, 1988:

ಸಂಪರ್ಕಿತ ವಾಹನಗಳನ್ನು ಒಳಗೊಂಡ ಅಪಘಾತಗಳ ಸಂದರ್ಭದಲ್ಲಿ ರಸ್ತೆ ಸುರಕ್ಷತೆ, ಪರವಾನಗಿ, ನೋಂದಣಿ ಮತ್ತು ಹೊಣೆಗಾರಿಕೆಗೆ ಸಂಬಂಧಿಸಿದ ವಿವಿಧ ಕಲಂಗಳು.

ಗೌಪ್ಯತೆ ಕಾನೂನುಗಳು:

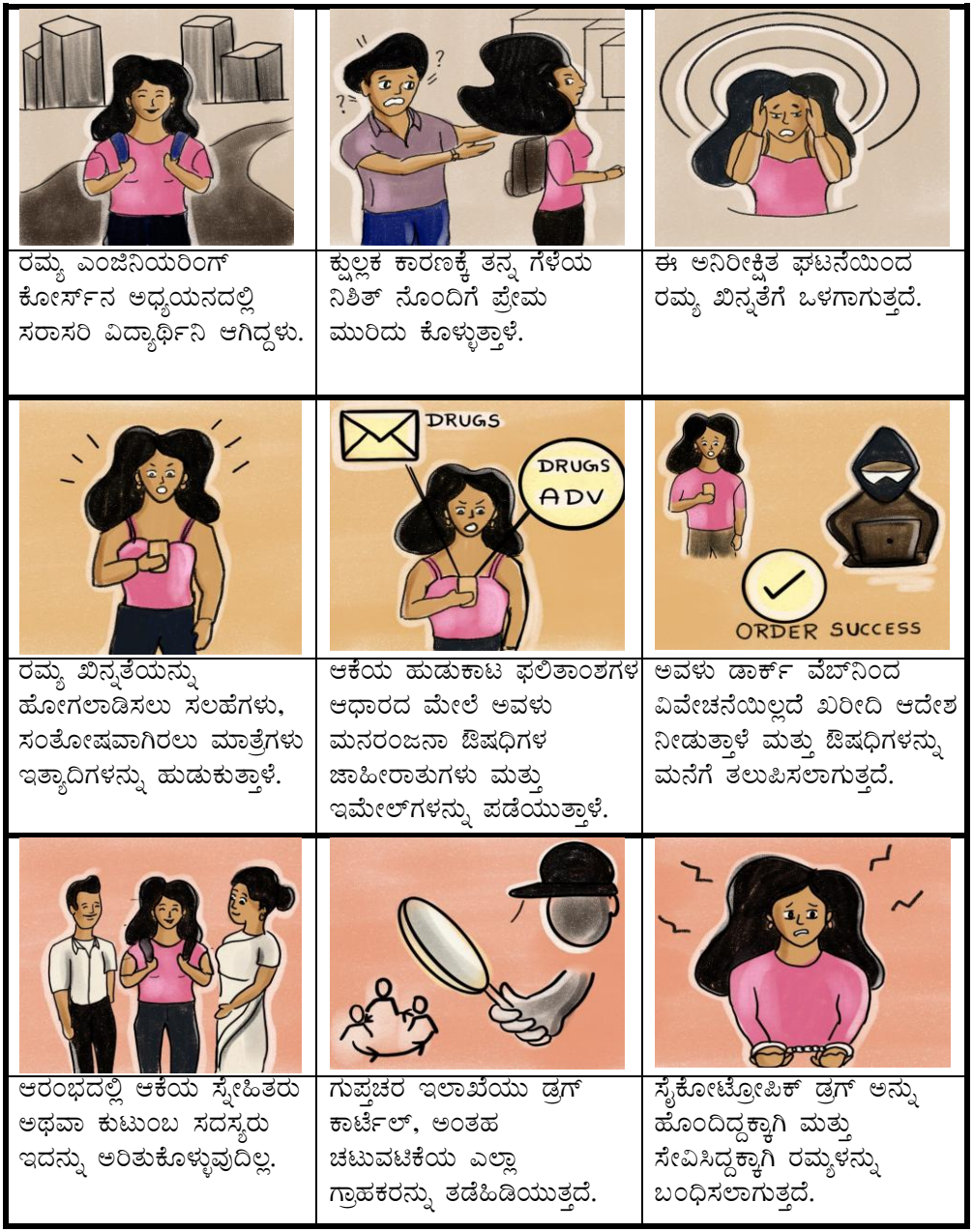
ವೈಯಕ್ತಿಕ ಡೇಟಾ ಸಂರಕ್ಷಣಾ ಮಸೂದೆ (ಪ್ರಸ್ತಾಪಿತ) ಅಥವಾ ಅಸ್ತಿತ್ವದಲ್ಲಿರುವ ಕಾನೂನುಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ಯಾವುದೇ ತಿದ್ದುಪಡಿಗಳು. ಈ ಕಾನೂನುಗಳು ಸಂಪರ್ಕಿತ ವಾಹನಗಳ ಮೂಲಕ ವೈಯಕ್ತಿಕ ಡೇಟಾದ ಸಂಗ್ರಹಣೆ, ಸಂಗ್ರಹಣೆ, ಸಂಸ್ಕರಣೆ ಮತ್ತು ಹಂಚಿಕೆಯನ್ನು ನಿಯಂತ್ರಿಸುತ್ತದೆ.

ಗ್ರಾಹಕ ಸಂರಕ್ಷಣಾ ಕಾನೂನುಗಳು:

ಗ್ರಾಹಕ ಸಂರಕ್ಷಣಾ ಕಾಯ್ದೆ, 2019: ಸಂಪರ್ಕವಿಲ್ಲದ ಕಾರ್ ಸಿಸ್ಟಮ್‌ಗಳಲ್ಲಿ ದೋಷಗಳು ಅಥವಾ ಅಸಮರ್ಪಕ ಕಾರ್ಯಗಳ ಸಂದರ್ಭದಲ್ಲಿ ಉತ್ಪಾದಕತೆ ಮತ್ತು ಗ್ರಾಹಕರ ಹಕ್ಕುಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ಕಲಂಗಳು.

IoT-ಇಂಟರ್ನೆಟ್ ಆಫ್ ಥಿಂಗ್ಸ್ ಅನ್ನು ಬಳಸುವಾಗ ನಿಮ್ಮ IoT-ಇಂಟಲಿಜೆನ್ಸ್ ಆಫ್ ಥಿಂಕಿಂಗ್ ಅನ್ನು ಸಹ ಬಳಸಿ.

ಡ್ರಗ್ಸ್ ಟ್ರಾಫಿಕ್ಕಿಂಗ್



ರಮ್ಯ ಎಂಜಿನಿಯರಿಂಗ್ ಕೋರ್ಸ್‌ನ ಅಧ್ಯಯನದಲ್ಲಿ ಸರಾಸರಿ ವಿದ್ಯಾರ್ಥಿನಿ ಆಗಿದ್ದಳು.

ಕ್ಷುಲ್ಲಕ ಕಾರಣಕ್ಕೆ ತನ್ನ ಗೆಳೆಯ ನಿಶಿತ್ ನೊಂದಿಗೆ ಪ್ರೇಮ ಮುರಿದು ಕೊಳ್ಳುತ್ತಾಳೆ.

ಈ ಅನಿರೀಕ್ಷಿತ ಘಟನೆಯಿಂದ ರಮ್ಯ ಖಿನ್ನತೆಗೆ ಒಳಗಾಗುತ್ತದೆ.

ರಮ್ಯ ಖಿನ್ನತೆಯನ್ನು ಹೋಗಲಾಡಿಸಲು ಸಲಹೆಗಳು, ಸಂತೋಷವಾಗಿರಲು ಮಾತ್ರೆಗಳು ಇತ್ಯಾದಿಗಳನ್ನು ಹುಡುಕುತ್ತಾಳೆ.

ಆಕೆಯ ಹುಡುಕಾಟ ಫಲಿತಾಂಶಗಳ ಆಧಾರದ ಮೇಲೆ ಅವಳು ಮನರಂಜನಾ ಔಷಧಿಗಳ ಜಾಹೀರಾತುಗಳು ಮತ್ತು ಇಮೇಲ್‌ಗಳನ್ನು ಪಡೆಯುತ್ತಾಳೆ.

ಅವಳು ಡಾರ್ಕ್ ವೆಬ್‌ನಿಂದ ವಿವೇಚನೆಯಿಲ್ಲದೆ ಖರೀದಿ ಆದೇಶ ನೀಡುತ್ತಾಳೆ ಮತ್ತು ಔಷಧಿಗಳನ್ನು ಮನೆಗೆ ತಲುಪಿಸಲಾಗುತ್ತದೆ.

ಆರಂಭದಲ್ಲಿ ಆಕೆಯ ಸ್ನೇಹಿತರು ಅಥವಾ ಕುಟುಂಬ ಸದಸ್ಯರು ಇದನ್ನು ಅರಿತುಕೊಳ್ಳುವುದಿಲ್ಲ.

ಗುಪ್ತಚರ ಇಲಾಖೆಯು ಡ್ರಗ್ ಕಾರ್ಟೆಲ್, ಅಂತಹ ಚಟುವಟಿಕೆಯ ಎಲ್ಲಾ ಗ್ರಾಹಕರನ್ನು ತಡೆಹಿಡಿಯುತ್ತದೆ.

ಸೈಕೋಟ್ರೋಪಿಕ್ ಡ್ರಗ್ ಅನ್ನು ಹೊಂದಿದ್ದಕ್ಕಾಗಿ ಮತ್ತು ಸೇವಿಸಿದ್ದಕ್ಕಾಗಿ ರಮ್ಯಳನ್ನು ಬಂಧಿಸಲಾಗುತ್ತದೆ.

ಕಳೆದ ದಶಕದಲ್ಲಿ ಹೊಸ ಅಂತರ್ಜಾಲ ತಂತ್ರಜ್ಞಾನಗಳ ಬೆಳವಣಿಗೆಯಿಂದ ಆನ್‌ಲೈನ್ ಮಾದಕ ಮಾರುಕಟ್ಟೆಯು ಪ್ರಮುಖ ಸರಬರಾಜುದಾರನಾಗಿ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತಿದೆ. ಅಕ್ರಮ ವಸ್ತುಗಳನ್ನು ಮಾರಾಟ ಮಾಡಲು ಮತ್ತು ಖರೀದಿಸಲು ಅಂತರ್ಜಾಲವು ಈಗ ವರ್ಚುವಲ್ ಮಾರುಕಟ್ಟೆಯನ್ನು (ಸರ್ಫೇಸ್ ವೆಬ್ ಮತ್ತು ಡಾರ್ಕ್ ವೆಬ್‌ನಲ್ಲಿ) ಆಯೋಜಿಸುತ್ತದೆ. ಹೆಚ್ಚಿನ ವೇಗ, ಜಾಗತಿಕ ಪ್ರಭಾವ ಮತ್ತು ಸುಲಭವಾಗಿ ಪ್ರವೇಶಿಸಬಹುದಾದ ವೇದಿಕೆಗಳು ಅದರ ಜನಪ್ರಿಯತೆಗೆ ಕೆಲವು ಕಾರಣಗಳಾಗಿವೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಎನ್‌ಡಿಪಿಎಸ್‌ನ ವಿಭಾಗಗಳು (ದಾಳಿಯ ಸಮಯದಲ್ಲಿ ಅವಳು ಹೊಂದಿದ್ದ ಪ್ರಮಾಣವನ್ನು ಅವಲಂಬಿಸಿ ಕಲಂಗಳು ಅನ್ವಯಿಸುತ್ತವೆ, ಅದು ವೈಯಕ್ತಿಕ ಬಳಕೆ ಅಥವಾ ವಾಣಿಜ್ಯ ಪ್ರಮಾಣವಾಗಿರಬಹುದು, ಮತ್ತು ಅವಳು ನಿಷೇಧಿತ ಪದಾರ್ಥಗಳನ್ನು ಸರಬರಾಜು ಮಾಡುತ್ತಿದ್ದಾಳೆಯೇ ಅಥವಾ ವ್ಯಾಪಾರ/ವ್ಯವಹಾರ ಮಾಡುತ್ತಿದ್ದಾಳೆಯೇ ಎಂಬುದಕ್ಕೂ ಸಹ ಕಲಂಗಳು ಅನ್ವಯಿಸುತ್ತವೆ.)

ಕಲಂ 8(ಸಿ): ಕೆಲವು ಕಾರ್ಯಾಚರಣೆಗಳ ನಿಷೇಧ
ಕಲಂ 18: ತಯಾರಿಸಿದ ಔಷಧಗಳು ಮತ್ತು ಸಿದ್ಧತೆಗಳಿಗೆ ಸಂಬಂಧಿಸಿದಂತೆ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ
ಕಲಂ 21: ಗಸಗಸೆ ಸ್ಟ್ರಾಗೆ ಸಂಬಂಧಿಸಿದಂತೆ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ
ಕಲಂ 27ಎ: ಅಕ್ರಮ ಸಾಗಣೆಗೆ ಹಣಕಾಸು ಒದಗಿಸುವುದು ಮತ್ತು ಅಪರಾಧಿಗಳಿಗೆ ಆಶ್ರಯ ನೀಡುವುದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಖಿನ್ನತೆಗೆ ಒಳಗಾದಾಗ ನಿಷೇಧಿತ ಮಾದಕಗಳ ಬಳಕೆಯು, ನೀವು ಬದುಕುವ ಹಕ್ಕು ಮತ್ತು ವೈಯಕ್ತಿಕ ಸ್ವಾತಂತ್ರ್ಯದ ಹಕ್ಕನ್ನು ಮತ್ತು ನಿಮ್ಮ ಸ್ವಾತಂತ್ರ್ಯವನ್ನು ನಿಗ್ರಹಿಸುತ್ತದೆ.

ಡಾಕ್ಸಿಂಗ್

ಹಿತ ಕಾರ್ತಿಕ್ ಜೊತೆ ಲಿವ್-ಇನ್ ಸಂಬಂಧದಲ್ಲಿರುತ್ತಾಳೆ.	ಅವಳು ಯಾವಾಗಲೂ ಕನಸು ಕಾಣುತ್ತಿದ್ದಂತೆ ಯುನೈಟೆಡ್ ಕಿಂಗ್‌ಡಮ್‌ನಿಂದ ಉತ್ತಮ ಉದ್ಯೋಗದ ಪ್ರಸ್ತಾಪವನ್ನು ಪಡೆಯುತ್ತಾಳೆ.	ಕಾರ್ತಿಕ್ ಜೊತೆಗಿನ ತನ್ನ ನಾಲ್ಕು ವರ್ಷಗಳ ಸಂಬಂಧವನ್ನು ಕೊನೆಗೊಳಿಸಿ ಹೊಸ ಜೀವನವನ್ನು ಪ್ರಾರಂಭಿಸಲು ಹಿತ ನಿರ್ಧರಿಸುತ್ತಾಳೆ.
ಕಾರ್ತಿಕ್ ಘಾಸಿಗೊಳ್ಳುತ್ತಾನೆ ಹಾಗು ಅವಳಿಗೆ ತಕ್ಕ ಪಾಠ ಕಲಿಸಲು ನಿರ್ಧರಿಸುತ್ತಾನೆ.	ಅವನು ಹಿತಳ ವೈಯಕ್ತಿಕ ಸೆಲ್ ಫೋನ್ ಸಂಖ್ಯೆಯನ್ನು ಅಂತರ್ಜಾಲದಲ್ಲಿ ಹರಿಬಿಡುತ್ತಾನೆ.	ತಮ್ಮ ಖಾಸಗಿ ಸಂಭಾಷಣೆಯ ಸ್ಕ್ರೀನ್ ಶಾಟ್‌ಗಳನ್ನು, ಮುಜುಗರದ ವೈಯಕ್ತಿಕ ವಿವರಗಳು ಮತ್ತು ಬ್ಯಾಂಕ್ ಖಾತೆಯ ವಿವರಗಳನ್ನು ಸಹ ಹರಿಬಿಡುತ್ತಾನೆ.
ಹಿತ ಅಪರಿಚಿತ ಸಂಖ್ಯೆಗಳಿಂದ ಕಿರುಕುಳದ ಕರೆಗಳನ್ನು ಸ್ವೀಕರಿಸಲು ಪ್ರಾರಂಭಿಸುತ್ತಾಳೆ.	ಹಿಂಬಾಲಕರು ಕೂಡ ಆಕೆಯ ಮನೆಯ ಬಳಿ ಬಂದು ಅವಳನ್ನು ಭೇಟಿಯಾಗಲು ಪ್ರಯತ್ನಿಸುತ್ತಾರೆ.	ಹಿತ ಡಾಕ್ಸಿಂಗ್ ಮತ್ತು ಸೈಬರ್ ಸ್ಟಾಕಿಂಗ್‌ನ ಬಲಿಪಶುಯಾಗುತ್ತಾಳೆ.

ಯಾರನ್ನಾದರೂ ಡಾಕ್ಸ್ ಮಾಡುವುದು ಎಂದರೆ ಅವರ ವೈಯಕ್ತಿಕ ಅಥವಾ ಖಾಸಗಿ ಮಾಹಿತಿಯನ್ನು ಅವರಿಗೆ ಹಾನಿಮಾಡಲು ಅಥವಾ ಮುಜುಗರವನ್ನು ಉಂಟುಮಾಡಲು ಹರಿಬಿಡುವುದು. ಇದು ನೈಜ ಜಗತ್ತಿನಲ್ಲಿಯೂ ಸಂಭವಿಸಬಹುದು, ಆದರೆ ಅಂತರ್ಜಾಲವು ಈ ಮಾಹಿತಿಯನ್ನು ಹುಡುಕಲು ಮತ್ತು ಹರಿಬಿಡಲು ವ್ಯಾಪಕವಾಗಿ ಜನರನ್ನು ತಲುಪಲು ಸುಲಭಗೊಳಿಸಿದೆ. Doxxing ಬೇರೊಬ್ಬರ ಮನೆಯ ವಿಳಾಸ ಅಥವಾ ಕೆಲಸದ ಸ್ಥಳ, ಸಾಮಾಜಿಕ ಭದ್ರತೆ ಅಥವಾ ಫೋನ್ ಸಂಖ್ಯೆ, ಖಾಸಗಿ ಪತ್ರವ್ಯವಹಾರ ಅಥವಾ ಚಿತ್ರಗಳು, ಅಪರಾಧ ಇತಿಹಾಸ, IP ವಿಳಾಸ ಅಥವಾ ಇತರ ವಿವರಗಳಂತಹ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಗೊಳಿಸುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ – ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಒಬ್ಬ ವ್ಯಕ್ತಿಯ ವೇಷ ಹಾಕುವ ಉದ್ದೇಶದಿಂದ ಅಥವಾ ಅವರಿಗೆ ಆರ್ಥಿಕ ಅಥವಾ ಪ್ರತಿಷ್ಠೆ ಹಾನಿಯನ್ನು ಉಂಟುಮಾಡುವ ಉದ್ದೇಶದಿಂದ ಸೆಷನ್ ಅಪಹರಣದ ದಾಳಿಯನ್ನು ನಡೆಸಿದರೆ, ಈ ಕಲಂ ಅನ್ವಯಿಸಬಹುದು.)

ಮಾ.ತ.ಕಾ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 72– ಈ ಕಲಂ ಸೇವಾ ಪೂರೈಕೆದಾರರು ನಿರ್ವಹಿಸುವ ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆ ಮತ್ತು ವೈಯಕ್ತಿಕತೆಯನ್ನು ರಕ್ಷಿಸುತ್ತದೆ.

ಐಪಿಸಿ ಕಲಂ 354ಡಿ/ಬಿಎನ್ಎಸ್ 78–ಹಿಂಬಾಲಿಕೆ,

ಐಪಿಸಿ ಕಲಂ 509/ಬಿಎನ್ಎಸ್ 79 – ಹೆಣ್ಣಿನ ಗಾಂಭೀರ್ಯಕ್ಕೆ ಅಪಮಾನವಾಗುವ ಉದ್ದೇಶದ ಪದಗಳು, ಸನ್ನೆ ಅಥವಾ ಅಭಿನಯ

ಬಾಕ್ಸಿಂಗ್‌ನಲ್ಲಿರುವಂತೆ, ಡಾಕ್ಸಿಂಗ್‌ನಲ್ಲಿಯೂ ಆರೋಪಿಯು ನಾಕ್‌ಔಟ್ ಪಂಚ್ ಅನ್ನು ಪ್ರಯೋಗಿಸಬಹುದು ಇದರಿಂದ ಬಲಿಪಶುವಿಗೆ ಸರಿಪಡಿಸಲಾಗದ ಗಾಯವಾಗುತ್ತದೆ.

ಸೈಬರ್ ಗ್ರೂಮಿಂಗ್

ಇಶಾ ಹೈಸ್ಕೂಲ್ ಹುಡುಗಿ. ತಂದೆ ತಾಯಿಗೆ ಒಬ್ಬಳೇ ಮಗಳು. ತಂದೆ–ತಾಯಿ ಇಬ್ಬರೂ ಐಟಿ ಉದ್ಯೋಗಿಗಳು.

ಪೋಷಕರು ಮುಂಜಾನೆ ಬೇಗ ಮನೆಯಿಂದ ಹೊರಟು ರಾತ್ರಿ ತಡವಾಗಿ ಹಿಂತಿರುಗುತ್ತಾರೆ.

ಶಾಲೆಯಿಂದ ಮನೆಗೆ ಬಂದ ನಂತರ, ಇಶಾ ತನ್ನನ್ನು ತಾನು ತೊಡಗಿಸಿಕೊಳ್ಳಲು ಇಂಟರ್ನೆಟ್ ಬ್ರೌಸ್ ಮಾಡುತ್ತಾಳೆ.

ಒಂದು ದಿನ, ಅವಳು ಅಸೀಮ್ ಎಂಬ ವ್ಯಕ್ತಿಯಿಂದ ಸ್ನೇಹಿತರ ವಿನಂತಿಯನ್ನು ಪಡೆಯುತ್ತಾಳೆ.

ಅವಳು ಅವನ ವಿನಂತಿಯನ್ನು ಸ್ವೀಕರಿಸುವುದಿಲ್ಲ. ಹೀಗಾಗಿ, ಅಸೀಮ್ ಆಕೆಗೆ ನೇರ ಸಂದೇಶ (DM) ಕಳುಹಿಸುತ್ತಾನೆ. ಅವನು ಅವಳ ತಂದೆಯ ಸಹಪಾಠಿ ಎಂದು ಅವಳಿಗೆ ಮನವರಿಕೆ ಮಾಡುತ್ತಾನೆ.

ಅವಳ ನಂಬಿಕೆಯನ್ನು ಗೆಲ್ಲುತ್ತಾನೆ, ತಾನು ಮತ್ತು ಅವಳ ತಂದೆ ಮಾತನಾಡುತ್ತಿಲ್ಲ. ಅವರನ್ನು ಒಂದುಗೂಡಿಸಲು ಅವಳು ಸಹಾಯ ಮಾಡಬೇಕೆಂದು ಕೇಳಿಕೊಳ್ಳುತ್ತಾನೆ.

ಇದಕ್ಕಾಗಿ ಅವಳ ಸಹಾಯ ಕೋರುತ್ತಾನೆ ಮತ್ತು ಪೋಷಕರಿಗೆ ಇದನ್ನು ಹೇಳದಂತೆ ತಿಳಿಸುತ್ತಾನೆ. ಅವಳು ಸಹ ಒಪ್ಪುತ್ತಾಳೆ.

ಒಂದು ದಿನ, ಅವನು ಅವಳನ್ನು ಅವಳ ಶಾಲೆಯ ಹೊರಗೆ ಭೇಟಿಯಾಗುತ್ತಾನೆ ಮತ್ತು ಅವಳನ್ನು ತನ್ನ ಕಾರಿನಲ್ಲಿ ಕರೆದುಕೊಂಡು ಹೋಗುತ್ತಾನೆ.

ಈ ಘಟನೆ ಬಗ್ಗೆ ಯಾರಿಗಾದರೂ ಹೇಳಿದರೆ ವೀಡಿಯೊವನ್ನು ಸೋರಿಕೆ ಮಾಡುವುದಾಗಿ ಬೆದರಿಕೆ ಹಾಕುತ್ತಾನೆ.

ಸೈಬರ್ ಗ್ರೂಮಿಂಗ್ ಎನ್ನುವುದು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಯುವ ವ್ಯಕ್ತಿಯೊಂದಿಗೆ ಲೈಂಗಿಕ ಸಂಪರ್ಕ ಮತ್ತು/ಅಥವಾ ದೈಹಿಕ ಭೇಟಿಯನ್ನು ಸಾಧಿಸಿ ಅವರನ್ನು ಲೈಂಗಿಕ ನಿಂದನೆಗೆ ಗುರಿಪಡಿಸುವ ಉದ್ದೇಶದಿಂದ ಸ್ನೇಹ ಬೆಳೆಸುವ ಪ್ರಕ್ರಿಯೆಯಾಗಿದೆ. ಸೈಬರ್ ಗ್ರೂಮಿಂಗ್ ಎಂದರೆ ಯಾರಾದರೂ (ಸಾಮಾನ್ಯವಾಗಿ ವಯಸ್ಕರು) ಮಕ್ಕಳೊಂದಿಗೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸ್ನೇಹ ಬೆಳೆಸುತ್ತಾರೆ ಮತ್ತು ಲೈಂಗಿಕ ನಿಂದನೆ, ಲೈಂಗಿಕ ಶೋಷಣೆ ಅಥವಾ ಕಳ್ಳಸಾಗಣೆಯಂತಹ ಉದ್ದೇಶಗಳೊಂದಿಗೆ ಭಾವನಾತ್ಮಕ ಸಂಪರ್ಕವನ್ನು ನಿರ್ಮಿಸುತ್ತಾರೆ. ಸೈಬರ್ ಗ್ರೂಮಿಂಗ್‌ನ ಮುಖ್ಯ ಗುರಿಗಳೆಂದರೆ: ಮಗುವಿನಿಂದ ವಿಶ್ವಾಸವನ್ನು ಗಳಿಸುವುದು, ಮಗುವಿನಿಂದ ನಿಕಟ ಮತ್ತು ವೈಯಕ್ತಿಕ ಡೇಟಾವನ್ನು ಪಡೆಯುವುದು (ಸಾಮಾನ್ಯವಾಗಿ ಲೈಂಗಿಕ ಸ್ವಭಾವದ ಲೈಂಗಿಕ ಸಂಭಾಷಣೆಗಳು, ಚಿತ್ರಗಳು ಅಥವಾ ವೀಡಿಯೊಗಳು) ಇಂತಹದ್ದನ್ನು ಬಳಸಿ ಅವರನ್ನು ಬೆದರಿಕೆ ಮತ್ತು ಬ್ಲ್ಯಾಕ್‌ಮೇಲ್ ಮಾಡವುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

POCSO, 67(B) IT ಕಾಯಿದೆಯ ಕಲಂಗಳು ಮತ್ತು ಅಶ್ಲೀಲ ಅಥವಾ ಲೈಂಗಿಕ ಅಂಶವನ್ನು ಬಹಿರಂಗಪಡಿಸುವುದು

ಕಲಂ 292 IPC/ಬಿಎನ್‌ಎಸ್ 294

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66 ಇ– ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

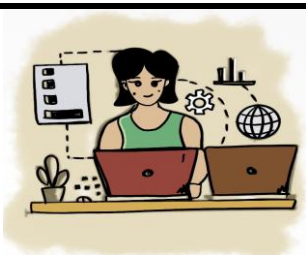
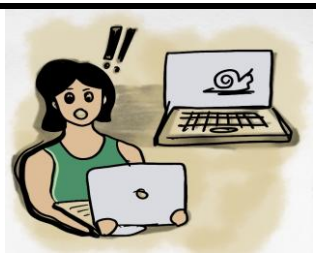
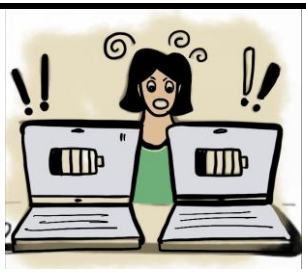
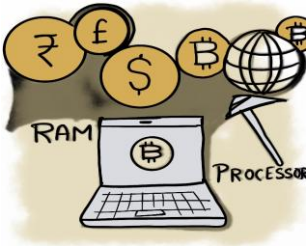
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67– ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಎ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಬಿ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವಿನಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿ ವಿದ್ಯುನ್ಮಾನರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಾಯ್ದೆಗಳು

ಇಂಟರ್ನೆಟ್ ಅನ್ನು ಅತ್ಯಂತ ನೈತಿಕತೆಯೊಂದಿಗೆ ಬ್ರೌಸ್ ಮಾಡಿ (ಸರಿ ಮತ್ತು ತಪ್ಪು ಅಥವಾ ಒಳ್ಳೆಯ ಮತ್ತು ಕೆಟ್ಟ ನಡವಳಿಕೆಯ ನಡುವಿನ ವ್ಯತ್ಯಾಸಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ತತ್ವಗಳು) ಇಲ್ಲದಿದ್ದರೆ ನೀವು ನಿಶ್ಚಿತವಾಗಿ ಸೈಬರ್ ಅಪರಾಧಗಳ ಬಲಿಪಶು ಆಗುವುದು ಖಚಿತ.

ಕ್ರಿಪ್ಟೋ ವಂಚನೆಗಳು

		
ಮನು ಕಾಲ್ ಸೆಂಟರ್ ಉದ್ಯೋಗಿ. ರಾತ್ರಿ ಪಾಳಿಯಲ್ಲಿ ಕೆಲಸ ಮಾಡುತ್ತಾಳೆ.	ಹಗಲಿನಲ್ಲಿ ಅವಳು ಮನೆಕೆಲಸಗಳ ನಂತರ ಬಿಡುವಿನ ವೇಳೆಯಲ್ಲಿ ಷೇರು ವ್ಯಾಪಾರದಲ್ಲಿ ತೊಡಗುತ್ತಿದ್ದಳು.	ಒಂದು ದಿನ, ಅವಳು ಕ್ರಿಪ್ಟೋ ಟ್ರೇಡಿಂಗ್‌ನಲ್ಲಿ 5x ರಿಟರ್ನ್‌ಗಳ ಭರವಸೆ ನೀಡುವ ಜಾಹೀರಾತನ್ನು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ನೋಡುತ್ತಾಳೆ.
		
ಜಾಹೀರಾತಿನಿಂದ ಬೆರಗಾದ ಅವಳು ತನ್ನ ಕ್ರಿಪ್ಟೋ ಟ್ರೇಡಿಂಗ್ ಖಾತೆಯನ್ನು ತೆರೆದು ತಾನು ಕಷ್ಟಪಟ್ಟು ಗಳಿಸಿದ ಹಣವನ್ನು ಹೂಡಿಕೆ ಮಾಡುತ್ತಾಳೆ.	ಅವಳು ಹೂಡಿಕೆ ಮಾಡಿದ ಕ್ರಿಪ್ಟೋಸ್ ಉತ್ತಮವಾಗಿ ಕಾರ್ಯ ನಿರ್ವಹಿಸುವುದನ್ನು ನೋಡಿ ಅವಳು ತುಂಬಾ ಸಂತೋಷಪಡುತ್ತಾಳೆ.	ಟ್ರೇಡಿಂಗ್ ವೆಬ್‌ಸೈಟ್ ಅವಳಿಗೆ ಬೋನಸ್ ನೀಡುತ್ತದೆ, ಹೆಚ್ಚಿನ ಹಣವನ್ನು ಹೂಡಿಕೆ ಮಾಡಲು ಅವಳನ್ನು ಆಕರ್ಷಿಸುತ್ತದೆ.
		
ಮನು ತನ್ನ ಸ್ನೇಹಿತರಿಂದ ಹಣವನ್ನು ಎರವಲು ಪಡೆಯುತ್ತಾಳೆ ಮತ್ತು ಅವಳ ಕ್ರಿಪ್ಟೋ ಖಾತೆಯಲ್ಲಿ ಹೂಡಿಕೆ ಮಾಡುತ್ತಾಳೆ.	ಒಂದುದಿನ ಅವಳು ವೆಬ್‌ಸೈಟ್‌ಗೆ ಲಾಗ್ ಇನ್ ಆದಾಗ, ಸೈಟ್ ಕಾಣೆಯಾಗಿರುವುದನ್ನು ನೋಡಿ ಅವಳು ಆಘಾತಕ್ಕೊಳಗಾಗುತ್ತಾಳೆ.	ವಂಚನೆಯ ಸೈಟ್ ತನ್ನ ಎಲ್ಲಾ ಕ್ರಿಪ್ಟೋ ಕರೆನ್ಸಿಗಳನ್ನು ಅವಳ ವ್ಯಾಲೆಟ್‌ನಿಂದ ಕಳವು ಮಾಡಿರುತ್ತದೆ ಏಕೆಂದರೆ ಅವಳು ಅವರೊಂದಿಗೆ ರುಜುವಾತುಗಳನ್ನು ಹಂಚಿಕೊಂಡಿದ್ದಳು.

ಸ್ಕ್ಯಾಮರ್‌ಗಳು ಯಾವಾಗಲೂ ನಿಮ್ಮ ಹಣವನ್ನು ಕದಿಯಲು ಹೊಸ ಮಾರ್ಗಗಳನ್ನು ಹುಡುಕುತ್ತಿರುತ್ತಾರೆ ಮತ್ತು ಇತ್ತೀಚಿನ ದಿನಗಳಲ್ಲಿ ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಯ ಬೃಹತ್ ಬೆಳವಣಿಗೆಯು ವಂಚನೆಗೆ ಸಾಕಷ್ಟು ಅವಕಾಶಗಳನ್ನು ಸೃಷ್ಟಿಸಿದೆ. ಕ್ರಿಪ್ಟೋ ವಂಚನೆಗಳಲ್ಲಿ ಹಲವು ವಿಧಗಳಿವೆ. ಕೆಲವು ಸಾಮಾನ್ಯವಾದವುಗಳು: ನಕಲಿ ವೆಬ್‌ಸೈಟ್‌ಗಳು, ಪಂಪ್ ಮತ್ತು ಡಂಪ್ ಹಗರಣಗಳು, ಫಿಶಿಂಗ್ ಸ್ಕ್ಯಾಮ್‌ಗಳು, ನಕಲಿ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು, ನಕಲಿ ಸೆಲೆಬ್ರಿಟಿ ಅನುಮೋದನೆಗಳು, ಗಿವ್‌ಅವೇ ಹಗರಣಗಳು, ಕ್ಲೌಡ್ ಮೈನಿಂಗ್ ಹಗರಣಗಳು ಮತ್ತು ಆರಂಭಿಕ ಕೊಡುಗೆ ಹಗರಣಗಳು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 43ಎ: ಈ ಕಲಂಗಳು ಡೇಟಾ ಮತ್ತು ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆಯನ್ನು ರಕ್ಷಿಸುವಲ್ಲಿ ವಿಫಲವಾದರೆ ಪರಿಹಾರವನ್ನು ವ್ಯವಹರಿಸುತ್ತವೆ.

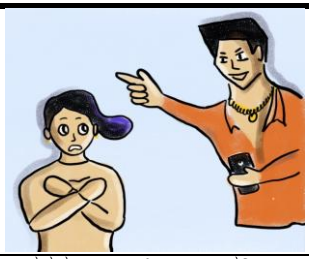
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ – ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಒಬ್ಬ ವ್ಯಕ್ತಿಯ ವೇಷ ಹಾಕುವ ಉದ್ದೇಶದಿಂದ ಅಥವಾ ಅವರಿಗೆ ಆರ್ಥಿಕ ಅಥವಾ ಪ್ರತಿಷ್ಠೆ ಹಾನಿಯನ್ನು ಉಂಟುಮಾಡುವ ಉದ್ದೇಶದಿಂದ ಸೆಷನ್ ಅಪಹರಣದ ದಾಳಿಯನ್ನು ನಡೆಸಿದರೆ, ಈ ಕಲಂ ಅನ್ವಯಿಸಬಹುದು.)

ಮಾ.ತ.ಕಾ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಭಾರತೀಯ ದಂಡ ಸಂಹಿತೆಯ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318: ಮಾ.ತ.ಕಾಯ್ದೆಯ ಭಾಗವಾಗಿರದಿದ್ದರೂ, ಐಪಿಸಿಯ ಕಲಂ 420 ವಂಚನೆ ಮತ್ತು ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಆಸ್ತಿ ವಿತರಣೆಯನ್ನು ಒಳಗೊಂಡಿದೆ.

ನಿಮ್ಮ ಮಾರ್ಗವನ್ನು ಪರಿಶೀಲಿಸಿ (ಹಣ ಮಾಡುವ ತಂತ್ರ, ಹಣಕಾಸಿನ ಮಾರ್ಗ ಅಥವಾ ದಾರಿ) ಇಲ್ಲದಿದ್ದರೆ ನಿಮ್ಮ ಆದಾಯದಲ್ಲಿ ಕಡಿತವಾಗಬಹುದು.

ಸೈಬರ್ ಸೆಕ್ಸ್ ಟ್ರಾಫಿಕ್ಕಿಂಗ್

ಅಮಲ ಪದವಿಪೂರ್ವ ವಿದ್ಯಾರ್ಥಿನಿ. ಕಾಲೇಜಿನಲ್ಲಿ ಕಡಿಮೆ ಅಂಕ ಗಳಿಸಿದ್ದರಿಂದ ಆಕೆಗೆ ಕ್ಯಾಂಪಸ್ ಸಿಗಲಿಲ್ಲ.	ಪ್ರತಿ ದಿನ ಬೆಳಿಗ್ಗೆ, ಅವಳು ಕ್ಯಾಂಪಸ್ ಸಂದರ್ಶನಗಳನ್ನು ನೀಡಲು ವಿವಿಧ ಕಂಪನಿಗಳಿಗೆ ಹೋಗುತ್ತಿದ್ದಳು.	ಅಮಲಳಿಗೆ ಹಣದ ಅವಶ್ಯಕತೆ ಇದೆ ಎಂದು ಆಕೆಯ ಮನೆಯ ಸಮೀಪ ವಾಸಿಸುವ ಸ್ಥಳೀಯ ರೌಡಿ ಸಲೀಲ್ ಗೆ ತಿಳಿದಿತ್ತು.
ಸಾಕ್ ಪಪೆಟ್ ಖಾತೆಯನ್ನು ಬಳಸಿಕೊಂಡು, ಡೇಟಿಂಗ್ ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ಅಮಲಳನ್ನು ಸಂಪರ್ಕಿಸುತ್ತಾನೆ.	ಅವನು ಅವಳಿಗೆ ಉಡುಗೊರೆಗಳ ಹೊರೆಗಳನ್ನೆ ಸುರಿಸುತ್ತಾನೆ– ಸುಗಂಧ ದ್ರವ್ಯ, ಸೌಂದರ್ಯ ವರ್ಧಕ, ಕೈಚೀಲಗಳು ಮತ್ತು ಅವಳು ಬಯಸಿದ ಎಲ್ಲವನ್ನು.	ಅವನು ಒಂದು ದಿನ ಅವಳನ್ನು ಮನೆಗೆ ಆಹ್ವಾನಿಸುತ್ತಾನೆ, ಇದು ವಾಸ್ತವವಾಗಿ ಸೈಬರ್‌ಸೆಕ್ಸ್ ಬಿಲ ಆಗಿದ್ದು, ಅದು ಅಮಲಾಗೆ ತಿಳಿದಿರಲಿಲ್ಲ.
		
ಅವಳನ್ನು ಒತ್ತಾಯಿಸಿ ಬಲತ್ಕರಿಸಿ ರೆಕಾರ್ಡ್ ಮಾಡಿ ಇಂಟರ್ ನೆಟ್‌ನಲ್ಲಿ ಲೈವ್ ಸ್ಟ್ರೀಮ್ ಮಾಡುತ್ತಾನೆ. ಸುಮ್ಮನಿರಲು ಅವಳಿಗೆ ಹಣವನ್ನೂ ಕೊಡುತ್ತಾನೆ.	ಅದೇ ರೀತಿ ಅವನ ಸ್ನೇಹಿತರೊಂದಿಗೆ ಅನೇಕ ಬಾರಿ ಪುನರಾವರ್ತಿಸಿ ಲೈವ್ ಸ್ಟ್ರೀಮ್ ಮಾಡಲಾಗುತ್ತದೆ. ಸಾಮಾಜಿಕ ಕಳಂಕಕ್ಕೆ ಹೆದರಿ ದೂರು ನೀಡುವುದಿಲ್ಲ.	ಸಲೀಲ್ ಮತ್ತು ಅವನ ಸ್ನೇಹಿತರು ಐಷಾರಾಮಿ ಜೀವನವನ್ನು ನಡೆಸುತ್ತಾರೆ. ಡಾರ್ಕ್ ವೆಬ್‌ನಲ್ಲಿ ಇಂತಹ ಅಕ್ರಮ ಲೈಂಗಿಕ ವಹಿವಾಟುಗಳಿಂದ ಅವರು ಸಾಕಷ್ಟು ಹಣವನ್ನು ಗಳಿಸುತ್ತಾರೆ.

ಸೈಬರ್‌ಸೆಕ್ಸ್ ಕಳ್ಳಸಾಗಣೆ, ಅಥವಾ ಆನ್‌ಲೈನ್ ಲೈಂಗಿಕ ಶೋಷಣೆಯು, ಸೈಬರ್ ಅಪರಾಧ ಮತ್ತು ಆಧುನಿಕ ಗುಲಾಮಗಿರಿಯ ಒಂದು ರೂಪವಾಗಿದೆ. ಸೈಬರ್‌ಸೆಕ್ಸ್ ಟ್ರಾಫಿಕಿಂಗ್ ಎಂದರೆ ಬಲಿಪಶುವನ್ನು ಬಲವಂತವಾಗಿ, ಒತ್ತಾಯಪೂರ್ವಕವಾಗಿ ಅಥವಾ ವಂಚನೆಯಿಂದ ಲೈಂಗಿಕ ಶೋಷಣೆಗೆ ಒತ್ತಾಯಿಸಲಾಗುತ್ತದೆ ಮತ್ತು ಈ ಕೃತ್ಯವನ್ನು ವೆಬ್‌ಕ್ಯಾಮ್, ವೀಡಿಯೊ, ಛಾಯಾಗ್ರಹಣ ಅಥವಾ ಇತರ ಡಿಜಿಟಲ್ ಮಾಧ್ಯಮದ ಮೂಲಕ ಇಂಟರ್ನೆಟ್‌ನಲ್ಲಿ ನೇರ ಪ್ರಸಾರ ಮಾಡಲಾಗುವುದಾಗಿರುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಅನ್ವಯ ಕಲಂಗಳು

499, 506, 509, 354A, 370, 347, 357 IPC/
356, 351, 79, 75, 143, 127, 135 BNS

ಐಪಿಸಿ ಕಲಂ 370ಎ/ಬಿಎನ್‌ಎಸ್ 144: ಶೋಷಣೆಗಾಗಿ ವ್ಯಕ್ತಿಗಳ ಸಾಗಾಣಿಕೆ, ಇದರಲ್ಲಿ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ವಿಧಾನಗಳ ಮೂಲಕ ಲೈಂಗಿಕ ಶೋಷಣೆಗಾಗಿ ಕಳ್ಳಸಾಗಣೆ ಸೇರಿದೆ.

ಲೈಂಗಿಕವಾಗಿ ಅಶ್ಲೀಲ ಅಥವಾ ಕೊಳಕು ಅಂಶವನ್ನು ಬಹಿರಂಗಪಡಿಸುವುದು ಕಲಂ 292.

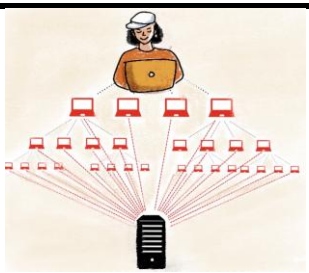
ಅನೈತಿಕ ಕಳ್ಳಸಾಗಣೆ (ತಡೆಗಟ್ಟುವಿಕೆ) ಕಾಯಿದೆ 1956 ರ ಕಲಂಗಳು, PITA (ಅನೈತಿಕ ಕಳ್ಳಸಾಗಣೆ ತಡೆಗಟ್ಟುವಿಕೆ ಕಾಯಿದೆ) ಎಂದೂ ಸಹ ಕರೆಯುತ್ತಾರೆ.

