

ಸೈಬರ್ ವಾರ್ತಿಕೆ

Cyber Vartika



ಏಪ್ರಿಲ್ 2022 | April 2022



ಸೈಬರ್ ವರ್ತಿಕಾನ್ನು ನಿಮ್ಮ ಸ್ನೇಹಿತರು ನಿಮಗೆ ಕಳಿಸಿದ್ದಲ್ಲಿ, ಪ್ರತಿ ತಿಂಗಳು ಅದನ್ನು ನೇರವಾಗಿ ಪಡೆಯಲು, ನಮ್ಮ ಸುದ್ದಿಪತ್ರಿಕೆಯ ಮುಕ್ತ ಚಂದಾದಾರರಾಗಿ! <https://zcmp.in/BH6y>

If Cyber Vartika was forwarded to you by a friend, get it directly every month by SUBSCRIBING HERE!

<https://zcmp.in/BH6y>



[CySecK CoE](#)



[CySecK](#)



[@CySecKCoE](#)



[CySecK](#)



[CySecKCoE](#)



[CySecK](#)

# ಮುನ್ನುಡಿ /Foreword

ನಲ್ಮೆಯ ಓದುಗರೆ,

ಡಿಜಿಟಲ್ ವಿಧಾನದ ಅನುಸರಣೆ ಈ ದಿನದ ಆದ್ಯತೆಯಾಗಿದೆ. ನಮ್ಮ ಸುತ್ತಲಿನ ಪರಿಸರದಲ್ಲಿ ಹುಡುಕಾಟ ನಡೆಸುವ ಮೊದಲು, ಬೇಕಾದ ಯಾವುದೇ ವಸ್ತುವನ್ನು, ನಮ್ಮ ಡಿವೈಸ್‌ಗಳ ಮೂಲಕ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹುಡುಕುತ್ತಿದ್ದೇವೆ. ಇಂಟರ್‌ನೆಟ್ ಬಳಕೆ ವ್ಯಾಪಕವಾಗುತ್ತಿದ್ದಂತೆ, ಅದರ ಜೊತೆ ಬರುವ ಅಪಾಯಗಳು ಕೂಡ ಹೆಚ್ಚಾಗುತ್ತಿವೆ. ಗುರುತಿನ ಮಾರ್ಪಡಿಸುವಿಕೆ, ಮೋಸ ಮಾಡುವುದು, ಮೋಸಹೋಗುವುದು ಮತ್ತು ಅನಾನುಕೂಲತೆಗೆ ಈಡಾಗುವುದು ಸಾಮಾನ್ಯವಾಗಿಬಿಟ್ಟಿದೆ. ಹಣದ ಆಸೆಗೆ ಅಥವಾ ಬೇರೆ ಯಾವುದೇ ಕಾರಣಗಳಿಗೆ ತುತ್ತಾಗಿ ಈ ರೀತಿಯ ಚಟುವಟಿಕೆಗಳನ್ನು ಆಪಾದಿತರು ಮಾಡುತ್ತಿದ್ದಾರೆ. ಕ್ರಿಪ್ಟೋ ಕರೆನ್ಸಿಗಳ ಹೆಚ್ಚಾದ ಬಳಕೆಯ ಕಾರಣದಿಂದ, ಲೆಕ್ಕಕ್ಕೆ ಸಿಗುತ್ತಿರುವ ಮತ್ತು ಸಿಗದ ಹಣವೆಷ್ಟು ಎಂಬುದೇ ಚರ್ಚಾಸ್ಪದ ವಿಷಯವಾಗಿದೆ. ಈ ರೀತಿ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ಮಾಡುವವರಿಗೆ ಗಡಿಯ ಮಿತಿ ಇಲ್ಲದಂತಾಗಿದೆ. ಸಾಮಾನ್ಯ ಅಪರಾಧಗಳಲ್ಲಿ ಕಾನೂನು ಜಾರಿಮಾಡುವ ಮತ್ತು ತನಿಖೆ ಕೈಗೊಳ್ಳುವ ಏಜೆನ್ಸಿಗಳ ವ್ಯಾಪ್ತಿಯ ಮಿತಿಯಿಲ್ಲದೆ, ಈ ಕೃತ್ಯಗಳಿಗೆ ಯಾವುದೇ ರೀತಿಯ ತಡೆ ಇಲ್ಲದಂತಾಗಿವೆ.

ಸೈಬರ್ ಜಗತ್ತಿನ ಅಪಾಯಗಳನ್ನು ನಿರ್ವಹಿಸಲು ಬಹುಮುಖ ವಿಧಾನಗಳನ್ನು ಅನುಸರಿಸಬೇಕಾಗುತ್ತದೆ. ತಾಂತ್ರಿಕ ಅಭಿವೃದ್ಧಿಯಲ್ಲಿ ಇನ್ನಷ್ಟು ಪ್ರಗತಿ ತರುವ ಮೂಲಕ, ಸುರಕ್ಷತೆಯನ್ನು ವಿನ್ಯಾಸದಲ್ಲಿ ಮತ್ತು ವ್ಯವಸ್ಥೆಯ ಮೂಲದಲ್ಲಿಯೇ ಅಳವಡಿಸಬೇಕಾಗುತ್ತದೆ. ಈ ಕಾರ್ಯ ಸಾಧಿಸಬೇಕಾದರೇ, ಸಂಶೋಧನಾ ಸಾಮರ್ಥ್ಯದಲ್ಲಿ ಸುಧಾರಣೆ ತರಲೇಬೇಕು. ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ನಿರ್ವಹಿಸುವ ಸರ್ಕಾರಗಳ ಸಾಮರ್ಥ್ಯವು ಸಹ ಹೆಚ್ಚಾಗಬೇಕು. ಸದ್ಯ ವ್ಯವಸ್ಥೆಯಲ್ಲಿರುವ ಸಂಪನ್ಮೂಲಗಳನ್ನು ಅಂದರೆ ಟೂಲ್‌ಗಳನ್ನು ಇನ್ನೂ ಬಲಪಡಿಸುವ ಜೊತೆಗೆ, ವಿಶೇಷವಾಗಿ ಸೈಬರ್ ಅಪರಾಧಗಳಿಗೆ ಸಂಬಂಧಪಟ್ಟಂತೆ ತೊಂದರೆಗಳನ್ನು ನಿರ್ವಹಿಸಲು, ಕಾನೂನು ಚೌಕಟ್ಟಿನಲ್ಲೂ ವಿಸ್ತರಣೆಯನ್ನು ತರಬೇಕಾಗಿದೆ. ಧೀರ್ಘಾವಧಿಯಲ್ಲಿ ಸಾಂಸ್ಥಿಕ ಸ್ವರೂಪವನ್ನು ಮರುವಿನ್ಯಾಸಗೊಳಿಸುವುದು ಅವಶ್ಯಕವಾಗಿದೆ.

ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ತಡೆಗಟ್ಟಲು ಇರುವ ಮತ್ತು ಮುಂದೆಯೂ ಅನುಸರಣೆ ಮಾಡಬೇಕಾದ ಒಂದೇ ಒಂದು ವಿಧಾನ ಎಂದರೆ - ಜಾಗೃತಿ. ಯಾವುದೋ ತೊಂದರೆಗೆ ಒಳಗಾಗುವ ಅಥವಾ ಒಳಗಾಗಿರುವ ಜಾಗೃತಿ ಮನುಷ್ಯನಲ್ಲಿ ಮೂಡುವವರೆಗೂ, ಸೂಕ್ತ ಕ್ರಮ ತೆಗೆದುಕೊಳ್ಳಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲ. ಪ್ರತಿಯೊಬ್ಬರು, ಮುಂದೆ ಎದುರಾಗಬಹುದಾದ ಅನಾಹುತಗಳನ್ನು ಗ್ರಹಿಸುವ ಛಾಯೆಯನ್ನು ಬೆಳೆಸಿಕೊಳ್ಳುವ ಜೊತೆಗೆ, ಯಾವಾಗಲೂ ಜಾಗೃತರಾಗಿರಬೇಕು. ತೊಂದರೆ ಎದುರಾದಾಗ, ಸದ್ಯದ ಕಾರ್ಯವಿಧಾನಗಳ ಜಾಗೃತಿಯು ಸರ್ಕಾರ ಮಧ್ಯ ಪ್ರವೇಶಿಸಿ ಸೂಕ್ತ ಕ್ರಮಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳಲು ಬಹಳ ನೆರವಾಗುತ್ತವೆ. ಜಾಗೃತಿ ಮೂಡಿಸಲು, ಅದರಲ್ಲಿಯೂ, ಮಕ್ಕಳು ಮತ್ತು ಯುವಕ-ಯುವತಿಯರಲ್ಲಿ ಜಾಗೃತಿ ಮೂಡಿಸಲು, ಅವರಿಗೆ ಸರಿಯಾದ ಮಾಹಿತಿ ನೀಡುವುದು ತುಂಬಾ ಮುಖ್ಯ ಪಾತ್ರವಹಿಸುತ್ತದೆ.

ಈ ಕಾರ್ಯವನ್ನು ಕಳಕಳಿಯಿಂದ ಸೈಬರ್ ವಾರ್ತಿಕ ಮಾಡುತ್ತಾ ಬರುತ್ತಿರುವುದನ್ನು ನಾನು ತುಂಬಾ ಸಂತೋಷದಿಂದ ಗಮನಿಸಿದ್ದೇನೆ. ನಾನು ಸೈಸೆಕ್ ತಂಡದ ಈ ಕೆಲಸವನ್ನು ಹೃತ್ಪೂರ್ವಕವಾಗಿ ಮೆಚ್ಚುತ್ತೇನೆ ಮತ್ತು ಅವರ ಈ ಕೆಲಸಕ್ಕೆ ಇನ್ನಷ್ಟು ಮನ್ನಣೆ ದೊರೆಯಲಿ ಎಂದು ಆಶಿಸುತ್ತೇನೆ. ಪ್ರಸ್ತುತ ಸೈಬರ್ ವಾರ್ತಿಕ ಸಂಚಿಕೆ, ನಿಮ್ಮೆಲ್ಲರಿಗೂ ಸಮಯೋಚಿತವೆನ್ನಿಸಿ, ತುಂಬಾ ಇಷ್ಟವಾಗುತ್ತದೆ ಎಂದು ನಾನು ಖಾತರಿಪಡಿಸುತ್ತೇನೆ.

ಸೂರ್ಯ ಪ್ರಕಾಶ್ ಬಿ ಎಸ್

ಸಹವರ್ತಿ ಮತ್ತು ಕಾರ್ಯಕ್ರಮ ನಿರ್ದೇಶಕರು, ದಕ್ಷಿಣ

Dear Readers,

Digital first is the new normal. Even before we look for things around us, we search within our devices. With usage being so widespread, risks are only natural. Risks of identity theft, being defrauded, duped and just plain inconvenience. Perpetrators of such activities maybe motivated financially, or otherwise. With the rise of cryptos, what is financial and what is not is a debate by itself. Most importantly these perpetrators are able to operate with impunity beyond boundaries – boundaries that limit law enforcement and investigation agencies that tackle traditional crimes.

Handling risks in the cyber universe will necessarily have to be multi-pronged. The development of technology itself will have to evolve so as to include safety by design and a default. This will need improvement in research capacity. The capacity of the governments to handle cyber crimes will need to be increased. This would range from strengthening current institutions with more tools and people, expanding the legal framework to address issues unique to cyber crimes, and reimagining institutional structure required in the long term.

The most important tool to tackle cyber crimes is, and will remain, awareness. Unless one becomes aware that something has gone amiss, no redressal action will be initiated. One has to be awake to the possibility and be constantly on the vigil. User awareness of the modus operandi is critical for the government agencies to come in and take necessary action. Information plays a crucial role in building awareness – especially amongst children and youth.

It is with great pleasure I notice that CyberVaartika has been performing this role with enthusiasm for sometime now. I commend the team at CySecK and wish them ever wider reach. I am sure you will find this issue relevant and timely.