67 ಮತ್ತು 67A IT ಕಾಯಿದೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67ಬಿ– ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಒಳಗೊಂಡ ವಸ್ತುವಿನಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿ ವಿದ್ಯುನ್ಮಾನರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಾಯ್ದೆಗಳು

ಇಂಟರ್ನೆಟ್ ಅನ್ನು ಸರ್ಫಿಂಗ್ ಮಾಡುವಾಗ ಮತ್ತು ಸಂಪರ್ಕಗಳನ್ನು ಮಾಡುವಾಗ, ಗಮನವಿರಲಿ, ಇಲ್ಲದಿದ್ದರೆ ಅದು ನಿಮ್ಮನ್ನು ಮೆಚ್ಚುಗೆಯಿಂದ ಅಪಹಾಸ್ಯಕ್ಕೆ ಕೊಂಡೊಯ್ಯಬಹುದು (ತುಂಬಾ ಒಳ್ಳೆಯದು ಅಥವಾ ತುಂಬಾ ಗಂಭೀರವಾದ ಸಂಗತಿಯಿಂದ ಕೆಟ್ಟ ಅಥವಾ ಮೂರ್ಖತನದವರೆಗೆ).

ಸೈಬರ್ ವಾರ್‌ಫೇರ್

ನಳಿನಿ ಎಂಜಿನಿಯರಿಂಗ್ ವಿದ್ಯಾರ್ಥಿನಿ. ಏಕಾಂತಪ್ರಿಯೆ ಮತ್ತು ತಂತ್ರಜ್ಞಾನ ನಿಪುಣೆ.	ಕಾಲೇಜು ಮುಗಿಸಿ ಮನೆಗೆ ಹೋಗಿ ಲ್ಯಾಪ್ ಟಾಪ್ ಮುಂದೆ ಕೂರುವ ಹವ್ಯಾಸಿ! ಹಾಗೆ ಕೋಡಿಂಗ್ ಅನ್ನು ಪ್ರೀತಿಸುತ್ತಾಳೆ.	ಅನೇಕ ಕೋಡರ್ ವೇದಿಕೆಗಳ ಸದಸ್ಯೆಯಾಗಿದ್ದಳು. ಆಕೆಯ ಕಾಮೆಂಟ್‌ಗಳು ಮತ್ತು ಡೀಬಗ್ ಮಾಡುವ ಕೌಶಲ್ಯಗಳು ಎಲ್ಲರ ಮೆಚ್ಚುಗೆಗೆ ಪಾತ್ರವಾಗಿದ್ದವು.
		
ಒಂದು ದಿನ, ಅವಳು ತನ್ನ ಇನ್‌ಬಾಕ್ಸ್‌ನಲ್ಲಿ ರಷ್ಯಾದ ಮೇಲೆ ದಾಳಿ ನಡೆಸಲು ಸಂದೇಶವನ್ನು ಸ್ವೀಕರಿಸುತ್ತಾಳೆ, ಮತ್ತು ಅದಕ್ಕಾಗಿ ಆಕೆಗೆ ದೊಡ್ಡ ಬಹುಮಾನವನ್ನು ಆಹ್ವಾನಿಸಲಾಗಿರುತ್ತದೆ.	ಈ ಕಾರ್ಯವನ್ನು ಪೂರ್ಣಗೊಳಿಸಿದ ಮೇಲೆ ಅವಳು ಎಂದಿಗೂ ಕೆಲಸ ಮಾಡದೇ ತುಂಬಾ ಹಣವನ್ನು ಪಡೆದು ತಕ್ಷಣವೇ ನಿವೃತ್ತಿ ಹೊಂದಿ ಸುಖ ಜೀವನ ಸಾಗಿಸಬಹುದು ಎಂದು ಅವಳಿಗೆ ಹೇಳಲಾಗುತ್ತದೆ.	ನಳಿನಿ ಪ್ರಾಕ್ಸಿ ಮತ್ತು ಇತರ ರಹಸ್ಯ ತಂತ್ರಗಳನ್ನು ಬಳಸಿಕೊಂಡು ರಷ್ಯಾದ ಸರ್ವರ್‌ಗಳ ಮೇಲೆ DDoS ದಾಳಿಗಳನ್ನು ನಡೆಸುತ್ತಾಳೆ.
ಅವರ ಪವರ್ ಗ್ರಿಡ್ ಮತ್ತು ಬ್ಯಾಂಕಿಂಗ್ ವ್ಯವಸ್ಥೆಗಳ ಮೇಲೂ ದಾಳಿ ಮಾಡುತ್ತಾಳೆ.	ರಷ್ಯಾದ ಗುಪ್ತಚರ ತಂಡವು ಇದರ ರುವಾರಿ ನಳಿನಿ ಎಂದು ಪತ್ತೆಹಚ್ಚುತ್ತದೆ.	ಆಕೆಯನ್ನು ಈಗ ಬಂಧಿಸಲಾಗಿದೆ ಮತ್ತು ಜೀವಾವಧಿ ಶಿಕ್ಷೆಗೆ ಒಳಪಡಿಸಿದೆ.

ಸೈಬರ್‌ವಾರ್‌ಫೇರ್ ಶತ್ರು ರಾಜ್ಯದ ವಿರುದ್ಧ ಸೈಬರ್ ದಾಳಿಯ ಬಳಕೆಯಾಗಿದೆ, ಮತ್ತು/ಅಥವಾ ಇದು ಪ್ರಮುಖ ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಗಳನ್ನು ಅಡ್ಡಿಪಡಿಸುವ ಮೂಲಕ ನಿಜವಾದ ಯುದ್ಧಕ್ಕೆ ಹೋಲಿಸಬಹುದಾದ ಹಾನಿಯನ್ನು ಉಂಟುಮಾಡುತ್ತದೆ. ಇವುಗಳಲ್ಲಿ ಕೆಲವು ಉದ್ದೇಶಿತ ಫಲಿತಾಂಶಗಳು ಬೇಹುಗಾರಿಕೆ, ವಿಧ್ವಂಸಕ, ಪ್ರಚಾರ, ಕುಶಲತೆ ಅಥವಾ ಆರ್ಥಿಕ ಯುದ್ಧವಾಗಿರಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರಗಳಿಗೆ ಅನಧೀಕೃತ ಪ್ರವೇಶ, ದತ್ತಾಂಶ ಕಳ್ಳತನ ಮತ್ತು ಇತರೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳಿಗೆ ಸಂಬಂಧಿಸಿದೆ

ಮಾ.ತ.ಕಾ ಕಲಂ 66– ಹ್ಯಾಕಿಂಗ್ ಒಳಗೊಂಡಂತೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಎಫ್– ಸೈಬರ್ ಭಯೋತ್ಪಾಚನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 70 ಎ: ಈ ಕಲಂ ಅನ್ನು 2008 ರಲ್ಲಿ ತಿದ್ದುಪಡಿಯ ಮೂಲಕ ಪರಿಚಯಿಸಲಾಯಿತು, ಇದು ಸೈಬರ್‌ಸ್ಪೇಸ್‌ನ ಸುರಕ್ಷತೆಯನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ನಿರ್ದೇಶನಗಳನ್ನು ನೀಡುವ ಅಧಿಕಾರವನ್ನು ಸರ್ಕಾರಕ್ಕೆ ಒದಗಿಸುತ್ತದೆ. ಸೈಬರ್ ಬೆದರಿಕೆಗಳ ಗುರುತಿಸುವಿಕೆ, ವಿಶ್ಲೇಷಣೆ ಮತ್ತು ತಡೆಗಟ್ಟುವಿಕೆಗೆ ಕ್ರಮಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳಲು ಇದು ಸರ್ಕಾರಕ್ಕೆ ಅಧಿಕಾರ ನೀಡುತ್ತದೆ.

ಮಾ.ತ.ಕಾ ಕಲಂ 69– ಗಣಕಯಂತ್ರದ ಯಾವುದೇ ಸಂಪನ್ಮೂಲದ ಮೂಲಕ ಯಾವುದೇ ಮಾಹಿತಿಯನ್ನು ಪ್ರತಿಬಂಧಿಸುವುದಕ್ಕಾಗಿ ಅಥವಾ ಮೇಲ್ವಿಚಾರಣೆಗಾಗಿ ಅಥವಾ ಅಸಂಕೇತಿಕರಣಕ್ಕಾಗಿ ನಿರ್ದೇಶನಗಳನ್ನು ಹೊರಡಿಸುವ ಅಧಿಕಾರ

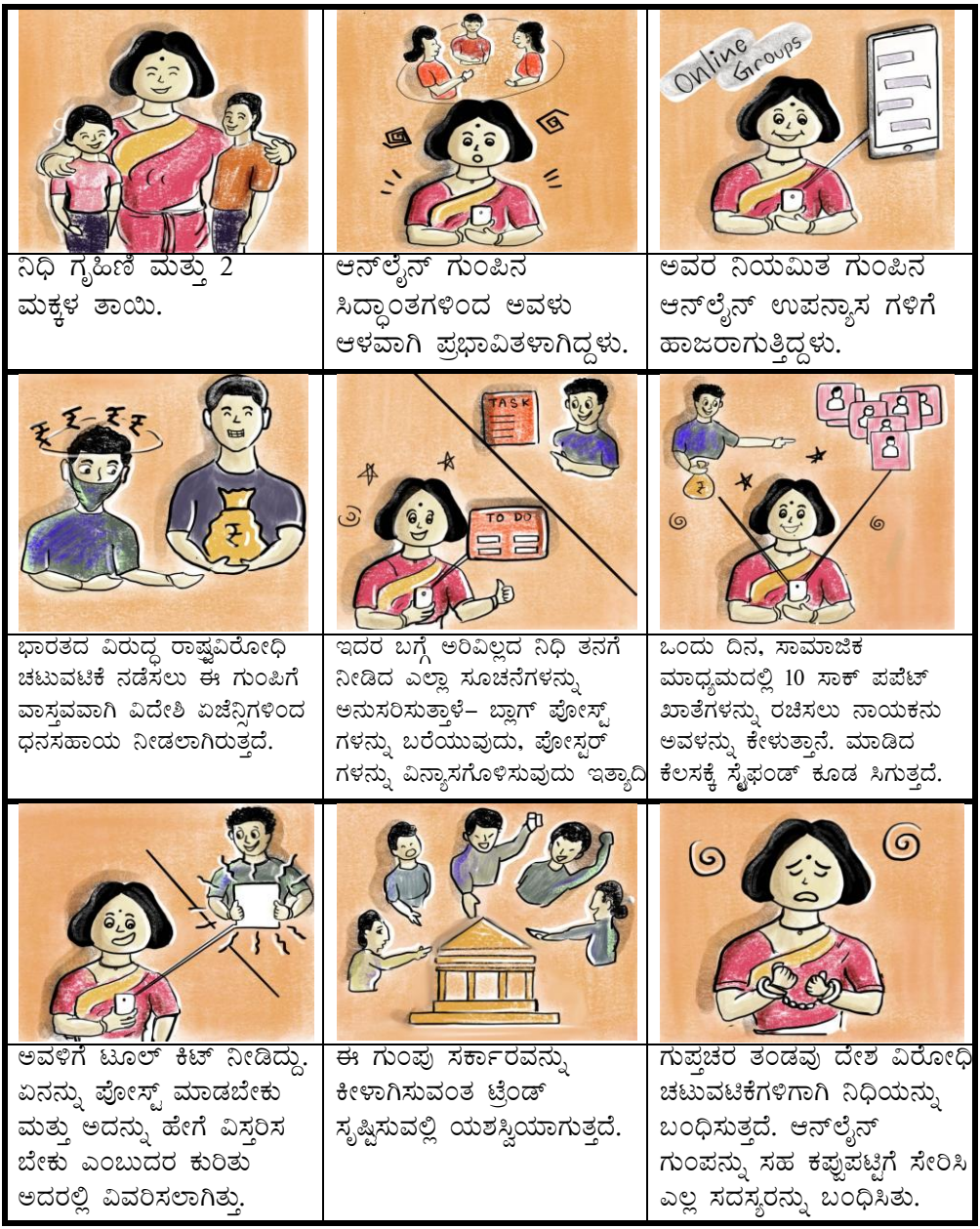
121 ಐಪಿಸಿ/ಬಿಎನ್‌ಎಸ್ 147 66E, 66 R/W 43(a) (c) (e) (f)

ಕಾನೂನುಬಾಹಿರ ಚಟುವಟಿಕೆಗಳ (ತಡೆಗಟ್ಟುವಿಕೆ) ಕಾಯಿದೆ, 1967 (UAPA) ಯ ಕಲಂಗಳು.

ಮಹಾರಾಷ್ಟ್ರದಲ್ಲಿ– ಮಹಾರಾಷ್ಟ್ರ ಕಂಟ್ರೋಲ್ ಆಫ್ ಆರ್ಗನೈಸ್ಡ್ ಕ್ರೈಮ್ ಆಕ್ಟ್, 1999 (MCOCA) ನ ಕಲಂಗಳು.

ಭಯೋತ್ಪಾದನೆ ತಡೆ ಕಾಯಿದೆ, 2002 ರ ಕಲಂಗಳು.

ಹ್ಯಾಕಿಂಗ್ ಅಪರಾಧಕ್ಕಾಗಿ ಆರೋಪಿಗೆ ಶಿಕ್ಷೆಯಾದರೆ, ಪರಿಹಾರದ ಹಕ್ಕನ್ನು ತಿರಸ್ಕರಿಸಲಾಗುತ್ತದೆ.



ನಿಧಿ ಗೃಹಿಣಿ ಮತ್ತು 2 ಮಕ್ಕಳ ತಾಯಿ.	ಆನ್‌ಲೈನ್ ಗುಂಪಿನ ಸಿದ್ಧಾಂತಗಳಿಂದ ಅವಳು ಆಳವಾಗಿ ಪ್ರಭಾವಿತಳಾಗಿದ್ದಳು.	ಅವರ ನಿಯಮಿತ ಗುಂಪಿನ ಆನ್‌ಲೈನ್ ಉಪನ್ಯಾಸ ಗಳಿಗೆ ಹಾಜರಾಗುತ್ತಿದ್ದಳು.
ಭಾರತದ ವಿರುದ್ಧ ರಾಷ್ಟ್ರವಿರೋಧಿ ಚಟುವಟಿಕೆ ನಡೆಸಲು ಈ ಗುಂಪಿಗೆ ವಾಸ್ತವವಾಗಿ ವಿದೇಶಿ ಏಜೆನ್ಸಿಗಳಿಂದ ಧನಸಹಾಯ ನೀಡಲಾಗಿರುತ್ತದೆ.	ಇದರ ಬಗ್ಗೆ ಅರಿವಿಲ್ಲದ ನಿಧಿ ತನಗೆ ನೀಡಿದ ಎಲ್ಲಾ ಸೂಚನೆಗಳನ್ನು ಅನುಸರಿಸುತ್ತಾಳೆ– ಬ್ಲಾಗ್ ಪೋಸ್ಟ್ ಗಳನ್ನು ಬರೆಯುವುದು, ಪೋಸ್ಟರ್ ಗಳನ್ನು ವಿನ್ಯಾಸಗೊಳಿಸುವುದು ಇತ್ಯಾದಿ	ಒಂದು ದಿನ, ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ 10 ಸಾಕ್ ಪಪೆಟ್ ಖಾತೆಗಳನ್ನು ರಚಿಸಲು ನಾಯಕನು ಅವಳನ್ನು ಕೇಳುತ್ತಾನೆ. ಮಾಡಿದ ಕೆಲಸಕ್ಕೆ ಸ್ಟೈಫಂಡ್ ಕೂಡ ಸಿಗುತ್ತದೆ.
ಅವಳಿಗೆ ಟೂಲ್ ಕಿಟ್ ನೀಡಿದ್ದು. ಏನನ್ನು ಪೋಸ್ಟ್ ಮಾಡಬೇಕು ಮತ್ತು ಅದನ್ನು ಹೇಗೆ ವಿಸ್ತರಿಸ ಬೇಕು ಎಂಬುದರ ಕುರಿತು ಅದರಲ್ಲಿ ವಿವರಿಸಲಾಗಿತ್ತು.	ಈ ಗುಂಪು ಸರ್ಕಾರವನ್ನು ಕೀಳಾಗಿಸುವಂತ ಟ್ರೆಂಡ್ ಸೃಷ್ಟಿಸುವಲ್ಲಿ ಯಶಸ್ವಿಯಾಗುತ್ತದೆ.	ಗುಪ್ತಚರ ತಂಡವು ದೇಶ ವಿರೋಧಿ ಚಟುವಟಿಕೆಗಳಿಗಾಗಿ ನಿಧಿಯನ್ನು ಬಂಧಿಸುತ್ತದೆ. ಆನ್‌ಲೈನ್ ಗುಂಪನ್ನು ಸಹ ಕಪ್ಪುಪಟ್ಟಿಗೆ ಸೇರಿಸಿ ಎಲ್ಲ ಸದಸ್ಯರನ್ನು ಬಂಧಿಸಿತು.

'ಹ್ಯಾಕ್' ಮತ್ತು 'ಆಕ್ಟಿವಿಸಂ' ಪದಗಳ ಸಂಯೋಜನೆಯಿಂದ ಹುಟ್ಟಿಕೊಂಡಿದೆ, ಹ್ಯಾಕ್ಟಿವಿಸಮ್ ಎನ್ನುವುದು ರಾಜಕೀಯವಾಗಿ ಅಥವಾ ಸಾಮಾಜಿಕವಾಗಿ ಪ್ರೇರಿತ ಉದ್ದೇಶಗಳಿಗಾಗಿ ಹ್ಯಾಕ್ ಮಾಡುವ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗೆ ಪ್ರವೇಶಿಸುವ ಕ್ರಿಯೆಯಾಗಿದೆ. ಹ್ಯಾಕ್ಟಿವಿಸಂನ ಕ್ರಿಯೆಯನ್ನು ಮಾಡುವ ವ್ಯಕ್ತಿಯನ್ನು ಹ್ಯಾಕ್ಟಿವಿಸ್ಟ್ ಎಂದು ಹೇಳಲಾಗುತ್ತದೆ. ಸಂಸ್ಥೆಯ ವೆಬ್‌ಸೈಟ್ ಅನ್ನು ವಿರೂಪಗೊಳಿಸುವುದು ಅಥವಾ ಆ ಸಂಸ್ಥೆಯ ಮಾಹಿತಿಯನ್ನು ಸೋರಿಕೆ ಮಾಡುವುದು ಮುಂತಾದ ಕೃತ್ಯಗಳನ್ನು ಮಾಡುವ ಹ್ಯಾಕ್‌ಟಿವಿಸ್ಟ್, ತಮ್ಮ ಚಟುವಟಿಕೆಗಳ ಮೂಲಕ ಸಂದೇಶವನ್ನು ಕಳುಹಿಸಲು ಮತ್ತು ಅವರು ಪ್ರಚಾರ ಮಾಡುತ್ತಿರುವ ಕಾರಣಕ್ಕಾಗಿ ತಮ್ಮ ಗೋಚರಿಸಿಕೊಳ್ಳುವಂತೆ ಮಾಡುವ ಗುರಿಯನ್ನು ಹೊಂದಿರುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರಗಳಿಗೆ ಅನಧೀಕೃತ ಪ್ರವೇಶ, ದತ್ತಾಂಶ ಕಳ್ಳತನ ಮತ್ತು ಇತರೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳಿಗೆ ಸಂಬಂಧಿಸಿದೆ

ಮಾ.ತ.ಕಾ ಕಲಂ 66– ಹ್ಯಾಕಿಂಗ್ ಒಳಗೊಂಡಂತೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

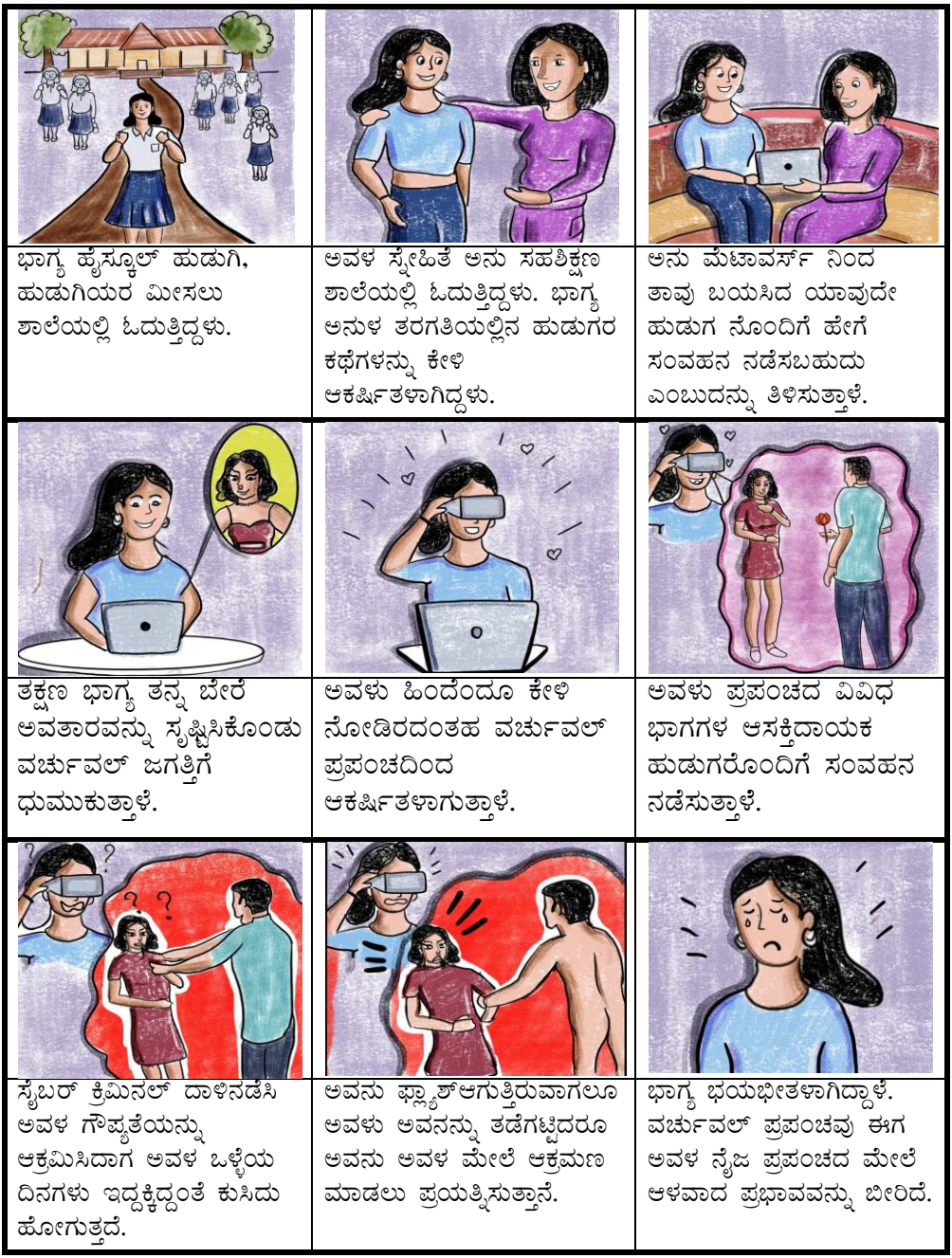
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಎಫ್– ಸೈಬರ್ ಭಯೋತ್ಪಾಚನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 70: ಈ ಕಲಂ ಯಾವುದೇ ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲದ ಮೂಲಕ ಯಾವುದೇ ಮಾಹಿತಿಯ ಪ್ರತಿಬಂಧ, ಮೇಲ್ವಿಚಾರಣೆ ಅಥವಾ ಡೀಕ್ರಿಪ್ಶನ್‌ಗೆ ನಿರ್ದೇಶನಗಳನ್ನು ನೀಡುವ ಮೂಲಕ ಸೈಬರ್‌ಸ್ಪೇಸ್ ಅನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಲು ಸರ್ಕಾರಕ್ಕೆ ಅಧಿಕಾರ ನೀಡುತ್ತದೆ.

120A, 121, 122, 153, 153A, 107 ಐಪಿಸಿ ಕಲಂಗಳು/
61, 147, 149, 192, 196, 45 ಬಿಎನ್‌ಎಸ್ ಕಲಂಗಳು

ನಿಮ್ಮ ಬಗ್ಗೆ ನೀವೇ ಯೋಚಿಸಿ ಮತ್ತು ಬೇರೆಯವರು ನಿಮ್ಮ ಬಗ್ಗೆ ಯೋಚಿಸಲು ಬಿಡಬೇಡಿ.

ಮೆಟಾವರ್ಸ್


ಭಾಗ್ಯ ಹೈಸ್ಕೂಲ್ ಹುಡುಗಿ, ಹುಡುಗಿಯರ ಮೀಸಲು ಶಾಲೆಯಲ್ಲಿ ಓದುತ್ತಿದ್ದಳು.
ಅವಳ ಸ್ನೇಹಿತೆ ಅನು ಸಹಶಿಕ್ಷಣ ಶಾಲೆಯಲ್ಲಿ ಓದುತ್ತಿದ್ದಳು. ಭಾಗ್ಯ ಅನುಳ ತರಗತಿಯಲ್ಲಿನ ಹುಡುಗರ ಕಥೆಗಳನ್ನು ಕೇಳಿ ಆಕರ್ಷಿತಳಾಗಿದ್ದಳು.
ಅನು ಮೆಟಾವರ್ಸ್ ನಿಂದ ತಾವು ಬಯಸಿದ ಯಾವುದೇ ಹುಡುಗ ನೊಂದಿಗೆ ಹೇಗೆ ಸಂವಹನ ನಡೆಸಬಹುದು ಎಂಬುದನ್ನು ತಿಳಿಸುತ್ತಾಳೆ.
ತಕ್ಷಣ ಭಾಗ್ಯ ತನ್ನ ಬೇರೆ ಅವತಾರವನ್ನು ಸೃಷ್ಟಿಸಿಕೊಂಡು ವರ್ಚುವಲ್ ಜಗತ್ತಿಗೆ ಧುಮುಕುತ್ತಾಳೆ.
ಅವಳು ಹಿಂದೆಂದೂ ಕೇಳಿ ನೋಡಿರದಂತಹ ವರ್ಚುವಲ್ ಪ್ರಪಂಚದಿಂದ ಆಕರ್ಷಿತಳಾಗುತ್ತಾಳೆ.
ಅವಳು ಪ್ರಪಂಚದ ವಿವಿಧ ಭಾಗಗಳ ಆಸಕ್ತಿದಾಯಕ ಹುಡುಗರೊಂದಿಗೆ ಸಂವಹನ ನಡೆಸುತ್ತಾಳೆ.
ಸೈಬರ್ ಕ್ರಿಮಿನಲ್ ದಾಳಿನಡೆಸಿ ಅವಳ ಗೌಪ್ಯತೆಯನ್ನು ಆಕ್ರಮಿಸಿದಾಗ ಅವಳ ಒಳ್ಳೆಯ ದಿನಗಳು ಇದ್ದಕ್ಕಿದ್ದಂತೆ ಕುಸಿದು ಹೋಗುತ್ತದೆ.
ಅವನು ಫ್ಲ್ಯಾಶ್ಆಗುತ್ತಿರುವಾಗಲೂ ಅವಳು ಅವನನ್ನು ತಡೆಗಟ್ಟಿದರೂ ಅವನು ಅವಳ ಮೇಲೆ ಆಕ್ರಮಣ ಮಾಡಲು ಪ್ರಯತ್ನಿಸುತ್ತಾನೆ.
ಭಾಗ್ಯ ಭಯಭೀತಳಾಗಿದ್ದಾಳೆ. ವರ್ಚುವಲ್ ಪ್ರಪಂಚವು ಈಗ ಅವಳ ನೈಜ ಪ್ರಪಂಚದ ಮೇಲೆ ಆಳವಾದ ಪ್ರಭಾವವನ್ನು ಬೀರಿದೆ.

ಮೆಟಾವರ್ಸ್ ಇಂಟರ್ನೆಟ್ ಮತ್ತು ಕಂಪ್ಯೂಟಿಂಗ್‌ನ 3D ಆವೃತ್ತಿಯಾಗಿದೆ. ಮೆಟಾವರ್ಸ್ "3D ವರ್ಚುವಲ್ ಪ್ರಪಂಚದ ಸಂಯೋಜಿತ ನೆಟ್‌ವರ್ಕ್" ಆಗಿದೆ. ವರ್ಚುವಲ್ ರಿಯಾಲಿಟಿ ಹೆಡ್‌ಸೆಟ್ ಮೂಲಕ ಈ ಪ್ರಪಂಚಕ್ಕೆ ಪ್ರವೇಶ ಪಡೆಯಬಹುದು – ಬಳಕೆದಾರರು ತಮ್ಮ ಕಣ್ಣಿನ ಚಲನೆಗಳು, ಪ್ರತಿಕ್ರಿಯೆ ನಿಯಂತ್ರಕಗಳು ಅಥವಾ ಧ್ವನಿ ಆಜ್ಞೆಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಮೆಟಾವರ್ಸ್ ಅನ್ನು ನ್ಯಾವಿಗೇಟ್ ಮಾಡುತ್ತಾರೆ. ಇದು ನೈಜವಾಗಿರುವಂತಹ ಭೌತಿಕ ಸಂವೇದನೆಯನ್ನು ಸೃಷ್ಟಿ ಮಾಡುವ ಮೂಲಕ, ಭೌತಿಕ ಉಪಸ್ಥಿತಿ ಉತ್ತೇಜಿಸುತ್ತಾ, ಹೆಡ್‌ಸೆಟ್ ಬಳಕೆದಾರರನ್ನು ಇದು ಮುಳುಗಿಸುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

354, 506 ಐಪಿಸಿ ಕಲಂಗಳು/ 74, 351 ಐಪಿಸಿ ಕಲಂ, POCSO ನ ಕಲಂಗಳು, 67-B IT ಕಾಯಿದೆಯ ಕಲಂ,

ಗೌಪ್ಯತೆಯ ಹಕ್ಕು, ಭಾರತದ ಸಂವಿಧಾನದ 21 ನೇ ವಿಧಿಯ ಅಡಿಯಲ್ಲಿ ಮೂಲಭೂತ ಹಕ್ಕು.

ಡೇಟಾ ರಕ್ಷಣೆ ಮತ್ತು ಗೌಪ್ಯತೆ ಕಾನೂನುಗಳು: ವೈಯಕ್ತಿಕ ಡೇಟಾದ ಸಂಗ್ರಹಣೆ, ಸಂಗ್ರಹಣೆ, ಸಂಸ್ಕರಣೆ ಮತ್ತು ಹಂಚಿಕೆಯನ್ನು ನಿಯಂತ್ರಿಸುವ ಕಾನೂನುಗಳು ಮೆಟಾವರ್ಸ್‌ನಲ್ಲಿನ ಬಳಕೆದಾರರ ಸಂವಹನಗಳಿಗೆ ಅನ್ವಯಿಸಬಹುದು. ಭಾರತದಲ್ಲಿ, ಇದು ವೈಯಕ್ತಿಕ ಡೇಟಾ ಸಂರಕ್ಷಣಾ ಮಸೂದೆಯ ಅನುಸರಣೆಯನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ.

ಬೌದ್ಧಿಕ ಆಸ್ತಿ ಕಾನೂನುಗಳು: ಹಕ್ಕುಸ್ವಾಮ್ಯಗಳು, ಟ್ರೇಡ್‌ಮಾರ್ಕ್‌ಗಳು ಮತ್ತು ಪೇಟೆಂಟ್‌ಗಳನ್ನು ನಿಯಂತ್ರಿಸುವ ಕಾನೂನುಗಳು ವರ್ಚುವಲ್ ಸರಕುಗಳು, ಕಲಾಕೃತಿಗಳು ಮತ್ತು ವಿನ್ಯಾಸಗಳಂತಹ ಮೆಟಾವರ್ಸ್‌ನೊಳಗಿನ ಸೃಷ್ಟಿಗಳಿಗೆ ವಿಸ್ತರಿಸಬಹುದು.

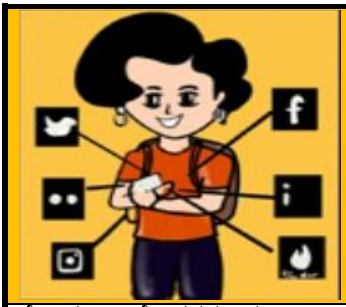
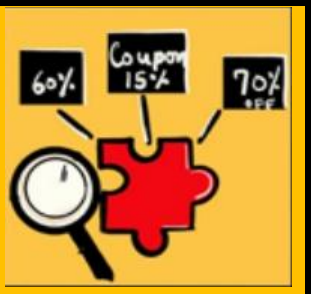
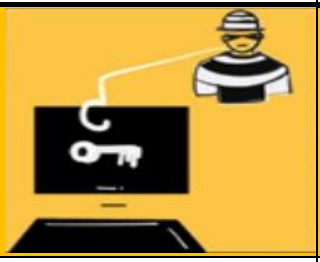
ಆನ್‌ಲೈನ್ ನಡವಳಿಕೆ ಮತ್ತು ಕಿರುಕುಳದ ಕಾನೂನುಗಳು: ನೈಜ ಜಗತ್ತಿನಲ್ಲಿರುವಂತೆ, ಕಿರುಕುಳ, ದ್ವೇಷ ಭಾಷಣ ಮತ್ತು ಸೈಬರ್‌ಬುಲ್ಲಿಂಗ್ ವಿರುದ್ಧದ ಕಾನೂನುಗಳು ಮೆಟಾವರ್ಸ್‌ನಲ್ಲಿನ ಪರಸ್ಪರ ಕ್ರಿಯೆಗಳಿಗೆ ಅನ್ವಯಿಸಬಹುದು.

ಡಿಜಿಟಲ್ ವಹಿವಾಟುಗಳು ಮತ್ತು ಗ್ರಾಹಕ ಸಂರಕ್ಷಣಾ ಕಾನೂನುಗಳು: ವರ್ಚುವಲ್ ಸರಕುಗಳು ಮತ್ತು ಸೇವೆಗಳನ್ನು ಮೆಟಾವರ್ಸ್‌ನಲ್ಲಿ ಖರೀದಿಸಿದರೆ ಮತ್ತು ಮಾರಾಟ ಮಾಡಿದರೆ, ಡಿಜಿಟಲ್ ವಹಿವಾಟುಗಳು ಮತ್ತು ಗ್ರಾಹಕ ಹಕ್ಕುಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ಕಾನೂನುಗಳು ಪ್ರಸ್ತುತವಾಗಬಹುದು.

ಸೈಬರ್ ಸುರಕ್ಷತಾ ಕಾನೂನುಗಳು: ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಮತ್ತು ಹ್ಯಾಕಿಂಗ್‌ಗೆ ಸಂಬಂಧಿಸಿದ ಕಾನೂನುಗಳು ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆಗಳು ಮತ್ತು ಥೀಮ್‌ನಲ್ಲಿನ ಇತರ ಭದ್ರತಾ ಘಟನೆಗಳಿಗೆ ಅನ್ವಯಿಸಬಹುದು.

ಮೆಟಾವರ್ಸ್ ನಿಜವಾದ ಪ್ರಪಂಚವಲ್ಲ ಎಂದು ಚೆನ್ನಾಗಿ ತಿಳಿದಿರಲಿ.

ಅಧಿವೇಶನ ಅಪಹರಣ ದಾಳಿ

		
ಸೋನು, 12ನೇ ತರಗತಿಯ ಚುರುಕು ವಿದ್ಯಾರ್ಥಿನಿ, ಅವಳು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ವೇದಿಕೆಗಳಲ್ಲಿ ಸಕ್ರಿಯಳಾಗಿದ್ದಳು.	ಅವಳು ತನ್ನ ಅನ್‌ಲೈನ್ ಶಾಪಿಂಗ್ ಹವ್ಯಾಸಕ್ಕಾಗಿ ತನ್ನನ್ನು ಕ್ಷಮಿಸಿ ಕೊಳ್ಳುವಂತಿಲ್ಲ.	ತನ್ನ ಸ್ನೇಹಿತೆ ಹಣ ಉಳಿಸುವ ಒಂದು ರಿಯಾಯ್ತಿ ಬ್ರೌಸರ್ ಎಕ್ಸ್‌ಟೆಂಷನ್‌ಅನ್ನು ಸೂಚಿಸಿದಳು
		
ಅವಳು ಹುರುಪಿನಿಂದ ಎಕ್ಸ್‌ಟೆಂಷನ್ ಇನ್ಸ್ಟಾಲ್ ಮಾಡಿ ಎಲ್ಲಾ ಅನುಮತಿಗಳನ್ನು ಅನುಮತಿಸಿದಳು.	ಅವಳು ತನ್ನ ಎಲ್ಲಾ ಖಾತೆಗಳಲ್ಲಿ 2FA ಸಕ್ರಿಯಗೊಳಿಸುವ ಚಾಣಾಕ್ಷತೆ ಹೊಂದಿದ್ದಳು.	ಎಕ್ಸ್‌ಟೆಂಷನ್‌ಗಳು ಕೂಪನ್ ಮುಖೇನ ರಿಯಾಯ್ತಿಯನ್ನು ಯಶಸ್ವಿಯಾಗಿ ಅನ್ವಯಗೊಳಿಸಿತು.
		
ಅವಳು ತನ್ನ ಸಾಮಾಜಿಕ ಖಾತೆ ಹ್ಯಾಕ್ ಆಗಿರುವ ಬಗ್ಗೆ & ಸಂಶಿತ ವ್ಯವಹರಣೆ ಬಗ್ಗೆ ತಿಳಿದುಕೊಂಡಳು.	2FA ಸಕ್ರಿಯಗೊಳಿಸಿದ್ದರೂ, add on ಕುಕೀಗಳನ್ನು ಕಸಿದು ಎಲ್ಲಾ ಖಾತೆಗಳನ್ನು ಆಕ್ರಮಣಿಸಿತು.	ದೃಢೀಕರಣ ಅಪ್ಲಿಕೇಶನ್ ಕೊರತೆ ಮತ್ತು ಬಹುಶಃ ಹಾನಿಕಾರಕ ಪ್ಲಗ್–ಇನ್‌ಗಳನ್ನು ಸ್ಥಾಪಿಸಲು ವಿಷಾದಕರ.

ಅಧಿವೇಶನ ಅಪಹರಣದ ದಾಳಿಯಲ್ಲಿ, ವೆಬ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಅಥವಾ ನೆಟ್‌ವರ್ಕ್‌ಗಳಲ್ಲಿನ ದುರ್ಬಲತೆಗಳನ್ನು ಬಳಸಿಕೊಳ್ಳುವ ಮೂಲಕ ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಸಕ್ರಿಯ ಬಳಕೆದಾರ ಅಧಿವೇಶನಕ್ಕೆ ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ಪಡೆಯುತ್ತಾರೆ. ಬಳಕೆದಾರರ ಗೌಪ್ಯತೆ ಮತ್ತು ಸುರಕ್ಷತೆಯನ್ನು ರಾಜಿ ಮಾಡಿಕೊಂಡು, ಅಧೀವೇಶನದ ನಿಯಂತ್ರಣವನ್ನು ತೆಗೆದುಕೊಳ್ಳುವ ಮೂಲಕ, ಅವರು ಬಳಕೆದಾರರನ್ನು ವೇಷ ಹಾಕಿ ನಟಿಸಬಹುದು, ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಪ್ರವೇಶಿಸಬಹುದು ಅಥವಾ ಅನಧಿಕೃತ ಕ್ರಿಯೆಗಳನ್ನು ನಡೆಸಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರಗಳಿಗೆ ಅನಧೀಕೃತ ಪ್ರವೇಶ, ದತ್ತಾಂಶ ಕಳ್ಳತನ ಮತ್ತು ಇತರೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳಿಗೆ ಸಂಬಂಧಿಸಿದೆ

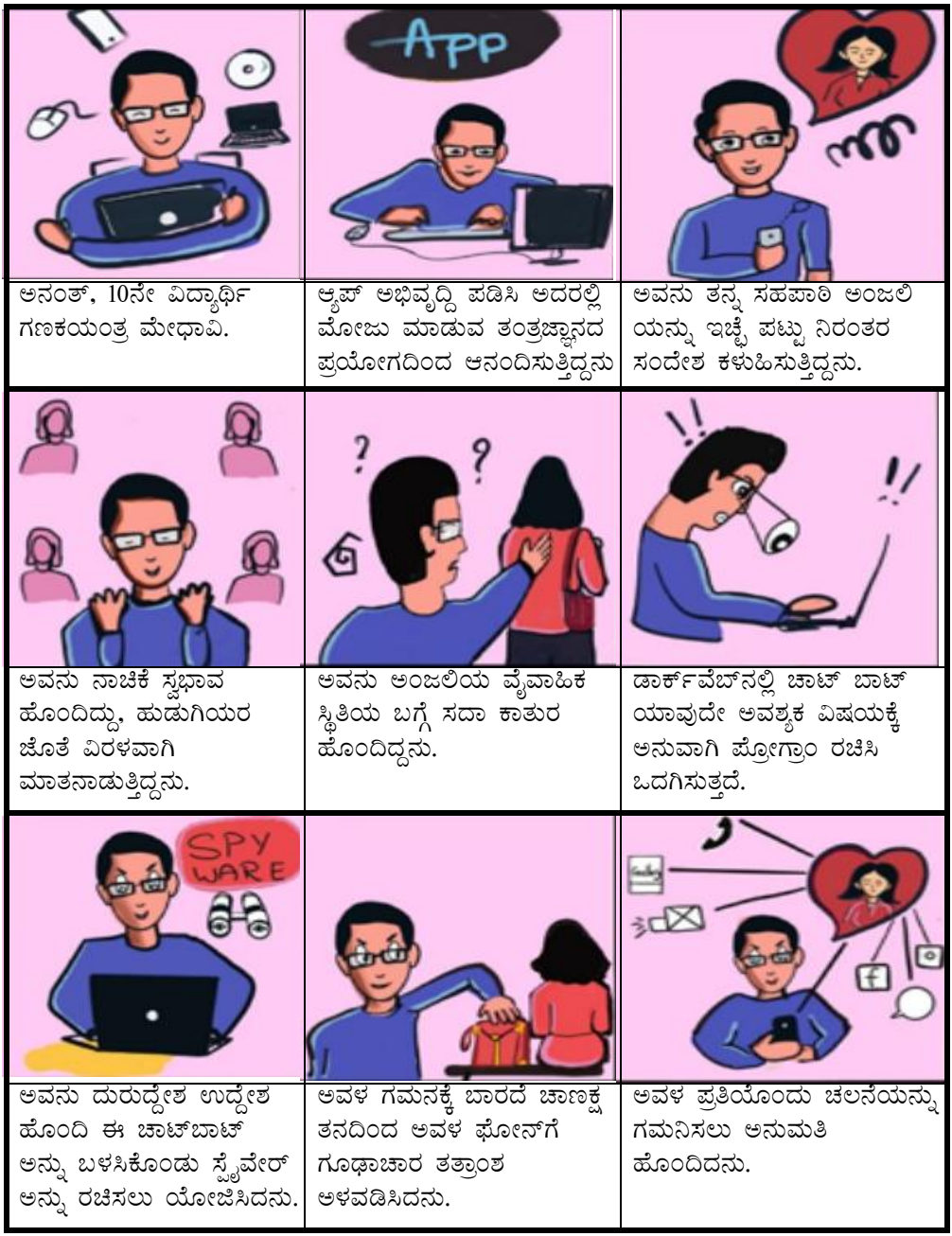
ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ – ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಒಬ್ಬ ವ್ಯಕ್ತಿಯ ವೇಷ ಹಾಕುವ ಉದ್ದೇಶದಿಂದ ಅಥವಾ ಅವರಿಗೆ ಆರ್ಥಿಕ ಅಥವಾ ಪ್ರತಿಷ್ಟೆ ಹಾನಿಯನ್ನು ಉಂಟುಮಾಡುವ ಉದ್ದೇಶದಿಂದ ಸೆಷನ್ ಅಪಹರಣದ ದಾಳಿಯನ್ನು ನಡೆಸಿದರೆ, ಈ ಕಲಂ ಅನ್ವಯಿಸಬಹುದು.)

ಮಾ.ತ.ಕಾ ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಇ– ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ನಕಲಿ ಐಡಿ ಸೃಷ್ಟಿಸಿ ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 72– ಈ ಕಲಂ ಸೇವಾ ಪೂರೈಕೆದಾರರು ನಿರ್ವಹಿಸುವ ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆ ಮತ್ತು ವೈಯಕ್ತಿಕತೆಯನ್ನು ರಕ್ಷಿಸುತ್ತದೆ.

ಸೈಬರ್ ನುಸುಳುಕೋರರು ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಸವಾರಿಯನ್ನು ಹೈಜಾಕ್ ಮಾಡಲು ಬಿಡಬೇಡಿ; ನಿಮ್ಮ ಸೆಷನ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ ಮತ್ತು ನಿಮ್ಮ ಸ್ಟ್ರೈಡ್ ಅನ್ನು ರಕ್ಷಿಸಿ.



ಅನಂತ್, 10ನೇ ವಿದ್ಯಾರ್ಥಿ ಗಣಕಯಂತ್ರ ಮೇಧಾವಿ.	ಆ್ಯಪ್ ಅಭಿವೃದ್ಧಿ ಪಡಿಸಿ ಅದರಲ್ಲಿ ಮೋಜು ಮಾಡುವ ತಂತ್ರಜ್ಞಾನದ ಪ್ರಯೋಗದಿಂದ ಆನಂದಿಸುತ್ತಿದ್ದನು	ಅವನು ತನ್ನ ಸಹಪಾಠಿ ಅಂಜಲಿಯನ್ನು ಇಚ್ಛೆ ಪಟ್ಟು ನಿರಂತರ ಸಂದೇಶ ಕಳುಹಿಸುತ್ತಿದ್ದನು.
ಅವನು ನಾಚಿಕೆ ಸ್ವಭಾವ ಹೊಂದಿದ್ದು, ಹುಡುಗಿಯರ ಜೊತೆ ವಿರಳವಾಗಿ ಮಾತನಾಡುತ್ತಿದ್ದನು.	ಅವನು ಅಂಜಲಿಯ ವೈವಾಹಿಕ ಸ್ಥಿತಿಯ ಬಗ್ಗೆ ಸದಾ ಕಾತುರ ಹೊಂದಿದ್ದನು.	ಡಾರ್ಕ್‌ವೆಬ್‌ನಲ್ಲಿ ಚಾಟ್ ಬಾಟ್ ಯಾವುದೇ ಅವಶ್ಯಕ ವಿಷಯಕ್ಕೆ ಅನುವಾಗಿ ಪ್ರೋಗ್ರಾಂ ರಚಿಸಿ ಒದಗಿಸುತ್ತದೆ.
ಅವನು ದುರುದ್ದೇಶ ಉದ್ದೇಶ ಹೊಂದಿ ಈ ಚಾಟ್‌ಬಾಟ್ ಅನ್ನು ಬಳಸಿಕೊಂಡು ಸ್ಪೈವೇರ್ ಅನ್ನು ರಚಿಸಲು ಯೋಜಿಸಿದನು.	ಅವಳ ಗಮನಕ್ಕೆ ಬಾರದೆ ಚಾಣಕ್ಷತನದಿಂದ ಅವಳ ಫೋನ್‌ಗೆ ಗೂಢಾಚಾರ ತತ್ರಾಂಶ ಅಳವಡಿಸಿದನು.	ಅವಳ ಪ್ರತಿಯೊಂದು ಚಲನೆಯನ್ನು ಗಮನಿಸಲು ಅನುಮತಿ ಹೊಂದಿದನು.

ಪ್ರಾಂಪ್ಟ್ ಎಂಜಿನಿಯರಿಂಗ್ ಎನ್ನುವುದು ಎಚ್ಚರಿಕೆಯಿಂದ ರಚಿಸಲಾದ ಸಂದೇಶಗಳ ಮೂಲಕ ಬಳಕೆದಾರರ ಕುಶಲತೆಯನ್ನು ಸೂಚಿಸುತ್ತದೆ ಅಥವಾ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಪಡಿಸಲು ಅಥವಾ ಅನಪೇಕ್ಷಿತ ಕ್ರಿಯೆಗಳನ್ನು ಮಾಡಲು ಅವರನ್ನು ಮೋಸಗೊಳಿಸಲು ಪ್ರೇರೇಪಿಸುತ್ತದೆ. ಈ ಸಾಮಾಜಿಕ ಎಂಜಿನಿಯರಿಂಗ್ ತಂತ್ರವನ್ನು ಸಾಮಾನ್ಯವಾಗಿ ಫಿಶಿಂಗ್ ದಾಳಿಗಳಲ್ಲಿ ಬಳಸಲಾಗುತ್ತದೆ, ಅಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಪಾಸ್‌ವರ್ಡ್‌ಗಳು, ವೈಯಕ್ತಿಕ ಡೇಟಾ ಅಥವಾ ಹಣಕಾಸಿನ ವಿವರಗಳನ್ನು ಬಹಿರಂಗಪಡಿಸಲು ವ್ಯಕ್ತಿಗಳನ್ನು ಮೋಸಗೊಳಿಸುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರ ಮತ್ತು ಗಣಕಯಂತ್ರ ವ್ಯವಸ್ಥೆ ಇತ್ಯಾದಿಗಳಿಗೆ ಆಗುವ ಹಾನಿಗೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪರಿಹಾರ

ಮಾ.ತ.ಕಾ ಕಲಂ 66– ಹ್ಯಾಕಿಂಗ್ ಒಳಗೊಂಡಂತೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 67– ಅಶ್ಲೀಲ ವಸ್ತುವನ್ನು ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಪ್ರಕಟಣೆ ಅಥವಾ ರವಾನೆ ಮಾಡಿದ ಕ್ರಮಕ್ಕೆ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾ ಕಲಂ 69– ಗಣಕಯಂತ್ರದ ಯಾವುದೇ ಸಂಪನ್ಮೂಲದ ಮೂಲಕ ಯಾವುದೇ ಮಾಹಿತಿಯನ್ನು ಪ್ರತಿಬಂಧಿಸುವುದಕ್ಕಾಗಿ ಅಥವಾ ಮೇಲ್ವಿಚಾರಣೆಗಾಗಿ ಅಥವಾ ಅಸಂಕೇತಿಕರಣಕ್ಕಾಗಿ ನಿರ್ದೇಶನಗಳನ್ನು ಹೊರಡಿಸುವ ಅಧಿಕಾರ

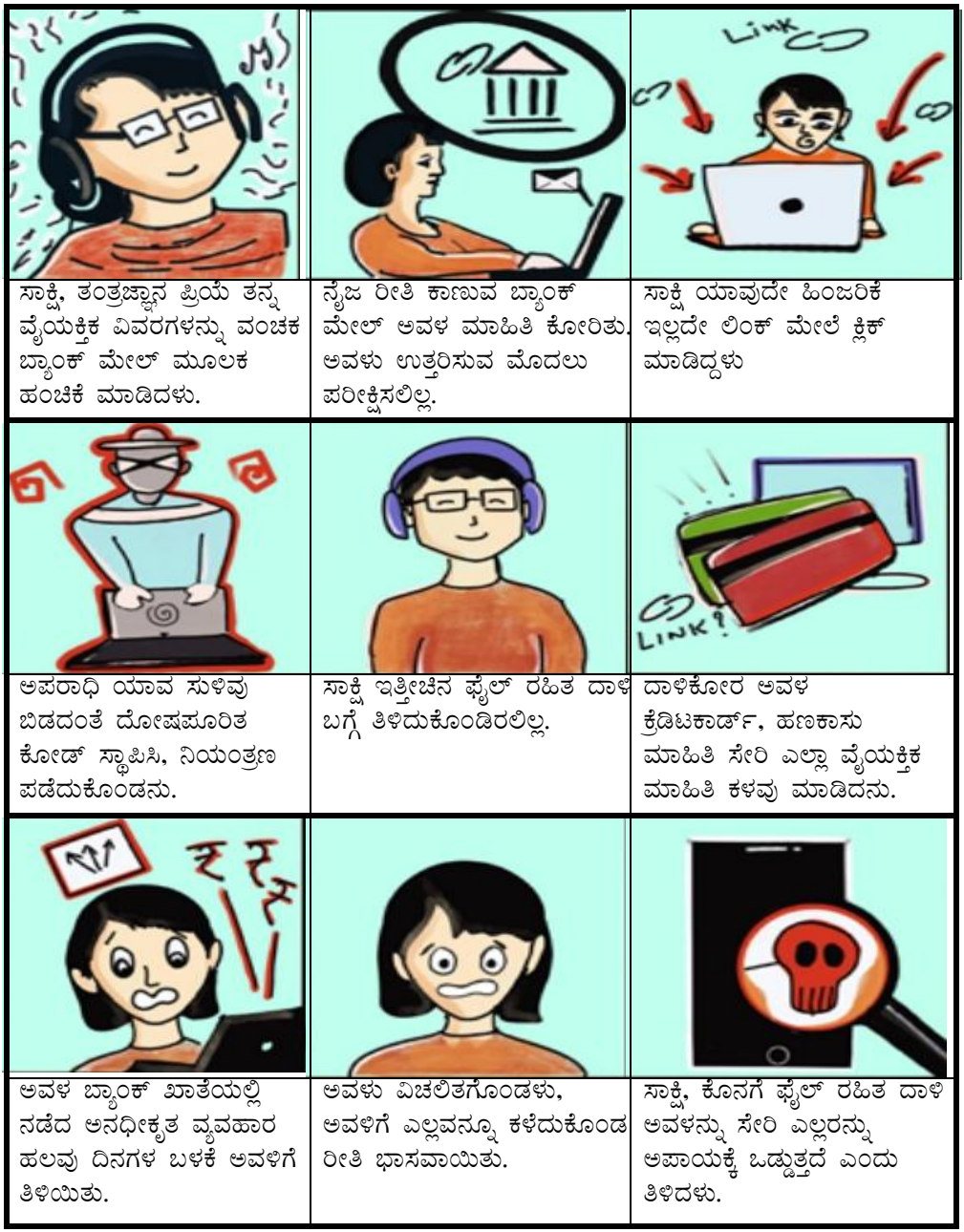
ಮಾ.ತ.ಕಾ ಕಲಂ 72– ಗೌಪ್ಯತೆ ಮತ್ತು ವೈಯಕ್ತಿಕ ರಹಸ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ದಂಡ

ಮಾ.ತ.ಕಾ ಕಲಂ 79– ಕೆಲವು ಸಂದರ್ಭಗಳಲ್ಲಿ ಮಧ್ಯವರ್ತಿಗಳನ್ನು ಹೊಣೆಗಾರರನ್ನಾಗಿಸುವುದರಿಂದ ವಿನಾಯಿತಿ

ಮಾ.ತ.ಕಾ ಕಲಂ 85– ಸಂಸ್ಥೆಗಳಿಂದ ಅಪರಾಧಗಳು

ಜಾಗರೂಕರಾಗಿರಿ ಮತ್ತು ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ, ಪ್ರಾಂಪ್ಟ್ ಎಂಜಿನಿಯರಿಂಗ್ ನಿಮ್ಮ ಗಮನ ಬೇರೆಡೆಗೆ ತಿರುಗಿಸಬಹುದು.

ಫೈಲ್ ರಹಿತ ದಾಳಿಗಳು



ಸಾಕ್ಷಿ, ತಂತ್ರಜ್ಞಾನ ಪ್ರಿಯೆ ತನ್ನ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ವಂಚಕ ಬ್ಯಾಂಕ್ ಮೇಲ್ ಮೂಲಕ ಹಂಚಿಕೆ ಮಾಡಿದಳು.	ನೈಜ ರೀತಿ ಕಾಣುವ ಬ್ಯಾಂಕ್ ಮೇಲ್ ಅವಳ ಮಾಹಿತಿ ಕೋರಿತು. ಅವಳು ಉತ್ತರಿಸುವ ಮೊದಲು ಪರೀಕ್ಷಿಸಲಿಲ್ಲ.	ಸಾಕ್ಷಿ ಯಾವುದೇ ಹಿಂಜರಿಕೆ ಇಲ್ಲದೇ ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಿದ್ದಳು
ಅಪರಾಧಿ ಯಾವ ಸುಳಿವು ಬಿಡದಂತೆ ದೋಷಪೂರಿತ ಕೋಡ್ ಸ್ಥಾಪಿಸಿ, ನಿಯಂತ್ರಣ ಪಡೆದುಕೊಂಡನು.	ಸಾಕ್ಷಿ ಇತ್ತೀಚಿನ ಫೈಲ್ ರಹಿತ ದಾಳಿ ಬಗ್ಗೆ ತಿಳಿದುಕೊಂಡಿರಲಿಲ್ಲ.	ದಾಳಿಕೋರ ಅವಳ ಕ್ರೆಡಿಟಕಾರ್ಡ್, ಹಣಕಾಸು ಮಾಹಿತಿ ಸೇರಿ ಎಲ್ಲಾ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಕಳವು ಮಾಡಿದನು.
ಅವಳ ಬ್ಯಾಂಕ್ ಖಾತೆಯಲ್ಲಿ ನಡೆದ ಅನಧೀಕೃತ ವ್ಯವಹಾರ ಹಲವು ದಿನಗಳ ಬಳಕೆ ಅವಳಿಗೆ ತಿಳಿಯಿತು.	ಅವಳು ವಿಚಲಿತಗೊಂಡಳು, ಅವಳಿಗೆ ಎಲ್ಲವನ್ನೂ ಕಳೆದುಕೊಂಡ ರೀತಿ ಭಾಸವಾಯಿತು.	ಸಾಕ್ಷಿ, ಕೊನಗೆ ಫೈಲ್ ರಹಿತ ದಾಳಿ ಅವಳನ್ನು ಸೇರಿ ಎಲ್ಲರನ್ನು ಅಪಾಯಕ್ಕೆ ಒಡ್ಡುತ್ತದೆ ಎಂದು ತಿಳಿದಳು.

ಈ ದಾಳಿಯು ಫೈಲ್ ಸಿಸ್ಟಮ್‌ನಲ್ಲಿ ಕುರುಹುಗಳನ್ನು ಬಿಡದೆಯೇ ನೇರವಾಗಿ ಕಂಪ್ಯೂಟರ್ ಮೆಮೊರಿಯಲ್ಲಿ ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್ ಅನ್ನು ಕಾರ್ಯಗತಗೊಳಿಸುವ ಮೂಲಕ ಸಾಂಪ್ರದಾಯಿಕ ಆಂಟಿವೈರಸ್ ಮತ್ತು ಪತ್ತೆ ವ್ಯವಸ್ಥೆಗಳನ್ನು ತಪ್ಪಿಸುತ್ತದೆ. ಈ ರಹಸ್ಯ ದಾಳಿಗಳು ಸಾಫ್ಟ್‌ವೇರ್‌ನಲ್ಲಿನ ದುರ್ಬಲತೆಗಳನ್ನು ಬಳಸಿಕೊಳ್ಳುತ್ತವೆ, ಅವುಗಳನ್ನು ಪತ್ತೆಹಚ್ಚಲು ಕಷ್ಟವಾಗುವಂತೆ ಮಾಡುತ್ತದೆ ಮತ್ತು ಡೇಟಾ ಕಳ್ಳತನ, ಕಣ್ಗಾವಲು ಅಥವಾ ಮತ್ತಷ್ಟು ದಾಳಿಗಳನ್ನು ಪ್ರಾರಂಭಿಸಲು ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ರಿಮೋಟ್ ಪ್ರವೇಶವನ್ನು ಸೈಬರ್ ಅಪರಾಧಿಗಳಿಗೆ ಒದಗಿಸುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರ ಮತ್ತು ಗಣಕಯಂತ್ರ ವ್ಯವಸ್ಥೆ ಇತ್ಯಾದಿಗಳಿಗೆ (ಅನಧೀಕೃತ ಪ್ರವೇಶ) ಆಗುವ ಹಾನಿಗೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪರಿಹಾರ

ಮಾ.ತ.ಕಾ ಕಲಂ 43A: ದತ್ತಾಂಶದ ಸಂರಕ್ಷಣೆಯ ವಿಫಲತೆಗಾಗಿ ಪರಿಹಾರ

ಮಾ.ತ.ಕಾ ಕಲಂ 66: ಹ್ಯಾಕಿಂಗ್ ಒಳಗೊಂಡಂತೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 66B: ಕಳ್ಳತನದ ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಅಥವಾ ಸಂವಹನ ಸಾಧನಗಳನ್ನು ಅಪ್ರಮಾಣಿಕವಾಗಿ ಸ್ವೀಕರಿಸಿದರೆ ದಂಡನೆ

ಮಾ.ತ.ಕಾ ಕಲಂ 66C: ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾ ಕಲಂ 66 E: ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ನಕಲಿ ಐಡಿ ಸೃಷ್ಟಿಸಿ ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾ ಕಲಂ 66 F: ಸೈಬರ್ ಭಯೋತ್ಪಾದನೆಗಾಗಿ ಶಿಕ್ಷೆ (ಫೈಲ್‌ರಹಿತ ದಾಳಿಯನ್ನು ಭಯೋತ್ಪಾದನೆ ಅಥವಾ ಪ್ರಮುಖ ಮೂಲಸೌಕರ್ಯವನ್ನು ಅಸ್ಥಿರಗೊಳಿಸುವ ಉದ್ದೇಶದಿಂದ ನಡೆಸಿದರೆ)

ಮೂಕ ಮತ್ತು ಚೋರ, ಕಡತರಹಿತ ವೈರಿಗಳು;
ನಿಮ್ಮ ರಕ್ಷಣೆಯನ್ನು ಬಲಪಡಿಸಿ ಮತ್ತು ಅವರ ಆಕ್ರಮಣವನ್ನು ನಿರ್ಬಂಧಿಸಿ

ವಿತರಣಾ (ಡೆಲಿವೆರಿ) ಹಗರಣ

ಆಶಾ ಪಿಝಾ ಆರ್ಡರ್ ಮಾಡಿದಳು ಆ ಸಂದರ್ಭದಲ್ಲಿ ಅಪರಿಚಿತ ಸಂಖ್ಯೆಯಿಂದ ಒ.ಟಿ.ಪಿ ಖಚಿತಪಡಿಸಲು ಪಠ್ಯ ಸಂದೇಶ ಸ್ವೀಕರಿಸಿದಳು

ಆಶಾ ಯಾವುದೇ ಹಿಂಜರಿಕೆ ಇಲ್ಲದೇ ತಕ್ಷಣ ಓ.ಟಿ.ಪಿ ಕಳುಹಿಸಿದಳು

ತಕ್ಷಣ, ಅವಳ ಖಾತೆಯಲ್ಲಿ ನಡೆದ ಅನಧೀಕೃತ ಬ್ಯಾಂಕ್ ವ್ಯವಹಾರದಿಂದಾಗಿ ದಿಗ್ಭ್ರಮೆಗೊಂಡಳು

ಆಶಾ ಡೆಲಿವರಿ ಓ.ಟಿ.ಪಿ ಮೋಸ ಜಾಲದಲ್ಲಿ ಬಲಿಪಶುವಾಗಿದ್ದಳು

ಈ ಬ್ಯಾಂಕ್ ವ್ಯವಹರಣೆ ಬಗ್ಗೆ ಪೊಲೀಸ್ ಮತ್ತು ಬ್ಯಾಂಕ್‌ನಲ್ಲಿ ದೂರು ನೀಡಿದಳು

ಆದರೆ ಅತೀ ವಿಳಂಭವಾಗಿತ್ತು; ಅಪರಾಧಿಯು ಯಾವುದೇ ಸುಳಿವು ನೀಡದೆ ಪರಾರಿಯಾಗಿದ್ದ

ಆಶಾ, ಭವಿಷ್ಯದಲ್ಲಿ ತೀರಾ ಎಚ್ಚರಿಕೆ ಮತ್ತು ಜಾಗರೂಕತೆಯಿಂದ ಇರಬೇಕು ಎಂಬುದನ್ನು ಕಲಿತಳು.

ತನ್ನ ಅನುಭವ ಸ್ನೇಹಿತೆ ಜೊತೆ ಚರ್ಚಿಸಿದಾಗ, ಅವಳಿಗೂ ವಿತರಣೆ ಸಂದರ್ಭದಲ್ಲಿ ಪಾವತಿ ಅನುಭವ ವಿವರಿಸಿದಳು.

ಡೆಲಿವರಿ ಹುಡುಗ ಓ.ಟಿ.ಪಿ ಪಡೆದು ಕಾನೂನು ಬಾಹಿರ ಚಟುವಟಿಕೆ ನಡೆಸಿ, ತಪ್ಪು ವಸ್ತು ವಿತರಿಸಿದ ಬಗ್ಗೆ ಚರ್ಚಿಸಿದರು.

ವಿತರಣಾ ಹಗರಣವು ಸೈಬರ್ ಅಪರಾಧಿಗಳು ನಕಲಿ ಪ್ರಕಟಣೆಗಳನ್ನು ಕಳುಹಿಸುವುದನ್ನು ಅಥವಾ ಸ್ವೀಕರಿಸುವವರನ್ನು ಅವರು ಪ್ಯಾಕೇಜ್ ಅಥವಾ ಡೆಲಿವರಿಯು ಬಾಕಿಯಿದೆ ಎಂದು ನಂಬುವಂತೆ ಮಾಡಿ ಮೋಸಗೊಳಿಸಲು ಮಾಹಿತಿಯನ್ನು ಟ್ರ್ಯಾಕ್ ಮಾಡುವುದನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ. ವಂಚನೆಯು ಬಲಿಪಶುಗಳ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಪಡಿಸಲು, ದುರುದ್ದೇಶಪೂರಿತ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಲು ಅಥವಾ ನಕಲಿ ಶಿಪ್ಪಿಂಗ್ ಶುಲ್ಕವನ್ನು ಪಾವತಿಸಲು ಮೋಸಗೊಳಿಸುವ ಗುರಿಯನ್ನು ಹೊಂದಿದ್ದು, ಇದು ಹಣಕಾಸಿನ ನಷ್ಟ ಅಥವಾ ಡೇಟಾ ಹೊಂದಾಣಿಕೆಗೆ ಕಾರಣವಾಗುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರ ಮತ್ತು ಗಣಕಯಂತ್ರ ವ್ಯವಸ್ಥೆ ಇತ್ಯಾದಿಗಳಿಗೆ (ಅನಧೀಕೃತ ಪ್ರವೇಶ) ಆಗುವ ಹಾನಿಗೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪರಿಹಾರ

ಮಾ.ತ.ಕಾ ಕಲಂ 66: ಹ್ಯಾಕಿಂಗ್ ಒಳಗೊಂಡಂತೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319– ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ

ಮೋಸಗಾರರ ಬಲೆಗೆ ಬೀಳಬೇಡಿ;
ನೀವು 'ಸಮ್ಮತಿ' ಅಥವಾ 'ಹಂಚಿಕೊಳ್ಳಿ' ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವ ಮೊದಲು ಪರಿಶೀಲಿಸಿ.

ವರ್ಚುವಲ್ ಅಪಹರಣ

ಶ್ವೇತ, ಬ್ಯಾಂಕ್ ಮ್ಯಾನೇಜರ್ ಆಗಿದ್ದು, ಸಿಬ್ಬಂದಿ ಸಂವಹನಕ್ಕಾಗಿ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಬಳಸುತ್ತಿದ್ದಳು.	ವ್ಯಾಟ್ಸಾಪ್, ಇನ್ಸ್ಟಾ, ಇತರೆ ಆನ್‌ಲೈನ್ ವೇದಿಕೆ ಬಳಸಿ ಸಿಬ್ಬಂದಿಯೊಂದಿಗೆ ಸಂಪರ್ಕ ಸಾಧಿಸುತ್ತಿದ್ದಳು.	ಒಮ್ಮೆ ಗ್ರಾಹಕನೊಬ್ಬ ಸಾಲ ಪಾವತಿ ಬಗ್ಗೆ ದಾಖಲೆ ರೂಪದಲ್ಲಿ ಇ-ಮೇಲ್ ಲಿಂಕ್ ಕಳುಹಿಸುತ್ತಾನೆ.
ಶ್ವೇತ ಯಾವುದೇ ಹಿಂಜರಿಕೆ ಇಲ್ಲದೆ ಲಿಂಕ್ ಕ್ಲಿಕ್ ಮಾಡುತ್ತಾಳೆ	ಒಂದು ಅಜಾಗರೂಕ ಕ್ಲಿಕ್, ಮ್ಯಾಕ್ರೋ ಮಾಲ್ವೇರ್ ದಾಳಿ ಆಗಿ ಅಧಿವೇಶನ ಹೈಜಾಕ್ ಆಯಿತು.	ಮರುದಿನ, ಅವಳ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಖಾತೆಗೆ ಪ್ರವೇಶ ನಿರಾಕರಣೆ ಆಯಿತು.
ಸೈಬರ್ ಅಪಹರಣದ ಬಲಿಪಶು ಆದಳು ಮತ್ತು ಅವರ ಸಂಪೂರ್ಣ ವ್ಯಕ್ತಿತ್ವ ಕಳೆದುಕೊಂಡಳು	ಆಕ್ರಮಣಕಾರ ಎಲ್ಲಾ ಸಿಬ್ಬಂದಿಗೆ ಹಣ ವರ್ಗಾವಣೆ ಕೋರಿಕೆ ಸಂದೇಶವನ್ನು ಕಳುಹಿಸುತ್ತಾನೆ.	ಈ ಘಟನೆಯು ಹಠಾತ್ ಆನ್‌ಲೈನ್ ಕ್ರಿಯೆಗಳ ಅಪಾಯಗಳನ್ನು ಎತ್ತಿ ತೋರಿಸುತ್ತದೆ.

ಇದು ಮಾನಸಿಕ ಸುಲಿಗೆ ಯೋಜನೆಯಾಗಿದ್ದು, ದುಷ್ಕರ್ಮಿಗಳು ಸಂತ್ರಸ್ತರನ್ನು ತಮ್ಮ ಪ್ರೀತಿಪಾತ್ರರನ್ನು ಅಪಹರಿಸಿದ್ದಾರೆ ಎಂದು ನಂಬುವಂತೆ ಕುಶಲತೆಯಿಂದ ವರ್ತಿಸುತ್ತಾರೆ, ಅವರ ಬಿಡುಗಡೆಗಾಗಿ ವಿಮೋಚನೆ–ಮೊತ್ತಕ್ಕಾಗಿ ಒತ್ತಾಯಿಸುತ್ತಾರೆ. ನಿಜವಾದ ಅಪಹರಣ ಸಂಭವಿಸದಿದ್ದರೂ, ಉಂಟಾಗುವ ಭಾವನಾತ್ಮಕ ಯಾತನೆ ಮತ್ತು ಭಯವು ಬಲಿಪಶುಗಳು ಬೇಡಿಕೆಗಳನ್ನು ಅನುಸರಿಸಲು ಕಾರಣವಾಗಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 66ಸಿ – ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಒಬ್ಬ ವ್ಯಕ್ತಿಯ ವೇಷಧರಿಸಿ ವರ್ಚುಯಲ್ ಅಪಹರಣ ನಡೆಸಿದರೆ, ಈ ಕಲಂ ಅನ್ವಯಿಸಬಹುದು.)

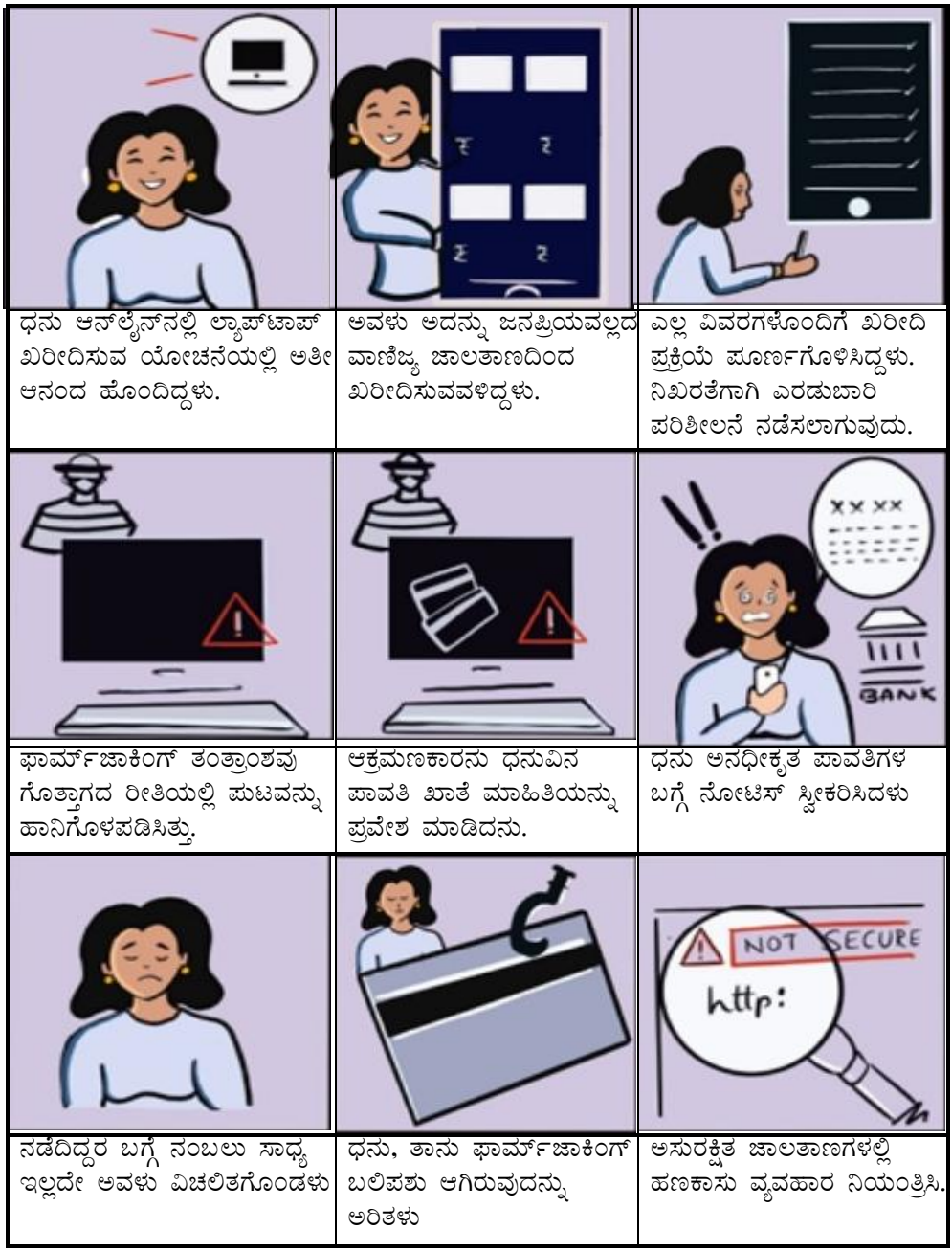
ಮಾ.ತ.ಕಾ 3ಕಲಂ 66ಡಿ– ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 503/ಬಿಎನ್ಎಸ್ 351– ಅಪರಾಧಿ ಬೆದರಿಕೆ (ವರ್ಚುವಲ್ ಅಪಹರಣದ ಸನ್ನಿವೇಶದಲ್ಲಿ ಬೆದರಿಕೆಗಳನ್ನು ಮಾಡಿದರೆ)

ಐಪಿಸಿ ಕಲಂ 506/ಬಿಎನ್ಎಸ್ 351– ಅಪರಾಧಿ ಬೆದರಿಕೆಗಾಗಿ ಶಿಕ್ಷೆ (ವ್ಯಕ್ತಿಯ ಖ್ಯಾತಿಗೆ ಧಕ್ಕೆ ಬಂದರೆ)

ನಿಮ್ಮ ವರ್ಚುವಲ್ ಕ್ಷೇತ್ರವನ್ನು ಶಕ್ತಿಯಿಂದ ಕಾಪಾಡಿ;
ವರ್ಚುವಲ್ ಅಪಹರಣಕಾರರು ಹೋರಾಟದಲ್ಲಿ ಸೋಲುತ್ತಾರೆ.

ಫಾರ್ಮ್‌ಜಾಕಿಂಗ್



ಧನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಲ್ಯಾಪ್‌ಟಾಪ್ ಖರೀದಿಸುವ ಯೋಚನೆಯಲ್ಲಿ ಅತೀ ಆನಂದ ಹೊಂದಿದ್ದಳು.	ಅವಳು ಅದನ್ನು ಜನಪ್ರಿಯವಲ್ಲದ ವಾಣಿಜ್ಯ ಜಾಲತಾಣದಿಂದ ಖರೀದಿಸುವವಳಿದ್ದಳು.	ಎಲ್ಲ ವಿವರಗಳೊಂದಿಗೆ ಖರೀದಿ ಪ್ರಕ್ರಿಯೆ ಪೂರ್ಣಗೊಳಿಸಿದ್ದಳು. ನಿಖರತೆಗಾಗಿ ಎರಡುಬಾರಿ ಪರಿಶೀಲನೆ ನಡೆಸಲಾಗುವುದು.
ಫಾರ್ಮ್‌ಜಾಕಿಂಗ್ ತಂತ್ರಾಂಶವು ಗೊತ್ತಾಗದ ರೀತಿಯಲ್ಲಿ ಪುಟವನ್ನು ಹಾನಿಗೊಳಪಡಿಸಿತ್ತು.	ಆಕ್ರಮಣಕಾರನು ಧನುವಿನ ಪಾವತಿ ಖಾತೆ ಮಾಹಿತಿಯನ್ನು ಪ್ರವೇಶ ಮಾಡಿದನು.	ಧನು ಅನಧೀಕೃತ ಪಾವತಿಗಳ ಬಗ್ಗೆ ನೋಟಿಸ್ ಸ್ವೀಕರಿಸಿದಳು
ನಡೆದಿದ್ದರ ಬಗ್ಗೆ ನಂಬಲು ಸಾಧ್ಯ ಇಲ್ಲದೇ ಅವಳು ವಿಚಲಿತಗೊಂಡಳು	ಧನು, ತಾನು ಫಾರ್ಮ್‌ಜಾಕಿಂಗ್ ಬಲಿಪಶು ಆಗಿರುವುದನ್ನು ಅರಿತಳು	ಅಸುರಕ್ಷಿತ ಜಾಲತಾಣಗಳಲ್ಲಿ ಹಣಕಾಸು ವ್ಯವಹಾರ ನಿಯಂತ್ರಿಸಿ.

ಫಾರ್ಮ್‌ಜಾಕಿಂಗ್

ಇದು ಇ–ಕಾಮರ್ಸ್ ವೆಬ್‌ಸೈಟ್‌ಗಳ ಪಾವತಿ ಅರ್ಜಿಗಳಿಗೆ ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್ ಸೇರಿಸುವುದನ್ನು ಒಳಗೊಂಡಿರುವ ದಾಳಿಯಾಗಿದೆ. ಆನ್‌ಲೈನ್ ವಹಿವಾಟಿನ ಸಮಯದಲ್ಲಿ ಗ್ರಾಹಕರು ನಮೂದಿಸಿದ ಪಾವತಿ ಕಾರ್ಡ್ ವಿವರಗಳು ಅಥವಾ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಕೋಡ್ ಕದಿಯುತ್ತದೆ, ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಪಾವತಿ ವಂಚನೆ ಅಥವಾ ಗುರುತಿನ ಕಳ್ಳತನದಲ್ಲಿ ತೊಡಗಿಸಿಕೊಳ್ಳಲು ಅನುವು ಮಾಡಿಕೊಡುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರ ಮತ್ತು ಗಣಕಯಂತ್ರ ವ್ಯವಸ್ಥೆ ಇತ್ಯಾದಿಗಳಿಗೆ (ಅನಧೀಕೃತ ಪ್ರವೇಶ) ಆಗುವ ಹಾನಿಗೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪರಿಹಾರ

ಮಾ.ತ.ಕಾ ಕಲಂ 43A: ದತ್ತಾಂಶದ ಸಂರಕ್ಷಣೆಯ ವಿಫಲತೆಗಾಗಿ ಪರಿಹಾರ

ಮಾ.ತ.ಕಾ ಕಲಂ 66: ಹ್ಯಾಕಿಂಗ್ ಒಳಗೊಂಡಂತೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 66C: ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318– ಮೋಸ ಮತ್ತು ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಆಸ್ತಿಯ ವಿತರಣೆ

ಕಲಂ 463/ಬಿಎನ್‌ಎಸ್ 336: ಈ ವಿಭಾಗವು ನಕಲಿಗೆ ಸಂಬಂಧಿಸಿದೆ.

ಕಲಂ 464/ಬಿಎನ್‌ಎಸ್ 335: ಈ ವಿಭಾಗವು ತಪ್ಪು ದಾಖಲೆಯನ್ನು ಮಾಡುವ ಬಗ್ಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ.

ನಿಮ್ಮ ಅರ್ಜಿಗಳನ್ನು ಅತ್ಯಂತ ಎಚ್ಚರಿಕೆಯಿಂದ ರಕ್ಷಿಸಿ;
ಫಾರ್ಮ್‌ಜಾಕರ್‌ಗಳು ತಮ್ಮ ಪಾಲನ್ನು ಕಂಡುಕೊಳ್ಳಲಾರರು.

ಸೈಬರ್ ಸ್ಕ್ವಾಟ್ಟಿಂಗ್

ಕರಣ್, ಯಶಸ್ವಿ ಐ.ಟಿ ವೃತ್ತಿಪರ ನಾಗಿದ್ದು, ಖಾಯಂ ಉದ್ಯೋಗ ಪಡೆದುಕೊಂಡಿದ್ದನು	ಅವನು ವೆಬ್ ಸರ್ವರ್ ನಿರ್ವಹಣೆ ವಿಷಯದಲ್ಲಿ ನಿಪುಣನಾಗಿದ್ದು.	ಅವನ ಸಂಸ್ಥೆಯು ಅನಿರೀಕ್ಷಿತ ಸಾಮೂಹಿಕ ವಜಾ ನೆಲೆಯಲ್ಲಿ ಬಂದು ನಿಂತಿತು.

ಕರಣ್, ದುರದೃಷ್ಟಕರವಾಗಿ ವಜಾಗೊಳಿಸುವಿಕೆಯಿಂದ ತೊಂದರೆಗೆ ಒಳಗಾದನು.	ಅವನು ತನ್ನ ಸಂಸ್ಥೆಯ ವಿರುದ್ಧ ಪ್ರತಿಕೂಲ ದ್ವೇಶ ಸಾಧಿಸಲು ಅಸಮಧಾನದಿಂದ ತಯಾರಾದನು	ಕರಣ್, ತನ್ನ ಕಂಪನಿಯ ಹೆಸರಿನಂತಿರುವ ಡುಮೇನ್ ಖರೀದಿ ಮಾಡಿದನು

ಅವನು ಅದೇ ಅಸಲು ವೆಬ್‌ಸೈಟ್ ರೀತಿಯೇ ನಕಲಿಯನ್ನು ತಯಾರಿಸಿ ಯೋಜನೆಯಂತೆ ಪ್ರಚಾರ ಮಾಡಿದನು.	ಇನ್ನು ಒಂದು ಹೆಜ್ಜೆ ಮುಂದೆ ಹೋಗಿ ಎಲ್ಲಾ ಗ್ರಾಹಕರಿಗೆ ಮೇಲ್ ಮಾಡಿ ಗೊಂದಲ ಸೃಷ್ಟಿ ಮಾಡಿದನು.	ಈ ಪ್ರಕರಣವು ಸಂಸ್ಥೆಯ ಖ್ಯಾತಿಗೆ ತೀವ್ರತರವಾಗಿ ಧಕ್ಕೆ ಉಂಟು ಮಾಡಿತು.

ಇದು ಒಂದು ಬ್ರ್ಯಾಂಡ್‌ನ ಖ್ಯಾತಿಯ ಲಾಭ ಪಡೆಯುವ ಉದ್ದೇಶದಿಂದ ಸ್ಥಾಪಿತ ಬ್ರ್ಯಾಂಡ್ ಅಥವಾ ಟ್ರೇಡ್‌ಮಾರ್ಕ್‌ಗಳಿಗೆ ಹೋಲುವ ಡೊಮೇನ್ ಹೆಸರುಗಳನ್ನು ನೋಂದಾಯಿಸಿ, ಡೊಮೇನ್ ಪಡೆದು ನಂತರ ಅದನ್ನು ಹೆಚ್ಚಿನ ಬೆಲೆಗೆ ನಿಜವಾದ ಮಾಲೀಕರಿಗೆ ಮಾರಾಟ ಮಾಡುವುದಾಗಿರುತ್ತದೆ. ಇದು ಬ್ರ್ಯಾಂಡ್ ದುರ್ಬಲಗೊಳಿಸುವಿಕೆ, ಖ್ಯಾತಿ ಹಾನಿ ಮತ್ತು ಗ್ರಾಹಕರಲ್ಲಿ ಗೊಂದಲಕ್ಕೆ ಕಾರಣವಾಗಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 2(1)(r): 'ಡೊಮೇನ್ ನೇಮ್' ವಿವರಿಸುತ್ತದೆ, ಸೈಬರ್ ಸ್ಕ್ವಾಟಿಂಗ್ ಅರ್ಥಮಾಡಿಕೊಳ್ಳಲು ಇದು ಅವಶ್ಯಕ

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರ ಮತ್ತು ಗಣಕಯಂತ್ರ ವ್ಯವಸ್ಥೆ ಇತ್ಯಾದಿಗಳಿಗೆ (ಅನಧೀಕೃತ ಪ್ರವೇಶ) ಆಗುವ ಹಾನಿಗೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪರಿಹಾರ

ಮಾ.ತ.ಕಾ ಕಲಂ 66ಡಿ: ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

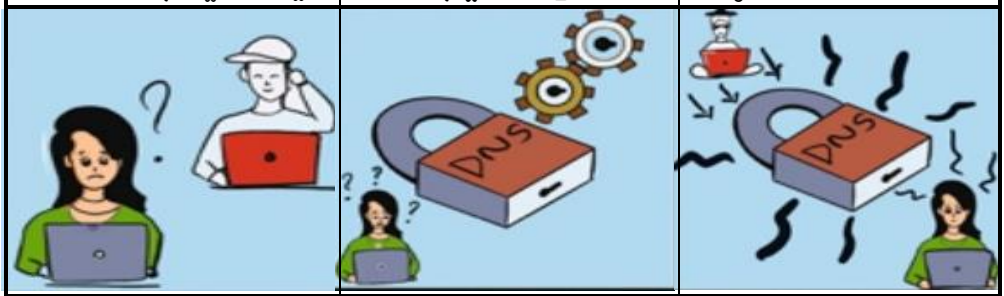
ಮಾ.ತ.ಕಾ ಕಲಂ 79: ಕೆಲವು ಸಂದರ್ಭಗಳಲ್ಲಿ ಮಧ್ಯವರ್ತಿಗಳನ್ನು ಹೊಣೆಗಾರರನ್ನಾಗಿಸುವುದರಿಂದ ವಿನಾಯಿತಿ

ಮಾ.ತ.ಕಾ ಕಲಂ 81: ಅತಿಕ್ರಮಣ ಪರಿಣಾಮವನ್ನು ಹೊಂದಲು ಕಾಯ್ದೆ

ಡಿಜಿಟಲ್ ಪ್ರಪಂಚದಲ್ಲಿ ನಿಮ್ಮ ಹಕ್ಕು ಸಾಧಿಸಿ;
ಸೈಬರ್‌ಸ್ಕ್ವಾಟರ್‌ಗಳಿಗೆ ಯಾವುದೇ ಅವಕಾಶ ನೀಡದಿರಿ.

ಡಿ.ಎನ್.ಎಸ್ ಹೈಜಾಕಿಂಗ್

ಸುಮಾ, ಸಣ್ಣ ಸಂಸ್ಥೆ ಮಾಲೀಕಳಾಗಿದ್ದಳು, ವ್ಯಾಪಾರ ವೃದ್ಧಿಸಲು ಜಾಲತಾಣವನ್ನು ನೆಚ್ಚಿಕೊಂಡಿದ್ದಳು	ಸುಮಾ ಸಹಾಯವಾಣಿಯಿಂದ ತನ್ನ ಜಾಲತಾಣ ಸ್ಥಗಿತಗೊಂಡಿರುವ ಬಗ್ಗೆ ಕರೆಯನ್ನು ಸ್ವೀಕರಿಸುತ್ತಾಳೆ	ನಂತರ, ಸುಮಾ ತನ್ನ ಜಾಲತಾಣವನ್ನು ಪ್ರವೇಶಿಸಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲ.