Surya Prakash B S

Fellow and Programme Director, DAKSH

# ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

## ವಂಚನೆ ಪ್ರಕರಣದಲ್ಲಿ ಸಿಕ್ಕಿಬಿದ್ದ ಖಾಸಗಿ ಸಾಲ ಸಂಸ್ಥೆಗಳು

ಬೆಂಗಳೂರು ಸೈಬರ್ ಕ್ರೈಮ್ ಪೊಲೀಸರು ಬರೋಬ್ಬರಿ ಒಂದು ಡಜನ್ ಖಾಸಗಿ ಕಂಪನಿಗಳನ್ನು ವಂಚನೆ ಪ್ರಕರಣದಲ್ಲಿ ಸೆರೆಹಿಡಿದಿದ್ದಾರೆ. ಈ ಉದ್ಯಮಗಳನ್ನು ಚೈನಾದ ಪ್ರಜೆಗಳು ನಿಯಂತ್ರಿಸುತ್ತಿದ್ದಾರೆ ಎಂದು ಹೇಳಲಾಗುತ್ತಿದ್ದು, ಅವರು ಸ್ಟಾರ್ಟ್‌ಫೋನ್ ಆಪ್‌ಗಳ ಮೂಲಕ ತ್ವರಿತ ಸಾಲ ಕೊಡುವುದಾಗಿ ನಂಬಿಸಿ ಅಮಾಯಕರಿಗೆ ಮೋಸ ಮಾಡುತ್ತಿದ್ದರು ಎಂದು ಕಂಡುಬಂದಿದೆ. ಫೆಬ್ರವರಿ 28 ಮತ್ತು ಏಪ್ರಿಲ್ 13ರ ನಡುವೆ, ಸೈಬರ್ ಕ್ರೈಮ್ ವಿಭಾಗವು ಇದಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ ಹತ್ತು ಪ್ರಕರಣಗಳನ್ನು ದಾಖಲಿಸಿದೆ.

ಶಂಕಿತ ಕಂಪನಿಗಳ ಪಟ್ಟಿಯಲ್ಲಿ ತೆಸೂಪಾ ಪ್ರೈ.ಲಿ., ಜಾಂಗ್ ಪ್ರೈ.ಲಿ., ಪೆನೋಲೋ ಪ್ರೈ.ಲಿ., ಮೊಸ್ಲಿ ಪ್ರೈ.ಲಿ., ಪಕೋಲಾ ಪ್ರೈ.ಲಿ., ಲೋಸ್ಕೂಪ್ ಪ್ರೈ.ಲಿ., ತಾಪ್ತಿಕಾ ಪ್ರೈ.ಲಿ., ಗೂಕೋ ಪ್ರೈ.ಲಿ., ಮೆನೇಸಿ ಪ್ರೈ.ಲಿ., ಸ್ಟಾರ್‌ಮೆಕ್ಸ್ ಪ್ರೈ.ಲಿ., ಜೋಲಿಚಿ ಪ್ರೈ.ಲಿ. ಹಾಗೂ ಯೂಮಿ ಇ-ಕಾಮರ್ಸ್ ಅಲಿಯಾಸ್ ಆಡ್‌ವ್ಯೂ ಟೆಕ್ನಾಲಜಿ ಪ್ರೈ.ಲಿ. ಸೇರಿವೆ.

## ಬೆಂಗಳೂರಿನಲ್ಲಿ ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿ ವಂಚಕರ ಬಂಧನ

ಹೆಚ್ಚಿನ ಬಡ್ಡಿಯ ಆಸೆ ತೋರಿಸಿ ಸಾವಿರಾರು ಹೂಡಿಕೆದಾರರಿಗೆ ಮಂಕುಬೂದಿ ಎರಚಿದ ಪ್ರಕರಣದಲ್ಲಿ ಒಬ್ಬ ಕ್ಯಾಬ್ ಡ್ರೈವರ್, ಒಬ್ಬ ಗುಜರಿ ವ್ಯಾಪಾರಿ ಮತ್ತು ಪೇಂಟರ್ ಹಾಗೂ ಒಬ್ಬ ಮೆಕ್ಯಾನಿಕ್ ಅನ್ನು ಬಂಧಿಸಲಾಗಿದೆ. ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿ ವ್ಯವಹಾರ ನಡೆಸುವ 'ಶೇರ್‌ಕ್ಯಾಶ್' ಕಂಪನಿಯ "ನಿರ್ದೇಶಕರ ಮಂಡಳಿ"ಯ ಸದಸ್ಯರಾಗಲು ಈ ಆರೋಪಿಗಳಿಗೆ 3 ಕೋಟಿ ರೂಪಾಯಿ ನೀಡಲಾಗಿದೆಯಂತೆ.

ಶೇರ್‌ಕ್ಯಾಶ್‌ನ ಸ್ಥಾಪಕರು ಮೊಬೈಲ್ ಮತ್ತು ಇಮೇಲ್ ಮೂಲಕ ಹೂಡಿಕೆದಾರರಿಗೆ ರಾಶಿರಾಶಿ ಮೆಸೇಜ್ ಕಳಿಸಿ, ನಿಮ್ಮ ಹಣವನ್ನು ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿ ವ್ಯಾಪಾರದಲ್ಲಿ ಹೂಡಿಕೆ ಮಾಡಿ ಎಂದು ಹೇಳುತ್ತಿದ್ದರು. ಹೂಡಿಕೆದಾರರು 'ಶೇರ್‌ಕ್ಯಾಶ್' ಆಪ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿಕೊಂಡು, ಹೂಡಿಕೆ ಶುರುಮಾಡಬೇಕಿತ್ತು ಎಂದು ಬೆಂಗಳೂರು ನಗರ ಪೊಲೀಸ್ ಆಯುಕ್ತರು ತಿಳಿಸಿದ್ದಾರೆ.

## ಆನ್‌ಲೈನ್ ವಂಚಕರಿಂದ ಕರ್ನಾಟಕದಲ್ಲಿ ಪ್ರತಿದಿನ ರೂ.19 ಲಕ್ಷ ವಂಚನೆ

ಕರ್ನಾಟಕದಲ್ಲಿ ಸೈಬರ್ ಕ್ರಿಮಿನಲ್‌ಗಳ ಹಾವಳಿ ವಿಪರೀತವಾಗಿದೆ. ಜನಸಾಮಾನ್ಯರೇ ಆಗಲಿ, ಸುಶಿಕ್ಷಿತರೇ ಆಗಲಿ ಅವರ ಮೋಸಜಾಲದಿಂದ ತಪ್ಪಿಸಿಕೊಳ್ಳಲು ಸಾಧ್ಯವಾಗುತ್ತಿಲ್ಲ. ಜನವರಿ 1, 2019ರಿಂದ ಫೆಬ್ರವರಿ 28, 2022ರ ನಡುವೆ ಸೈಬರ್ ವಂಚಕರು ಪ್ರತಿದಿನ 19 ರೂಪಾಯಿಯಷ್ಟು ದೋಚಿದ್ದಾರೆ ಎಂದು ಗೃಹ ಇಲಾಖೆಯ ದತ್ತಾಂಶಗಳು ಹೇಳುತ್ತಿವೆ.