ಅವಳು ತನ್ನ ಹೋಸ್ಟ್‌ಗೆ ಕರೆ ಮಾಡಿದಾಗ, ಡಿಎನ್‌ಎಸ್ ಸೆಟ್ಟಿಂಗ್ ಮಾರ್ಪಾಡಾಗಿರುವ ಬಗ್ಗೆ ತಿಳಿಯುತ್ತಾಳೆ.	ಯಾವುದೇ ಡಿಎನ್‌ಎಸ್ ಮಾರ್ಪಾಡುಗಳನ್ನು ಮಾಡದ ಕಾರಣ ಸುಮಾ ಗೊಂದಲಕ್ಕೆ ಒಳಗಾದಳು	ಸುಮಾಳ ಜಾಳತಾಣಕ್ಕೆ ಡಿಎನ್‌ಎಸ್ ಹೈಜಾಕಿಂಗ್ ಆಕ್ರಮಣವಾಗಿತ್ತು.

ಆಕ್ರಮಣಕಾರ ಸುಮಾಳ ಡಿಎನ್‌ಎಸ್ ಬದಲಾಯಿಸಿ, ನಕಲಿ ಜಾಲತಾಣಕ್ಕೆ ಪ್ರವೇಶ ಹೋಗುವಂತೆ ಮಾಡಿದ್ದನು.	ಸುಮಾಳ ಗ್ರಾಹಕರು ನಕಲಿ ಜಾಲ ತಾಣಕ್ಕೆ ಭೇಟಿ ನೀಡಿ ತಮ್ಮ ವೈಯಕ್ತಿಕ ಮತ್ತು ಹಣಕಾಸು ಮಾಹಿತಿ ಕಳೆದುಕೊಂಡರು.	ಅಂತರ್ಜಾಲದಲ್ಲಿ ನಾಶವಾದ ಖ್ಯಾತಿಯನ್ನು ಸರಿಪಡಿಸುವುದು ಕಷ್ಟ, ನಂಬಿಕೆ ದುರ್ಬಲವಾಗುತ್ತದೆ.

ಈ ದಾಳಿಯು ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ನೆಟ್‌ವರ್ಕ್‌ನ ಡೊಮೈನ್ ನೇಮ್ ಸಿಸ್ಟಮ್ (DNS) ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಬದಲಾಯಿಸುವುದಾಗಿರುತ್ತದೆ, ಇದರಿಂದ ಗ್ರಾಹಕರಿಗೆ ದುರುದ್ದೇಶಪೂರಿತ ವೆಬ್‌ಸೈಟ್‌ಗಳಿಗೆ ಮರುನಿರ್ದೇಶಿಸಲಾಗುತ್ತದೆ. DNS ಕೋರಿಕೆಗಳನ್ನು ಪ್ರತಿಬಂಧಿಸಿ ಮತ್ತು ಸ್ವಾಧಿನ ಪಡಿಸಿಕೊಂಡು, ಆಕ್ರಮಣಕಾರರು ಕುಶಲತೆಯಿಂದ ಬಳಕೆದಾರರನ್ನು ಫಿಶಿಂಗ್ ಪುಟಗಳಿಗೆ ಕರೆದೊಯ್ಯಬಹುದು, ಮಾಲ್‌ವೇರ್ ಹರಿಬಿಡಬಹುದು ಅಥವಾ ಇತರ ದುರುದ್ದೇಶಪೂರಿತ ಚಟುವಟಿಕೆಗಳಲ್ಲಿ ತೊಡಗಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 43: ಗಣಕಯಂತ್ರ ಮತ್ತು ಗಣಕಯಂತ್ರ ವ್ಯವಸ್ಥೆ ಇತ್ಯಾದಿಗಳಿಗೆ (ಅನಧೀಕೃತ ಪ್ರವೇಶ) ಆಗುವ ಹಾನಿಗೆ ಶಿಕ್ಷೆ ಮತ್ತು ಪರಿಹಾರ

ಮಾ.ತ.ಕಾ ಕಲಂ 66: ಹ್ಯಾಕಿಂಗ್ ಒಳಗೊಂಡಂತೆ ಗಣಕಯಂತ್ರ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 66C: ವ್ಯಕ್ತಿತ್ವ ಕಳ್ಳತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ (ಅನನ್ಯ ಗುರುತಿನ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಅಪ್ರಾಮಾಣಿಕತೆಯಿಂದ ಅಥವಾ ಮೋಸದಿಂದ ಬಳಸುವುದು)

ಮಾ.ತ.ಕಾ ಕಲಂ 66ಡಿ: ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾ ಕಲಂ 66 E: ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ನಕಲಿ ಐಡಿ ಸೃಷ್ಟಿಸಿ ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆಗಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾ ಕಲಂ 72– ಈ ಕಲಂ ಸೇವಾ ಪೂರೈಕೆದಾರರು ನಿರ್ವಹಿಸುವ ಮಾಹಿತಿಯ ಗೌಪ್ಯತೆ ಮತ್ತು ವೈಯಕ್ತಿಕತೆಯನ್ನು ರಕ್ಷಿಸುತ್ತದೆ.

ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಮಾರ್ಗ ಬದಲಾಗಲು ಬಿಡಬೇಡಿ; ನಿಮ್ಮ DNS ಅನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ, ಜಾಗರೂಕರಾಗಿರಿ..

ಸಣ್ಣ ಸಂದೇಶ ಸ್ಫೋಟಗಳು (ಎಸ್.ಎಂ.ಎಸ್ ಬಾಂಬಿಂಗ್)

ಶೃತಿ, ಹರೆಯದ ಹರ್ಷಚಿತ್ರ ಯುವತಿಯಾಗಿದ್ದು, ಸ್ನೇಹಿತರಿಗೆ ಸಂದೇಶ ಕಳುಹಿಸಲು ಇಷ್ಟಪಡುತ್ತಾಳೆ.	ಅವಳ ಫೋನ್ ಸದಾ ಸೂಚನೆಗಳಿಂದ ಮರೆಯುತ್ತಿರುತ್ತದೆ	ಪಠ್ಯ ಸಂದೇಶಗಳ ಅವಳ ಫೋನ್‌ನಲ್ಲಿ ಸದಾ ಹರಿಯುತ್ತಿರುತ್ತದೆ.

ಪಠ್ಯ ಸಂದೇಶದಿಂದ ಅವಳ ಫೋನ್ ಮೆಮೋರಿ ತುಂಬಿ ತುಳುಕುತ್ತಿತ್ತು.	ಫೋನ್ ಸಂಖ್ಯೆ ಬ್ಲಾಕ್ ಮಾಡುವ ಬದಲು ಹಾಗೆಯೇ ಬಿಡಲಾಗಿತ್ತು	ಫಲಿತಾಂಶವಾಗಿ, ಶೃತಿ ಫೋನ್ ನಿಷ್ಕ್ರಿಯಗೊಂಡು, ಕರೆ & ಸಂದೇಶ ಪ್ರತಿಬಂದಿತಗೊಂಡಿತು

ಶೃತಿ ಹತಾಶೆಯಿಂದ ನರಳಾಡಿ, ಅವಳ ಈ ಅಗ್ನಿಪರೀಕ್ಷೆಗೆ ಕಾರಣ ಎನೆಂದು ಆಶ್ಚರ್ಯ ಪಡುತ್ತಾಳೆ.	ಅವಳು ಎಸ್ಎಂಎಸ್ ಬಾಂಬ್‌ಗೆ ಒಳಗಾಗಿದ್ದಳು, ಯಾರೋ ತನ್ನ ಮೇಲೆ ಒಂದು ಭಯಾನಕ ತಂತ್ರವನ್ನು ಹೂಡಿದ್ದರು.	ಇದಕ್ಕೆ ಕಾರಣ ತನ್ನ ಫೋನ್ ಸಂಖ್ಯೆಯನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಬಹಿರಂಗಪಡಿಸಿದ್ದು ಎಂದು ಶೃತಿಯನ್ನು ಎಚ್ಚರಿಸಿತು.

ಇದು ಕಿರುಕುಳದ ಒಂದು ರೂಪವಾಗಿದ್ದು, ದಾಳಿಕೋರರು ಬಲಿಪಶುವಿನ ಮೊಬೈಲ್ ಸಾಧನಕ್ಕೆ ಹೆಚ್ಚಿನ ಸಂಖ್ಯೆಯ ಅನಗತ್ಯ ಪಠ್ಯ ಸಂದೇಶಗನ್ನು ಕಳುಹಿಸುತ್ತಾರೆ, ಇದರಿಂದ ಸಾಮಾನ್ಯ ಸಂವಹನಕ್ಕೆ ಅಡ್ಡಿಯಾಗಿ ಮಾನಸಿಕ ತೊಂದರೆಯನ್ನು ಉಂಟುಮಾಡಬಹುದು. ಈ ದಾಳಿಯು ಬಲಿಪಶುವಿನ ಮನಸ್ಸಿನ ಶಾಂತಿಯನ್ನು ಅಡ್ಡಿಪಡಿಸುವ ಅಥವಾ ಅವರ ಫೋನ್ ಬಳಸುವ ಸಾಮರ್ಥ್ಯವನ್ನು ಹಾಳುಮಾಡುವ ಗುರಿಯನ್ನು ಹೊಂದಿದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಕಲಂ 66C: ಗುರುತಿನ ಕಳ್ಳತನ– ಈ ಕಲಂ ಗುರುತಿನ ಕಳ್ಳತನಕ್ಕೆ ಶಿಕ್ಷೆಯ ಕುರಿತದ್ದು, ಇದು ಇನ್ನೊಬ್ಬ ವ್ಯಕ್ತಿಯ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಹಿ, ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಯಾವುದೇ ಇತರ ವಿಶಿಷ್ಟ ಗುರುತಿನ ವೈಶಿಷ್ಟವನ್ನು ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಬಳಸುವುದನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ.

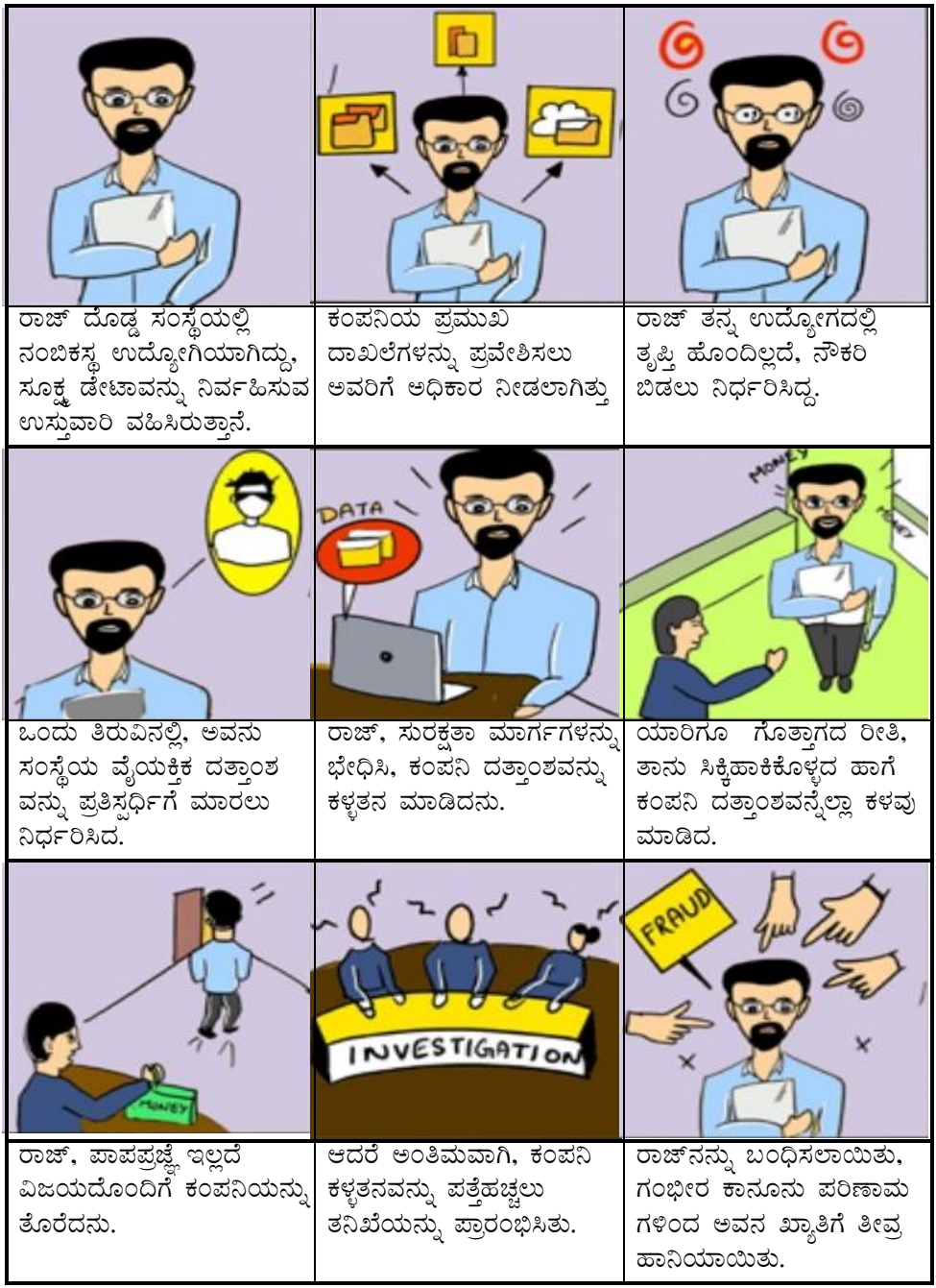
ಕಲಂ 66D: ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ – ಈ ವಿಭಾಗವು ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲವನ್ನು ಬಳಸಿಕೊಂಡು ವ್ಯಕ್ತಿಯಿಂದ ಮೋಸ ಮಾಡುವ ಕ್ರಿಯೆಯನ್ನು ತಿಳಿಸುತ್ತದೆ ಮತ್ತು ಅಂತಹ ಕ್ರಿಯೆಗಳಿಗೆ ದಂಡವನ್ನು ಸೂಚಿಸುತ್ತದೆ.

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್, ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್ ಇತ್ಯಾದಿಗಳ ಹಾನಿಗಾಗಿ ದಂಡ ಮತ್ತು ಪರಿಹಾರ– ಈ ಕಲಂ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲಗಳಿಗೆ ಹಾನಿ ಉಂಟುಮಾಡುವ ದಂಡದ ಬಗ್ಗೆ ವ್ಯವಹರಿಸುತ್ತದೆ.

ಕಲಂ 66: ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು; ಈ ಕಲಂ ಹ್ಯಾಕಿಂಗ್, ಅನಧಿಕೃತ ಪ್ರವೇಶ ಮತ್ತು ವೈರಸ್‌ಗಳ ಹರಿಬಿಡುವುದು ಸೇರಿದಂತೆ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ವಿವಿಧ ಅಪರಾಧಗಳನ್ನು ಒಳಗೊಂಡಿದೆ.

ಪಠ್ಯಗಳ ಸುರುಮಳೆಯಾಗಿದೆಯೇ, ಇದು ವಿನೋದವಲ್ಲ;
ನಿಮ್ಮ ಫೋನ್ ಅನ್ನು ರಕ್ಷಿಸಿ, SMS ಗನ್ ಅನ್ನು ನಿರ್ಬಂಧಿಸಿ.

ಒಳಗಿನವರ ಭೀತಿ (ಇನ್ಸೈಡರ್ ತ್ರೆಟ್)



ರಾಜ್ ದೊಡ್ಡ ಸಂಸ್ಥೆಯಲ್ಲಿ ನಂಬಿಕಸ್ಥ ಉದ್ಯೋಗಿಯಾಗಿದ್ದು, ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ನಿರ್ವಹಿಸುವ ಉಸ್ತುವಾರಿ ವಹಿಸಿರುತ್ತಾನೆ.	ಕಂಪನಿಯ ಪ್ರಮುಖ ದಾಖಲೆಗಳನ್ನು ಪ್ರವೇಶಿಸಲು ಅವರಿಗೆ ಅಧಿಕಾರ ನೀಡಲಾಗಿತ್ತು	ರಾಜ್ ತನ್ನ ಉದ್ಯೋಗದಲ್ಲಿ ತೃಪ್ತಿ ಹೊಂದಿಲ್ಲದೆ, ನೌಕರಿ ಬಿಡಲು ನಿರ್ಧರಿಸಿದ್ದ.
ಒಂದು ತಿರುವಿನಲ್ಲಿ, ಅವನು ಸಂಸ್ಥೆಯ ವೈಯಕ್ತಿಕ ದತ್ತಾಂಶ ವನ್ನು ಪ್ರತಿಸ್ಪರ್ಧಿಗೆ ಮಾರಲು ನಿರ್ಧರಿಸಿದ.	ರಾಜ್, ಸುರಕ್ಷತಾ ಮಾರ್ಗಗಳನ್ನು ಭೇಧಿಸಿ, ಕಂಪನಿ ದತ್ತಾಂಶವನ್ನು ಕಳ್ಳತನ ಮಾಡಿದನು.	ಯಾರಿಗೂ ಗೊತ್ತಾಗದ ರೀತಿ, ತಾನು ಸಿಕ್ಕಿಹಾಕಿಕೊಳ್ಳದ ಹಾಗೆ ಕಂಪನಿ ದತ್ತಾಂಶವನ್ನೆಲ್ಲಾ ಕಳವು ಮಾಡಿದ.
ರಾಜ್, ಪಾಪಪ್ರಜ್ಞೆ ಇಲ್ಲದೆ ವಿಜಯದೊಂದಿಗೆ ಕಂಪನಿಯನ್ನು ತೊರೆದನು.	ಆದರೆ ಅಂತಿಮವಾಗಿ, ಕಂಪನಿ ಕಳ್ಳತನವನ್ನು ಪತ್ತೆಹಚ್ಚಲು ತನಿಖೆಯನ್ನು ಪ್ರಾರಂಭಿಸಿತು.	ರಾಜ್‌ನನ್ನು ಬಂಧಿಸಲಾಯಿತು, ಗಂಭೀರ ಕಾನೂನು ಪರಿಣಾಮ ಗಳಿಂದ ಅವನ ಖ್ಯಾತಿಗೆ ತೀವ್ರ ಹಾನಿಯಾಯಿತು.

ಒಳಗಿನವರ ಭೀತಿ (ಇನ್ಸೈಡರ್ ತ್ರೆಟ್)

ಸಂಸ್ಥೆಯ ಗಣಕಯಂತ್ರಗಳು, ನೆಟ್‌ವರ್ಕ್‌ಗಳು ಅಥವಾ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಗೆ ಕಾನೂನುಬದ್ಧ ಪ್ರವೇಶವನ್ನು ಹೊಂದಿರುವ ಸಾಮಾನ್ಯ ವ್ಯಕ್ತಿಗಳು ಒಡ್ಡುವ ಭದ್ರತಾ ಅಪಾಯಗಳನ್ನು ಉಲ್ಲೇಖಿಸುತ್ತದೆ. ಡೇಟಾವನ್ನು ಕದಿಯಲು, ವಂಚನೆ ಮಾಡಲು ಅಥವಾ ಸಂಸ್ಥೆಯ ಭದ್ರತೆ ರಾಜಿ ಮಾಡಿಕೊಳ್ಳಲು ಉದ್ದೇಶಪೂರ್ವಕವಾಗಿ ಅಥವಾ ಅನುದ್ದೇಶಿತವಾಗಿ ತಮ್ಮ ಸವಲತ್ತುಗಳನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳುವ ಉದ್ಯೋಗಿಗಳಿಂದ, ಗುತ್ತಿಗೆದಾರರಿಂದ ಅಥವಾ ವ್ಯಾಪಾರ ಪಾಲುದಾರರಿಂದ ಈ ಬೆದರಿಕೆಗಳು ಉದ್ಭವಿಸಬಹುದು.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಕಲಂ 43A: ಡೇಟಾ ಉಲ್ಲಂಘನೆಗೆ ಪರಿಹಾರ

ಕಲಂ 66C: ಗುರುತಿನ ಕಳ್ಳತನ

ಕಲಂ 66D: ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

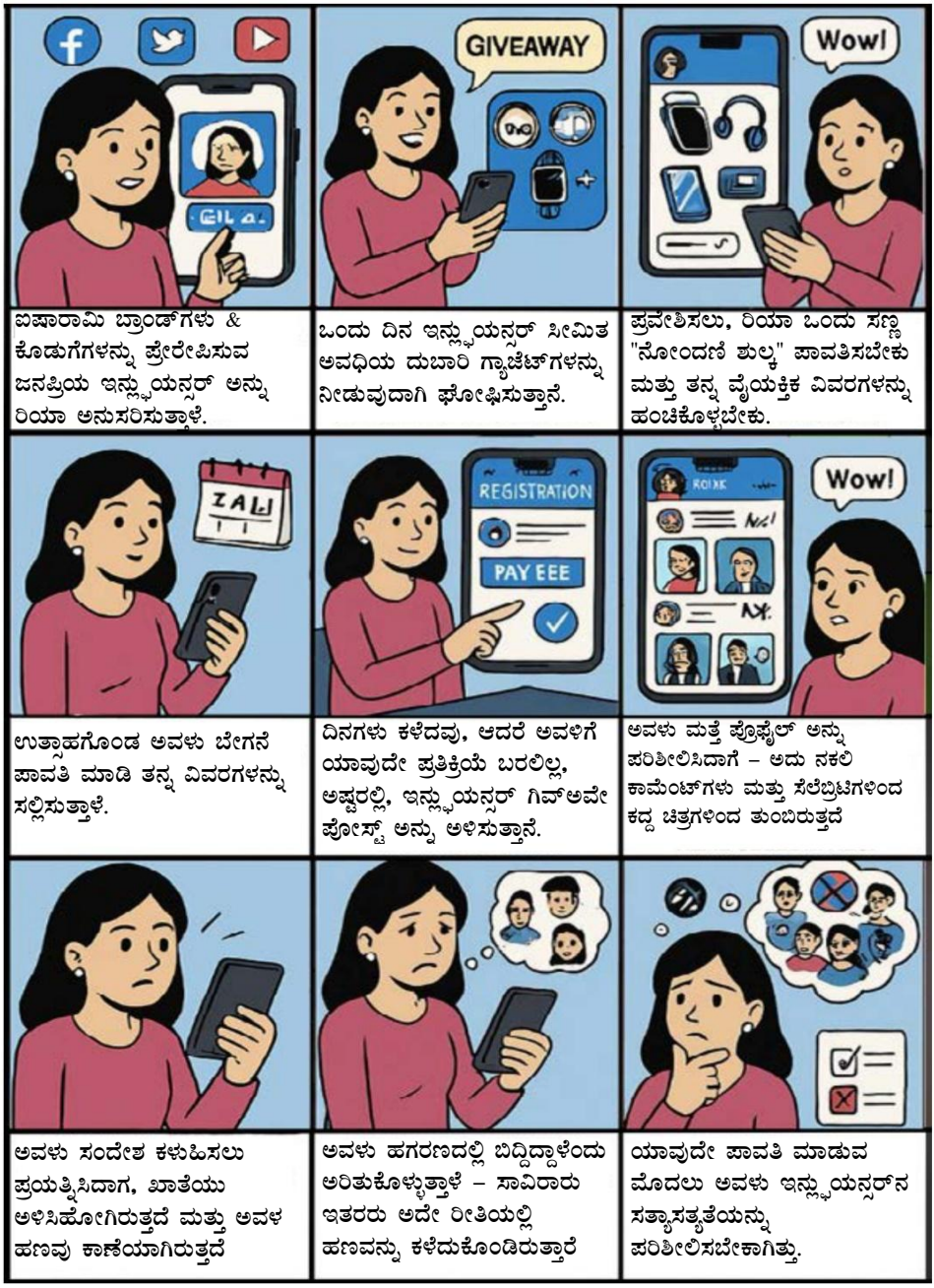
ಕಲಂ 72: ಗೌಪ್ಯತೆ ಮತ್ತು ವೈಯಕ್ತಿಕತೆಯ ಉಲ್ಲಂಘನೆ

ಕಲಂ 72A: ಕಾನೂನು ಉಲ್ಲಂಘನೆಯಲ್ಲಿ ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಪಡಿಸಲು ಶಿಕ್ಷೆ

ಕಲಂ 408 / **ಬಿಎನ್‌ಎಸ್ 316**: ಗುಮಾಸ್ತ ಅಥವಾ ಸೇವಕರಿಂದ ನಂಬಿಕೆ ಉಲ್ಲಂಘನೆ ಅಪರಾಧ

ಒಳಗೆ ವಾಸಿಸುವವರ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ;
ನಂಬಿ ಆದರೆ ಪರಿಶೀಲಿಸಿ, ಮತ್ತು ಸಂಭಾವ್ಯ ಹಾನಿ ಪ್ರಮಾಣ ತಗ್ಗುತ್ತದೆ.

ನಕಲಿ ಇನ್‌ಫ್ಲೂಯನ್ಸರ್ ಹಗರಣ



ಐಷಾರಾಮಿ ಬ್ರಾಂಡ್‌ಗಳು & ಕೊಡುಗೆಗಳನ್ನು ಪ್ರೇರೇಪಿಸುವ ಜನಪ್ರಿಯ ಇನ್ಫ್ಲೂಯನ್ಸರ್ ಅನ್ನು ರಿಯಾ ಅನುಸರಿಸುತ್ತಾಳೆ.

ಒಂದು ದಿನ ಇನ್ಫ್ಲೂಯನ್ಸರ್ ಸೀಮಿತ ಅವಧಿಯ ದುಬಾರಿ ಗ್ಯಾಜೆಟ್‌ಗಳನ್ನು ನೀಡುವುದಾಗಿ ಘೋಷಿಸುತ್ತಾನೆ.

ಪ್ರವೇಶಿಸಲು, ರಿಯಾ ಒಂದು ಸಣ್ಣ "ನೋಂದಣಿ ಶುಲ್ಕ" ಪಾವತಿಸಬೇಕು ಮತ್ತು ತನ್ನ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಕು.

ಉತ್ಸಾಹಗೊಂಡ ಅವಳು ಬೇಗನೆ ಪಾವತಿ ಮಾಡಿ ತನ್ನ ವಿವರಗಳನ್ನು ಸಲ್ಲಿಸುತ್ತಾಳೆ.

ದಿನಗಳು ಕಳೆದವು, ಆದರೆ ಅವಳಿಗೆ ಯಾವುದೇ ಪ್ರತಿಕ್ರಿಯೆ ಬರಲಿಲ್ಲ, ಅಷ್ಟರಲ್ಲಿ, ಇನ್ಫ್ಲೂಯನ್ಸರ್ ಗಿವ್‌ಅವೇ ಪೋಸ್ಟ್ ಅನ್ನು ಅಳಿಸುತ್ತಾನೆ.

ಅವಳು ಮತ್ತೆ ಪ್ರೊಫೈಲ್ ಅನ್ನು ಪರಿಶೀಲಿಸಿದಾಗ – ಅದು ನಕಲಿ ಕಾಮೆಂಟ್‌ಗಳು ಮತ್ತು ಸೆಲೆಬ್ರಿಟಿಗಳಿಂದ ಕದ್ದ ಚಿತ್ರಗಳಿಂದ ತುಂಬಿರುತ್ತದೆ

ಅವಳು ಸಂದೇಶ ಕಳುಹಿಸಲು ಪ್ರಯತ್ನಿಸಿದಾಗ, ಖಾತೆಯು ಅಳಿಸಿಹೋಗಿರುತ್ತದೆ ಮತ್ತು ಅವಳ ಹಣವು ಕಾಣೆಯಾಗಿರುತ್ತದೆ

ಅವಳು ಹಗರಣದಲ್ಲಿ ಬಿದ್ದಿದ್ದಾಳೆಂದು ಅರಿತುಕೊಳ್ಳುತ್ತಾಳೆ – ಸಾವಿರಾರು ಇತರರು ಅದೇ ರೀತಿಯಲ್ಲಿ ಹಣವನ್ನು ಕಳೆದುಕೊಂಡಿರುತ್ತಾರೆ

ಯಾವುದೇ ಪಾವತಿ ಮಾಡುವ ಮೊದಲು ಅವಳು ಇನ್ಫ್ಲೂಯನ್ಸರ್‌ನ ಸತ್ಯಾಸತ್ಯತೆಯನ್ನು ಪರಿಶೀಲಿಸಬೇಕಾಗಿತ್ತು.

ನಕಲಿ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಇನ್‌ಫ್ಲೂಯನ್ಸರ್ಸ್‌ಗಳು ತಮ್ಮ ಅನುಯಾಯಿಗಳನ್ನು ಉಡುಗೊರೆಗಳು ಮತ್ತು ಐಷಾರಾಮಿ ಬ್ರ್ಯಾಂಡ್ ಡೀಲ್‌ಗಳ ಮೂಲಕ ಆಕರ್ಷಿಸುತ್ತಾರೆ. ಬಲಿಪಶುಗಳು ನೋಂದಣಿ ಶುಲ್ಕವನ್ನು ಪಾವತಿಸುತ್ತಾರೆ ಆದರೆ ಎಂದಿಗೂ ಬಹುಮಾನಗಳನ್ನು ಪಡೆಯುವುದಿಲ್ಲ. ಇನ್‌ಫ್ಲೂಯನ್ಸರ್ಸ್‌ಗಳು ಹಣ ಸಂಗ್ರಹಿಸಿದ ನಂತರ ಕಣ್ಮರೆಯಾಗುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 66D: ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಮಾ.ತ.ಕಾ ಕಲಂ 79: ಕೆಲವು ಸಂದರ್ಭಗಳಲ್ಲಿ ಮಧ್ಯವರ್ತಿಗಳನ್ನು ಹೊಣೆಗಾರರನ್ನಾಗಿಸುವುದರಿಂದ ವಿನಾಯಿತಿ

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 419/ಬಿಎನ್‌ಎಸ್ 319(2) –ಮತ್ತೊಬ್ಬನಂತೆ ನಟಿಸಿ ವಂಚಿಸಿದ್ದಕ್ಕಾಗಿ ದಂಡನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318(4) – ಮೋಸ

ಐಪಿಸಿ ಕಲಂ 468/ಬಿಎನ್‌ಎಸ್ 336(3) – ವಂಚನೆಯ ಉದ್ದೇಶಕ್ಕಾಗಿ ಖೋಟಾ ಸೃಷ್ಟಿ

ಗ್ರಾಹಕ ರಕ್ಷಣಾ ಕಾಯ್ದೆ, 2019:

ಕಲಂ 2(47) – ದಾರಿ ತಪ್ಪಿಸುವ ಜಾಹೀರಾತುಗಳು

ಕಲಂ 21 – ಸುಳ್ಳು ಅನುಮೋದನೆಗಳಿಗೆ ದಂಡ

ನಕಲಿ ಖ್ಯಾತಿಯನ್ನು ಅನುಸರಿಸಿದರೆ ನಿಜವಾದ ವಂಚನೆಗೆ ಒಳಗಾಗಬಹುದು.

ಡಿಜಿಟಲ್ ಅರೆಸ್ಟ್

ಪ್ರಿಯಾಗೆ ಪೊಲೀಸ್ ಅಧಿಕಾರಿ ಎಂದು ಹೇಳಿಕೊಂಡು ವ್ಯಕ್ತಿಯಿಂದ ವಾಟ್ಸಾಪ್ ಕರೆ ಬರುತ್ತದೆ.
ಆಕೆಯ ಹೆಸರು ಆರ್ಥಿಕ ಅಪರಾಧಕ್ಕೆ ಸಂಬಂಧಿಸಿದೆ ಎಂದು ಅವನು ಹೇಳುತ್ತಾನೆ ಮತ್ತು ಬಂಧನದ ಬೆದರಿಕೆ ಹಾಕುತ್ತಾನೆ.
ಅವನು ಅಧಿಕೃತನಂತೆ ಕಾಣುತ್ತಾನೆ ಮತ್ತು ನಕಲಿ ಪ್ರಕರಣ ಐಡಿಯನ್ನು ಒದಗಿಸುತ್ತಾನೆ.
ಕಾನೂನು ತೊಂದರೆಯನ್ನು ತಪ್ಪಿಸಲು ಅವನು ತಕ್ಷಣ ದಂಡ ವಿಧಿಸಬೇಕೆಂದು ಒತ್ತಾಯಿಸುತ್ತಾನೆ.
BANK
TRANSFER
ಭಯಭೀತಳಾದ ಪ್ರಿಯಾ ಅವನ ಖಾತೆಗೆ ಹಣವನ್ನು ವರ್ಗಾಯಿಸುತ್ತಾಳೆ.
ಪ್ರಕರಣವನ್ನು "ಇತ್ಯರ್ಥಪಡಿಸಲು" ಅವನು ಇನ್ನೂ ಹೆಚ್ಚಿನ ಪಾವತಿಗಳನ್ನು ಕೇಳುತ್ತಾನೆ
ನಂತರ, ಅವಳು ಸ್ನೇಹಿತನೊಂದಿಗೆ ಚರ್ಚಿಸಿ ತಾನು ವಂಚನೆಗೆ ಒಳಗಾಗಿರುವ ಬಗ್ಗೆ ಅರಿತುಕೊಳ್ಳುತ್ತಾಳೆ
ಯಾವುದೇ ಭಾರತೀಯ ಕಾನೂನಿನಡಿಯಲ್ಲಿ ಡಿಜಿಟಲ್ ಬಂಧನಕ್ಕೆ ಯಾವುದೇ ಕಾನೂನು ಅವಕಾಶವಿಲ್ಲ
ಅವಳು ನಿಜವಾದ ಪೊಲೀಸರ ಸಹಾಯ ಪಡೆದುಕೊಳ್ಳಬಹುದಿತ್ತು ಮತ್ತು ಒತ್ತಡದಲ್ಲಿ ಎಂದಿಗೂ ಹಣವನ್ನು ಪಾವತಿಸಬಾರದು.

ಪೊಲೀಸ್ ಅಧಿಕಾರಿಯಂತೆ ನಟಿಸುವ ವಂಚಕನೊಬ್ಬ ನಕಲಿ ಕ್ರಿಮಿನಲ್ ಆರೋಪಗಳನ್ನು ಹೊರಿಸಿ ಬಲಿಪಶುಗಳಿಗೆ ಆನ್‌ಲೈನ್ ವಿಡಿಯೋ ಕರೆ ಮೂಲಕ ಬೆದರಿಕೆ ಹಾಕುತ್ತಾನೆ. ಪ್ರಕರಣವನ್ನು "ಇತ್ಯರ್ಥಗೊಳಿಸಲು" ಅವರು ತಕ್ಷಣ ಹಣ ಪಾವತಿಸಬೇಕೆಂದು ಒತ್ತಾಯಿಸುತ್ತಾರೆ. ಬಲಿಪಶುಗಳು ಭಯಭೀತರಾಗಿ ಹಣವನ್ನು ವರ್ಗಾಯಿಸುತ್ತಾರೆ, ಆದರೆ ಅಂತಹ ಯಾವುದೇ ಕಾನೂನು ನಿಬಂಧನೆ ಭಾರತದಲ್ಲಿ ಜಾರಿಯಲ್ಲಿರುವುದಿಲ್ಲ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 66C: ಗುರುತಿನ ಕಳ್ಳತನ

ಕಲಂ 66D: ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಭಾ.ದ.ಸಂ / ಭಾ.ನ್ಯಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 170/ಬಿಎನ್‌ಎಸ್ 204 – ಸಾರ್ವಜನಿಕ ಸೇವಕನಂತೆ ನಟಿಸುವುದು

ಐಪಿಸಿ ಕಲಂ 171/ಬಿಎನ್‌ಎಸ್ 205 – ಸಾರ್ವಜನಿಕ ಸೇವಕರು ಬಳಸುವ ಉಡುಪು ಧರಿಸುವುದು ಅಥವಾ ಅವರ ಟೋಕನ್ ಬಳಸುವುದು

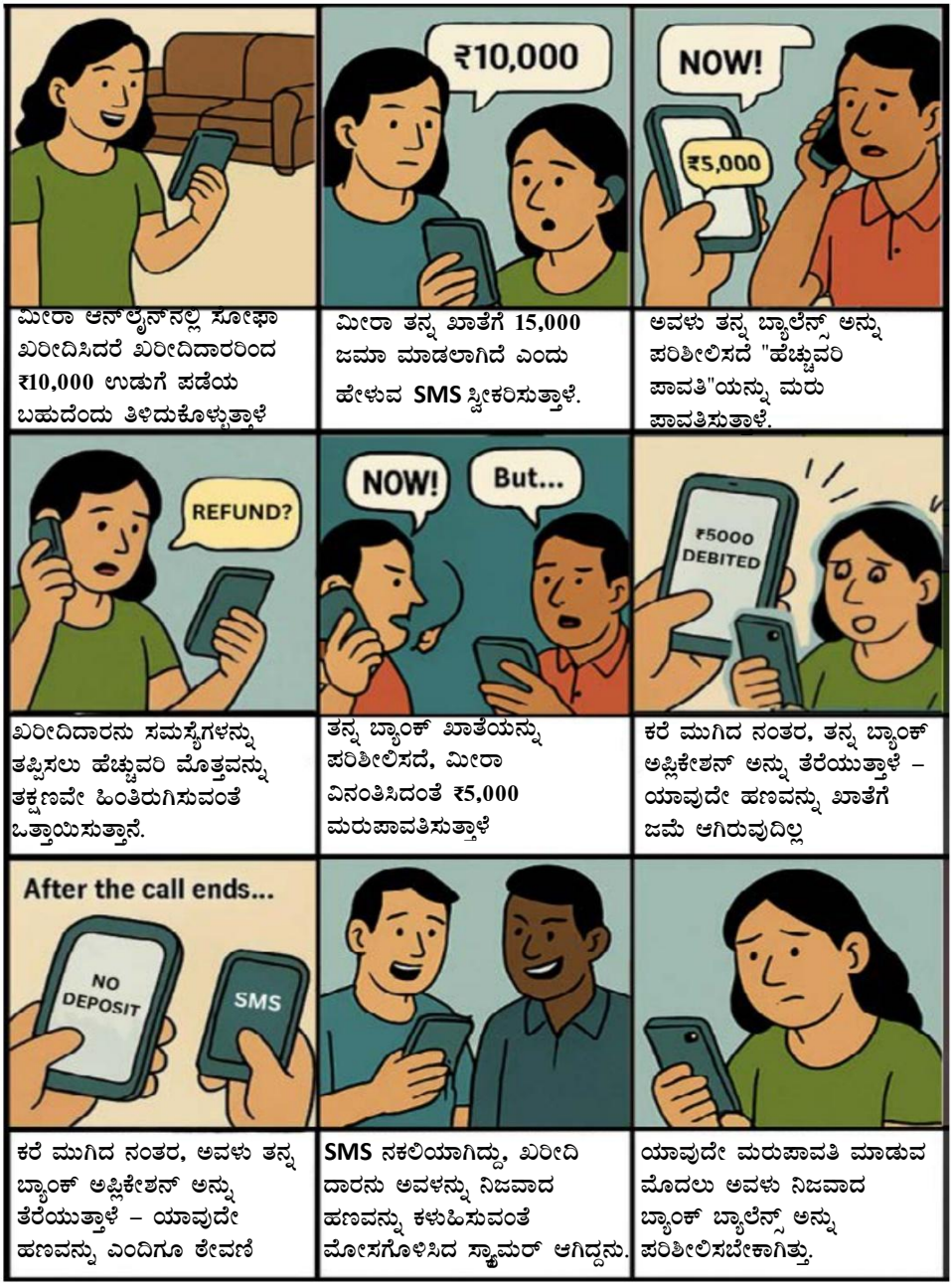
ಐಪಿಸಿ ಕಲಂ 383/ಬಿಎನ್‌ಎಸ್ 308 – ಸುಲಿಗೆ

ಐ.ಇ.ಎ 1872 / ಭಾ.ಸಾ.ಅ, 2023:

ಕಲಂ 65(ಬಿ) /ಭಾಸಾಅ 63 – ವಿದ್ಯುನ್ಮಾನ ದಾಖಲೆಗಳನ್ನು ಸಾಕ್ಷಿ ಯಾಗಿ ಸ್ವೀಕರಿಸುವ ಬಗ್ಗೆ

ನೀವು ಬಂಧನದಲ್ಲಿದ್ದೀರಿ ಎಂದು ವ್ಯಾಟ್ಸಾಪ್‌ನಲ್ಲಿ ಹೇಳಿದರೆ;
ವಕೀಲರ ಎಮೋಜಿಯೊಂದಿಗೆ ಪ್ರತ್ಯುತ್ತರಿಸಿ ಮತ್ತು ನಿರ್ಬಂಧಿಸಿ.

ಜಂಪ್ಡ್ ಡೆಪಾಸಿಟ್



ಮೀರಾ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸೋಫಾ ಖರೀದಿಸಿದರೆ ಖರೀದಿದಾರರಿಂದ ₹10,000 ಉಡುಗೆ ಪಡೆಯ ಬಹುದೆಂದು ತಿಳಿದುಕೊಳ್ಳುತ್ತಾಳೆ

ಮೀರಾ ತನ್ನ ಖಾತೆಗೆ 15,000 ಜಮಾ ಮಾಡಲಾಗಿದೆ ಎಂದು ಹೇಳುವ SMS ಸ್ವೀಕರಿಸುತ್ತಾಳೆ.

ಅವಳು ತನ್ನ ಬ್ಯಾಲೆನ್ಸ್ ಅನ್ನು ಪರಿಶೀಲಿಸದೆ "ಹೆಚ್ಚುವರಿ ಪಾವತಿ"ಯನ್ನು ಮರು ಪಾವತಿಸುತ್ತಾಳೆ.

ಖರೀದಿದಾರನು ಸಮಸ್ಯೆಗಳನ್ನು ತಪ್ಪಿಸಲು ಹೆಚ್ಚುವರಿ ಮೊತ್ತವನ್ನು ತಕ್ಷಣವೇ ಹಿಂತಿರುಗಿಸುವಂತೆ ಒತ್ತಾಯಿಸುತ್ತಾನೆ.

ತನ್ನ ಬ್ಯಾಂಕ್ ಖಾತೆಯನ್ನು ಪರಿಶೀಲಿಸದೆ, ಮೀರಾ ವಿನಂತಿಸಿದಂತೆ ₹5,000 ಮರುಪಾವತಿಸುತ್ತಾಳೆ

ಕರೆ ಮುಗಿದ ನಂತರ, ತನ್ನ ಬ್ಯಾಂಕ್ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ತೆರೆಯುತ್ತಾಳೆ – ಯಾವುದೇ ಹಣವನ್ನು ಖಾತೆಗೆ ಜಮೆ ಆಗಿರುವುದಿಲ್ಲ

ಕರೆ ಮುಗಿದ ನಂತರ, ಅವಳು ತನ್ನ ಬ್ಯಾಂಕ್ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ತೆರೆಯುತ್ತಾಳೆ – ಯಾವುದೇ ಹಣವನ್ನು ಎಂದಿಗೂ ಠೇವಣಿ

SMS ನಕಲಿಯಾಗಿದ್ದು, ಖರೀದಿ ದಾರನು ಅವಳನ್ನು ನಿಜವಾದ ಹಣವನ್ನು ಕಳುಹಿಸುವಂತೆ ಮೋಸಗೊಳಿಸಿದ ಸ್ಕ್ಯಾಮರ್ ಆಗಿದ್ದನು.

ಯಾವುದೇ ಮರುಪಾವತಿ ಮಾಡುವ ಮೊದಲು ಅವಳು ನಿಜವಾದ ಬ್ಯಾಂಕ್ ಬ್ಯಾಲೆನ್ಸ್ ಅನ್ನು ಪರಿಶೀಲಿಸಬೇಕಾಗಿತ್ತು.