ಕರ್ನಾಟಕದ ಗೃಹಮಂತ್ರಿ ಅರಗ ಜ್ಞಾನೇಂದ್ರ ಅವರು ಈ ಅಂಕಿಅಂಶಗಳನ್ನು ಇತ್ತೀಚೆಗಷ್ಟೇ ವಿಧಾನ ಪರಿಷತ್‌ನಲ್ಲಿ ಬಿಡುಗಡೆ ಮಾಡಿದರು.

## ನಿಷೇಧಿತ ಲೋನ್ ಆಪ್‌ಗಳು ಮತ್ತೊಂದು ರೂಪದಲ್ಲಿ ಪ್ರತ್ಯಕ್ಷ

ವಂಚನೆ ಮೊಕದ್ದಮೆಗಳಲ್ಲಿ ಆರೋಪಿಗಳಾಗಿದ್ದ ನಿಷೇಧಿತ ಲೋನ್ ಆಪ್‌ಗಳ ಪ್ರವರ್ತಕರು, ಪಟ್ಟುಬಿಡದೇ ಈ ವಲಯಕ್ಕೆ ಮತ್ತೆ ಮತ್ತೆ ಲಗ್ನಿ ಇಡುತ್ತಿದ್ದಾರೆ. ಆದರೆ ಈ ಸಲ ಅವರ ಲೋಕೇಶನ್‌ಗಳು ಬದಲಾಗಿವೆಯಷ್ಟೇ.

ಕೆಲವರು ಹೊಸ ಆಪ್‌ಗಳನ್ನು ಬಿಡುಗಡೆ ಮಾಡಿದ್ದು, ತಮಗೆ ಹಣ ಬಾಕಿ ಉಳಿಸಿಕೊಂಡಿರುವ ಗ್ರಾಹಕರನ್ನು ಪಿಡಿಸಲು ಸಿಬ್ಬಂದಿಯನ್ನು ನೇಮಿಸಿದ್ದಾರೆ. ಈ ಆಪ್‌ಗಳನ್ನು ಬೆಂಗಳೂರು ಮತ್ತು ದೆಹಲಿಯಿಂದ ನಿಯಂತ್ರಿಸಲಾಗುತ್ತಿದ್ದು, ತೆಲಂಗಾಣದ ಜನರು ಇವನ್ನು ಹೆಚ್ಚಾಗಿ ಬಳಸುತ್ತಿದ್ದಾರೆ.

## ರಸ್ತೆಯನ್ನೇ ಸೈಟ್ ಎಂದು ನಂಬಿಸಿದ್ದ ಮೂವರು ಬೆಂಗಳೂರು ಪೊಲೀಸರ ಬಲಿಗೆ

ದಾಖಲೆಗಳನ್ನು ತಿರುಚುವ ಮೂಲಕ ಸಾರ್ವಜನಿಕ ರಸ್ತೆಯನ್ನೇ ವಸತಿ ಪ್ರದೇಶ ಎಂದು ನಂಬಿಸಿ, ಅದರ ಮೇಲೆ ಸಹಕಾರಿ ಬ್ಯಾಂಕೊಂದರಲ್ಲಿ 50 ಲಕ್ಷ ಸಾಲ ಪಡೆದಿದ್ದ ಆರೋಪದಡಿ ಇಬ್ಬರು ಮಹಿಳೆಯರು ಹಾಗೂ ಒಬ್ಬ ಪುರುಷನನ್ನು ಬಂಧಿಸಲಾಗಿದೆ.

ಈ ವಂಚಕರು ಲೇಔಟ್ ಒಂದರ ಅನುಮೋದಿತ ಬ್ಲಾಕ್‌ಪಿಂಟ್ ಅನ್ನು ತಿರುಚಿ, ರಸ್ತೆಯನ್ನೇ ಮನೆ ಕಟ್ಟುತ್ತಿರುವ ಸೈಟ್ ಎಂದು ತೋರಿಸಿದ್ದರು. ನಕಲಿ ದಾಖಲೆಗಳ ಮೂಲಕ, ಆ ಪ್ಲಾಟ್‌ನ ನೋಂದಣಿಯನ್ನೂ ಮಾಡಿಸಿದ್ದರು. 2006ರಲ್ಲಿ, ಈ ಅಸ್ತಿಯನ್ನು ವ್ಯಕ್ತಿಯೊಬ್ಬರಿಗೆ ಮಾರಿ, ವಂಚಕರಲ್ಲಿ ಒಬ್ಬರು ಅದನ್ನು ಮತ್ತೆ ಖರೀದಿಸಿದ್ದರು. 2015ರಲ್ಲಿ ಬಿಬಿಎಂಪಿ ಅದರ ಖಾತಾ ರದ್ದುಗೊಳಿಸಿತು. ಆದರೆ ಈ ಎಲ್ಲಾ ವಿವರಗಳನ್ನು ಆರೋಪಿಗಳು ಬ್ಯಾಂಕಿನಿಂದ ಮುಚ್ಚಿಟ್ಟಿದ್ದಾರೆ. ಅವರ ಮೇಲೆ ವಂಚನೆ, ಕಳ್ಳ ರುಜು ಹಾಗೂ ಕ್ರಿಮಿನಲ್ ಪಿತೂರಿ ಪ್ರಕರಣಗಳನ್ನು ದಾಖಲಿಸಲಾಗಿದೆ.