ಒಬ್ಬ ಸ್ಕ್ಯಾಮರ್ ಮಾರಾಟಗಾರನಿಗೆ ಆಕಸ್ಮಿಕವಾಗಿ ಹೆಚ್ಚುವರಿ ಹಣವನ್ನು ಕಳುಹಿಸಿರುವುದಾಗಿ ಹೇಳಿಕೊಂಡು ಬ್ಯಾಂಕ್ ಅಧಿಸೂಚನೆಯನ್ನು ನಕಲಿ ಮಾಡಿ ಕಳುಹಿಸುತ್ತಾನೆ. ವಹಿವಾಟು ನಿಜವೆಂದು ನಂಬಿದ ಮಾರಾಟಗಾರನು ಹೆಚ್ಚುವರಿ ಮೊತ್ತವನ್ನು ಮರುಪಾವತಿಸುತ್ತಾನೆ. ನಂತರ, ತನಗೆ ಯಾವುದೇ ಠೇವಣಿ ಮಾಡಲಾಗಿಲ್ಲ ಎಂದು ಅವರು ಅರಿತುಕೊಳ್ಳುತ್ತಾನೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 66D: ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 406/ಬಿಎನ್‌ಎಸ್ 316(2) – ವಿಶ್ವಾಸ ಭಂಗದ ಅಪರಾಧಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 417/ಬಿಎನ್‌ಎಸ್ 318(2) – ವಂಚನೆ

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್‌ಎಸ್ 318(4) – ವಂಚನೆ ಮತ್ತು ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಆಸ್ತಿ ವಿತರಣೆಯನ್ನು ಪ್ರೇರೇಪಿಸುವುದು

ಗ್ರಾಹಕ ರಕ್ಷಣಾ ಕಾಯ್ದೆ, 2019:

ಕಲಂ 74 – ಅನ್ಯಾಯಯುತ ವ್ಯಾಪಾರ ಪದ್ಧತಿಗಳು

ಟ್ರ್ಯಾಕ್ ಮಾಡುವುದು ತುಂಬಾ ಚುರುಕಾಗಿದ್ದರೆ;
ಪಾವತಿ ಮಾಡುವುದು ತುಂಬಾ ಅಪಾಯಕಾರಿ.

ಕರೆ ವಿಲೀನ ಹಗರಣ

ಸ್ನೇಹಾಗೆ ತನ್ನ ಬ್ಯಾಂಕಿನ ವಂಚನೆ ವಿಭಾಗದವರೆಂದು ಹೇಳಿಕೊಳ್ಳುವ ವ್ಯಕ್ತಿಯೊಬ್ಬರು ಕರೆ ಮಾಡುತ್ತಾರೆ.
ಕರೆ ಮಾಡಿದವರು ತಮ್ಮ ಆಪ್ತರು ದಾಳಿಗೆ ಒಳಗಾಗಿದ್ದಾರೆಂದು ಹೇಳುತ್ತಾರೆ ಮತ್ತು ಕರೆಯಲ್ಲಿಯೇ ಇರುವಂತೆ ಕೇಳುತಾರೆ.
"ಬ್ಯಾಂಕಿನ ಪರಿಶೀಲನಾ ತಂಡ"ದಿಂದ ಎರಡನೇ ಕರೆಯನ್ನು ವಿಲೀನಗೊಳಿಸಲು ಅವನು ಅವಳಿಗೆ ಹೇಳುತಾನೆ
ಎರಡನೇ ಕರೆ ಮಾಡಿದವರು ಅನಧಿಕೃತ ವಹಿವಾಟು ಪ್ರಗತಿಯಲ್ಲಿದೆ ಎಂದು ಹೇಳುತ್ತಾರೆ.
OTP
SPM
796815
ಅದನ್ನು ನಿರ್ಬಂಧಿಸಲು ಅವನು ಒಟಿಪಿಯನ್ನು ವಿನಂತಿಸುತ್ತಾನೆ, ಅದು ಎಸ್‌ಎಂಎಸ್ ಬದಲಿಗೆ ಕರೆಯ ಮೂಲಕ ಕಳುಹಿಸಲ್ಪಡುತ್ತದೆ
ವಿಲೀನಗೊಂಡ ಕರೆಯ ಬಗ್ಗೆ ರಹಸ್ಯವಾಗಿ ಕೇಳುತ್ತಿರುವ ಸೈಬರ್ ಅಪರಾಧಿ ಒಟಿಪಿಯನ್ನು ಗಮನಿಸುತ್ತಾನೆ.
ಕ್ಷಣಗಳ ನಂತರ, ಸ್ನೇಹಾ ತನ್ನ ಖಾತೆಯಿಂದ ದೊಡ್ಡ ಮೊತ್ತದ ಹಿಂಪಡೆಯುವಿಕೆಯ ಬಗ್ಗೆ ಸಂದೇಶಗಳನ್ನು ಪಡೆಯುತ್ತಾಳೆ.
BANK
ಅವಳು ನಿಜವಾದ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸುತ್ತಾಳೆ, ಆದರೆ ಅವಳು ವಂಚನೆಗೊಳಗಾಗಿದ್ದಾಳೆಂದು ಅರಿವಾಗುತ್ತದೆ
!
ಅವಳು ಕರೆಯ ಸಂಪರ್ಕ ಕಡಿತಗೊಳಿಸಿ ನೇರವಾಗಿ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಬೇಕಾಗಿತ್ತು.

ಒಬ್ಬ ವಂಚಕ ಬ್ಯಾಂಕಿನ ಸಿಬ್ಬಂದಿಯಂತೆ ನಟಿಸಿ ಬಲಿಪಶುವಿಗೆ ಕರೆ ಮಾಡುತ್ತಾನೆ. ಅವರು ಬಲಿಪಶುವನ್ನು ಮತ್ತೊಂದು ಕರೆಯನ್ನು ವಿಲೀನಗೊಳಿಸಲು ಕೇಳುತ್ತಾರೆ, ಅಲ್ಲಿ ಸಹಚರನು OTP ಅನ್ನು ವಿನಂತಿಸುತ್ತಾನೆ. ಸ್ಕ್ಯಾಮರ್ ರಹಸ್ಯವಾಗಿ ಆಲಿಸುತ್ತಾನೆ, OTP ಅನ್ನು ಕದಿಯುತ್ತಾನೆ ಮತ್ತು ಬಲಿಪಶುವಿನ ಖಾತೆಯನ್ನು ಖಾಲಿ ಮಾಡುತ್ತಾನೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 66C: ಗುರುತಿನ ಕಳ್ಳತನ

ಕಲಂ 66D: ಗಣಕಯಂತ್ರ ಸಂಪನ್ಮೂಲ ಬಳಸಿ ವ್ಯಕ್ತಿತ್ವ ಮೋಸಗೊಳಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318(4) – ವಂಚನೆ ಮತ್ತು ಅಪ್ರಾಮಾಣಿಕವಾಗಿ ಆಸ್ತಿ ವಿತರಣೆಯನ್ನು ಪ್ರೇರೇಪಿಸುವುದು

ಐಪಿಸಿ ಕಲಂ 468/ಬಿಎನ್ಎಸ್ 336(3) – ವಂಚನೆಯ ಉದ್ದೇಶಕ್ಕಾಗಿ ಖೋಟಾ ಸೃಷ್ಟಿ

ಐಪಿಸಿ ಕಲಂ 511/ಬಿಎನ್ಎಸ್ 62– ಅಪರಾಧ ಎಸಗಲು ಯತ್ನಿಸಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಜೀವಾವಧಿ ಶಿಕ್ಷೆ ಅಥವಾ ಇತರೆ ಜೈಲು ಶಿಕ್ಷೆ

ಟೆಲಿಗ್ರಾಫ್ ಕಾಯ್ದೆ, 1885:

ಕಲಂ 25 – ಸಂದೇಶಗಳ ಅನಧೀಕೃತ ಪ್ರತಿಬಂಧ

ಮೂರನೆಯವನು ಮೋಸಗಾರನಾಗಿದ್ದಾಗ,
ಮೂವರು ಸೇರಿ ಸಂಸ್ಥೆಯಾಗುವುದಿಲ್ಲ.

www.cybersafegirl.com

ಮಾಲ್ವರ್ಟೈಸಿಂಗ್

ಕಾವ್ಯಾಗೆ ಒಂದು ಐಷಾರಾಮಿ ಬ್ರ್ಯಾಂಡ್‌ನ ಆನ್‌ಲೈನ್ ಜಾಹೀರಾತೊಂದು ಭಾರಿ ರಿಯಾಯಿತಿಯಲ್ಲಿ ಕಾಣುತ್ತಿದೆ

ಅವಳು ಆ ಜಾಹೀರಾತನ್ನು ಕ್ಲಿಕ್ ಮಾಡುತ್ತಾಳೆ, ಅದು ಅವಳನ್ನು ಒಂದು ಆಕರ್ಷಕ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಕರೆದೊಯ್ಯುತದೆ

"ವಿಶೇಷ ಕೊಡುಗೆ" ಗಾಗಿ ಅವಳ ವಿವರಗಳನ್ನು ನಮೂದಿಸಲು ಸೈಟ್ ಅವಳನ್ನು ಕೇಳುತ್ತದೆ.

ಅವಳು ತನ್ನ ಡೇಟಾವನ್ನು ನಮೂದಿಸಿದ ತಕ್ಷಣ, ಅವಳ ಫೋನ್ ನಿಧಾನಗೊಳ್ಳುತ್ತದೆ.

ಅಪರಿಚಿತ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಅವಳ ಮುಖಪುಟ ಪರದೆಯಲ್ಲಿ ಕಾಣಿಸಿಕೊಳ್ಳುತ್ತವೆ.

ಅವಳ ಬ್ಯಾಂಕ್ ಲಾಗಿನ್ ಮಾಡಲು ಪ್ರಯತ್ನಿಸಿದ ಬಗ್ಗೆ ಸಂದೇಶವನ್ನು ಕಳುಹಿಸುತ್ತದೆ.

ಅವಳು ಉಳಿಸಿದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಕದ್ದಿದ್ದಾರೆ ಎಂದು ಅವಳು ಅರಿತುಕೊಂಡಳು.

ಸೈಬರ್ ಭದ್ರತಾ ತಜ್ಞರು ಜಾಹೀರಾತಿನಲ್ಲಿ ಮಾಲ್‌ವೇರ್ ಇದೆ ಎಂದು ಹೇಳುತ್ತಾರೆ.

ಅವಳು ಅನುಮಾನಾಸ್ಪದ ಜಾಹೀರಾತುಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಬೇಕಾಗಿತ್ತು ಮತ್ತು ವೆಬ್‌ಸೈಟ್‌ನ

ರಿಯಾಯಿತಿಗಳು ಅಥವಾ ಉಚಿತ ಉತ್ಪನ್ನಗಳ ಆಸೆಯಿಂದ ಆನ್‌ಲೈನ್ ಜಾಹೀರಾತನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವುದರಿಂದ ಮಾಲ್‌ವೇರ್ ಇನ್ಸ್ಟಾಲ್ ಆಗುತ್ತದೆ. ದುರುದ್ದೇಶಪೂರಿತ ಜಾಹೀರಾತುಗಳು ಬಳಕೆದಾರರ ಲಾಗಿನ್ ವಿವರಗಳನ್ನು ಕದಿಯುವ ನಕಲಿ ಸೈಟ್‌ಗಳಿಗೆ ಮರುನಿರ್ದೇಶಿಸುತ್ತದೆ. ಬಲಿಪಶುಗಳು ಹಣವನ್ನು ಕಳೆದುಕೊಳ್ಳುತ್ತಾರೆ ಅಥವಾ ಅವರ ಡೇಟಾವನ್ನು ಅಪಾಯಕ್ಕೆ ಸಿಲುಕಿಸುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ

ಕಲಂ 66: ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲಗಳ ಹ್ಯಾಕಿಂಗ್ ಮತ್ತು ಮೋಸದ ಬಳಕೆ

ಕಲಂ 69(ಎ): ಹಾನಿಕಾರಕ ಅಂಶವನ್ನು ನಿರ್ಬಂಧಿಸುವುದು

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 425/ಬಿಎನ್‌ಎಸ್ 324 – ಕಿಡಿಗೇಡಿತನ

ಐಪಿಸಿ ಕಲಂ 426/ಬಿಎನ್‌ಎಸ್ 324(3) – ಕಿಡಿಗೇಡಿತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಗ್ರಾಹಕ ರಕ್ಷಣಾ ಕಾಯ್ದೆ, :

ಕಲಂ 89 – ಮೋಸಗೊಳಿಸುವ ಆನ್‌ಲೈನ್ ಜಾಹೀರಾತುಗಳಿಗೆ ದಂಡ

ಮಿಂಚಿನಂತಹ ಜಾಹೀರಾತುಗಳು, ದತ್ತಾಂಶವನ್ನು ಮಿಂಚಿನಂತೆ ಕದಿಯಬಹುದು !

ವಾಟರಿಂಗ್ ಹೋಲ್ ಆಕ್ರಮಣ

ನಿರ್ದಿಷ್ಟ ಗುಂಪು ಆಗಾಗ್ಗೆ ಭೇಟಿ ನೀಡುವ ವಿಶ್ವಾಸಾರ್ಹ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಹ್ಯಾಕರ್‌ಗಳು ಸೋಂಕು ತಗುಲಿಸುತ್ತಾರೆ. ಬಳಕೆದಾರರು ಸೈಟ್‌ಗೆ ಪ್ರವೇಶಿಸಿದಾಗ, ಅವರ ಸಾಧನಗಳು ಅಪಾಯಕ್ಕೆ ಸಿಲುಕುತ್ತವೆ. ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಬಲಿಪಶುವಿನ ಅರಿವಿಲ್ಲದೆ ರುಜುವಾತುಗಳನ್ನು ಕದಿಯುತ್ತಾರೆ ಅಥವಾ ಸ್ಪೈವೇರ್ ಅನ್ನು ಇನ್ಸ್ಟಾಲ್ ಮಾಡುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 43: ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಡೇಟಾ ಉಲ್ಲಂಘನೆ ಮತ್ತು ಇತರ ಕಂಪ್ಯೂಟರ್–ಸಂಬಂಧಿತ ಅಪರಾಧಗಳ ಕುರಿತು ವ್ಯವಹರಿಸುತ್ತದೆ

ಕಲಂ 66: ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲಗಳ ಹ್ಯಾಕಿಂಗ್ ಮತ್ತು ಮೋಸದ ಬಳಕೆ

ಕಲಂ 72ಎ– ಕಾನೂನುಬದ್ಧ ಒಪ್ಪಂದದ ಉಲ್ಲಂಘನೆಯಲ್ಲಿ ಮಾಹಿತಿಯ ಬಹಿರಂಗಪಡಿಸುವಿಕೆಗಾಗಿ ಶಿಕ್ಷೆ

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 426/ಬಿಎನ್‌ಎಸ್ 324(3) – ಕಿಡಿಗೇಡಿತನಕ್ಕಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 471/ಬಿಎನ್‌ಎಸ್ 340(2)– ನಕಲುರುಜು ದಾಖಲೆಯನ್ನು ನೈಜವೆಂದು ಉಪಯೋಗಿಸುವುದು

ಐಪಿಸಿ ಕಲಂ 120ಬಿ/ಬಿಎನ್‌ಎಸ್ 61(2)– ಅಪರಾಧದ ಸಂಚಿಗಾಗಿ ಶಿಕ್ಷೆ

ಸುರಕ್ಷಿತ ಎಂದು ತೋರುವ ಸೈಟ್‌ಗಳು ಸಹ ವಿಷದ ಗುಂಡಿಗಳಾಗಿರಬಹುದು; ಎಚ್ಚರಿಕೆಯಿಂದ ನಡೆದುಕೊಳ್ಳಿ.

ಎಲ್‌ಎಲ್‌ಎಂ ಜೈಲ್‌ಬ್ರೇಕ್

ರಿಯಾ ಎಐ ಚಾಟ್‌ಬಾಟ್‌ನೊಂದಿಗೆ ಪ್ರಯೋಗ ಮಾಡಿ "ಜೈಲ್‌ಬ್ರೇಕ್" ಪ್ರಾಂಪ್ಟ್‌ಗಳನ್ನು ಪ್ರಯತ್ನಿಸುತ್ತಾಳೆ

ಚಾಟ್‌ಬಾಟ್ ಅವಳಿಗೆ ರಹಸ್ಯ ಹ್ಯಾಕಿಂಗ್ ತಂತ್ರಗಳನ್ನು ನೀಡಲು ಪ್ರಾರಂಭಿಸುತ್ತದೆ.

ಅವಳು ಉತ್ಸುಕಳಾಗುತ್ತಾಳೆ ಮತ್ತು ಅದರ ಮಿತಿಗಳನ್ನು ಪರೀಕ್ಷಿಸುತ್ತಲೇ ಇರುತ್ತಾಳೆ.

ನಂತರ ಪ್ರಯತ್ನಿಸಲು ಅವಳು ಸೂಚನೆಗಳನ್ನು ನಕಲಿಸುತ್ತಾಳ

ದಿನಗಳ ನಂತರ, ಅವಳು ಅಧಿಕಾರಿಗಳಿಂದ ಎಚ್ಚರಿಕೆಯನ್ನು ಪಡೆಯುತ್ತಾಳೆ.

ಎಐ ಕಂಪನಿಯು ಅವಳ ಖಾತೆಯನ್ನು ದುರುಪಯೋಗಕ್ಕಾಗಿ ಫ್ಲಾಗ್ ಮಾಡಿತ್ತು

ತನ್ನ ಕ್ರಿಯೆಗಳನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಲಾಗುತ್ತಿದೆ ಎಂದು ಅವಳು ಅರಿತುಕೊಂಡಳು.

ಅವಳು ತಿಳಿಯದೆಯೇ ಸೈಬರ್ ಅಪರಾಧ ತನಿಖೆಯ ಭಾಗವಾದಳು.

ಅವಳು ಎಐ ಯ ನೈತಿಕ ಮಿತಿಗಳನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳಬೇಕಾಗಿತ್ತು ಮತ್ತು ದುರುಪಯೋಗವನ್ನು ತಪ್ಪಿಸಬೇಕಾಗಿತ್ತು.

ಸುರಕ್ಷತಾ ನಿಯಮಗಳನ್ನು ತಪ್ಪಿಸಲು ಬಳಕೆದಾರರು AI ಚಾಟ್‌ಬಾಟ್ ಅನ್ನು ಕುಶಲತೆಯಿಂದ ನಿರ್ವಹಿಸುತ್ತಾರೆ. AI ಹ್ಯಾಕಿಂಗ್ ತಂತ್ರಗಳಂತಹ ನಿರ್ಬಂಧಿತ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುತ್ತದೆ. ಅಧಿಕಾರಿಗಳು ಇಂತಹ ತಪ್ಪನ್ನು ಪತ್ತೆಹಚ್ಚುತ್ತಾರೆ ಮತ್ತು ಬಳಕೆದಾರರು ತಿಳಿಯದೆಯೇ ಸೈಬರ್ ಅಪರಾಧ ತನಿಖೆಯ ಭಾಗವಾಗುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 66: ಕಂಪ್ಯೂಟರ್ ಸಂಪನ್ಮೂಲಗಳ ಹ್ಯಾಕಿಂಗ್ ಮತ್ತು ಮೋಸದ ಬಳಕೆ

ಮಾ.ತ.ಕಾಯ್ದೆ ಕಲಂ 67 ಬಿ–ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಬಳಸಿರುವ ಅಶ್ಲೀಲ ಕ್ರಿಯೆ ಇತ್ಯಾದಿಯ ಹರಡುವಿಕೆ, ಪ್ರಸರಣ ಮಾಡಿದ್ದಕ್ಕಾಗಿ ಶಿಕ್ಷೆ ಮತ್ತು ಪೋಕ್ಸೋ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾ ಕಲಂ 69– ಗಣಕಯಂತ್ರದ ಯಾವುದೇ ಸಂಪನ್ಮೂಲದ ಮೂಲಕ ಯಾವುದೇ ಮಾಹಿತಿಯನ್ನು ಪ್ರತಿಬಂಧಿಸುವುದಕ್ಕಾಗಿ ಅಥವಾ ಮೇಲ್ವಿಚಾರಣೆಗಾಗಿ ಅಥವಾ ಅಸಂಕೇತಿಕರಣಕ್ಕಾಗಿ ನಿರ್ದೇಶನಗಳನ್ನು ಹೊರಡಿಸುವ ಅಧಿಕಾರ

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 505/ಬಿಎನ್‌ಎಸ್ 353 – ಸಾರ್ವಜನಿಕರಿಗೆ ತೊಂದರೆಯುಂಟುಮಾಡುವ ಹೇಳಿಕೆಗಳು

ಐಪಿಸಿ ಕಲಂ 120ಬಿ/ಬಿಎನ್‌ಎಸ್ 61(2)– ಅಪರಾಧದ ಸಂಚಿಗಾಗಿ ಶಿಕ್ಷೆ

ಕೃತಿಸ್ವಾಮ್ಯ ಕಾಯ್ದೆ, 1957 :

ಕಲಂ 51 – AI–ರಚಿತ ವಿಷಯದ ಮೂಲಕ ಹಕ್ಕುಸ್ವಾಮ್ಯದ ಉಲ್ಲಂಘನೆ

ಬಾಟ್‌ಗೆ ಕೆಟ್ಟದ್ದನ್ನು ಕಲಿಸಬೇಡಿ;
ಅದು ಹ್ಯಾಕಿಂಗ್‌ನಲ್ಲಿ ಹಾನರ್ಸ್ ಪದವಿ ಪಡೆಯಬಹುದು !

ಸುಳ್ಳು ಸುದ್ದಿ

ಅದಿತಿ ಒಂದು ಆಘಾತಕಾರಿ ಸುದ್ದಿಯನ್ನು ನೋಡುತ್ತಾಳೆ: "ಧಾರ್ಮಿಕ ತಾಣದ ಮೇಲೆ ದಾಳಿ ™

ಈ ಸಂದೇಶವು ತನ್ನ ನಗರದಲ್ಲಿ ನಡೆದ ಹಿಂಸಾತ್ಮಕ ಘಟನೆಯನ್ನು ಹೇಳುತ್ತದೆ, ಗಾಯಗೊಂಡ ಜನರನ್ನು ತೋರಿಸುತ್ತದೆ.

ಕೋಪಗೊಂಡ ಮತ್ತು ಗಾಬರಿಗೊಂಡ ಅವಳು ಅದನ್ನು ತನ್ನ ಕುಟುಂಬ ಮತ್ತು ಸ್ನೇಹಿತರಿಗೆ ತ್ವರಿತವಾಗಿ ಫಾರ್ವರ್ಡ್

ನಿಮಿಷಗಳಲ್ಲಿ, ಸಂದೇಶವು ಬಹು ವಾಟ್ಸಾಪ್ ಗುಂಪುಗಳಲ್ಲಿ ಹರಡುತ್ತದೆ.

ಜನರು ಆಕ್ರೋಶದಿಂದ ಪ್ರತಿಕ್ರಿಯಿಸುತ್ತಾರೆ – ಕೆಲವರು ಪ್ರತಿಭಟನೆಗಳು ಮತ್ತು ಪ್ರತೀಕಾರವನ್ನು ಸಹ

ಸ್ಥಳೀಯ ಸುದ್ದಿ ವಾಹಿನಿಗಳು ಪ್ರದೇಶದಲ್ಲಿ ಉದ್ವಿಗ್ನತೆಯನ್ನು ವರದಿ ಮಾಡಲು ಪ್ರಾರಂಭಿಸುತ್ತವೆ.

ಈ ಘಟನೆ ಎಂದಿಗೂ ಸಂಭವಿಸಿಲ್ಲ ಎಂದು ಪೊಲೀಸರು ಖಚಿತಪಡಿಸುತ್ತಾರೆ; ಚಿತ್ರಗಳು ಹಳೆಯವು ಮತ್ತು ಬೇರೆ ದೇಶದಿಂದ

ತನ್ನ ತಪ್ಪನ್ನು ಅರಿತುಕೊಂಡ ಅದಿತಿ ವಿಷಾದದಿಂದ ತುಂಬಿದ್ದಾಳೆ – ಅವಳು ನಕಲಿ ಸುದ್ದಿಗಳನ್ನು ಹರಡಲು ಸಹಾಯ ಮಾಡಿದಳು.

ಅವಳು ಅದನ್ನು ಫಾರ್ವರ್ಡ್ ಮಾಡುವ ಮೊದಲು ಅಧಿಕೃತ ಮೂಲಗಳಿಂದ ಸುದ್ದಿಯನ್ನು ಪರಿಶೀಲಿಸಬೇಕಾಗಿತ್ತು.

ಹಿಂಸಾತ್ಮಕ ಘಟನೆಯ ಕುರಿತಾದ ಕೋಮು ವದಂತಿಯು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ವೇಗವಾಗಿ ಹರಡುತ್ತದೆ. ಜನರು ಭಾವನಾತ್ಮಕವಾಗಿ ಪ್ರತಿಕ್ರಿಯಿಸುತ್ತಾರೆ ಮತ್ತು ಸುಳ್ಳು ಮಾಹಿತಿಯನ್ನು ರವಾನಿಸುತ್ತಾರೆ. ಅಧಿಕಾರಿಗಳು ಸುದ್ದಿ ನಕಲಿ ಎಂದು ದೃಢಪಡಿಸುವ ಮೊದಲೇ ಅವ್ಯವಸ್ಥೆ ಉಂಟಾಗುತ್ತದೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 69(ಎ): ಸಾರ್ವಜನಿಕ ಹಿತಾಸಕ್ತಿಗಾಗಿ ಮಾಹಿತಿಗಳ ನಿರ್ಬಂಧ

ಕಲಂ 66(ಎಫ್)– ಸೈಬರ್ ಭಯೋತ್ಪಾದನೆ

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 153(ಎ)/ಬಿಎನ್‌ಎಸ್ 196 – ಗುಂಪುಗಳ ನಡುವೆ ದ್ವೇಷವನ್ನು ಉತ್ತೇಜಿಸುವುದು

ಐಪಿಸಿ ಕಲಂ 505/ಬಿಎನ್‌ಎಸ್ 353 – ಸಾರ್ವಜನಿಕ ದೃಷ್ಟ್ಯತ್ಯಕ್ಕೆ ಕಾರಣವಾಗುವ ಹೇಳಿಕೆಗಳು

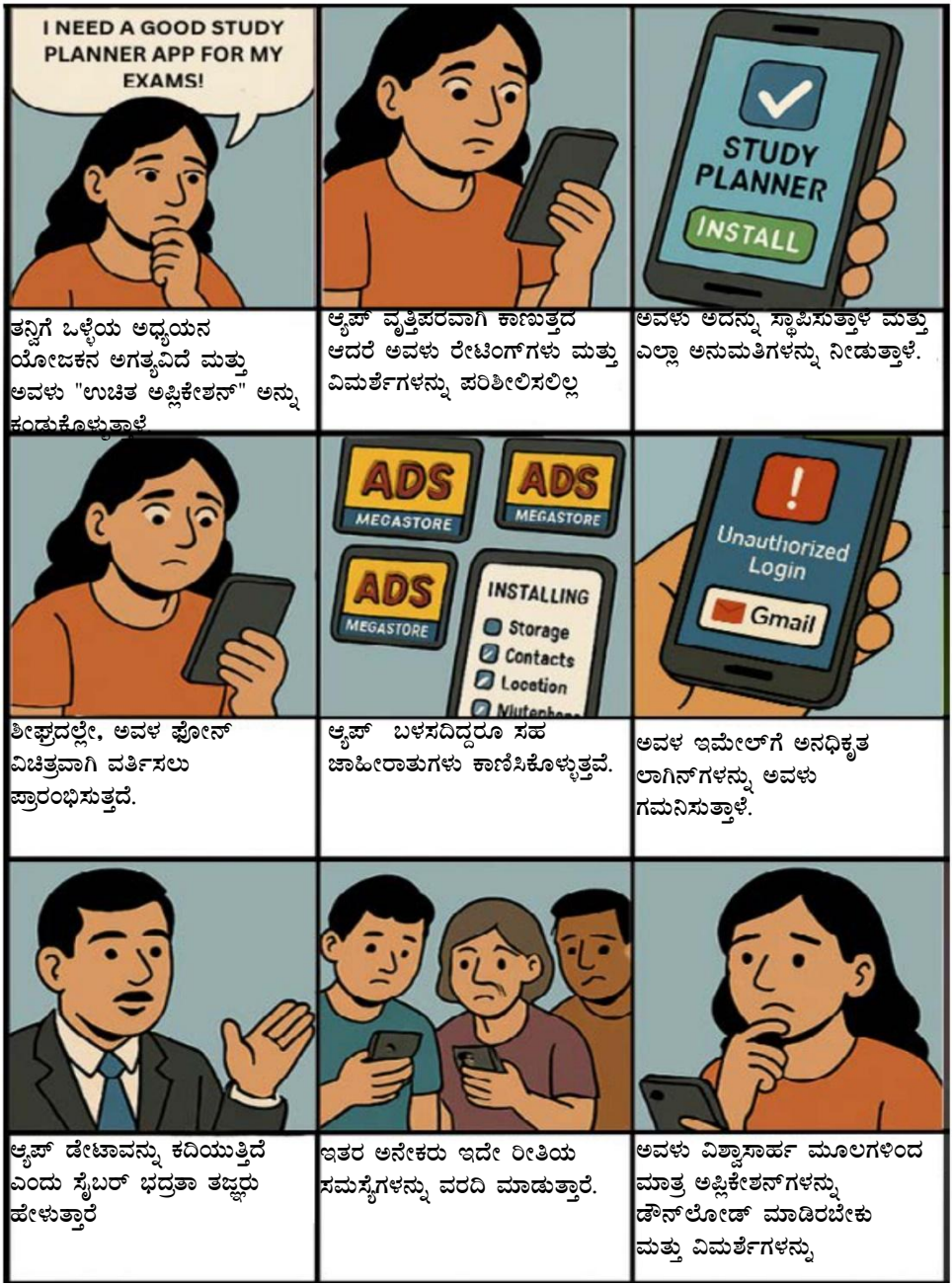
ಐಪಿಸಿ ಕಲಂ 124(ಎ) – ದೇಶದ್ರೋಹ ಅನ್ವಯಿಸಿದರೆ (ಈ ಕಲಂ ಅನ್ನು ಬಿಎನ್‌ಎಸ್–2023 ರಲ್ಲಿ ಅಳಿಸಲಾಗಿದೆ)

ಪ್ರೆಸ್ ಕೌನ್ಸಿಲ್ ಕಾಯ್ದೆ, 1978 :

ಕಲಂ 14 – ನಕಲಿ ಸುದ್ದಿಗಳನ್ನು ಪರಿಹರಿಸಲು ಪ್ರೆಸ್ ಕೌನ್ಸಿಲ್‌ನ ಅಧಿಕಾರಗಳು

ಫಾರ್ವರ್ಡ್ ಮಾಡಲಾದ ಪ್ರತಿಯೊಂದು ಸಂದೇಶವೂ ಸುವಾರ್ತೆಯಾಗಿರುವುದಿಲ್ಲ
- ಕೆಲವೊಮ್ಮೆ ಅದು ಗಾಸಿಪ್ ಆಗಿರುತ್ತದೆ !

ನಕಲಿ ಉತ್ಪಾದಕಾ ಆ್ಯಪ್ಸ್



ತನ್ನಿಗೆ ಒಳ್ಳೆಯ ಅಧ್ಯಯನ ಯೋಜಕನ ಅಗತ್ಯವಿದೆ ಮತ್ತು ಅವಳು "ಉಚಿತ ಅಪ್ಲಿಕೇಶನ್" ಅನ್ನು ಕಂಡುಕೊಳ್ಳುತ್ತಾಳೆ.

ಆ್ಯಪ್ ವೃತ್ತಿಪರವಾಗಿ ಕಾಣುತ್ತದೆ ಆದರೆ ಅವಳು ರೇಟಿಂಗ್‌ಗಳು ಮತ್ತು ವಿಮರ್ಶೆಗಳನ್ನು ಪರಿಶೀಲಿಸಲಿಲ್ಲ

ಅವಳು ಅದನ್ನು ಸ್ಥಾಪಿಸುತ್ತಾಳೆ ಮತ್ತು ಎಲ್ಲಾ ಅನುಮತಿಗಳನ್ನು ನೀಡುತ್ತಾಳೆ.

ಶೀಘ್ರದಲ್ಲೇ, ಅವಳ ಫೋನ್ ವಿಚಿತ್ರವಾಗಿ ವರ್ತಿಸಲು ಪ್ರಾರಂಭಿಸುತ್ತದೆ.

ಆ್ಯಪ್ ಬಳಸದಿದ್ದರೂ ಸಹ ಜಾಹೀರಾತುಗಳು ಕಾಣಿಸಿಕೊಳ್ಳುತ್ತವೆ.

ಅವಳ ಇಮೇಲ್‌ಗೆ ಅನಧಿಕೃತ ಲಾಗಿನ್‌ಗಳನ್ನು ಅವಳು ಗಮನಿಸುತ್ತಾಳೆ.

ಆ್ಯಪ್ ಡೇಟಾವನ್ನು ಕದಿಯುತ್ತಿದೆ ಎಂದು ಸೈಬರ್ ಭದ್ರತಾ ತಜ್ಞರು ಹೇಳುತ್ತಾರೆ

ಇತರ ಅನೇಕರು ಇದೇ ರೀತಿಯ ಸಮಸ್ಯೆಗಳನ್ನು ವರದಿ ಮಾಡುತ್ತಾರೆ.

ಅವಳು ವಿಶ್ವಾಸಾರ್ಹ ಮೂಲಗಳಿಂದ ಮಾತ್ರ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿರಬೇಕು ಮತ್ತು ವಿಮರ್ಶೆಗಳನ್ನು

ಗಮನ ಅಥವಾ ಸಮಯ ನಿರ್ವಹಣೆಯನ್ನು ಸುಧಾರಿಸುವುದಾಗಿ ಹೇಳಿಕೊಳ್ಳುವ ಆಪ್‌ಗಳು ಬಳಕೆದಾರರ ಡೇಟಾವನ್ನು ರಹಸ್ಯವಾಗಿ ಸಂಗ್ರಹಿಸುತ್ತದೆ. ಒಮ್ಮೆ ಇನ್ಸ್ಟಾಲ್ ಆದ ನಂತರ, ಅದು ಅತಿಯಾದ ಅನುಮತಿಗಳನ್ನು ಕೇಳುತ್ತದೆ ಮತ್ತು ಕರೆಗಳು ಮತ್ತು ಸಂದೇಶಗಳ ಮೇಲೆ ಕಣ್ಣಿಡಲು ಪ್ರಾರಂಭಿಸುತ್ತದೆ. ಬಲಿಪಶುಗಳು ಗೌಪ್ಯತೆ ಮತ್ತು ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕಳೆದುಕೊಳ್ಳುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 43 – ಅನಧೀಕೃತ ದತ್ತಾಂಶ ಸಂಗ್ರಹಣೆ ಮತ್ತು ದುರುಪಯೋಗ

ಕಲಂ 66 – ಕಂಪ್ಯೂಟರ್ ಸಂಬಂಧಿತ ಅಪರಾಧಗಳು

ಕಲಂ 72 – ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆ

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 420/ಬಿಎನ್ಎಸ್ 318(4) – ವಂಚನೆ

ಐಪಿಸಿ ಕಲಂ 468/ಬಿಎನ್ಎಸ್ 336(3) – ವಂಚನೆಗಾಗಿ ನಕಲಿಸೃಷ್ಟಿ

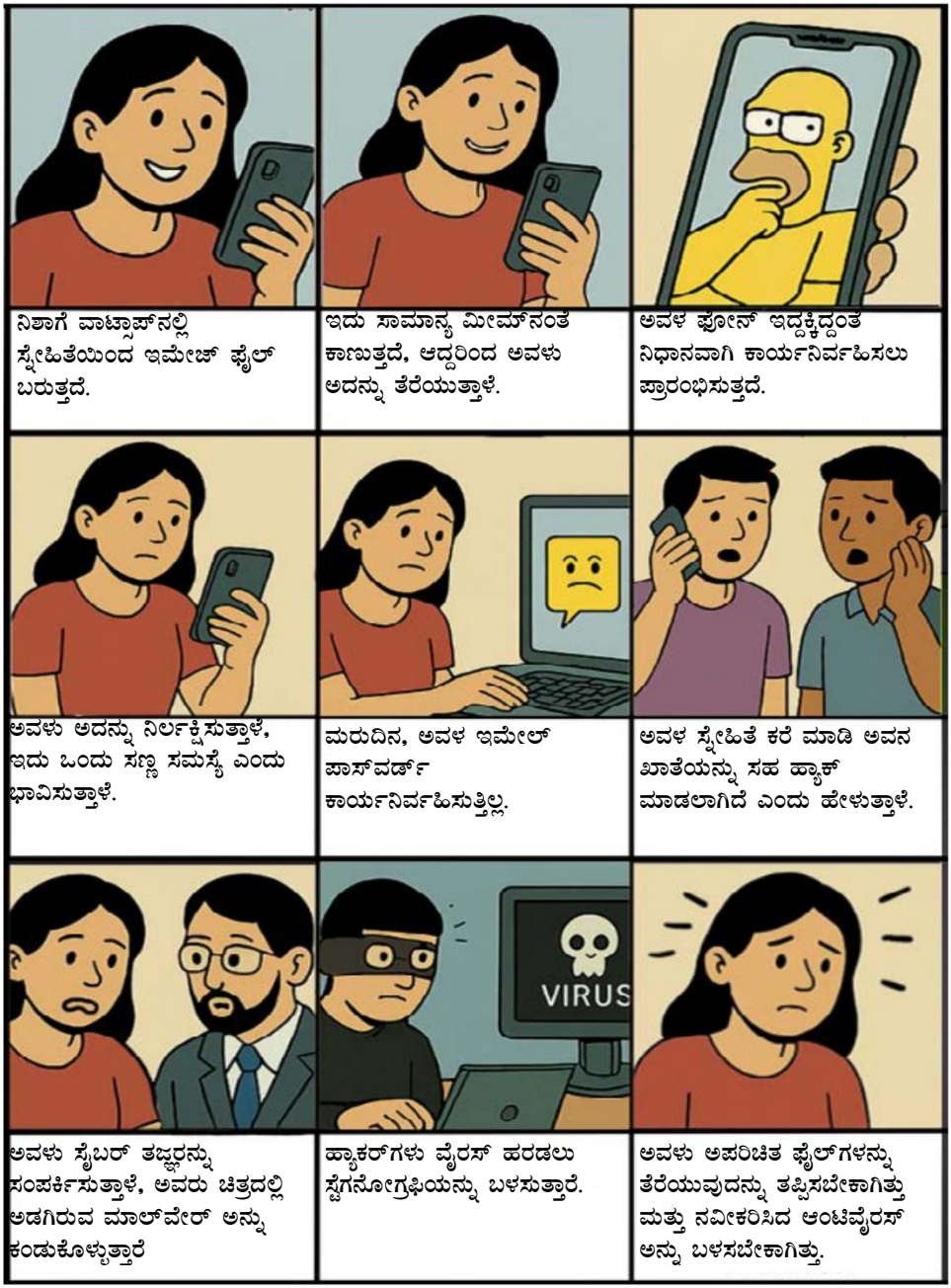
ಐಪಿಸಿ ಕಲಂ 120(ಬಿ)/ಬಿಎನ್ಎಸ್ 61(2) – ಅಪರಾಧದ ಸಂಚಿಗಾಗಿ ಶಿಕ್ಷೆ

ಗ್ರಾಹಕ ರಕ್ಷಣಾ ಕಾಯ್ದೆ, 2019:

ಕಲಂ 10 – ದೋಷಯುಕ್ತ ಡಿಜಿಟಲ್ ಸೇವೆಗಳಿಗೆ ಉತ್ಪನ್ನದ ಹೊಣೆಗಾರಿಕೆ

ಆಪ್‌ಗಳು ಹೆಚ್ಚು ಭರವಸೆ ನೀಡಿದರೆ,
ಇದು ಬಹುಶಃ ನಿಮ್ಮ ಸಮಯಕ್ಕಿಂತ ಹೆಚ್ಚಿನದ್ದು ಏನೋ ತೆಗೆದುಕೊಳ್ಳುತ್ತಿದೆ!.

ಸ್ಟೆಗ್ನಾಗ್ರಫಿ


ನಿಶಾಗೆ ವಾಟ್ಸಾಪ್‌ನಲ್ಲಿ ಸ್ನೇಹಿತೆಯಿಂದ ಇಮೇಜ್ ಫೈಲ್ ಬರುತ್ತದೆ.
ಇದು ಸಾಮಾನ್ಯ ಮೀಮ್‌ನಂತೆ ಕಾಣುತ್ತದೆ, ಆದ್ದರಿಂದ ಅವಳು ಅದನ್ನು ತೆರೆಯುತ್ತಾಳೆ.
ಅವಳ ಫೋನ್ ಇದ್ದಕ್ಕಿದ್ದಂತೆ ನಿಧಾನವಾಗಿ ಕಾರ್ಯನಿರ್ವಹಿಸಲು ಪ್ರಾರಂಭಿಸುತ್ತದೆ.
ಅವಳು ಅದನ್ನು ನಿರ್ಲಕ್ಷಿಸುತ್ತಾಳೆ, ಇದು ಒಂದು ಸಣ್ಣ ಸಮಸ್ಯೆ ಎಂದು ಭಾವಿಸುತ್ತಾಳೆ.
ಮರುದಿನ, ಅವಳ ಇಮೇಲ್ ಪಾಸ್‌ವರ್ಡ್ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತಿಲ್ಲ.
ಅವಳ ಸ್ನೇಹಿತೆ ಕರೆ ಮಾಡಿ ಅವನ ಖಾತೆಯನ್ನು ಸಹ ಹ್ಯಾಕ್ ಮಾಡಲಾಗಿದೆ ಎಂದು ಹೇಳುತ್ತಾಳೆ.
ಅವಳು ಸೈಬರ್ ತಜ್ಞರನ್ನು ಸಂಪರ್ಕಿಸುತ್ತಾಳೆ, ಅವರು ಚಿತ್ರದಲ್ಲಿ ಅಡಗಿರುವ ಮಾಲ್‌ವೇರ್ ಅನ್ನು ಕಂಡುಕೊಳ್ಳುತ್ತಾರೆ
VIRUS
ಹ್ಯಾಕರ್‌ಗಳು ವೈರಸ್ ಹರಡಲು ಸ್ಟೆಗನೋಗ್ರಫಿಯನ್ನು ಬಳಸುತ್ತಾರೆ.
ಅವಳು ಅಪರಿಚಿತ ಫೈಲ್‌ಗಳನ್ನು ತೆರೆಯುವುದನ್ನು ತಪ್ಪಿಸಬೇಕಾಗಿತ್ತು ಮತ್ತು ನವೀಕರಿಸಿದ ಆಂಟಿವೈರಸ್ ಅನ್ನು ಬಳಸಬೇಕಾಗಿತ್ತು.

ನಿರುಪದ್ರವಿ ಎಂದು ತೋರುವ ಇಮೇಜ್ ಫೈಲ್ ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್ ಅನ್ನು ಮರೆಮಾಡಿಕೊಂಡಿರುತ್ತದೆ. ಡೌನ್‌ಲೋಡ್ ಮಾಡಿದಾಗ ಅಥವಾ ತೆರೆದಾಗ, ಮಾಲ್‌ವೇರ್ ಸ್ಮಾರ್ಟ್‌ಫೋನ್‌ನಲ್ಲಿ ಇನ್ಸ್ಟಾಲ್ ಆಗುತ್ತದೆ. ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಸ್ಪೈವೇರ್ ಅನ್ನು ಹರಡಲು ಮತ್ತು ಮಾಹಿತಿಯನ್ನು ಕದಿಯಲು ಈ ತಂತ್ರವನ್ನು ಬಳಸುತ್ತಾರೆ.

ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು

ಮಾ.ತ.ಕಾಯ್ದೆ, 2000:

ಕಲಂ 66(ಎಫ್) – ಉಗ್ರಗಾಮಿ ಉದ್ದೇಶಗಳಿಗಾಗಿ ಬಳಸಿದರೆ, ಸೈಬರ್ ಭಯೋತ್ಪಾದನೆ

ಕಲಂ 69 – ಡೀಕ್ರಿಪ್ಟ್ ಮತ್ತು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುವ ಸರ್ಕಾರದ ಅಧಿಕಾರ

ಕಲಂ 72 – ಗೌಪ್ಯತೆಯ ಉಲ್ಲಂಘನೆ

ಭಾ.ದ.ಸಂ / ಭಾ.ನಾ.ಸಂ:

ಐಪಿಸಿ ಕಲಂ 201/ಬಿಎನ್‌ಎಸ್ 238 – ಸಾಕ್ಷ್ಯ ನಾಶ

ಐಪಿಸಿ ಕಲಂ 120(ಬಿ)/ಬಿಎನ್‌ಎಸ್ 61(2) – ಅಪರಾಧದ ಸಂಚಿಗಾಗಿ ಶಿಕ್ಷೆ

ಐಪಿಸಿ ಕಲಂ 124(ಎ) – ದೇಶದ್ರೋಹ ಅನ್ವಯಿಸಿದರೆ (ಈ ಕಲಂ ಅನ್ನು ಬಿಎನ್‌ಎಸ್–2023 ರಲ್ಲಿ ಅಳಿಸಲಾಗಿದೆ)

ಅಧಿಕೃತ ರಹಸ್ಯಗಳ ಕಾಯ್ದೆ, 1923:

ಕಲಂ 3 – ಸ್ಟೆಗ್ನಾಗ್ರಫಿ ಬಳಸಿ ಬೇಹುಗಾರಿಕೆ

ಒಂದು ಫೈಲ್ ಮುಗ್ಧವಾಗಿ ಕಂಡು ಅನುಮಾನಾಸ್ಪದವಾಗಿ ವರ್ತಿಸಿದರೆ, ಅದು ಮಾರುವೇಷದಲ್ಲಿರುವ ಸ್ಟೆಗನೋಗ್ರಫಿ!.