## 16 ಯೂಟ್ಯೂಬ್ 'ನ್ಯೂಸ್' ಚಾನೆಲ್‌ಗಳನ್ನು ನಿಷೇಧಿಸಿದ ಭಾರತ ಸರ್ಕಾರ

ದೇಶದ ಭದ್ರತೆ, ವಿದೇಶಾಂಗ ವ್ಯವಹಾರಗಳು ಮತ್ತು ಸಾರ್ವಜನಿಕ ಸುವ್ಯವಸ್ಥೆಯ ಬಗ್ಗೆ ತಪ್ಪು ಮಾಹಿತಿ ಹಬ್ಬಿಸುತ್ತಿರುವ ಹಿನ್ನೆಲೆಯಲ್ಲಿ, ಭಾರತ ಸರ್ಕಾರದ ಮಾಹಿತಿ ಮತ್ತು ಸಂವಹನ ಸಚಿವಾಲಯವು 16 ಯೂಟ್ಯೂಬ್ 'ನ್ಯೂಸ್' ಚಾನೆಲ್‌ಗಳನ್ನು ನಿಷೇಧಿಸಿದೆ. ಸುಳ್ಳುಸುದ್ದಿ ಹಬ್ಬಿಸಲೆಂದೇ ಈ ಚಾನೆಲ್‌ಗಳನ್ನು ಬಳಸಲಾಗುತ್ತಿತ್ತು ಎಂದು ಕಂಡುಬಂದಿದೆ.

ಸಚಿವಾಲಯವು ತನ್ನ ಆಪತ್ಯಾಲೀನ ಅಧಿಕಾರವನ್ನು ಬಳಸಿ, ಡಿಸೆಂಬರ್ ಮತ್ತು ಜನವರಿ ನಡುವೆ 55 ಯೂಟ್ಯೂಬ್ ಚಾನೆಲ್‌ಗಳು ಹಾಗೂ ಹಲವಾರು ಟ್ವಿಟರ್ ಮತ್ತು ಫೇಸ್‌ಬುಕ್ ಖಾತೆಗಳ ಮೇಲೆ ನಿರ್ಬಂಧ ಹೇರಿದೆ.



# Top Cyber News

## **Private loan firms booked in cheating case**

Bengaluru cyber crime police have arrested a dozen private companies for defrauding. The businesses are supposedly controlled by Chinese nationals who prey on innocents by offering them immediate loans using smartphone apps. Between February 28 and April 13, the cybercrime unit recorded ten cases.

Tesupa Pvt Ltd, Zong Pvt Ltd, Pesolo Private Ltd, Mosli Pvt Ltd, Pakola Pvt Ltd, Loscoop Pvt Ltd, Taptica Pvt Ltd, Gooko Pvt Ltd, Menasi Pvt Ltd, Starmex Pvt Ltd, Jolichi Pvt Ltd, and Yoomi Ecommerce Allias Adviev Technology Pvt Ltd are among the suspected companies.

## **Loan apps that were blocked have resurfaced in a new guise**

Promoters of prohibited lending apps, against whom fraud lawsuits have been filed, are steadily re-entering the sector, albeit from different locations.

Some have launched new apps and employed personnel to harass clients who owe them money. The apps are run out of Bangalore and Delhi, with Telangana residents as users.

## **Fraudsters arrested for cryptocurrency fraud in Bengaluru**

A cab driver, a scrap merchant cum painter, and a mechanic arrested for duping several thousands of investors of money on the pretext of high interest. The accused received Rs 3 Crore as remuneration for becoming 'board of directors for 'ShareHash' company, dealing in cryptocurrency.

Bengaluru city police commissioner said the founder directors of ShareHash lured the investors through bulk messages sent on mobiles and emails displaying their money will be invested in the Crypto Currency business. Investors were to download the 'ShareHash' app and start investing.

## **Trio arrested for showing the road as a residential site in Bengaluru**

Two women and a man have been charged for forging documents to show a road as a residential area and mortgaging it to obtain a Rs 50 lakh loan from a cooperative bank.

The crooks had tampered with the layout's approved blueprint and depicted the road as a construction site. With forged paperwork, they were able to register the plot. In 2006, the property was sold to an individual, and one of the fraudsters later bought it. In 2015, the BBMP canceled its khata. However, these details were hidden from the bank by the suspects. A case of cheating, forgery, and criminal conspiracy has been filed against them.

## **Online scamsters dupe victims of Rs 19 lakh every day in Karnataka**

In Karnataka, cybercriminals have been on the run. Nobody seemed to be safe from them, whether they be vast groups of people or well-educated individuals. Between January 1, 2019 and February 28, 2022, scammers in Karnataka looted Rs 19 lakh per day from their victims, according to data from the home department.

Araga Jnanendra, the home minister, recently delivered the statistics to the legislative council.

## **Indian government blocks 16 YouTube 'news' channels**

India's Ministry of Information and Broadcasting blocked 16 YouTube "news" channels for allegedly promoting misinformation about the country's national security, foreign relations, and public order. It was discovered that these channels were being used to spread fake news.

The ministry utilised its emergency powers to restrict 55 YouTube channels, as well as several Twitter and Facebook accounts, in December and January.





# Online frauds ಆನ್‌ಲೈನ್ ಮೋಸಗಳು

## On the pretext of solving personal problems, 'astrologers' defraud a businessman of Rs 46 lakh.

The victim came across the scamsters through a website in August 2021. One of them promised to help him out with his problems. He also requested money from the victim under the guise of different pujas and ceremonies, to which the businessman transferred Rs 46 lakh in instalments from August 2021 to March 2022. The astrologers disappeared after receiving the money, and the victim subsequently approached the cybercrime police in this regard and lodged a complaint.