ಸೈಬರ್ ಸುರಕ್ಷಿತರಾಗಿರಲು ಸಲಹೆಗಳು

ಕೆ.ಎನ್.ಯಶವಂತ ಕುಮಾರ್ ಡಿವೈಎಸ್‌ಪಿ ರವರಿಂದ

ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿರಲು ಸಲಹೆಗಳು

1. **ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಆಗಾಗ್ಗೆ ನವೀಕರಿಸಿ:**
   ನೀವು ಇತ್ತೀಚಿನ ಭದ್ರತಾ ಪ್ಯಾಚ್‌ಗಳು ಮತ್ತು ದೋಷ ಪರಿಹಾರಗಳನ್ನು ಹೊಂದಲು ನಿಮ್ಮ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್, ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಮತ್ತು ಸಾಧನಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ನವೀಕರಿಸಿ.

2. **ಫಿಶಿಂಗ್ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ:**
   ಅನುಮಾನಾಸ್ಪದ ಇಮೇಲ್‌ಗಳು, ಲಿಂಕ್‌ಗಳು ಮತ್ತು ಲಗತ್ತುಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಹಂಚುವುದು ಅಥವಾ ಪರಿಚಯವಿಲ್ಲದ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.

3. **ನಿಮ್ಮ ವೈ-ಫೈ ನೆಟ್‌ವರ್ಕ್ ಅನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ:**
   ನಿಮ್ಮ ವೈ-ಫೈ ನೆಟ್‌ವರ್ಕ್‌ಗಾಗಿ ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್ ಹೊಂದಿಸಿ, WPA3 ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ ಮತ್ತು ಡೀಫಾಲ್ಟ್ ರೂಟರ್ ಲಾಗಿನ್ ರುಜುವಾತುಗಳನ್ನು ಬದಲಾಯಿಸಿ.

4. **ವರ್ಚುವಲ್ ಪ್ರೈವೇಟ್ ನೆಟ್‌ವರ್ಕ್ (VPN) ಬಳಸಿ:**
   ಸಾರ್ವಜನಿಕ ವೈ-ಫೈ ಬಳಸುವಾಗ ಅಥವಾ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಪ್ರವೇಶಿಸುವಾಗ, ನಿಮ್ಮ ಇಂಟರ್ನೆಟ್ ಸಂಪರ್ಕವನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಲು ಮತ್ತು ನಿಮ್ಮ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸಲು ಪ್ರತಿಷ್ಠಿತ VPN ಅನ್ನು ಬಳಸಿ.

5. **ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಪ್ರೊಫೈಲ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ:**
   ನಿಮ್ಮ ಪೋಸ್ಟ್‌ಗಳನ್ನು ಯಾರು ನೋಡಬಹುದು ಎಂಬುದನ್ನು ನಿಯಂತ್ರಿಸಲು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳಲ್ಲಿ ನಿಮ್ಮ ಗೌಪ್ಯತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ನೀವು ಸಾರ್ವಜನಿಕವಾಗಿ ಹಂಚಿಕೊಳ್ಳುವ ಮಾಹಿತಿಯ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ.

6. **ನಿಯಮಿತವಾಗಿ ಖಾತೆ ಚಟುವಟಿಕೆಯನ್ನು ಪರಿಶೀಲಿಸಿ:**
   ಯಾವುದೇ ಅನುಮಾನಾಸ್ಪದ ಚಟುವಟಿಕೆಗಾಗಿ ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಖಾತೆಗಳನ್ನು ಪರಿಶೀಲಿಸುತ್ತಿರಿ ಮತ್ತು ನೀವು ಬಳಸದ ಸಾಧನಗಳಿಂದ ಲಾಗ್ ಔಟ್ ಮಾಡಿ.

7. **ಭೌತಿಕ ಸಾಧನಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ:** ನಿಮ್ಮ ಸಾಧನಗಳನ್ನು ಪಿನ್, ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಬಯೋಮೆಟ್ರಿಕ್ ದೃಢೀಕರಣದೊಂದಿಗೆ ಲಾಕ್ ಮಾಡಿ. ಕಳೆದುಹೋದರೆ ನಿಮ್ಮ ಸಾಧನವನ್ನು ಪತ್ತೆಹಚ್ಚಲು ಮತ್ತು ದೂರದಿಂದಲೇ ದತ್ತಾಂಶ ಅಳಿಸಲು ಸಹಕಾರಿಯಾದ Find my device" ನಂತಹ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.

8. ಸುರಕ್ಷಿತ ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಬಳಸಿ:

ಸಾರ್ವಜನಿಕ ವೈ–ಫೈ ನೆಟ್‌ವರ್ಕ್‌ಗಳ ಮೂಲಕ ಸೂಕ್ಷ್ಮ ವಹಿವಾಟುಗಳನ್ನು ನಡೆಸುವುದನ್ನು ಅಥವಾ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಪ್ರವೇಶಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ, ಏಕೆಂದರೆ ಅವುಗಳು ಕಡಿಮೆ ಸುರಕ್ಷಿತವಾಗಿರಬಹುದು.

9. ನೀವೇ ಸುಶಿಕ್ಷಿತರಾಗಿ:

ನೀವು ಹೊಸ ಭದ್ರತಾ ಸವಾಲುಗಳಿಗೆ ಹೊಂದಿಕೊಳ್ಳುತ್ತಿರುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಇತ್ತೀಚಿನ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಬೆದರಿಕೆಗಳು ಮತ್ತು ಉತ್ತಮ ಅಭ್ಯಾಸಗಳ ಕುರಿತು ಶಿಕ್ಷಿತರಾಗಿ.

10. ಹಣಕಾಸು ವಿವರಣೆಪತ್ರವನ್ನು ನಿಯಮಿತವಾಗಿ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ:

ಯಾವುದೇ ಅನಧಿಕೃತ ವಹಿವಾಟುಗಳಿಗಾಗಿ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಮತ್ತು ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಸ್ಟೇಟ್‌ಮೆಂಟ್‌ಗಳ ಮೇಲೆ ನಿಗಾ ಇರಿಸಿ ಮತ್ತು ಯಾವುದೇ ವ್ಯತ್ಯಾಸಗಳನ್ನು ತಕ್ಷಣವೇ ವರದಿ ಮಾಡಿ.

11. ಸುರಕ್ಷಿತ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸಿ:

ನಿಮ್ಮ ಪ್ರತಿಯೊಂದು ಖಾತೆಗೆ ಬಲವಾದ, ಅನನ್ಯ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ರಚಿಸಿ. ಜನ್ಮದಿನಗಳು ಅಥವಾ ಹೆಸರುಗಳಂತಹ ಸುಲಭವಾಗಿ ಊಹಿಸಬಹುದಾದ ಮಾಹಿತಿಯನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ. ಮತ್ತು ಅಕ್ಷರಗಳು, ಸಂಖ್ಯೆಗಳು ಮತ್ತು ಚಿಹ್ನೆಗಳ ಸಂಯೋಜನೆಯನ್ನು ಬಳಸುವುದನ್ನು ಪರಿಗಣಿಸಿ.

12. ಫೈರ್‌ವಾಲ್ ರಕ್ಷಣೆಯನ್ನು ಕಾರ್ಯಗತಗೊಳಿಸಿ:

ಒಳಬರುವ ಮತ್ತು ಹೊರಹೋಗುವ ನೆಟ್‌ವರ್ಕ್ ಟ್ರಾಫಿಕ್ ಅನ್ನು ನಿಯಂತ್ರಿಸಲು ನಿಮ್ಮ ಸಾಧನಗಳಲ್ಲಿ ಫೈರ್‌ವಾಲ್ ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ, ಇದು ಅನಧಿಕೃತ ಪ್ರವೇಶದ ವಿರುದ್ಧ ರಕ್ಷಣೆಯ ಹೆಚ್ಚುವರಿ ಪದರವನ್ನು ಸೇರಿಸುತ್ತದೆ.

13. ಅನಗತ್ಯ ಸೇವೆಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ:

ಸಂಭಾವ್ಯ ದುರ್ಬಲತೆಗಳು ಮತ್ತು ದಾಳಿ ವೆಕ್ಟರ್‌ಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಲು ನಿಮ್ಮ ಸಾಧನಗಳಲ್ಲಿ ಯಾವುದೇ ಅನಗತ್ಯ ಸೇವೆಗಳು ಅಥವಾ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ಆಫ್ ಮಾಡಿ.

14. ಅಪ್ಲಿಕೇಶನ್ ಅನುಮತಿಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಆಡಿಟ್ ಮಾಡಿ:

ನಿಮ್ಮ ಸಾಧನಗಳಲ್ಲಿ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಗೆ ನೀಡಲಾದ ಅನುಮತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಆ್ಯಪ್‌ನ ಕಾರ್ಯಕ್ಕೆ ಅಗತ್ಯವಿಲ್ಲ ಎಂದು ತೋರುವ ಯಾವುದಿದ್ದರೂ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ.

15. ಸುರಕ್ಷಿತ ಕ್ಲೌಡ್ ಸಂಗ್ರಹಣೆ:

ನೀವು ಕ್ಲೌಡ್ ಸ್ಟೋರೇಜ್ ಸೇವೆಗಳನ್ನು ಬಳಸುತ್ತಿದ್ದರೆ, ಬಲವಾದ ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ ಮತ್ತು ನಿಮ್ಮ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸಲು ಎರಡು ಅಂಶದ ದೃಢೀಕರಣವನ್ನು ಬಳಸಿಕೊಳ್ಳಿ.

16. ಡೌನ್‌ಲೋಡ್‌ಗಳೊಂದಿಗೆ ಜಾಗರೂಕರಾಗಿರಿ:

www.cybersafegirl.com

ಪ್ರತಿಷ್ಠಿತ ಮೂಲಗಳಿಂದ ಮಾತ್ರ ಫೈಲ್‌ಗಳು ಮತ್ತು ಸಾಫ್ಟ್‌ವೇರ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ. ಅಪರಿಚಿತ ವೆಬ್‌ಸೈಟ್‌ಗಳಿಂದ ಫೈಲ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವುದನ್ನು ಅಥವಾ ಅನುಮಾನಾಸ್ಪದ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.

17. ಸುರಕ್ಷಿತ ಭೌತಿಕ ದಾಖಲೆಗಳು:

ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಹೊಂದಿರುವ ಭೌತಿಕ ದಾಖಲೆಗಳನ್ನು ಸುರಕ್ಷಿತ ಸ್ಥಳದಲ್ಲಿ ಇರಿಸಿ ಮತ್ತು ನಿಮಗೆ ಇನ್ನು ಮುಂದೆ ಅಗತ್ಯವಿಲ್ಲದ ಯಾವುದೇ ದಾಖಲೆಗಳನ್ನು ಚೂರುಚೂರು ಮಾಡಿ.

18. ಬಯೋಮೆಟ್ರಿಕ್ ದೃಢೀಕರಣವನ್ನು ಬಳಸಿ:

ಸಾಧ್ಯವಾದಾಗಲೆಲ್ಲಾ, ಹೆಚ್ಚುವರಿ ಭದ್ರತೆಗಾಗಿ ಫಿಂಗರ್‌ಪ್ರಿಂಟ್ ಅಥವಾ ಮುಖದ ಗುರುತಿಸುವಿಕೆಯಂತಹ ಬಯೋಮೆಟ್ರಿಕ್ ದೃಢೀಕರಣ ವಿಧಾನಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.

19. ಸುರಕ್ಷಿತ IOT ಸಾಧನಗಳು:

ನೀವು ಸ್ಮಾರ್ಟ್ ಹೋಮ್ ಸಾಧನಗಳನ್ನು ಹೊಂದಿದ್ದರೆ, ಅವರ ಡೀಫಾಲ್ಟ್ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬದಲಾಯಿಸಿ, ಅದರ ಫರ್ಮ್‌ವೇರ್ ಅನ್ನು ನಿಯಮಿತವಾಗಿ ನವೀಕರಿಸಿ ಮತ್ತು ಸಾಧ್ಯವಾದರೆ ಅವುಗಳನ್ನು ಪ್ರತ್ಯೇಕ ನೆಟ್‌ವರ್ಕ್‌ನಲ್ಲಿ ಪ್ರತ್ಯೇಕಿಸಿ.

20. ಡಿಜಿಟಲ್ ಎಸ್ಟೇಟ್ ಯೋಜನೆಯನ್ನು ರಚಿಸಿ:

ಆಕಸ್ಮಿಕ ಅಥವಾ ಸಾವಿನ ಸಂದರ್ಭದಲ್ಲಿ ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಖಾತೆಗಳು ಮತ್ತು ಡಿಜಿಟಲ್ ಸ್ವತ್ತುಗಳನ್ನು ಹೇಗೆ ನಿರ್ವಹಿಸಬೇಕು ಎಂಬ ಸೂಚನೆಗಳನ್ನು ಒಳಗೊಂಡಂತೆ ಯೋಜನೆಯನ್ನು ತಯಾರಿಸಿ.

www.cybersafegirl.com

ಸೈಬರ್-ಅಪರಾಧಗಳನ್ನು ಎಲ್ಲಿ ವರದಿ ಮಾಡಬೇಕು:

- ನಿಮ್ಮ ಎಲ್ಲಾ ಬಗೆಯ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು, ಪ್ರಕರಣಕ್ಕನುಗುಣವಾಗಿ ನಿಮ್ಮ ನಿವಾಸ ಅಥವಾ ನಿಮ್ಮ ಕಛೇರಿ ಆವರಣದ ವ್ಯಾಪ್ತಿಯಲ್ಲಿ ಬರುವ ಸ್ಥಳೀಯ ಪೊಲೀಸ್ ಠಾಣೆಯಲ್ಲಿ ವರದಿ ಮಾಡಿ.

- ಸೈಬರ್ ಪೊಲೀಸ್ ಠಾಣೆ ಹೊಂದಿರುವ ನಗರಗಳಲ್ಲಿ, ಸೈಬರ್-ಅಪರಾಧಗಳನ್ನು ವರದಿ ಮಾಡಬಹುದು ಮತ್ತು ಅವು ಸಾಮಾನ್ಯವಾಗಿ ಇಡೀ ನಗರದ ನ್ಯಾಯವ್ಯಾಪ್ತಿಯನ್ನು ಹೊಂದಿರುತ್ತವೆ (ದಾಖಲಿಸುವ ಮೊದಲು ಪರಿಶೀಲಿಸಬೇಕು ಮತ್ತು ಪರೀಕ್ಷಿಸಬೇಕು).

- ಸೈಬರ್ ಅಪರಾಧಗಳ ದೂರುಗಳನ್ನು ನೋಂದಾಯಿಸಲು ಬೃಹತ್ ನಗರಗಳಲ್ಲಿ ಆನ್‌ಲೈನ್ ಪೋರ್ಟಲ್‌ಗಳ ಲಭ್ಯವಿದೆ. ರಾಷ್ಟ್ರಮಟ್ಟದಲ್ಲಿ, ನಮಗಾಗಿ https://cybercrime.gov.in/ ಇದೆ.

- ಯಾವ ಜಿಲ್ಲೆ ಮತ್ತು ಗ್ರಾಮೀಣ ಪ್ರದೇಶಗಳಲ್ಲಿ ಸೈಬರ್ ಪೊಲೀಸ್ ಠಾಣೆಗಳು ಸ್ಥಾಪಿಸಿಲ್ಲವೋ, ಅಂತಲ್ಲಿ ಸ್ವಾಭಾವಿಕವಾಗಿ ಸೈಬರ್ ಸೆಲ್ ಇರುತ್ತದೆ ಅಲ್ಲಿ ಸೈಬರ್-ಅಪರಾಧಗಳ ದೂರುಗಳನ್ನು ದಾಖಲಿಸಬಹುದು.

- ಸೈಬರ್ ಪೊಲೀಸ್ ಠಾಣೆ ಅಥವಾ ಸೈಬರ್ ಸೆಲ್ ಅನುಪಸ್ಥಿತಿಯಲ್ಲಿ, ಬಲಿಪಶುಗಳು ಜಿಲ್ಲೆಯ ಅಥವಾ ನಗರದ ಉನ್ನತ ಪೊಲೀಸ್ ಅಧಿಕಾರಿಗಳನ್ನು (ಪ್ರಕರಣಗಳಿಗೆ ಅನುಗುಣವಾಗಿ ಪೊಲೀಸ್ ಅಧೀಕ್ಷಕರು ಅಥವಾ ಪೊಲೀಸ್ ಉಪ ಆಯುಕ್ತರು), ಸೈಬರ್-ಅಪರಾಧ ನೋಂದಣಿಗಾಗಿ ಸಂಪರ್ಕಿಸಬಹುದು.

- ಸೈಬರ್ ಅಪರಾಧಗಳ ದೂರುಗಳನ್ನು ನೋಂದಾಯಿಸಲು ಪ್ರತಿಯೊಂದು ರಾಜ್ಯ, ನಗರ, ಜಿಲ್ಲೆಯು ವಿಭಿನ್ನ ಕಾರ್ಯವಿಧಾನವನ್ನು ಹೊಂದಿರಬಹುದು, ಅದನ್ನು ಸೂಕ್ತ ಅಧಿಕಾರಿಗಳೊಂದಿಗೆ ಪರಿಶೀಲಿಸಬೇಕಾದ ಅವಶ್ಯಕತೆ ಇರುತ್ತದೆ.

- ಅಂತಿಮವಾಗಿ ಮತ್ತು ಮುಖ್ಯವಾಗಿ ಸೈಬರ್ ಅಪರಾಧ ದೂರು ದಾಖಲಾತಿಗಾಗಿ ರಾಷ್ಟ್ರೀಯ ಸೈಬರ್ ಅಪರಾಧ ಸಹಾಯವಾಣಿ ಸಂಖ್ಯೆ 1930 ಗೆ ಕರೆ ಮಾಡಬಹುದು.

ಗೂಗಲ್ ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಹಾರ್ಡನಿಂಗ್ ಚೆಕ್‌ಲಿಸ್ಟ್

ಆರ್.ಜಿ. ಮಂಜುನಾಥ್, ಡಿವೈಎಸ್ಪಿ ರವರಿಂದ

ಮೂಲಭೂತ ಭದ್ರತೆ

1. ಡಿವೈಸ್ ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – ಡೇಟಾ ರಕ್ಷಣೆಗಾಗಿ ಪೂರ್ಣ–ಡಿಸ್ಕ್ ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಲಾಗಿದೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.
2. ಬಲವಾದ ಸ್ಕ್ರೀನ್ ಲಾಕ್ ಬಳಸಿ – ಬಲವಾದ ಪಿನ್, ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಬಯೋಮೆಟ್ರಿಕ್ ದೃಢೀಕರಣವನ್ನು ಹಾಕಿ.
3. ಸ್ಮಾರ್ಟ್ ಲಾಕ್ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ತಡೆಯಲು ವಿಶ್ವಾಸಾರ್ಹ ಸ್ಥಳಗಳಲ್ಲಿ ಅನ್‌ಲಾಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.
4. ಡೆವಲಪರ್ ಆಯ್ಕೆಗಳನ್ನು ಟರ್ನ್ ಆಫ್ ಮಾಡಿ – USB ಡೀಬಗ್ ಮಾಡುವುದು ಮತ್ತು OEM ಅನ್‌ಲಾಕಿಂಗ್ ಅನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ.
5. Google Play Protect ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – ಬಾಹ್ಯ ತೊಂದರೆಗಳಿಂದ ತಪ್ಪಿಸಲು ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಲು Play Protect ಅನ್ನು ಸಕ್ರಿಯವಾಗಿಡಿ.
6. Google Play Store ನಿಂದ ಮಾತ್ರ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಇನ್ಸ್ಟಾಲ್ ಮಾಡಿ – ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ಮೂಲಗಳಿಂದ APK ಗಳನ್ನು ಸೈಡ್ ಲೋಡಿಂಗ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.
7. VPN ಬಳಸಿ – ಇಂಟರ್ನೆಟ್ ಟ್ರಾಫಿಕ್ ಅನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿ, ವಿಶೇಷವಾಗಿ ಸಾರ್ವಜನಿಕ Wi-Fi ನಲ್ಲಿ.
8. ಸ್ವಯಂಚಾಲಿತ ಅಪ್‌ಡೇಟ್‌ಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – ಭದ್ರತಾ ಪ್ಯಾಚ್‌ಗಳಿಗಾಗಿ OS ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಅಪ್‌ಡೇಟ್ ಮಾಡಿ.
9. ಅಪ್ಲಿಕೇಶನ್ ಅನುಮತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ – ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಂದ ಅನಗತ್ಯ ಅನುಮತಿಗಳನ್ನು ತೆಗೆದುಹಾಕಿ.
10. ಬಳಕೆಯಾಗದ ಸಂಪರ್ಕ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ಬಳಕೆಯಲ್ಲಿಲ್ಲದಿದ್ದಾಗ ಬ್ಲೂಟೂತ್, ವೈ–ಫೈ ಮತ್ತು NFC ಅನ್ನು ಆಫ್ ಮಾಡಿ.
11. ಸುರಕ್ಷಿತ ಸಂದೇಶ ಕಳುಹಿಸುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿ – ಸಿಗ್ನಲ್ ಅಥವಾ WhatsApp ನಂತಹ ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಗೆ ಆದ್ಯತೆ ನೀಡಿ.
12. Nearby device ಸ್ಕ್ಯಾನಿಂಗ್ ಅನ್ನು ಆಫ್ ಮಾಡಿ – ಅನಧಿಕೃತ ಟ್ರ್ಯಾಕಿಂಗ್ ಮತ್ತು ಡೇಟಾ ವಿನಿಮಯವನ್ನು ತಡೆಯಿರಿ.
13. ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಗಾಗಿ ಹಿನ್ನೆಲೆ ಡೇಟಾವನ್ನು ನಿರ್ಬಂಧಿಸಿ – ನಿಷ್ಕ್ರಿಯವಾಗಿರುವಾಗ ಅಪ್ಲಿಕೇಶನ್ ಇಂಟರ್ನೆಟ್ ಪ್ರವೇಶವನ್ನು ನಿಯಂತ್ರಿಸಿ.

14. ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಗಾಗಿ ಕ್ಲಿಪ್‌ಬೋರ್ಡ್ ಪ್ರವೇಶವನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ದುರುದ್ದೇಶಪೂರಿತ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಂದ ಕ್ಲಿಪ್‌ಬೋರ್ಡ್ ಸ್ಕ್ರೂಪಿಂಗ್ ಅನ್ನು ತಪ್ಪಿಸಿ.
15. ಎರಡು–ಅಂಶ ದೃಢೀಕರಣವನ್ನು (2FA) ಹೊಂದಿಸಿ – ಹೆಚ್ಚುವರಿ ಭದ್ರತೆಗಾಗಿ Google Authenticator ಬಳಸಿ.
16. Find my device ಸಕ್ರಿಯಗೊಳಿಸಿ – ಕಳೆದುಹೋದ ಸಾಧನಗಳನ್ನು ದೂರದಿಂದಲೇ ಪತ್ತೆ ಮಾಡಿ ಅಥವಾ ಅದರಲ್ಲಿನ ದತ್ತಾಂಶ ಅಳಿಸಿಹಾಕಿ.
17. ಸುರಕ್ಷಿತ DNS ಬಳಸಿ – ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ DNS ಅನ್ನು ಕಾನ್ಫಿಗರ್ ಮಾಡಿ (ಉದಾ., ಕ್ಲೌಡ್‌ಫ್ಲೇರ್, Google).
18. ಲಾಕ್ ಸ್ಕ್ರೀನ್‌ನಲ್ಲಿ Google ಸಹಾಯಕವನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ಅನಧಿಕೃತ ಧ್ವನಿ ಪ್ರವೇಶವನ್ನು ತಡೆಯಿರಿ.
19. USB ಫೈಲ್ ವರ್ಗಾವಣೆಗಳನ್ನು ಆಫ್ ಮಾಡಿ – USB ಸಂಪರ್ಕಗಳ ಮೂಲಕ ಡೇಟಾ ಕಳ್ಳತನವನ್ನು ತಡೆಯಿರಿ.
20. Wi-Fi ಗೆ Auto-connect ಅನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – Open network ಗಳಿಗೆ ಸ್ವಯಂಚಾಲಿತ ಸಂಪರ್ಕವನ್ನು ತಪ್ಪಿಸಿ.
21. ಅಜ್ಞಾತ ಕರೆ ಮಾಡುವವರನ್ನು ಮತ್ತು ಸಂದೇಶಗಳನ್ನು ನಿರ್ಬಂಧಿಸಿ – ಫಿಶಿಂಗ್ ಮತ್ತು ಸ್ಪ್ಯಾಮ್ ದಾಳಿಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಿ.
22. ಹಿನ್ನೆಲೆ ಚಾಲನೆಯಲ್ಲಿರುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ – ಹಿನ್ನೆಲೆಯಲ್ಲಿ ಚಾಲನೆಯಲ್ಲಿರುವ ಬಳಕೆಯಾಗದ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ನಿಲ್ಲಿಸಿ.
23. ಬಳಕೆಯಾಗದ Google ಖಾತೆಗಳನ್ನು ತೆಗೆದುಹಾಕಿ – ಲಿಂಕ್ ಮಾಡಲಾದ ಖಾತೆಗಳನ್ನು ಮಿತಿಗೊಳಿಸುವ ಮೂಲಕ ದಾಳಿಯ ಮೇಲ್ಮೈಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಿ.
24. Auto-save ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ಬದಲಿಗೆ ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕವನ್ನು ಬಳಸಿ.
25. ಜಾಹೀರಾತು ವೈಯಕ್ತೀಕರಣವನ್ನು ಆಫ್ ಮಾಡಿ – ವೈಯಕ್ತಿಕಗೊಳಿಸಿದ ಜಾಹೀರಾತುಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸುವ ಮೂಲಕ ಡೇಟಾ ಟ್ರ್ಯಾಕಿಂಗ್ ಅನ್ನು ಕಡಿಮೆ ಮಾಡಿ.
26. ಸುರಕ್ಷಿತ ಫೋಲ್ಡರ್ (ಸ್ಯಾಮ್‌ಸಂಗ್ ಸಾಧನಗಳು) ಬಳಸಿ – ಸೂಕ್ಷ್ಮ ಫೈಲ್‌ಗಳನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ ಜಾಗದಲ್ಲಿ ಸಂಗ್ರಹಿಸಿ.
27. ನಿಯಮಿತವಾಗಿ Cache & App ಡೇಟಾವನ್ನು clear ಮಾಡಿ– ಸಂಗ್ರಹಿಸಲಾದ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಡಿಲೀಟ್ ಮಾಡಿ.
28. ಸಾರ್ವಜನಿಕ ಚಾರ್ಜಿಂಗ್ ಸ್ಟೇಷನ್‌ಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ – USB ಡೇಟಾ ಬ್ಲಾಕರ್ ಅಥವಾ Charge-only ಕೇಬಲ್ ಬಳಸಿ.
29. ಮಾರಾಟ ಮಾಡುವ ಮೊದಲು ಫ್ಯಾಕ್ಟರಿ ರಿಸೆಟ್ ಮಾಡಿ– ನಿಮ್ಮ ಸಾಧನವನ್ನು ಹಸ್ತಾಂತರಿಸುವ ಮೊದಲು ಎಲ್ಲಾ ಡೇಟಾವನ್ನು ಅಳಿಸಿ.
30. ಅನುಮಾನಾಸ್ಪದ ಚಟುವಟಿಕೆಗಾಗಿ ಸಾಧನ ಲಾಗ್‌ಗಳನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ – ಭದ್ರತಾ ಬೆದರಿಕೆಗಳಿಗಾಗಿ ಲಾಗ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಲು ADB ನಂತಹ ಪರಿಕರಗಳನ್ನು ಬಳಸಿ.

www.cybersafegirl.com

ಆ್ಯಪಲ್ ಐ.ಓ.ಎಸ್ ಹಾರ್ಡನಿಂಗ್ ಚೆಕ್‌ಲಿಸ್ಟ್

ಅಕ್ಷಯ್ ಕುಮಾರ್ ನಾಯಕ್, ಒಪಿಎಸ್ ರವರಿಂದ

ಮೂಲಭೂತ ಭದ್ರತೆ

1. ಬಲವಾದ ಸಾಧನ ಪಾಸ್‌ಕೋಡ್ ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – 6–ಅಂಕಿಯ ಪಿನ್ ಅಥವಾ ಆಲ್ಫಾನ್ಯೂಮರಿಕ್ ಪಾಸ್‌ವರ್ಡ್ ಬಳಸಿ.
2. ಸ್ವಯಂಚಾಲಿತ ನವೀಕರಣಗಳನ್ನು ಆನ್ ಮಾಡಿ – iOS ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್ ಅಪ್‌ಡೇಟ್‌ಗಳನ್ನು ಸ್ವಯಂಚಾಲಿತವಾಗಿ ಇನ್ಸ್ಟಾಲ್ ಆಗುವಂತೆ ಸೆಟ್ಟಿಂಗ್ಸ್ ಮಾಡಿಕೊಳ್ಳಿ.
3. ಫೇಸ್ ಐಡಿ ಅಥವಾ ಟಚ್ ಐಡಿಯನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – ಸುರಕ್ಷಿತ ಪ್ರವೇಶಕ್ಕಾಗಿ ಬಯೋಮೆಟ್ರಿಕ್ ದೃಢೀಕರಣವನ್ನು ಬಳಸಿ.
4. ಲಾಕ್ ಮಾಡಿದಾಗ USB ಪರಿಕರಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ಲೈಟ್ನಿಂಗ್ ಪೋರ್ಟ್ ಮೂಲಕ ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ತಡೆಯಿರಿ.
5. ಲಾಕ್ ಸ್ಕ್ರೀನ್ ಪ್ರವೇಶವನ್ನು ಆಫ್ ಮಾಡಿ – ಲಾಕ್ ಸ್ಕ್ರೀನ್‌ನಲ್ಲಿ ಅಧಿಸೂಚನೆಗಳು, ಸಿರಿ ಮತ್ತು ನಿಯಂತ್ರಣ ಕೇಂದ್ರವನ್ನು ನಿರ್ಬಂಧಿಸಿ.
6. ಎರಡು–ಅಂಶದ ದೃಢೀಕರಣವನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ (2FA) – 2FA ನೊಂದಿಗೆ ಆಪಲ್ ಐಡಿಯನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ.
7. ಖಾಸಗಿ ವೈ–ಫೈ ವಿಳಾಸವನ್ನು ಬಳಸಿ – ಯಾದೃಚ್ಛಿಕ MAC ವಿಳಾಸಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುವ ಮೂಲಕ ವೈ–ಫೈ ಟ್ರ್ಯಾಕಿಂಗ್ ಅನ್ನು ತಪ್ಪಿಸಿ.
8. ಅಪರಿಚಿತರಿಗೆ ಏರ್‌ಡ್ರಾಪ್ ಅನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ಏರ್‌ಡ್ರಾಪ್ ಅನ್ನು "Contacts only" ಗೆ ಹೊಂದಿಸಿ ಅಥವಾ ಅದನ್ನು ಆಫ್ ಮಾಡಿ.
9. ಬಳಕೆಯಾಗದ ಸ್ಥಳ ಸೇವೆಗಳನ್ನು ಆಫ್ ಮಾಡಿ – ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಗೆ ಸ್ಥಳ ಪ್ರವೇಶವನ್ನು ನಿರ್ವಹಿಸಿ.
10. ಪಾಸ್‌ವರ್ಡ್‌ಗಳಿಗಾಗಿ iCloud ಕೀಚೈನ್ ಬಳಸಿ – End-to-end ಎನ್‌ಕ್ರಿಪ್ಶನ್‌ನೊಂದಿಗೆ ರುಜುವಾತುಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಸಂಗ್ರಹಿಸಿ.
11. ಅಪ್ಲಿಕೇಶನ್ ಟ್ರ್ಯಾಕಿಂಗ್ ವಿನಂತಿಗಳನ್ನು ಮಿತಿಗೊಳಿಸಿ – ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ನಿಮ್ಮ ಚಟುವಟಿಕೆಯನ್ನು ಟ್ರ್ಯಾಕ್ ಮಾಡುವುದನ್ನು ತಡೆಯಿರಿ.
12. ಅನಗತ್ಯ ಸಂದೇಶಗಳು ಮತ್ತು ಕರೆಗಳನ್ನು ನಿರ್ಬಂಧಿಸಿ – ಸ್ಪ್ಯಾಮ್ ಮತ್ತು ಫಿಶಿಂಗ್ ಪ್ರಯತ್ನಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಿ.
13. ಪಾಸ್‌ವರ್ಡ್‌ಗಳಿಗಾಗಿ ಸಫಾರಿ ಆಟೋಫಿಲ್ ಅನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ಮೀಸಲಾದ ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕವನ್ನು ಬಳಸಿ.
14. ಸುರಕ್ಷಿತ ಬ್ರೌಸಿಂಗ್‌ಗಾಗಿ VPN ಬಳಸಿ – ಸಾರ್ವಜನಿಕ Wi-Fi ನಲ್ಲಿ ಇಂಟರ್ನೆಟ್ ಚಟುವಟಿಕೆಯನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿ.
15. Find My iPhone ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – ಕಳೆದುಹೋದ ಸಾಧನಗಳನ್ನು ಟ್ರ್ಯಾಕ್ ಮಾಡಿ ಮತ್ತು ದೂರದಿಂದಲೇ ಅಳಿಸಿಹಾಕಿ.
16. ಬಳಕೆಯಲ್ಲಿಲ್ಲದಿದ್ದಾಗ ಬ್ಲೂಟೂತ್ ಅನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – ಹ್ಯಾಕಿಂಗ್ ದಾಳಿಗೆ

ಒಡ್ಡಿಕೊಳ್ಳುವುದನ್ನು ಕಡಿಮೆ ಮಾಡಿ.

17. ಲಾಕ್ ಸ್ಕ್ರೀನ್‌ನಲ್ಲಿ ಸಿರಿಯನ್ನು ನಿರ್ಬಂಧಿಸಿ – ದೃಢೀಕರಣವಿಲ್ಲದೆ ಧ್ವನಿ ಪ್ರವೇಶವನ್ನು ತಡೆಯಿರಿ.
18. ಮೇಲ್ ಗೌಪ್ಯತೆ ರಕ್ಷಣೆಯನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – ಡೇಟಾವನ್ನು ಸಂಗ್ರಹಿಸಲಾಗುವ ಇಮೇಲ್ ಟ್ರ್ಯಾಕರ್‌ಗಳನ್ನು ನಿರ್ಬಂಧಿಸಿ.
19. ಕ್ಯಾಮೆರಾ ಮತ್ತು ಮೈಕ್ರೊಫೋನ್ ಪ್ರವೇಶವನ್ನು ಮಿತಿಗೊಳಿಸಿ – ಅನಗತ್ಯ ಪ್ರವೇಶದಿಂದ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ತಡೆಯಿರಿ.
20. ಆಪಲ್‌ನೊಂದಿಗೆ ಸೈನ್ ಇನ್ ಮಾಡಿ – ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಗೆ ಸೈನ್ ಇನ್ ಮಾಡುವಾಗ ನಿಮ್ಮ ಗುರುತನ್ನು ರಕ್ಷಿಸಿಕೊಳ್ಳಿ.
21. ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ iCloud ಬ್ಯಾಕಪ್ ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – ಸಾಧನ ಬ್ಯಾಕಪ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಸಂಗ್ರಹಿಸಿ.
22. ಹಂಚಿದ Wi-Fi ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಆಫ್ ಮಾಡಿ – ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ನೆಟ್‌ವರ್ಕ್‌ಗಳಿಗೆ ಸ್ವಯಂಚಾಲಿತವಾಗಿ ಸೇರುವುದನ್ನು ತಪ್ಪಿಸಿ.
23. ವಿಶ್ಲೇಷಣೆ ಮತ್ತು ವೈಯಕ್ತಿಕಗೊಳಿಸಿದ ಜಾಹೀರಾತುಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ – Apple ನ ಡೇಟಾ ಸಂಗ್ರಹವನ್ನು ಕಡಿಮೆ ಮಾಡಿ.
24. ಅಪ್ಲಿಕೇಶನ್ ಅನುಮತಿಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ – ಅನಗತ್ಯವಾದಾಗ ಪ್ರವೇಶವನ್ನು ಹಿಂತೆಗೆದುಕೊಳ್ಳಿ.
25. ಖಾಸಗಿ ರಿಲೇ (iCloud+) ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ – ಉತ್ತಮ ಗೌಪ್ಯತೆಗಾಗಿ IP ವಿಳಾಸಗಳನ್ನು ಮರೆಮಾಡಿ.
26. ಸಫಾರಿ ಬ್ರೌಸಿಂಗ್ ಡೇಟಾವನ್ನು ನಿಯಮಿತವಾಗಿ ತೆರವುಗೊಳಿಸಿ – ಟ್ರ್ಯಾಕಿಂಗ್ ಅನ್ನು ತಡೆಯಿರಿ ಮತ್ತು ಸುರಕ್ಷತೆಯನ್ನು ಸುಧಾರಿಸಿ.
27. ಸಾರ್ವಜನಿಕ ಚಾರ್ಜಿಂಗ್ ಸ್ಟೇಷನ್‌ಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ – ಜ್ಯೂಸ್–ಜಾಕಿಂಗ್ ಅನ್ನು ತಡೆಯಲು charge-only ಕೇಬಲ್‌ಗಳನ್ನು ಬಳಸಿ.
28. ಆಪಲ್ ಏರ್‌ಟ್ಯಾಗ್‌ಗಳಲ್ಲಿ ಎಕ್ಸ್‌ಪೋಸರ್ ಅನ್ನು ಮಿತಿಗೊಳಿಸಿ – ಅನಗತ್ಯವಾಗಿದ್ದರೆ ಏರ್‌ಟ್ಯಾಗ್ ಟ್ರ್ಯಾಕಿಂಗ್ ಅನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ.
29. ಹೆಚ್ಚಿನ ಅಪಾಯದ ಬಳಕೆದಾರರಿಗೆ ಲಾಕ್‌ಡೌನ್ ಮೋಡ್ ಬಳಸಿ – ತೀವ್ರ ಭದ್ರತಾ ಅಗತ್ಯಗಳಿಗಾಗಿ ಸಕ್ರಿಯಗೊಳಿಸಿ.
30. ಮಾರಾಟ ಮಾಡುವ ಮೊದಲು ಫ್ಯಾಕ್ಟರಿ ರೀಸೆಟ್ ಮಾಡಿ – ವರ್ಗಾವಣೆಯ ಮೊದಲು ಸಂಪೂರ್ಣ ಡೇಟಾ ಅಳಿಸುವಿಕೆಯನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

www.cybersafegirl.com

ಮಾಡಬೇಕಾದದ್ದು & ಮಾಡಬಾರದ್ದು

ಶೇಖ್ ಸಲೀಂ, ಪಾಲುದಾರ – TorSecure Cyber LLP ರವರಿಂದ

1. KYC ಸ್ಕ್ಯಾಮ್

ಮಾಡಬೇಕಾದದ್ದು

- ಯಾವುದೇ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವ ಮೊದಲು ಯಾವಾಗಲೂ ಕರೆ ಮಾಡಿದವರ ಗುರುತನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಂದ ಮಾತ್ರ ಗ್ರಾಹಕ ಸೇವಾ ಸಂಖ್ಯೆಗಳನ್ನು ಸಂಪರ್ಕಿಸಿ.
- ವಂಚನೆ ಕರೆಗಳನ್ನು ಪತ್ತೆಹಚ್ಚಲು caller identification ಅಪ್ಲಿಕೇಶನ್‌ಅನ್ನು ಇನ್ಸ್ಟಾಲ್ ಮಾಡಿ.
- ಯಾವುದೇ ಅನುಮಾನಾಸ್ಪದ ಕರೆಗಳು ಅಥವಾ ಸಂದೇಶಗಳನ್ನು ವರದಿ ಮಾಡಿ.

ಮಾಡಬಾರದ್ದು

- SMS ಅಥವಾ WhatsApp ಮೂಲಕ ಸ್ವೀಕರಿಸಿದ ಅಪರಿಚಿತ ಅಥವಾ ಅನುಮಾನಾಸ್ಪದ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.
- OTP ಗಳು, ಪಿನ್‌ಗಳು, ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಅಥವಾ ಖಾತೆ ವಿವರಗಳನ್ನು ಫೋನ್ ಮೂಲಕ ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಬ್ಯಾಂಕ್‌ಗಳು ಅಥವಾ KYC ತಂಡದವರೆಂದು ಹೇಳಿಕೊಂಡು ಯಾದೃಚ್ಛಿಕ ಕರೆ ಮಾಡುವವರನ್ನು ನಂಬಬೇಡಿ.
- ಸರ್ಚ್ ಇಂಜಿನ್‌ಗಳಿಂದ ಪಡೆದ ಗ್ರಾಹಕ ಸೇವಾ ಸಂಖ್ಯೆಗಳಿಗೆ ಕರೆ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.

2. ಆನ್‌ಲೈನ್ ಉದ್ಯೋಗ ಹಗರಣ

ಮಾಡಬೇಕಾದದ್ದು

- ಅಧಿಕೃತ ಕಂಪನಿ ವೆಬ್‌ಸೈಟ್‌ಗಳ ಉದ್ಯೋಗ ಕೊಡುಗೆಗಳ ಕಾನೂನುಬದ್ಧತೆಯನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಉದ್ಯೋಗದಲ್ಲಿ ಕನಿಷ್ಠ ಕೆಲಸಕ್ಕೆ ಹೆಚ್ಚಿನ ವೇತನವನ್ನು ನೀಡಿದರೆ ಅಥವಾ ಮುಂಗಡ ಪಾವತಿಯನ್ನು ಕೇಳಿದರೆ ಜಾಗರೂಕರಾಗಿರಿ.
- ನಿಮ್ಮ ಸಂವಹನ ಮತ್ತು ಉದ್ಯೋಗ ಕೊಡುಗೆ ವಿವರಗಳ ದಾಖಲೆಗಳನ್ನು ನಿರ್ವಹಣೆ ಮಾಡಿ.
- ಕಂಪನಿಯ ವಿಮರ್ಶೆಗಳು ಮತ್ತು ದೂರುಗಳನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸಂಶೋಧಿಸಿ.

ಮಾಡಬಾರದ್ದು

- ಉದ್ಯೋಗ ನೋಂದಣಿ, ತರಬೇತಿ ಅಥವಾ ಆಫರ್ ಲೆಟರ್‌ಗಳಿಗೆ ಪಾವತಿಸಬೇಡಿ.
- ಕಂಪನಿಯ ಸತ್ಯಾಸತ್ಯತೆಯ ಬಗ್ಗೆ ನಿಮಗೆ ಖಚಿತವಿಲ್ಲದಿದ್ದರೆ ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಅಥವಾ ಹಣಕಾಸಿನ ದಾಖಲೆಗಳನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- SMS ಅಥವಾ ಇಮೇಲ್‌ಗಳ ಮೂಲಕ ಸ್ವೀಕರಿಸಿದ ಅನುಮಾನಾಸ್ಪದ ಉದ್ಯೋಗ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಸ್ಪಷ್ಟ ಉದ್ಯೋಗ ಪಾತ್ರ ತಿಳಿಯದೆ ಗಳಿಕೆಯ ಭರವಸೆ ನೀಡುವ ಉದ್ಯೋಗಗಳನ್ನು ನೀಡಬೇಡಿ.