### ವೈಯಕ್ತಿಕ ಸಮಸ್ಯೆ ಬಗೆಹರಿಸುವುದಾಗಿ ನಂಬಿಸಿ, ವ್ಯಾಪಾರಸ್ಥನಿಂದ 46 ಲಕ್ಷ ದೋಚಿದ 'ಜ್ಯೋತಿಷಿಗಳು'

ಆಗಸ್ಟ್ 2021ರಲ್ಲಿ ವ್ಯಾಪಾರಿಯೊಬ್ಬರು ವೆಬ್‌ಸೈಟ್‌ನಿಂದ ಮೂಲಕ ಈ ವಂಚಕರ ಸಂಪರ್ಕಕ್ಕೆ ಬಂದರು. ಅವರಲ್ಲೊಬ್ಬ, ವ್ಯಾಪಾರಿಯ ಸಮಸ್ಯೆಗಳನ್ನು ಬಗೆಹರಿಸುವುದಾಗಿ ನಂಬಿಸಿದ್ದ. ಯಾವ್ಯಾವುದೋ ಪೂಜೆ-ಪುನಸ್ಕಾರಗಳ ಹೆಸರಿನಲ್ಲಿ ಅವರ ಬಳಿ ಹಣಕ್ಕಾಗಿ ಬೇಡಿಕೆ ಇಟ್ಟಿದ್ದ. ಆಗಸ್ಟ್ 2021ರಿಂದ ಮಾರ್ಚ್ 2022ರ ನಡುವೆ ಈ ವ್ಯಾಪಾರಿಯು ಹಲವಾರು ಕಂತುಗಳಲ್ಲಿ ಬರೋಬ್ಬರಿ 46 ಲಕ್ಷ ರೂಪಾಯಿಗಳನ್ನು ವಂಚಕರಿಗೆ ವರ್ಗಾಯಿಸಿದ್ದರು. ಹಣ ಪಡೆದ ವಂಚಕರು ತಲೆಮರೆಸಿಕೊಂಡಾಗ, ಆತಂಕಗೊಂಡ ವ್ಯಾಪಾರಿಯು ಸೈಬರ್‌ಕ್ರೈಮ್ ಪೊಲೀಸರನ್ನು ಸಂಪರ್ಕಿಸಿ ಪ್ರಕರಣ ದಾಖಲಿದ್ದರು.

## In a job scam in Bengaluru, a bus conductor was duped of Rs. 4 lakhs

After promising to secure her son a job at Yeshwanthpur railway station, a couple posing as a loco pilot and a helper with Southern Railways defrauded a woman of about 4 lakh in cash and gold.

### ಉದ್ಯೋಗ ಕೊಡಿಸುವುದಾಗಿ ನಂಬಿಸಿ ಬಸ್ ಕಂಡಕ್ಟರ್‌ಗೆ 4 ಲಕ್ಷ ವಂಚನೆ

ತಾವು ದಕ್ಷಿಣ ರೈಲ್ವೇಯ ಲೋಕೋಪೈಲಟ್ ಮತ್ತು ಹೆಲ್ಪರ್ ಎಂದು ಸುಳ್ಳು ಹೇಳಿಕೊಂಡ ಇಬ್ಬರು ವ್ಯಕ್ತಿಗಳು, ಮಹಿಳಾ ಬಸ್ ಕಂಡಕ್ಟರ್ ಮಗನಿಗೆ ಯಶವಂತಪುರ ರೈಲ್ವೇ ನಿಲ್ದಾಣದಲ್ಲಿ ಕೆಲಸ ಕೊಡಿಸುವುದಾಗಿ ನಂಬಿಸಿ, 4 ಲಕ್ಷ ಮೌಲ್ಯದ ಹಣ ಮತ್ತು ಒಡವೆಯೊಂದಿಗೆ ತಲೆಮರೆಸಿಕೊಂಡಿದ್ದಾರೆ.

## Man arrested for online investment scam

A 25-year-old MBA graduate has been charged with defrauding people online by promising to double their money. The accused set up a number of fake social media accounts and targeted people with fraudulent investment proposals. He is said to have gotten the idea for the online scam after being scammed out of Rs 5,000 under the pretence of having his online account verified.

### ಆನ್‌ಲೈನ್ ಹೂಡಿಕೆ ಹಗರಣದಲ್ಲಿ ಒಬ್ಬನ ಬಂಧನ

ನಿಮ್ಮ ಹಣವನ್ನು ಎರಡು ಪಟ್ಟು ಮಾಡಿಕೊಡುತ್ತೇನೆ ಎಂದು ನಂಬಿಸಿ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಜನರಿಗೆ ವಂಚಿಸುತ್ತಿದ್ದ 25 ವರ್ಷದ ಎಂಬಿವ ಪದವೀಧರನ ಮೇಲೆ ಪ್ರಕರಣ ದಾಖಲಾಗಿದೆ. ಆರೋಪಿಯು ಹಲವಾರು ನಕಲಿ ಸೋಶಿಯಲ್ ಮೀಡಿಯಾ ಖಾತೆಗಳನ್ನು ಸೃಷ್ಟಿಸಿ, ಸಾಕಷ್ಟು ಜನರ ಜೊತೆ ಈ ಹೂಡಿಕೆಯ ಬಗ್ಗೆ ಮಾತಾಡಿದ್ದ. ಆನ್‌ಲೈನ್ ಖಾತೆಯ ವರಿಫಿಕೇಶನ್ ಹೆಸರಿನಲ್ಲಿ ತನ್ನ ಬಳಿಯಿದ್ದ 5000 ರೂಪಾಯಿ ಕಳೆದುಕೊಂಡ ಬಳಿಕ, ಆರೋಪಿಗೆ ಇಂತಹದೊಂದು ಆನ್‌ಲೈನ್ ಹಗರಣದ ಉಪಾಯ ಹೊಳೆದಿದೆ ಎಂದು ಹೇಳಲಾಗುತ್ತಿದೆ.



# ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು

## Awareness Posters



### ಕುಟುಂಬದ ಇಂಟರ್ನೆಟ್ ಸುರಕ್ಷತೆಗೆ ಪರಿಶೀಲನಾ ಪಟ್ಟಿ

	ಇಂಟರ್ನೆಟ್ ಸುರಕ್ಷತೆ ಸಲಹೆಗಳು	12 ವರ್ಷದೊಳಗಿನ ಮಕ್ಕಳಿಗೆ	ಯುವಕರಿಗೆ (13-19)	ಪೋಷಕರಿಗೆ
	ಇಂಟರ್ನೆಟ್‌ನ ಅಪಾಯಗಳ ಬಗ್ಗೆ ಅರಿತುಕೊಳ್ಳಿ	✓	✓	✓
	ಇಂಟರ್ನೆಟ್‌ನಲ್ಲಿ ಸಿಗುವ ಕಂಡ-ಕಂಡ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ	✓	✓	✓
	ಹಂಚಿಕೊಂಡು ಅಕೌಂಟ್‌ಬಳಸುವುದನ್ನು ನಿಲ್ಲಿಸಿ	✓	✓	✓
	ಅಪರಿಚಿತರ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ	✓	✓	✓
	ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿ ಎಲ್ಲವನ್ನೂ ಹಂಚಿಕೊಳ್ಳುವುದು ಬೇಡ		✓	✓
	ಸುರಕ್ಷಿತ ವೆಬ್‌ಸೈಟ್‌ಗಳಿಂದ ಮಾತ್ರ ಖರೀದಿ ಮತ್ತು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ		✓	✓
	ಪೈವೆಸಿ/ಗೌಪ್ಯತೆ ಸೆಟ್ಟಿಂಗ್‌ಗಳ ಬಗ್ಗೆ ಅರಿತುಕೊಳ್ಳಿ		✓	✓
	ಇಂಟರ್ನೆಟ್ ಸಂಪರ್ಕವನ್ನು ಸುರಕ್ಷಿತವಾಗಿ			✓
	ನಿಮ್ಮ ಡೆಬಿಟ್/ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಮಾಹಿತಿಯನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಎಂದಿಗೂ ಸೇವ್ ಮಾಡಬೇಡಿ			✓
	ಆನ್‌ಲೈನ್ ಸೆಕ್ಯೂರಿಟಿಯ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ			✓