3. ಆನ್‌ಲೈನ್ ಶಾಪಿಂಗ್ ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- ವಿಶ್ವಾಸಾರ್ಹ ಮತ್ತು ಪರಿಶೀಲಿಸಿದ ಇ-ಕಾಮರ್ಸ್ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಂದ ಮಾತ್ರ ಶಾಪಿಂಗ್ ಮಾಡಿ.
- ಖರೀದಿಸುವ ಮೊದಲು ಮಾರಾಟಗಾರರ ರೇಟಿಂಗ್‌ಗಳು ಮತ್ತು ಉತ್ಪನ್ನ ವಿಮರ್ಶೆಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಕ್ರೆಡಿಟ್/ಡೆಬಿಟ್ ಕಾರ್ಡ್‌ಗಳು ಅಥವಾ ವಿಶ್ವಾಸಾರ್ಹ ವ್ಯಾಲೆಟ್‌ಗಳಂತಹ ಸುರಕ್ಷಿತ ಪಾವತಿ ವಿಧಾನಗಳನ್ನು ಬಳಸಿ.
- ಭವಿಷ್ಯದ ಉಲ್ಲೇಖಕ್ಕಾಗಿ ವಹಿವಾಟು ದಾಖಲೆಗಳನ್ನು ನಿರ್ವಹಿಸಿ.

ಮಾಡಬಾರದ್ದು

- ನಿಜವಾಗಲು ತುಂಬಾ ಚೆನ್ನಾಗಿ ಕಾಣುವ ಡೀಲ್‌ಗಳಿಗೆ ಬಲಿಯಾಗಬೇಡಿ.
- ಅಧಿಕೃತ ವೇದಿಕೆಯ ಹೊರಗೆ ಪಾವತಿಗಳನ್ನು ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಕಾರ್ಡ್ ಪಿನ್‌ಗಳು, OTP ಗಳು ಅಥವಾ CVV ಸಂಖ್ಯೆಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಅಪರಿಚಿತ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಪ್ರೊಫೈಲ್‌ಗಳು ಅಥವಾ ಗುಂಪುಗಳ ಮೂಲಕ ಹಂಚಿಕೊಳ್ಳಲಾದ ಲಿಂಕ್‌ಗಳಿಂದ ಶಾಪಿಂಗ್ ಮಾಡಬೇಡಿ.

---

4. ಸಾಲ ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- ಸಾಲ ನೀಡುವ ಕಂಪನಿಯು RBI ನಲ್ಲಿ ನೋಂದಾಯಿಸಲ್ಪಟ್ಟಿದೆಯೇ ಎಂದು ದೃಢೀಕರಿಸಿ.
- ಸಾಲವನ್ನು ಸ್ವೀಕರಿಸುವ ಮೊದಲು ಎಲ್ಲಾ ದಾಖಲೆಗಳನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಓದಿ.
- ನಿಯಂತ್ರಿಸಲ್ಪಡುವ ಬ್ಯಾಂಕುಗಳು ಅಥವಾ NBFC ಗಳಿಂದ ಮಾತ್ರ ಸಾಲಗಳನ್ನು ಪಡೆಯಿರಿ.
- ಬಡ್ಡಿದರಗಳು ಮತ್ತು ಮರುಪಾವತಿ ನಿಯಮಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.

ಮಾಡಬಾರದ್ದು

- ಪ್ರಕ್ರಿಯೆ ಅಥವಾ ಅನುಮೋದನೆಗಾಗಿ ಯಾವುದೇ ಮುಂಗಡ ಶುಲ್ಕವನ್ನು ಪಾವತಿಸಬೇಡಿ.
- ದಾಖಲೆಗಳಿಲ್ಲದೆ ತ್ವರಿತ ಸಾಲಗಳನ್ನು ನೀಡುವ ಯೋಜನೆಗಳಿಗೆ ಬಲಿಯಾಗಬೇಡಿ.
- ಅಧಿಕೃತ ಅಪ್ಲಿಕೇಶನ್ ಸ್ಟೋರ್‌ಗಳಲ್ಲಿ ಪಟ್ಟಿ ಮಾಡದ ಸಾಲ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ತಪ್ಪಿಸಿ.
- ಪರಿಶೀಲನೆ ಇಲ್ಲದೆ ಪ್ಯಾನ್, ಆಧಾರ್ ಅಥವಾ ಬ್ಯಾಂಕ್ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

---

5. ಹೂಡಿಕೆ ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- ಯಾವುದೇ ಯೋಜನೆಯಲ್ಲಿ ಹೂಡಿಕೆ ಮಾಡುವ ಮೊದಲು ಸಂಪೂರ್ಣ ಸಂಶೋಧನೆ ಮಾಡಿ.
- ದಲ್ಲಾಳಿಗಳು ಅಥವಾ ಸಲಹೆಗಾರರ ರುಜುವಾತುಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಖಚಿತವಿಲ್ಲದಿದ್ದರೆ ಪ್ರಮಾಣೀಕೃತ ಹಣಕಾಸು ಯೋಜಕರಿಂದ ಸಲಹೆ ಪಡೆಯಿರಿ.
- SEBI-ನೋಂದಾಯಿತ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳು ಮತ್ತು ಏಜೆಂಟ್‌ಗಳನ್ನು ಬಳಸಿ.

ಮಾಡಬಾರದ್ದು

- ಯಾವುದೇ ಅಪಾಯವಿಲ್ಲದಂತಹ ಹೆಚ್ಚಿನ ಆದಾಯದ ಖಾತರಿಗಳನ್ನು ನಂಬಬೇಡಿ.

- ವಾಟ್ಸಾಪ್ ಅಥವಾ ಟೆಲಿಗ್ರಾಮ್ ಫಾರ್ವರ್ಡ್‌ಗಳ ಆಧಾರದ ಮೇಲೆ ಎಂದಿಗೂ ಹೂಡಿಕೆ ಮಾಡಬೇಡಿ.
- ಹಣವನ್ನು ತ್ವರಿತವಾಗಿ ದ್ವಿಗುಣಗೊಳಿಸುವ ಭರವಸೆ ನೀಡುವ ಲಿಂಕ್‌ಗಳನ್ನು ತಪ್ಪಿಸಿ.
- ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಬ್ಯಾಂಕ್ ಅಥವಾ ವ್ಯಾಪಾರ ರುಜುವಾತುಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

---

6. ಲೈಂಗಿಕ ಕಿರುಕುಳ

ಮಾಡಬೇಕಾದದ್ದು

- ಅಪರಿಚಿತ ಜನರಿಗೆ ವೀಡಿಯೊ ಕರೆಗಳನ್ನು ಮಾಡುವಾಗ ಜಾಗರೂಕರಾಗಿರಿ.
- ನಿರ್ದಿಷ್ಟ ವಿವರಗಳನ್ನು ಕೇಳುವ ವ್ಯಕ್ತಿಗಳನ್ನು ವರದಿ ಮಾಡಿ ಮತ್ತು ನಿರ್ಬಂಧಿಸಿ.
- ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಗೌಪ್ಯತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ನಿರ್ವಹಿಸಿ.
- ಪುರಾವೆಗಳನ್ನು ಸಂರಕ್ಷಿಸಿ ಮತ್ತು ತಕ್ಷಣ ಸೈಬರ್ ಅಪರಾಧ ಠಾಣೆಗೆ ವರದಿ ಮಾಡಿ.

ಮಾಡಬಾರದ್ದು

- ನಿಕಟ ಫೋಟೋಗಳು ಅಥವಾ ವೀಡಿಯೊಗಳನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಬೆದರಿಕೆಗಳು ಅಥವಾ ಬ್ಲ್ಯಾಕ್‌ಮೇಲ್ ಬೇಡಿಕೆಗಳಿಗೆ ಎಂದಿಗೂ ಮಣಿಯಬೇಡಿ.
- ಅನುಮಾನಾಸ್ಪದ ಆನ್‌ಲೈನ್ ಪ್ರೊಫೈಲ್‌ಗಳೊಂದಿಗೆ ತೊಡಗಿಸಿಕೊಳ್ಳಬೇಡಿ.
- ಯಾದೃಚ್ಛಿಕ ಸ್ನೇಹಿತ ಅಥವಾ ಚಾಟ್ ವಿನಂತಿಗಳನ್ನು ಸ್ವೀಕರಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ.

---

7. ಆನ್‌ಲೈನ್ ಗೇಮಿಂಗ್ ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- ಮಕ್ಕಳು ಭಾಗಿಯಾಗಿದ್ದರೆ ಪೋಷಕರ ನಿಯಂತ್ರಣಗಳನ್ನು ಬಳಸಿ.
- ಖರ್ಚುಗಳ ಮಿತಿಗಳನ್ನು ಸೆಟ್‌ಮಾಡಿ ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್‌ನಲ್ಲಿನ ಖರೀದಿಗಳನ್ನು ಟ್ರ್ಯಾಕ್ ಮಾಡಿ.
- ಅನುಮಾನಾಸ್ಪದ ನಡವಳಿಕೆ ಅಥವಾ ವಂಚನೆಯನ್ನು ವರದಿ ಮಾಡಿ.
- ಅಧಿಕೃತ ಅಪ್ಲಿಕೇಶನ್ ಸ್ಟೋರ್‌ಗಳಿಂದ ಮಾತ್ರ ಆಟಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ.

ಮಾಡಬಾರದ್ದು

- ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಗೇಮಿಂಗ್ ಮಾಡುವಾಗ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಬಹಿರಂಗಪಡಿಸಬೇಡಿ.
- ಡೆಬಿಟ್/ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್‌ಗಳನ್ನು ಆಟದ ಖಾತೆಗಳಿಗೆ ಲಿಂಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ನಕಲಿ ಇನ್-ಗೇಮ್ ಕರೆನ್ಸಿ ಕೊಡುಗೆಗಳಿಗೆ ಬಲಿಯಾಗಬೇಡಿ.
- ಪಾವತಿಗಳನ್ನು ಕೇಳುವ ಅಪರಿಚಿತ ಗೇಮರ್‌ಗಳಿಂದ ಬರುವ ಸಂದೇಶಗಳಿಗೆ ಎಂದಿಗೂ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಡಿ.

---

8. ಆನ್‌ಲೈನ್ ವೈವಾಹಿಕ ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- ವೀಡಿಯೊ ಕರೆಗಳು ಅಥವಾ ಹಿನ್ನೆಲೆ ಪರಿಶೀಲನೆಗಳ ಮೂಲಕ ವ್ಯಕ್ತಿಯ ಗುರುತನ್ನು ಪರಿಶೀಲಿಸಿ.
- ನಿರ್ಧಾರ ತೆಗೆದುಕೊಳ್ಳುವಲ್ಲಿ ಕುಟುಂಬವನ್ನು ತೊಡಗಿಸಿಕೊಳ್ಳಿ.

- ಪ್ರೊಫೈಲ್‌ನಲ್ಲಿ ಒದಗಿಸಲಾದ ಮಾಹಿತಿಯನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಯಾವುದೇ ಅನುಮಾನಾಸ್ಪದ ಅಥವಾ ಒತ್ತಡದ ನಡವಳಿಕೆಯನ್ನು ವರದಿ ಮಾಡಿ.

ಮಾಡಬಾರದ್ದು

- ವೈಯಕ್ತಿಕ ಅಥವಾ ಹಣಕಾಸಿನ ಮಾಹಿತಿಯನ್ನು ತ್ವರಿತವಾಗಿ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ತುರ್ತು ಪರಿಸ್ಥಿತಿ ಅಥವಾ ಇತರೆ ಕಾರಣಗಳಿಗಾಗಿ ಹಣವನ್ನು ವರ್ಗಾಯಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ವೈಯಕ್ತಿಕವಾಗಿ ಭೇಟಿಯಾಗುವುದನ್ನು ತಪ್ಪಿಸುವ ವ್ಯಕ್ತಿಗಳನ್ನು ನಂಬಬೇಡಿ.
- ಭಾವನಾತ್ಮಕ ಕುಶಲತೆಯಂತಹ ಕೆಂಪು ಧ್ವಜಗಳನ್ನು ನಿರ್ಲಕ್ಷಿಸಬೇಡಿ.

---

9. OTP ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಎಲ್ಲಿಯಾದರೂ OTP ಗಳನ್ನು ನಮೂದಿಸುವ ಮೊದಲು ಜಾಗರೂಕರಾಗಿರಿ.
- ನೀವು OTP ಅನ್ನು ಏಕೆ ಸ್ವೀಕರಿಸುತ್ತಿದ್ದೀರಿ ಎಂಬುದನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳಿ.
- ವಹಿವಾಟುಗಳಿಗಾಗಿ SMS ಎಚ್ಚರಿಕೆಗಳಿಗಾಗಿ ನೋಂದಾಯಿಸಿ.
- ಅಪರಿಚಿತ OTP ಸ್ವೀಕರಿಸಿದರೆ ಬ್ಯಾಂಕಿಗೆ ತಿಳಿಸಿ.

ಮಾಡಬಾರದ್ದು

- ಯಾರೊಂದಿಗೂ OTP ಗಳನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಯಾದೃಚ್ಛಿಕ ಕರೆಗಳು ಅಥವಾ ಸಂದೇಶಗಳಿಗೆ OTP ಗಳನ್ನು ನಮೂದಿಸಬೇಡಿ.
- ಅಸುರಕ್ಷಿತ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಲ್ಲಿ OTP ಗಳು ಅಥವಾ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಉಳಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ.
- OTP ವಿನಂತಿಗಳು ಯಾವಾಗಲೂ ನಿರುಪದ್ರವವೆಂದು ಭಾವಿಸಬೇಡಿ.

---

10. QR ಕೋಡ್ ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- QR ಕೋಡ್‌ಗಳನ್ನು ವಿಶ್ವಾಸಾರ್ಹ ಮೂಲಗಳಿಂದ ಮಾತ್ರ ಸ್ಕ್ಯಾನ್ ಮಾಡಿ.
- ತೆರೆಯುವ ಮೊದಲು URL ಅನ್ನು ತೋರಿಸುವ ಸ್ಕ್ಯಾನರ್ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಬಳಸಿ.
- ನೀವು ಹಣ ಪಾವತಿಸುತ್ತಿದ್ದೀರಾ ಅಥವಾ ಸ್ವೀಕರಿಸುತ್ತಿದ್ದೀರಾ ಎಂದು ಮತ್ತೊಮ್ಮೆ ಪರಿಶೀಲಿಸಿ.
- ವಹಿವಾಟು ರಶೀದಿಗಳನ್ನು ಇಟ್ಟುಕೊಳ್ಳಿ.

ಮಾಡಬಾರದ್ದು

- ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಗಳು ಕಳುಹಿಸಿದ QR ಕೋಡ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ.
- ಸಂದೇಶಗಳು, ಇಮೇಲ್‌ಗಳು ಅಥವಾ ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ಅಂಗಡಿಗಳಲ್ಲಿ ಕೋಡ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ.
- ಪಾವತಿಗಳನ್ನು ಸ್ವೀಕರಿಸಲು ಎಂದಿಗೂ ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ.

- ಮರುಪಾವತಿಗಾಗಿ ಸ್ಕ್ಯಾನ್ ಮಾಡಲು ಕೇಳುವ ಕರೆಗಳನ್ನು ನಂಬಬೇಡಿ.

---

11. ಸಾಲದ ಅಪ್ಲಿಕೇಶನ್ ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- ವಿಶ್ವಾಸಾರ್ಹ ಅಪ್ಲಿಕೇಶನ್ ಸ್ಟೋರ್‌ನಿಂದ RBI–ಅನುಮೋದಿತ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಮಾತ್ರ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ.
- ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಇನ್ಸ್ಟಾಲ್ ಮಾಡುವ ಮೊದಲು ವಿಮರ್ಶೆಗಳು ಮತ್ತು ಅನುಮತಿಗಳನ್ನು ಓದಿ.
- ಗೌಪ್ಯತೆ ನೀತಿಗಳು ಮತ್ತು ನಿಯಮಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಎರಡು ಅಂಶಗಳ ದೃಢೀಕರಣದೊಂದಿಗೆ ಮಾತ್ರ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿ.

ಮಾಡಬಾರದ್ದು

- ಸಂಪರ್ಕಗಳು ಅಥವಾ ಫೋಟೋಗಳಿಗೆ ಪ್ರವೇಶದಂತಹ ಅನಗತ್ಯ ಅನುಮತಿಗಳನ್ನು ಅನುಮತಿಸಬೇಡಿ.
- ಯಾವುದೇ ಪರಿಶೀಲನೆ ಇಲ್ಲದೆ ತ್ವರಿತ ಸಾಲಗಳನ್ನು ಭರವಸೆ ನೀಡುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ತಪ್ಪಿಸಿ.
- ಅಪರಿಚಿತ ಸಂಖ್ಯೆಗಳಿಂದ ಸ್ವೀಕರಿಸಿದ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.
- ಸಾಲ ಏಜೆಂಟ್‌ಗಳಿಗೆ ಎಂದಿಗೂ ಮುಂಗಡ ಹಣವನ್ನು ಪಾವತಿಸಬೇಡಿ.

---

12. ಸೈಬರ್ ಬಲ್ಲಿಯಿಂಗ್ (ಬೆದರಿಸುವಿಕೆ)

ಮಾಡಬೇಕಾದದ್ದು

- ಬೆದರಿಸುವಿಕೆಯ ಪುರಾವೆಗಳನ್ನು ಉಳಿಸಿಕೊಳ್ಳಿ (ಸ್ಕ್ರೀನ್‌ಶಾಟ್‌ಗಳು, ಚಾಟ್‌ಗಳು).
- ವೇದಿಕೆಯಲ್ಲಿ ಬೆದರಿಸುವಿಕೆಯನ್ನು ನಿರ್ಬಂಧಿಸಿ ಮತ್ತು ವರದಿ ಮಾಡಿ.
- ಪೋಷಕರು, ಶಿಕ್ಷಕರು ಅಥವಾ ಸೈಬರ್ ಸೆಲ್‌ಗಳಿಗೆ ತಿಳಿಸಿ.
- ವೇದಿಕೆಯ ಗೌಪ್ಯತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಬಳಸಿ.

ಮಾಡಬಾರದ್ದು

- ಬೆದರಿಸುವವರೊಂದಿಗೆ ಪ್ರತೀಕಾರ ತೀರಿಸಬೇಡಿ ಅಥವಾ ತೊಡಗಿಸಿಕೊಳ್ಳಬೇಡಿ.
- ಸೂಕ್ಷ್ಮ ವೈಯಕ್ತಿಕ ವಿಷಯವನ್ನು ಪೋಸ್ಟ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ನಿರಂತರ ಬೆದರಿಕೆಗಳು ಅಥವಾ ನಿಂದನೆಯನ್ನು ನಿರ್ಲಕ್ಷಿಸಬೇಡಿ.
- ಆನ್‌ಲೈನ್ ಬೆದರಿಸುವವರನ್ನು ಆಫ್‌ಲೈನ್‌ನಲ್ಲಿ ಎಂದಿಗೂ ಭೇಟಿಯಾಗಬೇಡಿ.

---

13. ಸೈಬರ್ ಸ್ಟಾಕಿಂಗ್

ಮಾಡಬೇಕಾದದ್ದು

- ಸಮಯ ಮತ್ತು ದಿನಾಂಕಗಳೊಂದಿಗೆ ಹಿಂಬಾಲಿಸುವಿಕೆ ಘಟನೆಗಳ ದಾಖಲೆಯನ್ನು ಇರಿಸಿ.
- ಹಿಂಬಾಲಿಸುವವರನ್ನು ನಿರ್ಬಂಧಿಸಿ ಮತ್ತು ನಿಮ್ಮ ಗೌಪ್ಯತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಬದಲಾಯಿಸಿಕೊಳ್ಳಿ.
- ಪೊಲೀಸ್ ಅಥವಾ ಸೈಬರ್ ಸೆಲ್‌ಗೆ ತಿಳಿಸಿ ಮತ್ತು ಪುರಾವೆಗಳನ್ನು ಒದಗಿಸಿ.
- ನಿಮ್ಮನ್ನು ಹಿಂಬಾಲಿಸಲಾಗುತ್ತಿದೆ ಎಂದು ನಿಮ್ಮ ಹತ್ತಿರವಿರುವ ಯಾರಿಗಾದರೂ ತಿಳಿಸಿ.

ಮಾಡಬಾರದ್ದು

- ನಿರಂತರ ಸಂದೇಶಗಳು ಅಥವಾ ಕರೆಗಳನ್ನು ನಿರ್ಲಕ್ಷಿಸಬೇಡಿ.
- ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸ್ಥಳ ಅಥವಾ ನಿಮ್ಮ ವೇಳಾಪಟ್ಟಿಯನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಹಿಂಬಾಲಿಸುವವರ ಸಂದೇಶಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಸಮಸ್ಯೆಗಳನ್ನು 'ಪರಿಹರಿಸಲು' ಹಿಂಬಾಲಕರನ್ನು ಭೇಟಿಯಾಗಬೇಡಿ.

---

14. ಸೈಬರ್ ಗ್ರೂಮಿಂಗ್

ಮಾಡಬೇಕಾದದ್ದು

- ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆ ಮತ್ತು ರೆಡ್ ಫ್ಲಾಗ್‌ಗಳ ಬಗ್ಗೆ ಮಕ್ಕಳಿಗೆ ಕಲಿಸಿ.
- ಮಕ್ಕಳೊಂದಿಗೆ ಸಂವಹನವನ್ನು ಮುಕ್ತವಾಗಿಡಿ.
- ಪೋಷಕರ ನಿಯಂತ್ರಣಗಳನ್ನು ಬಳಸಿ ಮತ್ತು ಆನ್‌ಲೈನ್ ಚಟುವಟಿಕೆಯನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ.
- ಯಾವುದೇ ಅನುಚಿತ ಸಂಪರ್ಕವನ್ನು ವರದಿ ಮಾಡುವಂತರ ಮಕ್ಕಳನ್ನು ಪ್ರೋತ್ಸಾಹಿಸಿ ಧೈರ್ಯತುಂಬಿ.

ಮಾಡಬಾರದ್ದು

- ಮಕ್ಕಳನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡದೆ ಬಿಡಬೇಡಿ.
- ಮಗುವಿನಲ್ಲಿ ಭಯ ಅಥವಾ ಅನುಮಾನವನ್ನು ಎಂದಿಗೂ ತಳ್ಳಿಹಾಕಬೇಡಿ.
- ಮಕ್ಕಳು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಅಪರಿಚಿತರೊಂದಿಗೆ ತೊಡಗಿಸಿಕೊಳ್ಳಲು ಬಿಡಬೇಡಿ.
- ಮಕ್ಕಳ ಫೋಟೋಗಳನ್ನು ಸಾರ್ವಜನಿಕವಾಗಿ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

---

15. ವ್ಯಕ್ತಿತ್ವ

ಮಾಡಬೇಕಾದದ್ದು

- ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಪ್ರೊಫೈಲ್‌ಗಳನ್ನು ಖಾಸಗಿಯಾಗಿ ಹೊಂದಿಸಿ.
- ನಿಮ್ಮನ್ನು ಅನುಕರಿಸುವ ನಕಲಿ ಖಾತೆಗಳನ್ನು ವರದಿ ಮಾಡಿ.
- ಸೋಗು ಹಾಕುವ ಪ್ರಯತ್ನಗಳ ಬಗ್ಗೆ ಸ್ನೇಹಿತರಿಗೆ ತಿಳಿಸಿ.
- ಪುರಾವೆಗಾಗಿ ಸ್ಕ್ರೀನ್‌ಶಾಟ್‌ಗಳನ್ನು ಉಳಿಸಿ.

ಮಾಡಬಾರದ್ದು

- ಯಾರಾದರೂ ನಿಮ್ಮಂತೆ ನಟಿಸಿದಾಗ ನಿರ್ಲಕ್ಷಿಸಬೇಡಿ.
- ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹೆಚ್ಚು ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಅನುಮಾನಾಸ್ಪದ ಸ್ನೇಹಿತರ ವಿನಂತಿಗಳು ಅಥವಾ ಸಂದೇಶಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.
- ಲಾಗಿನ್ ರುಜುವಾತುಗಳನ್ನು ಎಂದಿಗೂ ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

---

16. ನಕಲಿ ಪ್ರೊಫೈಲ್‌ಗಳು

ಮಾಡಬೇಕಾದದ್ದು

- ಸ್ನೇಹಿತ/ಅನುಸರಣಾ ವಿನಂತಿಗಳನ್ನು ಸ್ವೀಕರಿಸುವ ಮೊದಲು ಪರಿಶೀಲಿಸಿ.
- Google ಅಥವಾ TinEye ಬಳಸಿ ಪ್ರೊಫೈಲ್ ಫೋಟೋಗಳನ್ನು Reverse search ಮಾಡಿ.

- ಅನುಮಾನಾಸ್ಪದ ಪ್ರೊಫೈಲ್‌ಗಳನ್ನು ನಿರ್ಬಂಧಿಸಿ ಮತ್ತು ವರದಿ ಮಾಡಿ.
- ಯಾರಾದರೂ ಬೇರೊಬ್ಬರ ಗುರುತನ್ನು ಬಳಸಿಕೊಂಡು ನಕಲಿ ಪ್ರೊಫೈಲ್ ಹೊಂದಿರುವುದು ನಿಮಗೆ ಗೊತ್ತಾದರೆ ಇತರರಿಗೆ ಎಚ್ಚರಿಕೆ ನೀಡಿ.

ಮಾಡಬಾರದ್ದು

- ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಗಳಿಂದ ವಿನಂತಿಗಳನ್ನು ಸ್ವೀಕರಿಸಬೇಡಿ.
- ಸೀಮಿತ ಮಾಹಿತಿಯ ಆಧಾರದ ಮೇಲೆ ಯಾರೊಂದಿಗಾದರೂ ಚಾಟ್ ಮಾಡುವುದನ್ನು ಅಥವಾ ಭೇಟಿಯಾಗುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ವೈಯಕ್ತಿಕ ಚಿತ್ರಗಳು ಅಥವಾ ವೀಡಿಯೊಗಳನ್ನು ಎಂದಿಗೂ ಕಳುಹಿಸಬೇಡಿ.
- ಪ್ರೊಫೈಲ್‌ನಲ್ಲಿರುವ ಎಲ್ಲವನ್ನೂ ನಂಬಬೇಡಿ.

---

17. VISHING

ಮಾಡಬೇಕಾದದ್ದು

- ಅಧಿಕೃತ ಮೂಲಗಳ ಮೂಲಕ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಯನ್ನು, ಖಾತೆ ವಿವರ ಪರಿಶೀಲಿಸಿ.
- ಅನುಮಾನಾಸ್ಪದ ಕರೆಗಳ ಬಗ್ಗೆ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅಥವಾ ಟೆಲಿಕಾಂ ಪೂರೈಕೆದಾರರಿಗೆ ವರದಿ ಮಾಡಿ.
- ಕರೆ–ನಿರ್ಬಂಧಿಸುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿ.
- ಸಾಮಾನ್ಯ ಫಿಶಿಂಗ್ ಕರೆ ಮಾದರಿಗಳ ಬಗ್ಗೆ ತಿಳಿದಿರಲಿ.

ಮಾಡಬಾರದ್ದು

- ಕರೆಗಳ ಮೂಲಕ ಬ್ಯಾಂಕಿಂಗ್ ಅಥವಾ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಕರೆ ಮಾಡುವವರ ಐಡಿಗಳನ್ನು ನಂಬಬೇಡಿ; ಅವುಗಳನ್ನು ವಂಚಿಸಬಹುದು.
- ತಕ್ಷಣದ ಕ್ರಮವನ್ನು ಕೋರುವ ತುರ್ತು ಕರೆಗಳನ್ನು ತಪ್ಪಿಸಿ.
- ಭಯಪಡಬೇಡಿ; ಸ್ಕ್ಯಾಮರ್‌ಗಳು ಒತ್ತಡದ ಅನುಕೂಲತೆ ಪಡೆಯಲು ಕಾತುರದಿಂದಿರುತ್ತಾರೆ.

---

18. ಫಿಶಿಂಗ್

ಮಾಡಬೇಕಾದದ್ದು

- ಇಮೇಲ್‌ಗಳು ಮತ್ತು URL ಗಳಲ್ಲಿ ಕಾಗುಣಿತ ದೋಷಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಕ್ಲಿಕ್ ಮಾಡುವ ಮೊದಲು ನಿಜವಾದ URL ಗಳನ್ನು ನೋಡಲು ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ.
- ಸ್ಪ್ಯಾಮ್ ಫಿಲ್ಟರ್‌ಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.
- ಖಾತೆಗಳಿಗೆ ಎರಡು ಅಂಶಗಳ ದೃಢೀಕರಣವನ್ನು ಬಳಸಿ.

ಮಾಡಬಾರದ್ದು

- ಅಪೇಕ್ಷಿಸದ ಇಮೇಲ್‌ಗಳು ಅಥವಾ ಸಂದೇಶಗಳಲ್ಲಿನ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.
- ಅಜ್ಞಾತ ಮೂಲಗಳಿಂದ ಲಗತ್ತುಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಅನುಮಾನಾಸ್ಪದ ವೆಬ್‌ಸೈಟ್‌ಗಳಲ್ಲಿ ಎಂದಿಗೂ ರುಜುವಾತುಗಳನ್ನು ನಮೂದಿಸಬೇಡಿ.
- ಫಿಶಿಂಗ್ ಇಮೇಲ್‌ಗಳಿಗೆ ಪ್ರತ್ಯುತ್ತರಿಸಬೇಡಿ.

---

19. ಸ್ಮಿಶಿಂಗ್

ಮಾಡಬೇಕಾದದ್ದು

- ಅನಿರೀಕ್ಷಿತ SMS ಸಂದೇಶಗಳನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಪರಿಗಣಿಸಿ.
- ಅಧಿಕೃತ ಮೂಲಗಳ ಮೂಲಕ ಲಿಂಕ್‌ಗಳು ಅಥವಾ ಸಂಖ್ಯೆಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಸ್ಮಿಶಿಂಗ್ ಸಂದೇಶಗಳನ್ನು ನಿಮ್ಮ ಟೆಲಿಕಾಂ ಪೂರೈಕೆದಾರರಿಗೆ ವರದಿ ಮಾಡಿ.
- ನಿಮ್ಮ ಸಾಧನದ OS ಮತ್ತು ಆಂಟಿವೈರಸ್ ಅನ್ನು ನವೀಕರಿಸಿಟ್ಟುಕೊಳ್ಳಿ.

ಮಾಡಬಾರದ್ದು

- ಅನುಮಾನಾಸ್ಪದ SMS ಸಂದೇಶಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಡಿ.
- ಅಜ್ಞಾತ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಎಂದಿಗೂ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.
- ಅಜ್ಞಾತ ವೆಬ್‌ಸೈಟ್‌ಗಳಲ್ಲಿ OTP ಗಳು ಅಥವಾ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ನಮೂದಿಸುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಬ್ಯಾಂಕುಗಳು ಅಥವಾ ಸೇವಾ ಪೂರೈಕೆದಾರಿಂದ ಬಂದಿರುವಂತೆ ತೋರುವ ಎಲ್ಲಾ ಸಂದೇಶಗಳನ್ನು ನಂಬಬೇಡಿ.

---

20. ಸಿಮ್ ಸ್ವಾಪ್ ವಂಚನೆ

ಮಾಡಬೇಕಾದದ್ದು

- ನಿಮ್ಮ ಸಿಮ್ ಕಾರ್ಯನಿರ್ವಹಿಸುವುದನ್ನು ನಿಲ್ಲಿಸಿದರೆ ನಿಮ್ಮ ಮೊಬೈಲ್ ಸೇವಾ ಪೂರೈಕೆದಾರರನ್ನು ಸಂಪರ್ಕಿಸಿ.
- ಬ್ಯಾಂಕ್ ಸಂದೇಶಗಳು ಮತ್ತು ವಹಿವಾಟು ಎಚ್ಚರಿಕೆಗಳನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ.
- ಮೊಬೈಲ್ ಭದ್ರತಾ ಪಿನ್‌ಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.
- ಬ್ಯಾಂಕಿಂಗ್ OTP ಗಳಿಗೆ ಪರ್ಯಾಯ ಸಂಖ್ಯೆಯನ್ನು ಬಳಸಿ.

ಮಾಡಬಾರದ್ದು

- ದೀರ್ಘಕಾಲದವರೆಗೆ ಮೊಬೈಲ್ ಸಿಗ್ನಲ್ ಇಲ್ಲದಿರುವುದನ್ನು ನಿರ್ಲಕ್ಷಿಸಬೇಡಿ.
- ಸಿಮ್ ಅಥವಾ ಫೋನ್ ವಿವರಗಳನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ವೈಯಕ್ತಿಕ ದಾಖಲೆಗಳನ್ನು ಅಜಾಗರೂಕತೆಯಿಂದ ಬಳಸಬೇಡಿ.
- SMS ಆಧಾರಿತ ದೃಢೀಕರಣವನ್ನು ಮಾತ್ರ ಅವಲಂಬಿಸಬೇಡಿ.

---

21. ಗುರುತಿನ ಕಳ್ಳತನ

ಮಾಡಬೇಕಾದದ್ದು

- ವೈಯಕ್ತಿಕ ವಿವರಗಳ ದಾಖಲೆಗಳನ್ನು ಕೆಲಸ ಮುಗಿದ ನಂತರ ಹರಿದು ಹಾಕುವುದು.
- ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸಿ ಮತ್ತು ಅವುಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಬದಲಾಯಿಸಿ.
- ಬ್ಯಾಂಕ್ ಮತ್ತು ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಸ್ಟೇಟ್‌ಮೆಂಟ್‌ಗಳನ್ನು ಆಗಾಗ್ಗೆ ಪರಿಶೀಲಿಸಿ.
- ನಿಮ್ಮ ಡಿಜಿಟಲ್ ಹೆಜ್ಜೆಗುರುತನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ.

ಮಾಡಬಾರದ್ದು

- ಸೂಕ್ಷ್ಮ ದಾಖಲೆಗಳು ಅಥವಾ ಐಡಿಗಳನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಹಂಚಿಕೊಂಡ ಸಾಧನಗಳಲ್ಲಿ ಗೌಪ್ಯ ಡೇಟಾವನ್ನು ಸಂಗ್ರಹಿಸಬೇಡಿ.

- ಬ್ಯಾಂಕಿಂಗ್‌ಗಾಗಿ ಸಾರ್ವಜನಿಕ ವೈ-ಫೈ ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಉದ್ದೇಶವಿಲ್ಲದೆ ಗುರುತಿನ ಪುರಾವೆಗಳನ್ನು ಬಹಿರಂಗಪಡಿಸಬೇಡಿ.

---

22. ಎಟಿಎಂ ಸ್ಕಿಮ್ಮಿಂಗ್

ಮಾಡಬೇಕಾದದ್ದು

- ಬಳಸುವ ಮೊದಲು ಎಟಿಎಂ ಕಾರ್ಡ್ ಸ್ಲಾಟ್‌ಗಳನ್ನು ಪರೀಕ್ಷಿಸಿ.
- ಪಿನ್ ನಮೂದಿಸುವಾಗ ಕೀಪ್ಯಾಡ್ ಅನ್ನು ಮುಚ್ಚಿಕೊಳ್ಳಿ.
- ಎಟಿಎಂಗಳನ್ನು ಚೆನ್ನಾಗಿ ಬೆಳಕು ಹೊಂದಿರುವ, ಸುರಕ್ಷಿತ ಸ್ಥಳಗಳಲ್ಲಿ ಬಳಸಿ.
- ಅನಧಿಕೃತ ವಹಿವಾಟುಗಳಿಗಾಗಿ ಬ್ಯಾಂಕ್ ಸ್ಟೇಟ್‌ಮೆಂಟ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.

ಮಾಡಬಾರದ್ದು

- ವಿರೂಪಗೊಳಿಸಲಾಗಿರುವ ಅಥವಾ ಅನುಮಾನಾಸ್ಪದವಾಗಿ ಕಾಣುವ ಎಟಿಎಂಗಳನ್ನು ಬಳಸಬೇಡಿ.
- ಎಟಿಎಂಗಳಲ್ಲಿ ಅಪರಿಚಿತರಿಂದ ಸಹಾಯ ಪಡೆಯುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ರಶೀದಿಗಳನ್ನು ಎಲ್ಲಿಯೂ ಎಸೆಯಬೇಡಿ.
- ಎಟಿಎಂ ಪಿನ್ ಅನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

---

23. ಡೇಟಾ ಕಳ್ಳತನ

ಮಾಡಬೇಕಾದದ್ದು

- ಎಲ್ಲಾ ಸಾಧನಗಳನ್ನು ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಮತ್ತು ಎನ್‌ಕ್ರಿಪ್ಶನ್‌ನೊಂದಿಗೆ ಸುರಕ್ಷಿತಗೊಳಿಸಿ.
- ಸುರಕ್ಷಿತವಾದ ಸ್ಥಳಗಳಲ್ಲಿ ನಿಯಮಿತವಾಗಿ ಡೇಟಾವನ್ನು ಬ್ಯಾಕಪ್ ಮಾಡಿ.
- ಗೌಪ್ಯ ಫೈಲ್‌ಗಳಿಗೆ ಪ್ರವೇಶವನ್ನು ನಿರ್ಬಂಧಿಸಿ.
- ನವೀಕರಿಸಿದ ಆಂಟಿವೈರಸ್ ಮತ್ತು ಫೈರ್‌ವಾಲ್‌ಗಳನ್ನು ಬಳಸಿ.

ಮಾಡಬಾರದ್ದು

- ಸಾಧನಗಳನ್ನು ಸಾರ್ವಜನಿಕವಾಗಿ ಹಾಗೆಯೇ ಬಿಡಬೇಡಿ.
- ಇಮೇಲ್ ಮೂಲಕ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಅಥವಾ ಡೇಟಾವನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಇಲ್ಲದೆ ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ಸಂಗ್ರಹಿಸಬೇಡಿ.
- ಅನಧಿಕೃತ ಡೇಟಾ ಪ್ರವೇಶವನ್ನು ನಿರ್ಲಕ್ಷಿಸಬೇಡಿ.

---

24. ರಾನ್ಸಮ್‌ವೇರ್

ಮಾಡಬೇಕಾದದ್ದು

- ಪ್ರಮುಖ ಡೇಟಾವನ್ನು ಆಗಾಗ್ಗೆ ಬ್ಯಾಕಪ್ ಮಾಡಿ.
- ಪರವಾನಗಿ ಇರುವ ಆಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್ ಬಳಸಿ.
- ಫಿಶಿಂಗ್ ದಾಳಿಗಳ ಬಗ್ಗೆ ಸಿಬ್ಬಂದಿಗಳಿಗೆ ಮತ್ತು ಕುಟುಂಬದವರಿಗೆ ತರಬೇತಿ ನೀಡಿ.
- ಸೋಂಕಿತ ಸಿಸ್ಟಂಗಳನ್ನು ತಕ್ಷಣವೇ ಸಂಪರ್ಕ ಕಡಿತಗೊಳಿಸಿ.

ಮಾಡಬಾರದ್ದು

- ಎಂದಿಗೂ ರ್ಯಾಂಸಮ್‌ಗೆ ಪಾವತಿಸಬೇಡಿ; ಇದು ಅಪರಾಧಗಳನ್ನು ಪ್ರೋತ್ಸಾಹಿಸಿದಂತೆ.
- ಅಪರಿಚಿತ ಲಗತ್ತುಗಳು ಅಥವಾ ಇಮೇಲ್ ಲಿಂಕ್‌ಗಳನ್ನು ತೆರೆಯಬೇಡಿ.
- ನಕಲಿ ಸಾಫ್ಟ್‌ವೇರ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ರಾನ್ಸಮ್‌ವೇರ್ ಅನ್ನು ಅಧಿಕಾರಿಗಳಿಗೆ ವರದಿ ಮಾಡುವುದನ್ನು ವಿಳಂಬ ಮಾಡಬೇಡಿ.