 **ಸೌಕರ್ಯ**  
ಸೈಬರ್ ಸೆಕ್ಯೂರಿಟಿ ಕರ್ನಾಟಕ

ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ




# ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು



## Awareness Posters

### INTERNET SAFETY CHECKLIST FOR FAMILY

	INTERNET SAFETY TIPS	For Kids (less than 12yrs)	For Teenagers (13-19yrs)	For Parents
	Know the dangers of the Internet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Never click random links on the Internet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Avoid using a shared account	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Beware of strangers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Avoid sharing too much on social media		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Shop or download from secure websites only		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Know the privacy settings		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Never save your debit/credit card information online			<input checked="" type="checkbox"/>
	Keep Internet connection secure			<input checked="" type="checkbox"/>
	Monitor online security			<input checked="" type="checkbox"/>







# ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು

## Awareness Posters






ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ  
ಸೈಬರ್ ಸೆಕ್ಯೂರಿಟಿ ಕರ್ನಾಟಕ



**ಸಿಮ್ ಮಾರ್ಪಡಿಸಿ ವಂಚಿಸುವ ಜನರಿದ್ದಾರೆ ಜೋಕೆ**




**ಹೆಲೋ, ಜೋಸೆಫ್ ಅವರಾ! ನಾನು ಸುರೇಶ್. "XYZ" ಮೊಬೈಲ್ ಸೇವೆ ಸಂಸ್ಥೆ ಇಂದ ಪೋನ್ ಮಾಡ್ತಾ ಇದ್ದೆನಿ. ನಿಮ್ಮ ಪೋನ್‌ನಲ್ಲಿ ಇರೋ ಸಿಮ್ ಕಾರ್ಡ್ ತುಂಬಾ ಹಳೆಯದಿದೆ. ನಿಮ್ಮ ಬದಲಾಗಿರೋ ಬಾಕಿರಿ ಪ್ರಕಾರ, ನಿಮ್ಮ ನಿಮ್ಮ ಸಿಮ್ ಕಾರ್ಡ್‌ನ ಅಬಾಕೋಟೆ ಮಾರ್ಪಡಿಸಿಕೊಳ್ಳುತ್ತೇ. ಇಲ್ಲದೆ ಹೋದರೆ, ನಿಮ್ಮ ಸೇವಾಕಾರ್ಡ್ ಹನ್ನೆರಡು ಒದ್ದಾಡಬೇಕಾಗುತ್ತೆ. ಇದನ್ನು ತಪ್ಪಿಸಿಕೊಳ್ಳಲು ನಾನು ನಿಮಗೆ ಈಗ ಕಳಿಸಿಕೊಡೋ ರೀಟ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಿ. ನಿಮ್ಮ ಆಕಸ್ಮಿಕವಾಗಿ ಗಳಿಸುವಂತೆ ಸಲ್ಲಿಸಿ.**

**ಓಹೋ! ನನಗೆ ಇದರ ಬಗ್ಗೆ ಗೊತ್ತಿಲ್ಲ. ಇರಲಿ, ನಾನಿಗಾಗಿ ಬೇಕಾದ ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳನ್ನು ಮಾರ್ಪಡಿಸಿ ಮುಕ್ತಿಸಿ.**

**ಕೆಲವು ದಿನಗಳ ನಂತರ....**

**ನನ್ನ ಪೋನ್‌ನಲ್ಲಿ ಯಾಕೋ ನೆಟ್ ವರ್ಕ್ ಇಲ್ಲಲ್ಲ! ನಾಲ್ಕು ಕಾಲ್ ಮಾಡ್ ಮಾಡೋದಕ್ಕೆ ಆಗ್ತಿಲ್ಲ. ಯಾವ ಕಾಲ್ ಕೂಡ ಬರ್ತಾ ಇಲ್ಲ.**

**ನಾನೇ ಜೋಸೆಫ್ ಅವರ ಹೆಸರಿನಲ್ಲಿ ಮೊಬೈಲ್ ಸೇವೆ ನೀಡೋದ ಹತ್ತಿರ ಹೋಗಿ. ಜೋಸೆಫ್ ಅವರ ಹತ್ತಿರ ಸುಳ್ಳು ಹೇಳಿ ಕೊಡೊಂದಿದ್ದೆ. ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳನ್ನು ಕೊಟ್ಟು ಸಿಮ್ ಬದಲಾವಣೆ ಮಾಡಿ ಕೊಡೋದಕ್ಕೆ ರಿಕ್ವೆಸ್ಟ್ ಮಾಡ್ತೆ. ಸೇವೆ ನೀಡೋರು ಹಿಂದಿನ ಸಿಮ್ ರಿಕ್ವೆಸ್ಟ್‌ನಿಗಾಗಿ ಮಾದ್ರಿ. ನಾನೇ ಜೋಸೆಫ್ ಅವರ ಪ್ರಸಾರ ನನಗೆ ಹೊಸ ಸಿಮ್ ಕಾರ್ಡ್ ಕೊಟ್ಟು, ಈಗ ಅವರಿಗೆ ಹೋಲಬೇಕಾದ OTP ಮತ್ತೆ ಹೇಗಾದ ವಹಿವಾಟಿನ ಮಾಹಿತಿಗಳನ್ನು ನೀಡಬೇಕಿ ನನಗೆ ಬರ್ತದೆ.**