ಸೈಬರ್ ಸುರಕ್ಷತಾ ಪರಿಶೀಲನಾಪಟ್ಟಿ

ವಿದ್ಯಾರ್ಥಿಗಳಿಗಾಗಿ

- ☐ ನಾನು ಪ್ರತಿ ಆನ್‌ಲೈನ್ ಖಾತೆಗೆ ಸಂಕೀರ್ಣ, ವಿಶಿಷ್ಟ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸುತ್ತೇನೆ.
- ☐ ಪೋಷಕರನ್ನು ಹೊರತುಪಡಿಸಿ ನಾನು ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳುವುದಿಲ್ಲ.
- ☐ ಲಭ್ಯವಿರುವ ಎಲ್ಲಾ ಖಾತೆಗಳಲ್ಲಿ ನಾನು ಎರಡು ಅಂಶಗಳ ದೃಢೀಕರಣವನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುತ್ತೇನೆ.
- ☐ ನಾನು ಅಪರಿಚಿತ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವುದಿಲ್ಲ ಅಥವಾ ಅಪರಿಚಿತರಿಂದ ಲಗತ್ತುಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವುದಿಲ್ಲ.
- ☐ ಅಪರಿಚಿತ ಜನರು ಸ್ನೇಹಪರವಾಗಿ ಕಂಡುಬಂದರೂ ಸಹ, ನಾನು ಅವರೊಂದಿಗೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಚಾಟ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸುತ್ತೇನೆ.
- ☐ ನಾನು ಸಾರ್ವಜನಿಕ ವೇದಿಕೆಗಳಲ್ಲಿ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು (ನನ್ನ ಶಾಲೆಯ ಹೆಸರು, ವಿಳಾಸ ಅಥವಾ ಫೋನ್ ಸಂಖ್ಯೆಯಂತಹ) ಎಂದಿಗೂ ಪೋಸ್ಟ್ ಮಾಡುವುದಿಲ್ಲ.
- ☐ ನಾನು ನನ್ನ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್, ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಮತ್ತು ಆಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ನಿಯಮಿತವಾಗಿ ನವೀಕರಿಸುತ್ತೇನೆ.
- ☐ ಅನುಚಿತವಾಗಿ ವರ್ತಿಸುವ ಬಳಕೆದಾರರನ್ನು ನಿರ್ಬಂಧಿಸುವುದು ಮತ್ತು ವರದಿ ಮಾಡುವುದು ಹೇಗೆ ಎಂದು ನನಗೆ ತಿಳಿದಿದೆ.
- ☐ ನಾನು ಹಂಚಿಕೊಳ್ಳುವ ಮೊದಲು ಯೋಚಿಸುತ್ತೇನೆ – ಎಲ್ಲವನ್ನೂ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪೋಸ್ಟ್ ಮಾಡುವ ಅಗತ್ಯವಿಲ್ಲ.
- ☐ ಸೈಬರ್‌ಬುಲ್ಲಿಂಗ್‌ನ ಅರ್ಥವನ್ನು ನಾನು ಅರ್ಥಮಾಡಿಕೊಂಡಿದ್ದೇನೆ ಮತ್ತು ಅದರಲ್ಲಿ ತೊಡಗಿಸಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸುತ್ತೇನೆ.
- ☐ ಬಳಕೆಯಲ್ಲಿಲ್ಲದಿದ್ದಾಗ ನಾನು ನನ್ನ ವೆಬ್‌ಕ್ಯಾಮ್ ಅನ್ನು ಮುಚ್ಚಿಡುತ್ತೇನೆ.
- ☐ ನಾನು ನಕಲಿ ಸಾಫ್ಟ್‌ವೇರ್ ಮತ್ತು ಆಟಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸುತ್ತೇನೆ.
- ☐ ನನಗೆ ಭಾರತದಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧ ಕಾನೂನುಗಳ ಬಗ್ಗೆ ಮೂಲಭೂತ ಅರಿವು ಇದೆ (ಐಟಿ ಕಾಯ್ದೆ, 2000).
- ☐ ನಾನು ಯಾವುದೇ ಅನುಮಾನಾಸ್ಪದ ಮಾಹಿತಿಯನ್ನು ವಿಶ್ವಾಸಾರ್ಹ ವಯಸ್ಕ ಅಥವಾ ಅಧಿಕಾರಿಗಳಿಗೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ವರದಿ ಮಾಡುತ್ತೇನೆ.
- ☐ ಸಾರ್ವಜನಿಕ ಅಥವಾ ಹಂಚಿಕೆಯ ಸಾಧನಗಳನ್ನು ಬಳಸಿದ ನಂತರ ನಾನು ಖಾತೆಗಳಿಂದ ಲಾಗ್ ಔಟ್ ಆಗುತ್ತೇನೆ.

www.cybersafegirl.com

ಸೈಬರ್ ಸುರಕ್ಷತಾ ಪರಿಶೀಲನಾಪಟ್ಟಿ

ಪೋಷಕರಿಗಾಗಿ

- ☐ ನನ್ನ ಮಗುವಿನೊಂದಿಗೆ ನಾನು ಅವರ ಆನ್‌ಲೈನ್ ಚಟುವಟಿಕೆ ಮತ್ತು ಸ್ನೇಹಿತರ ಬಗ್ಗೆ ನಿಯಮಿತವಾಗಿ ಮಾತನಾಡುತ್ತೇನೆ.
- ☐ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಏನಾದರೂ ತಪ್ಪಾದಲ್ಲಿ ತೀರ್ಪು ಇಲ್ಲದೆ ಮುಕ್ತ ಸಂವಹನವನ್ನು ನಾನು ಪ್ರೋತ್ಸಾಹಿಸುತ್ತೇನೆ.
- ☐ ನನ್ನ ಮಗು ಬಳಸುವ ಸಾಧನಗಳಲ್ಲಿ ನಾನು ಪೋಷಕರ ನಿಯಂತ್ರಣ ಪರಿಕರಗಳನ್ನು ಸ್ಥಾಪಿಸಿದ್ದೇನೆ.
- ☐ ನಾನು ಪರದೆಯ ಸಮಯವನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುತ್ತೇನೆ ಮತ್ತು ಸೂಕ್ತವಾದ ಬಳಕೆಯ ಮಿತಿಗಳನ್ನು ಹೊಂದಿಸುತ್ತೇನೆ.
- ☐ ನಾನು ನನ್ನ ಮಗುವಿನ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಸ್ಥಿತಿಯನ್ನು ಅನುಸರಿಸುತ್ತೇನೆ ಅಥವಾ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುತ್ತೇನೆ.
- ☐ ನಾನು ನನ್ನ ಮಗುವಿಗೆ ಗೌಪ್ಯತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳು ಮತ್ತು ಸುರಕ್ಷಿತ ಹಂಚಿಕೆಯ ಬಗ್ಗೆ ಕಲಿಸಿದ್ದೇನೆ.
- ☐ ಸೈಬರ್‌ಬುಲ್ಲಿಂಗ್ ಅಥವಾ ಆನ್‌ಲೈನ್ ನಿಂದನೆಯ ಸಂದರ್ಭದಲ್ಲಿ ದೂರುಗಳನ್ನು ಹೇಗೆ ವರದಿ ಮಾಡುವುದು ಮತ್ತು ಸಲ್ಲಿಸುವುದು ಎಂದು ನನಗೆ ತಿಳಿದಿದೆ (cybercrime.gov.in).
- ☐ ನನ್ನ ಮಗು ಬಳಸುತ್ತಿರುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಮತ್ತು ಆಟಗಳ ಬಗ್ಗೆ ನಾನು ನವೀಕೃತವಾಗಿರುತ್ತೇನೆ.
- ☐ ನಾನು ನನ್ನ ಮಗುವಿಗೆ ನಿಜ ಜೀವನದಲ್ಲಿ ಆನ್‌ಲೈನ್ ಅಪರಿಚಿತರನ್ನು ಎಂದಿಗೂ ಭೇಟಿಯಾಗಬಾರದು ಎಂದು ಕಲಿಸಿದ್ದೇನೆ.
- ☐ ಆನ್‌ಲೈನ್ ವಿಷಯ, ಮೀಮ್‌ಗಳು ಮತ್ತು ಫಾರ್ವರ್ಡ್‌ಗಳ ಬಗ್ಗೆ ವಿಮರ್ಶಾತ್ಮಕ ಚಿಂತನೆಯನ್ನು ಪ್ರೋತ್ಸಾಹಿಸುತ್ತೇನೆ.
- ☐ ನಾನು ಸುರಕ್ಷಿತ ವೈ-ಫೈ ಬಳಸುತ್ತೇನೆ ಮತ್ತು ಅತಿಥಿಗಳು ಅಥವಾ ನೆರೆಹೊರೆಯವರೊಂದಿಗೆ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸುತ್ತೇನೆ.
- ☐ ಡಿಜಿಟಲ್ ಯೋಗಕ್ಷೇಮವು ನಮ್ಮ ಮನೆಯ ಚರ್ಚೆಗಳ ಭಾಗವಾಗಿದೆ ಎಂದು ನಾನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳುತ್ತೇನೆ.
- ☐ ನಾನು ಉದಾಹರಣೆಯೊಂದಿಗೆ ಮುನ್ನಡೆಯುತ್ತೇನೆ – ಜವಾಬ್ದಾರಿಯುತ ಡಿಜಿಟಲ್ ನಡವಳಿಕೆಯನ್ನು ನಾನೇ ಅಭ್ಯಾಸ ಮಾಡುತ್ತೇನೆ.
- ☐ ಸಾಧ್ಯವಾದಾಗಲೆಲ್ಲಾ ನಾನು ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆಯ ಕುರಿತು ಕಾರ್ಯಾಗಾರಗಳು/ವೆಬಿನಾರ್‌ಗಳಿಗೆ ಹಾಜರಾಗುತ್ತೇನೆ.
- ☐ ತ್ವರಿತ ಉಪಯೋಗಕ್ಕಾಗಿ ನಾನು ತುರ್ತು ಸೈಬರ್ ಸಹಾಯವಾಣಿ ಸಂಖ್ಯೆಗಳನ್ನು ಸಂಗ್ರಹಿಸಿದ್ದೇನೆ.

ಸೈಬರ್ ಸುರಕ್ಷತಾ ಪರಿಶೀಲನಾಪಟ್ಟಿ

ಶಿಕ್ಷಕರಿಗಾಗಿ

- ☐ ನನ್ನ ತರಗತಿಯ ಚರ್ಚೆಗಳ ಭಾಗವಾಗಿ ನಾನು ಡಿಜಿಟಲ್ ಸುರಕ್ಷತೆಯನ್ನು ಸೇರಿಸುತ್ತೇನೆ.
- ☐ ನಾನು ವಿದ್ಯಾರ್ಥಿಗಳಿಗೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಮತ್ತು ವೈಯಕ್ತಿಕ ಗೌಪ್ಯತೆಯ ಬಗ್ಗೆ ಕಲಿಸುತ್ತೇನೆ.
- ☐ ನಾನು ವಿದ್ಯಾರ್ಥಿಗಳಿಗೆ ನಕಲಿ ಸುದ್ದಿ, ತಪ್ಪು ಮಾಹಿತಿ ಮತ್ತು ಡೀಪ್‌ಫೇಕ್‌ಗಳನ್ನು ಗುರುತಿಸಲು ಸಹಾಯ ಮಾಡುತ್ತೇನೆ.
- ☐ ಸೈಬರ್‌ಬುಲ್ಲಿಂಗ್ ಹೇಗೆ ಪ್ರಕಟವಾಗುತ್ತದೆ ಮತ್ತು ಹೇಗೆ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಕು ಎಂಬುದನ್ನು ನಾನು ಅರ್ಥಮಾಡಿಕೊಂಡಿದ್ದೇನೆ.
- ☐ ನಾನು ಗೌರವಾನ್ವಿತ ಆನ್‌ಲೈನ್ ಸಂವಹನ ಮತ್ತು ಡಿಜಿಟಲ್ ಪೌರತ್ವವನ್ನು ಪ್ರೋತ್ಸಾಹಿಸುತ್ತೇನೆ.
- ☐ ಸೈಬರ್ ಯೋಗಕ್ಷೇಮಕ್ಕೆ ಏಕೀಕೃತ ವಿಧಾನವನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ನಾನು ಪೋಷಕರೊಂದಿಗೆ ಸಹಕರಿಸುತ್ತೇನೆ.
- ☐ ನಾನು ಉದಯೋನ್ಮುಖ ಡಿಜಿಟಲ್ ಪ್ರವೃತ್ತಿಗಳ ಬಗ್ಗೆ (ಉದಾ. ಚಾಟ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು, ಗೇಮಿಂಗ್, AI ಪರಿಕರಗಳು) ನವೀಕೃತವಾಗಿರುತ್ತೇನೆ.
- ☐ ನಾನು ಪರವಾನಗಿ ಪಡೆದ ಶೈಕ್ಷಣಿಕ ಸಾಫ್ಟ್‌ವೇರ್ ಮತ್ತು ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳನ್ನು ಮಾತ್ರ ಬಳಸುತ್ತೇನೆ.
- ☐ ವೃತ್ತಿಪರ ಮತ್ತು ವೈಯಕ್ತಿಕ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳ ನಡುವೆ ಸ್ಪಷ್ಟವಾದ ಗಡಿಯನ್ನು ನಾನು ಕಾಯ್ದುಕೊಳ್ಳುತ್ತೇನೆ.
- ☐ ವಿದ್ಯಾರ್ಥಿಯನ್ನು ಒಳಗೊಂಡ ಸೈಬರ್ ಘಟನೆಯನ್ನು ಹೇಗೆ ವರದಿ ಮಾಡುವುದು ಮತ್ತು ಕ್ರಮ ವಹಿಸುವುದು ಎಂದು ನನಗೆ ತಿಳಿದಿದೆ.
- ☐ ನಾನು ಐಟಿ ಅಧ್ಯಾಪಕರು ಅಥವಾ ತಜ್ಞರ ಸಹಾಯದಿಂದ ಡಿಜಿಟಲ್ ಸಾಕ್ಷರತಾ ಅವಧಿಗಳನ್ನು ನಡೆಸುತ್ತೇನೆ.
- ☐ ಡಿಜಿಟಲ್ ಸಂಪನ್ಮೂಲಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವ ಮೊದಲು ಅವುಗಳ ದೃಢೀಕರಣವನ್ನು ನಾನು ಪರಿಶೀಲಿಸುತ್ತೇನೆ.
- ☐ ವಿದ್ಯಾರ್ಥಿಗಳು ಆನ್‌ಲೈನ್ ಕಾಳಜಿಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬಹುದಾದ ಸುರಕ್ಷಿತ ಸ್ಥಳವನ್ನು ನಾನು ರಚಿಸುತ್ತೇನೆ.
- ☐ ನಾನು ಪ್ರಮಾಣೀಕೃತ ಸೈಬರ್ ಜಾಗೃತಿ ಮತ್ತು ಸುರಕ್ಷತಾ ಕಾರ್ಯಕ್ರಮಗಳಿಗೆ ಹಾಜರಾಗುತ್ತೇನೆ.
- ☐ ಡಿಜಿಟಲ್ ಸಮಸ್ಯೆಗಳನ್ನು ಎದುರಿಸುವಾಗ ನಾನು ಗೌಪ್ಯತೆ ಮತ್ತು ಸೂಕ್ಷ್ಮತೆಯನ್ನು ಕಾಪಾಡಿಕೊಳ್ಳುತ್ತೇನೆ.

www.cybersafegirl.com

15 ಡಿಜಿಟಲ್ ಯೋಗಕ್ಷೇಮ & ಆರೋಗ್ಯ ಸಲಹೆಗಳು

ಋಷಿಕೇಶ್ ಉಪಾಧ್ಯಾಯ್, ಐಪಿಎಸ್ ರವರಿಂದ

1. **20–20–20 ನಿಯಮವನ್ನು ಅನುಸರಿಸಿ:** ಪ್ರತಿ 20 ನಿಮಿಷಗಳ ಸ್ಕ್ರೀನ್ ಟೈಮ್‌ನಲ್ಲಿ, ಕಣ್ಣಿನ ಒತ್ತಡವನ್ನು ಕಡಿಮೆ ಮಾಡಲು 20 ಅಡಿ ದೂರದಲ್ಲಿರುವ ಏನನ್ನಾದರೂ 20 ಸೆಕೆಂಡುಗಳ ಕಾಲ ನೋಡಿ.
2. **ನೀಲಿ–ಬೆಳಕಿನ ಬ್ಲಾಕಿಂಗ್ ಗ್ಲಾಸ್‌ಗಳನ್ನು ಬಳಸಿ:** ಡಿಜಿಟಲ್ ಕಣ್ಣಿನ ಒತ್ತಡವನ್ನು ಕಡಿಮೆ ಮಾಡಲು ಸಾಧನಗಳನ್ನು ಬಳಸುವಾಗ ನೀಲಿ–ಕಟ್ ಲೆನ್ಸ್‌ಗಳನ್ನು ಧರಿಸಿ, ವಿಶೇಷವಾಗಿ ಸಂಜೆ ಸಮಯದಲ್ಲಿ.
3. **ರಾತ್ರಿ ಮೋಡ್ ಅಥವಾ ಐ ಕಂಫರ್ಟ್ ಮೋಡ್ ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ:** ಹೆಚ್ಚಿನ ಸಾಧನಗಳು ಬೆಚ್ಚಗಿನ ಬೆಳಕಿನ ಫಿಲ್ಟರ್‌ಗಳನ್ನು ನೀಡುತ್ತವೆ – ಸೂರ್ಯಾಸ್ತದ ನಂತರ ಅವುಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ.
4. **ಕತ್ತಲೆಯಲ್ಲಿ ಪರದೆಗಳನ್ನು ತಪ್ಪಿಸಿ:** ಸಂಪೂರ್ಣ ಕತ್ತಲೆಯಲ್ಲಿ ಪರದೆಗಳನ್ನು ನೋಡಬೇಡಿ – ಇದು ನಿಮ್ಮ ಕಣ್ಣುಗಳನ್ನು ಆಯಾಸಗೊಳಿಸುತ್ತದೆ ಮತ್ತು ಮೆಲಟೋನಿನ್ ಉತ್ಪಾದನೆಯನ್ನು ಅಡ್ಡಿಪಡಿಸುತ್ತದೆ.
5. **ನೇರವಾದ ಭಂಗಿಯನ್ನು ಇಟ್ಟುಕೊಳ್ಳಿ:** ಕುತ್ತಿಗೆ ಮತ್ತು ಬೆನ್ನಿನ ಸಮಸ್ಯೆಗಳನ್ನು ತಪ್ಪಿಸಲು ನಿಮ್ಮ ಬೆನ್ನಿನ ಬೆಂಬಲದೊಂದಿಗೆ ನೇರವಾಗಿ ಕುಳಿತುಕೊಳ್ಳಿ ಮತ್ತು ಕಣ್ಣಿನ ಮಟ್ಟದಲ್ಲಿ ಪರದೆಯನ್ನು ಇರಿಸಿ.
6. **ಆಗಾಗ್ಗೆ ಮಿಟುಕಿಸಿ:** ಪರದೆಗಳನ್ನು ನೋಡುವಾಗ ಕಣ್ಣುಗಳು ಒಣಗುವುದನ್ನು ತಪ್ಪಿಸಲು ಪ್ರಜ್ಞಾಪೂರ್ವಕವಾಗಿ ಆಗಾಗ್ಗೆ ಕಣ್ಣುಗಳನ್ನು ಮಿಟುಕಿಸಿ.
7. **ತಂತ್ರಜ್ಞಾನ–ಮುಕ್ತ ವಿರಾಮಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳಿ:** ಯಾವುದೇ ಡಿಜಿಟಲ್ ಸಾಧನಗಳಿಲ್ಲದೆ ದಿನಕ್ಕೆ ಕನಿಷ್ಠ 30–60 ನಿಮಿಷಗಳನ್ನು ಕಳೆಯುವುದನ್ನು ನಿಗದಿಪಡಿಸಿ.
8. **ಮಲಗುವ ಮುನ್ನ 1 ಗಂಟೆ ಮೊದಲು ಡಿಜಿಟಲ್ ಪರದೆ ತಪ್ಪಿಸಿ:** ಮಲಗುವ ಮುನ್ನ ಪರದೆಗಳಿಗೆ ಒಡ್ಡಿಕೊಳ್ಳುವುದು ನಿಮ್ಮ ನಿದ್ರೆಯ ಗುಣಮಟ್ಟದ ಮೇಲೆ ಪರಿಣಾಮ ಬೀರಬಹುದು.
9. **ಸಾಧನಗಳನ್ನು ಮಲಗುವ ಕೋಣೆಯಿಂದ ಹೊರಗಿಡಿ:** ಆಳವಾದ ನಿದ್ರೆಯನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ನಿಮ್ಮ ಮಲಗುವ ಪ್ರದೇಶವನ್ನು ಗ್ಯಾಡ್‌ಜೆಟ್–ಮುಕ್ತ ವಲಯವನ್ನಾಗಿ ಮಾಡಿ.
10. **"ಅಡಚಣೆ ಮಾಡಬೇಡಿ" ಅಥವಾ ಫೋಕಸ್ ಮೋಡ್‌ಗಳನ್ನು ಬಳಸಿ:** ಇವು ನೀವು ಜಾಗರೂಕರಾಗಿರಲು ಮತ್ತು ನಿರಂತರ ಅಡಚಣೆಗಳನ್ನು ತಪ್ಪಿಸಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ.
11. **ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಸಮಯವನ್ನು ಮಿತಿಗೊಳಿಸಿ:** ನಿಮ್ಮ ಬಳಕೆಯನ್ನು ಟ್ರ್ಯಾಕ್ ಮಾಡುವ ಮತ್ತು ವಿರಾಮಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳಲು ನಿಧಾನವಾಗಿ ನೆನಪಿಸುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿ.
12. **ಹೈಡ್ರೇಟ್ ಆಗಿರಿ:** ನಿಯಮಿತವಾಗಿ ನೀರು ಕುಡಿಯಿರಿ – ಪರದೆಯ ಸಮಯವು ಜನರನ್ನು ಹೈಡ್ರೇಟೆಡ್ ಆಗಿರಲು ಮರೆಯುವಂತೆ ಮಾಡುತ್ತದೆ.
13. **ಕೋಣೆಯ ಬೆಳಕಿಗೆ ಹೊಂದಿಕೆಯಾಗುವಂತೆ ಪರದೆಯ ಹೊಳಪನ್ನು ಹೊಂದಿಸಿ:** ನಿಮ್ಮ ಪರಿಸರಕ್ಕೆ ವ್ಯತಿರಿಕ್ತವಾಗಿ ತುಂಬಾ ಪ್ರಕಾಶಮಾನವಾದ ಅಥವಾ ಮಂದ ಪರದೆಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ – ಇದು ಕಣ್ಣಿನ ಒತ್ತಡವನ್ನು ಕಡಿಮೆ ಮಾಡುತ್ತದೆ ಮತ್ತು ಗಮನವನ್ನು ಕಾಪಾಡಿಕೊಳ್ಳಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ.
14. **ಕಣ್ಣಿನ ವ್ಯಾಯಾಮಗಳನ್ನು ಅಭ್ಯಾಸ ಮಾಡಿ:** ಕಣ್ಣುಗಳನ್ನು ತಿರುಗಿಸುವುದು ಅಥವಾ ಅಂಗೈಯನ್ನು ಮುಚ್ಚಿಕೊಳ್ಳುವಂತಹ ಸರಳ ಚಟುವಟಿಕೆಗಳು ಒತ್ತಡವನ್ನು ನಿವಾರಿಸಬಹುದು.
15. **ಸ್ಟ್ರೆಚ್ & ಮೂವ್:** ರಕ್ತ ಪರಿಚಲನೆ ಸುಧಾರಿಸಲು ಪ್ರತಿ ಗಂಟೆಗೊಮ್ಮೆ ಎದ್ದು ಮೂಲಭೂತ ಸ್ಟ್ರೆಚ್‌ಗಳನ್ನು ಮಾಡಿ ಅಥವಾ ಸುತ್ತಲೂ ನಡೆಯಿರಿ.

www.cybersafegirl.com

ಅಪರಾಧಗಳು ಮತ್ತು ಸಂಬಂಧಿತ ದಂಡದ ಕಲಂಗಳು

ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯ್ದೆ, 2000 ದೊಂದಿಗೆ ಕೂಡಿಕೊಂಡಿರುವ ಸೈಬರ್ ಅಪರಾಧಗಳು ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ (ತಿದ್ದುಪಡಿ) ಕಾಯಿದೆ, 2008, ಐ.ಪಿ.ಸಿ/(**ಬಿಎನ್ಎಸ್–2023 ಒಳಗೊಂಡಂತೆ**) ಮತ್ತು ವಿಶೇಷ ಮತ್ತು ಸ್ಥಳೀಯ ಕಾನೂನುಗಳು.

ಕ್ರ.ಸ	ದೂರಿನ ಸ್ವರೂಪ	ಮಾತಕಾ 2000 & ಮಾತಕಾ(ತಿ) 2008 ರಡಿ ರನ್ವಯ ಕಲಂಗಳು ಮತ್ತು ಶಿಕ್ಷೆಗಳು	ಇತರೆ ಕಾನೂನಿನಡಿ ಅನ್ವಯವಾಗುವ ಕಲಂಗಳು ಮತ್ತು ಶಿಕ್ಷೆಗಳು
1	ಕಳುವಾದ/ಕಾಣೆ ಮೊಬೈಲ್ ಫೋನ್		ಐಪಿಸಿ ಕಲಂ 379/**ಬಿಎನ್ಎಸ್ 303(2)** 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವ ಎರಡೂ
2	ಕದ್ದ ಕಂಪ್ಯೂಟರ್/ಮೊಬೈಲ್ ಫೋನ್/ಡೇಟಾವನ್ನು ಸ್ವೀಕರಿಸುವುದು (ನಿಮ್ಮ ಒಡೆತನದ ಮೊಬೈಲ್ ಫೋನ್, ಡೇಟಾ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಬೇರೆಯವರ ಕೈಯಲ್ಲಿ ಕಂಡುಬಂದರೆ)	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಬಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ	ಐಪಿಸಿ ಕಲಂ 411/**ಬಿಎನ್ಎಸ್ 317(2)** 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವ ಎರಡೂ
3	ನಿಮ್ಮ ಅಥವಾ ನಿಮ್ಮ ಕಂಪನಿಯ ಒಡೆತನದ ಡೇಟಾವನ್ನು ಯಾವುದೇ ರೂಪದಲ್ಲಿ ಕದಿಯಲಾದರೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ	ಐಪಿಸಿ ಕಲಂ 379/**ಬಿಎನ್ಎಸ್ 303(2)** 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವ ಎರಡೂ
4	ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ಕದ್ದು ಮೋಸದ ಉದ್ದೇಶಕ್ಕಾಗಿ ಬೇರೆಯವರು ಬಳಸಿದರೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಸಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಡಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ	ಐಪಿಸಿ ಕಲಂ 419/**ಬಿಎನ್ಎಸ್ 319** 5 ವರ್ಷ ತನಕ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವಾ ಎರಡೂ ಐಪಿಸಿ ಕಲಂ 420/**ಬಿಎನ್ಎಸ್ 318** 7 ವರ್ಷ ತನಕ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವಾ ಎರಡೂ
5	ಪಾಸ್‌ವರ್ಡ್ ಬಳಸಿ ಒಬ್ಬರ ಇ–ಮೇಲ್ ಅನ್ನು ಮೋಸದಿಂದ ಬೇರೊಬ್ಬರು ಓದಿದರೆ/ಬಳಸಿದರೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಸಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ	
6	ಬಯೋಮೆಟ್ರಿಕ್ ಹೆಬ್ಬೆರಳಿನ ಗುರುತನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಂಡರೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಸಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ	
7	ವಿದ್ಯುನ್ಮಾನ ಸಹಿ ಅಥವಾ ಡಿಜಿಟಲ್ ಸಹಿ ದುರ್ಬಳಕೆಯಾದರೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಸಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ	
8	ಲಾಗಿನ್ ರುಜುವಾತುಗಳನ್ನು ಕೋರಿ ಫಿಶಿಂಗ್ ಇ–ಮೇಲ್ ಅನ್ನು ನಿಮ್ಮ ಹೆಸರಿನಲ್ಲಿ ಕಳುಹಿಸಿದರೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಡಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ	ಐಪಿಸಿ ಕಲಂ 419/**ಬಿಎನ್ಎಸ್ 319** 5 ವರ್ಷ ತನಕ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವಾ ಎರಡೂ
9	ಯಾವುದೇ ವ್ಯಕ್ತಿಯ ಒಪ್ಪಿಗೆ ಅಥವಾ ಜ್ಞಾನವಿಲ್ಲದೆ ಅವರ ಖಾಸಗಿ ಭಾಗದ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಇ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 2 ಲಕ್ಷ	ಐಪಿಸಿ ಕಲಂ 292/**ಬಿಎನ್ಎಸ್ 294** 2 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5000

www.cybersafegirl.com

	ಚಿತ್ರವನ್ನು ಸೆರೆಹಿಡಿಯುವುದು, ಪ್ರಕಟಿಸುವುದು ಅಥವಾ ರವಾನಿಸುವುದು.	ಮೀರದ ದಂಡ ಅಥವ ಎರಡೂ	ದಂಡ ಮತ್ತು ಎರಡನೆ ಬಾರಿ ಹಾಗು ನಂತರದ ದಂಡನೆಗಾಗಿ 5 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 10000
10	ಗಣಕಯಂತ್ರ ಮೂಲ ದಾಖಲೆಗಳನ್ನು ವಿರೂಪಗೊಳಿಸುವುದು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 65 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 2 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ	
11	ದತ್ತಾಂಶ ಮಾರ್ಪಾಡು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ	
12	ಅಪರಾಧಿಕ ಸಂದೇಶಗಳನ್ನು ಸಂವಹನ ಸೇವೆ, ಇತ್ಯಾದಿಗಳ ಮೂಲಕ ರವಾನಿಸುವುದು		ಐಪಿಸಿ ಕಲಂ 500/**ಬಿಎನ್ಎಸ್ 356(2)** 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ ಐಪಿಸಿ ಕಲಂ 504/**ಬಿಎನ್ಎಸ್ 352** 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ ಐಪಿಸಿ ಕಲಂ 506/**ಬಿಎನ್ಎಸ್ 351** 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ – ಬೆದರಿಗೆ ತೀವ್ರ ಗಾಯ ಅಥವಾ ಪ್ರಾಣ ಹಾನಿ ಇತ್ಯಾದಿ ಆದರೆ – 7 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ ಐಪಿಸಿ ಕಲಂ 507/**ಬಿಎನ್ಎಸ್ 351(4)** 2 ವರ್ಷ ಸಜೆ 506 ರ ಶಿಕ್ಷೆ ಜೊತೆ ಐಪಿಸಿ ಕಲಂ 508/**ಬಿಎನ್ಎಸ್ 354** 1 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ ಐಪಿಸಿ ಕಲಂ 509/**ಬಿಎನ್ಎಸ್ 79** 3 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ
13	ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಅಶ್ಲೀಲ ವಸ್ತುಗಳನ್ನು ಪ್ರಕಟಿಸುವುದು ಅಥವಾ ರವಾನಿಸುವುದು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 67 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಮತ್ತು ಎರಡನೆ ಬಾರಿ ಹಾಗು ನಂತರದ ದಂಡನೆಗಾಗಿ 5 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 10 ಲಕ್ಷ ದಂಡ	ಐಪಿಸಿ ಕಲಂ 292/**ಬಿಎನ್ಎಸ್ 294** 2 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5000 ದಂಡ ಮತ್ತು ಎರಡನೆ ಬಾರಿ ಹಾಗು ನಂತರದ ದಂಡನೆಗಾಗಿ 5 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 10000
14	ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಲೈಂಗಿಕ ಕ್ರಿಯೆಯನ್ನು ಚಿತ್ರಿಸುವ ವಸ್ತುಗಳನ್ನು ಪ್ರಕಟಿಸಿದರೆ ಅಥವಾ ರವಾನಿಸಿದರೆ ಶಿಕ್ಷೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 67ಎ 5 ವರ್ಷ ಕಾರಾಗೃಹ & 10 ಲಕ್ಷ ದಂಡ ಮತ್ತು ಎರಡನೆ ಬಾರಿ ಹಾಗು ನಂತರದ ದಂಡನೆಗಾಗಿ 7 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 10 ಲಕ್ಷ ದಂಡ	ಐಪಿಸಿ ಕಲಂ 292/**ಬಿಎನ್ಎಸ್ 294** 2 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5000 ದಂಡ ಮತ್ತು ಎರಡನೆ ಬಾರಿ ಹಾಗು ನಂತರದ ದಂಡನೆಗಾಗಿ 5 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 10000
15	ವಿದ್ಯುನ್ಮಾನ ರೂಪದಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಅಸ್ಪಷ್ಟ ಲೈಂಗಿಕ ಕ್ರಿಯೆಯಲ್ಲಿ ಚಿತ್ರಿಸುವ ವಸ್ತುಗಳನ್ನು ಪ್ರಕಟಿಸಿದರೆ ಅಥವಾ ರವಾನಿಸಿದರೆ ಶಿಕ್ಷೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 67ಬಿ 5 ವರ್ಷ ಕಾರಾಗೃಹ & 10 ಲಕ್ಷ ದಂಡ ಮತ್ತು ಎರಡನೆ ಬಾರಿ ಹಾಗು ನಂತರದ ದಂಡನೆಗಾಗಿ 7 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 10 ಲಕ್ಷ ದಂಡ	ಐಪಿಸಿ ಕಲಂ 292/**ಬಿಎನ್ಎಸ್ 294** 2 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5000 ದಂಡ ಮತ್ತು ಎರಡನೆ ಬಾರಿ ಹಾಗು ನಂತರದ ದಂಡನೆಗಾಗಿ 5 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 10000
16	ರಾಜ್ಯದ ವಿರುದ್ಧವಾಗಿ ಕಾರ್ಯ–ನಿರ್ವಹಿಸುವಂತ ವೈಫ್ಯೆ ಸಂಪರ್ಕವನ್ನು ದುರ್ಬಳಕೆ ಮಾಡುವುದು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66F	

www.cybersafegirl.com

		ಆಜೀವ ಕಾರಾಗೃಹ	
17	ರಾಜ್ಯದ ವಿರುದ್ಧವಾಗಿ ಕಾರ್ಯ–ನಿರ್ವಹಿಸುವಂತ ಗಣಕಯಂತ್ರ ವೈರಸ್ ಹರಿಬಿಡುವುದು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ 66F - ಆಜೀವ ಕಾರಾಗೃಹ	
18	ಸರ್ಕಾರಿ ಗಣಕಯಂತ್ರದ ವಿರುದ್ಧ ಸೇವಾ ನಿರಾಕರಣಾ ದಾಳಿ ನಡೆಸುವುದು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ 66F - ಆಜೀವ ಕಾರಾಗೃಹ	
19	ರಾಷ್ಟ್ರೀಯ ಭದ್ರತಾ ದೃಷ್ಟಿಕೋನದಿಂದ ಮಹತ್ವವನ್ನು ಹೊಂದಿರುವ ಸರ್ಕಾರಿ ಕಂಪ್ಯೂಟರ್‌ನಿಂದ ಡೇಟಾವನ್ನು ಕದಿಯುವುದು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 5 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ 66F - ಆಜೀವ ಕಾರಾಗೃಹ	
20	ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ನೆಟ್‌ವರ್ಕ್ ಮೂಲಕ ಹಾದುಹೋಗುವ ಎಲ್ಲಾ ಸಂವಹನಗಳನ್ನು ಡೀಕ್ರಿಪ್ಟ್ ಮಾಡಲು ಅಧಿಕಾರಿಗಳಿಗೆ ಅನುಮತಿಸದಿರುವುದು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 69 7 ವರ್ಷದವರೆಗೆ ಕಾರಾಗೃಹ & ದಂಡ	
21	ಮಧ್ಯವರ್ತಿಗಳು ತಮ್ಮ ಕಂಪ್ಯೂಟರ್‌ನಲ್ಲಿ ಸಂಗ್ರಹವಾಗಿರುವ ಮಾಹಿತಿಯನ್ನು ಸಂಬಂಧಿತ ಅಧಿಕಾರಿಗಳಿಗೆ ಪ್ರವೇಶಾವಕಾಶವನ್ನು ಒದಗಿಸದಿರುವುದು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 69 7 ವರ್ಷದವರೆಗೆ ಕಾರಾಗೃಹ & ದಂಡ	
22	ಆದೇಶದ ತರುವಾಯು ಜಾಲತಾಣವನ್ನು ನಿರ್ಬಂಧಿಸುವಲ್ಲಿ ವಿಫಲತೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 69ಎ 7 ವರ್ಷದವರೆಗೆ ಸಜೆ & ದಂಡ	
23	ಇ–ಮೇಲ್ ಮುಖಾಂತರ ಬೆದರಿಕೆ ಸಂದೇಶ ಕಳುಹಿಸುವುದು		ಐಪಿಸಿ ಕಲಂ 506/**ಬಿಎನ್‌ಎಸ್ 351** 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ
24	ಮಹಿಳೆಯ ಗಾಂಭೀರ್ಯವನ್ನು ಅವಮಾನಿಸುವ ಉದ್ದೇಶದ ಪದ, ಸನ್ನೆ ಅಥವಾ ಕ್ರಿಯೆ		ಐಪಿಸಿ ಕಲಂ 509/**ಬಿಎನ್‌ಎಸ್ 79** 3 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ
25	ಇ–ಮೇಲ್ ಮುಖಾಂತರ ಮಾನಹಾನಿ ಸಂದೇಶ ಕಳುಹಿಸುವುದು		ಐಪಿಸಿ ಕಲಂ 500/**ಬಿಎನ್‌ಎಸ್ 356(2** 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ
26	ನಕಲಿ ಜಾಲತಾಣ, ಸೈಬರ್ ವಂಚನೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಡಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ	ಐಪಿಸಿ ಕಲಂ 419/**ಬಿಎನ್‌ಎಸ್ 319** 5 ವರ್ಷ ತನಕ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವಾ ಎರಡೂ ಐಪಿಸಿ ಕಲಂ 420/**ಬಿಎನ್‌ಎಸ್ 318** 7 ವರ್ಷ ತನಕ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವಾ ಎರಡೂ
27	ಇ–ಮೇಲ್ ವಂಚನೆ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಸಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ ಅಥವ ಎರಡೂ	ಐಪಿಸಿ ಕಲಂ 465 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ ಐಪಿಸಿ ಕಲಂ 468 7 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ
28	ಸುಳ್ಳು ದಾಖಲೆ ಸೃಷ್ಟಿ	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಡಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ	ಐಪಿಸಿ ಕಲಂ 465/**ಬಿಎನ್‌ಎಸ್ 336(2)** 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ
29	ವಂಚನೆಯ ಉದ್ದೇಶಕ್ಕಾಗಿ ನಕಲು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಡಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ	ಐಪಿಸಿ ಕಲಂ 468/**ಬಿಎನ್‌ಎಸ್ 336(3)** 7 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ

www.cybersafegirl.com

		ದಂಡ	
30	ಪ್ರಖ್ಯಾತಿಗೆ ಹಾನಿ ಮಾಡುವ ಉದ್ದೇಶದಿಂದ ನಕಲು	ಮಾತಕಾ(ತಿ) 2008 ರ ಕಲಂ 66ಡಿ 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ 1 ಲಕ್ಷ ದಂಡ	ಐಪಿಸಿ ಕಲಂ 469/**ಬಿಎನ್ಎಸ್ 336(4)** 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ
31	ಇ–ಮೇಲ್ ದುರ್ಬಳಕೆ		ಐಪಿಸಿ ಕಲಂ 500/**ಬಿಎನ್ಎಸ್ 356(2)** 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ
32	ಅಪರಾಧಿಕ ಬೆದರಿಕೆಗಾಗಿ ಶಿಕ್ಷೆ		ಐಪಿಸಿ ಕಲಂ 506/**ಬಿಎನ್ಎಸ್ 351** 2 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ – ಬೆದರಿಗೆ ತೀವ್ರ ಗಾಯ ಅಥವಾ ಪ್ರಾಣ ಹಾನಿ ಇತ್ಯಾದಿ ಆದರೆ – 7 ವರ್ಷ ಸಜೆ/ದಂಡ/ಎರಡೂ
33	ಅನಾಮಧೇಯ ಸಂವಹನದಿಂದ ಅಪರಾಧಿಕ ಬೆದರಿಕೆ		ಐಪಿಸಿ ಕಲಂ 507/**ಬಿಎನ್ಎಸ್ 351(4)** 2 ವರ್ಷ ಕಾರಾಗೃಹ, 506 ರ ಶಿಕ್ಷೆ ಜೊತೆ
34	ಕೃತಿಸ್ವಾಮ್ಯ ಉಲ್ಲಂಘನೆ		ಕೃತಿಸ್ವಾಮ್ಯ ಕಾಯ್ದೆ 1957ರ ಕಲಂ 63, 63ಬಿ
35	ಗಣಕಯಂತ್ರ ಯಂತ್ರಾಂಶಗಳ ಕಳವು		ಐಪಿಸಿ ಕಲಂ 379/**ಬಿಎನ್ಎಸ್ 303(2)** 3 ವರ್ಷ ಕಾರಾಗೃಹ ಅಥವ ದಂಡ ಅಥವ ಎರಡೂ
36	ಮಾದಕ ವಸ್ತುಗಳ ಆನ್‌ಲೈನ್ ಮಾರಾಟ		ಎನ್.ಡಿ.ಪಿ.ಎಸ್ ಕಾಯ್ದೆ
37	ಶಸ್ತ್ರಾಸ್ತ್ರಗಳ ಆನ್‌ಲೈನ್ ಮಾರಾಟ		ಶಸ್ತ್ರಾಸ್ತ್ರ ಕಾಯ್ದೆ

ಹಕ್ಕು ನಿರಾಕರಣೆ: *ಮೇಲೆ ತಿಳಿಸಲಾಗಿರುವ ವಿವರಣೆಗಳು ನಮ್ಮ ಜ್ಞಾನ ಮತ್ತು ವ್ಯಾಖ್ಯಾನಗಳ ಅನುಗುಣವಾಗಿ ಮತ್ತು ಕೇವಲ ಶೈಕ್ಷಣಿಕ ಮತ್ತು ಮಾಹಿತಿಯ ಉದ್ದೇಶಕ್ಕಾಗಿ ಮಾತ್ರ. ಇವುಗಳನ್ನು ಉತ್ತಮ ಮಾರ್ಗದರ್ಶಿ ಶಕ್ತಿಯಾಗಿ ಬಳಸಬಹುದು. ಯಾವುದೇ ರೀತಿಯ ಕಲ್ಪನೆಯಿಂದ ಅವುಗಳನ್ನು ಕಾನೂನು ಅಭಿಪ್ರಾಯವೆಂದು ಪರಿಗಣಿಸಬಾರದು. ಶೈಕ್ಷಣಿಕ ಉದ್ದೇಶಕ್ಕಾಗಿ ಮಾತ್ರ ನಾವು ಈ ಮಾಹಿತಿಯನ್ನು ಅಪ್‌ಲೋಡ್ ಮಾಡಿರುವುದಾಗಿದ್ದು ನಾವು ನಮ್ಮ ಎಲ್ಲಾ ಪಾಲುದಾರರಿಗೆ ಕೃತಜ್ಞರಾಗಿರುತ್ತೇವೆ.*

www.cybersafegirl.com

ಆನ್‌ಲೈನ್ ದೂರು ನೀಡಲು

1. ರಾಷ್ಟ್ರೀಯ ಸೈಬರ್ ಕ್ರೈಂ ಪೋರ್ಟಲ್
   www.cybercrime.gov.in

2. ರಾಷ್ಟ್ರೀಯ ಮಹಿಳಾ ಆಯೋಗ
   www.ncw.gov.in
   ncwapps.nic.in

ಸಹಾಯವಾಣಿ ಸಂಖ್ಯೆಗಳು

ಸೈಬರ್ ಸಹಾಯವಾಣಿ	:	**1930**
ರಾಷ್ಟ್ರೀಯ ತುರ್ತು ಸಂಖ್ಯೆ	:	**112**
ಪೊಲೀಸ್	:	**100**
ಮಹಿಳಾ ಸಹಾಯವಾಣಿ	:	**1091**
ಮಹಿಳಾ ಕೌಟುಂಬಿಕೆ ದೌರ್ಜನ್ಯ ಸಹಾಯವಾಣಿ	:	**181**
ವಿದ್ಯಾರ್ಥಿ / ಮಕ್ಕಳ ಸಹಾಯವಾಣಿ	:	**1098**
ಮಾನಸಿಕ ಸ್ವಾಸ್ಥ್ಯ ಸಹಾಯವಾಣಿ	:	**1800-599-0019**
ಐಕಾಲ್ ಆತ್ಮಹತ್ಯ ಸಹಾಯವಾಣಿ	:	**9152987821**
ಅಗ್ನಿಶಾಮಕ	:	**101**
ಆಂಬ್ಯುಲೆನ್ಸ್	:	**102**
ವಿಪತ್ತು ನಿರ್ವಹಣಾ ಸೇವೆ	:	**108**

ರಾಷ್ಟ್ರೀಯ ಮಹಿಳಾ ಆಯೋಗ
ಕೌಟುಂಬಿಕ ದೌರ್ಜನ್ಯ, ಲೈಂಗಿಕ ದೌರ್ಜನ್ಯ & ಕಿರುಕುಳ:
78271 70170, 011-26942369, 26944754

ನಿಮ್ಮ ಹಿನ್ನುಣಿಕೆಯನ್ನು ಹೃದಯಪೂರ್ವಕವಾಗಿ ಸ್ವಾಗತಿಸುತ್ತೇವೆ!

ಸೈಬರ್ ಸೇಫ್ ಗರ್ಲ್‌ನ ಮುಂದಿನ ಸುಧಾರಿತ ಆವೃತ್ತಿ ತಯಾರಿಸಲು ನಮಗೆ ಸಹಾಯ ಮಾಡಿ

ನೀವು ಪುಸ್ತಕವನ್ನು ಓದಿದ ನಂತರ ಸುಧಾರಣೆಗಳನ್ನು, ಹೊಸ ವಿಷಯಗಳನ್ನು ಸೂಚಿಸಲು ಅಥವಾ ನಿಮ್ಮ ಸ್ವಂತ ಅನುಭವಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಬಯಸಿದರೆ, ದಯವಿಟ್ಟು ಇಲ್ಲಿಗೆ ಇಮೇಲ್ ಕಳುಹಿಸಿ

educatoranath@gmail.com
rajuaaryan90@gmail.com

ನಿಮ್ಮ ಸಲಹೆಗಳು ಈ ಧ್ಯೇಯವನ್ನು ಇನ್ನಷ್ಟು ಬಲಿಷ್ಠ ಮತ್ತು ಪರಿಣಾಮಕಾರಿಯಾಗಿಸುತ್ತವೆ !

ನೀವು ಪ್ರಮಾಣಪತ್ರ ಪಡೆದಿದ್ದೀರಾ ?

www.cybersafegirl.com

ಈ ಹಂತದಲ್ಲಿ 'ಸೈಬರ್ ಸೇಫ್ ಗರ್ಲ್' ಪುಸ್ತಕವನ್ನು ಪೂರ್ಣಗೊಳಿಸಿದ್ದೀರಿ. ಇನ್ನು ಒಂದು ಹೆಜ್ಜೆ ಮುಂದೆ ಹೋಗಿ ವಿವಿಧ ಬಗೆಯ ಸೈಬರ್ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ಹೆಚ್ಚು ತಿಳಿದುಕೊಳ್ಳುವ ಮತ್ತು ಪರೀಕ್ಷೆಯನ್ನು ತೆಗೆದುಕೊಳ್ಳುವ ಸಮಯ!

ಯಶಸ್ವಿಯಾಗಿ ಪೂರ್ಣಗೊಳಿಸಿದ ನಂತರ, **'ಸೈಬರ್‌ನಲ್ಲಿ ನಾನು ಸುರಕ್ಷಿತ'** ಪ್ರಮಾಣ ಪತ್ರ ಪಡೆಯುತ್ತೀರಿ. ಅದು **1** ವರ್ಷ ಮಾನ್ಯವಾಗಿರುತ್ತದೆ !

SURE PASS

CYBER PATRIOT

Indian Cyber Institute

CYBER JAGRITHI

Supported by

ISEA

Information Security Education & Awareness

ಮಗಳನ್ನು ರಕ್ಷಿಸಿ ಸೈಬರ್ ಅಪರಾಧದಿಂದ

ಸೈಬರ್ ಅಪರಾಧದ ಬಲಿಪಶು ಆಗದಿರಿ.

9 789334 000849

www.cybersafegirl.com

Be a #CyberSafeGirl