**\*ವಂಚನೆ ಮಾಡುವವರು ಬ್ಯಾಂಕ್ ಅಕೌಂಟ್ ಗೆ, ಲಿಂಕ್ ಆಗಿರುವ ನಿಮ್ಮ ಸೋಲಾದಾಯಕ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಯ ನೆಲೆ ಸಿಮ್ ಕಾರ್ಡ್ (ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸಿಮ್ ಕಾರ್ಡ್ ಸಹಿತ) ಅನ್ನು ನಿಮ್ಮ ಹಿಂದಿನ ಸಿಮ್‌ಗೆ ಅಕ್ಟಿವ್ ಗಳಿಸಿಕೊಳ್ಳುವ ಪರಿಶ್ರಮವನ್ನು ಮಾಡಿ.**

**\*ಈ ರೀತಿ ಸಮಾಜವನ್ನು ವಂಚಿಸುತ್ತಿರುವ ಸಾಂಕ್ರಿಯ ವಿದಾನಗಳಾದ ವಿಶಿಂಗ್, ಫಿಶಿಂಗ್ ಮತ್ತು ಸ್ವಿಪಿಂಗ್‌ನಿಂದ ಬಹಳ ಜಾಗರೂಕರಾಗಿರಿ.**


**ಇಂತಹ ವಿದಾನಗಳನ್ನು ಬಳಸಿಕೊಳ್ಳುವ ವಂಚಿತರು ಜನರ ವೈಯಕ್ತಿಕ ಮತ್ತು ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಕದಿಯುತ್ತಾರೆ.**

- ನಿಮ್ಮ ಫೋನ್ ಸಂಬರ್ ಇನ್‌ಸೈಕ್ರಿಪ್ಟ್ ಆದರೆ ಅದರ ವ್ಯಾಪ್ತಿ ಪ್ರದೇಶದ ಬಳಗಿಲ್ಲದ ಹೋದರೆ, ನಿಮ್ಮ ಮೊಬೈಲ್ ಸೇವಾಪಾಲಿಕೆಯ ಪರಿಶೀಲಿಸಿಕೊಳ್ಳಿ.
- #ಸೈಬರ್‌ಸುರಕ್ಷತೆ ಮತ್ತು #ಸೈಬರ್‌ಅರಿವು ಪಡೆದುಕೊಳ್ಳಿ.


 @CySeckCoE



K-Tech CoE for Cyber Security  
Cyber Security Karnataka



**BEWARE OF SIM SWAP FRAUDS**




**Hello Mr. Joseph, I am Suresh, calling from "XYZ" service provider. The SIM you have on your phone is old, and according to our updated policy, you will have to upgrade your SIM; otherwise, you will lose access to your network. To avoid this, you will have to resubmit your documents by clicking on the link I am sending now.**

**I was not aware of this! I will submit the documents right away.**


**After a few days...**

**Why do I have no network on my phone? I can't make any calls, nor am I receiving any.**

**I approached the service provider posing as Mr. Joseph with his documents and requested for swim swap. The service provider deactivated the sim and gave me a new one. I can get all the OTPs and financial alerts directly.**



- "Fraudsters may obtain a duplicate SIM card (including electronic SIM) for the registered mobile number linked to the customer's bank account by gaining access to the customer's SIM card.
- Be wary of social engineering techniques such as vishing, phishing, and smishing, which try to steal your personal and confidential information.
- Check with your service provider if your phone number is inactive or out of range.
- Stay #cybersecure and #cyberaware

 @CySeckCoE



# ಸೈಸಿಕ್ ಜಾಗೃತಿ ಭಂಡಾರ

## ಗುರುತು ನಿರ್ವಹಣಾ ದಿನ

12 ಏಪ್ರಿಲ್ 2022

ಗುರುತು ನಿರ್ವಹಣಾ ದಿನವನ್ನು ಡಿಜಿಟಲ್ ಗುರುತುಗಳ ನಿರ್ವಹಣೆ ಮತ್ತು ಭದ್ರತೆಯ ಬಗ್ಗೆ ಅರಿವು ಮೂಡಿಸಲು ಏಪ್ರಿಲ್ ತಿಂಗಳ ಎರಡನೇ ಮಂಗಳವಾರ ಆಚರಿಸಲಾಗುತ್ತದೆ.

### ಗುರುತು ನಿರ್ವಹಣಾ ದಿನ ಏಕೆ ಮುಖ್ಯವಾಗುತ್ತದೆ?

ಎಲ್ಲರಿಗೂ ಒಂದು ಡಿಜಿಟಲ್ ಗುರುತು ಇದ್ದು, ಅದರಲ್ಲಿ ಸವಿಸ್ತಾರವಾದ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಇರುತ್ತದೆ. ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿನ ನಿಮ್ಮ ಪ್ರೊಫೈಲ್, ಸರ್ಚ್ ಇಂಜಿನ್ ಇತಿಹಾಸ ಅಥವಾ ಈಮೇಲ್ ಅಕೌಂಟ್‌ಗಳು, ಹೀಗೆ ಯಾವುದೇ ಮೂಲಗಳಿಂದ ದೊರೆಯುವ ಮಾಹಿತಿಗಳು, ಹ್ಯಾಕರ್‌ಗಳಿಗೆ ತುಂಬಾ ಸಹಾಯಕವಾಗುತ್ತವೆ. ಅದೃಷ್ಟವಶಾತ್, ಈ ಕೆಳಗಿನ ಕೆಲವು ರೂಢಿಗಳು ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಗುರುತುಗಳ ಭದ್ರತೆಯನ್ನು ಹೆಚ್ಚಿಸಲು ದಾರಿ ಮಾಡಿಕೊಡುತ್ತವೆ. ಅವು ಯಾವುವೆಂದರೆ:



#### ಮಲ್ಟಿ ಫ್ಯಾಕ್ಟರ್ ಅಥೆಂಟಿಕೇಶನ್

ಮಲ್ಟಿ ಫ್ಯಾಕ್ಟರ್ ಅಥೆಂಟಿಕೇಶನ್‌ಬಹಳ ಸುರಕ್ಷಿತ ದೃಢೀಕರಣ ವಿಧಾನಗಳನ್ನು ಅಂದರೆ, ಬಯೋಮೆಟ್ರಿಕ್ ದೃಢೀಕರಣ ಅಥವಾ ನಿಮ್ಮ ಫೋನ್ ಅಥವಾ ಮೊಬೈಲ್ ಸಾಧನಕ್ಕೆ ಕಳಿಸಿಕೊಡಲಾಗುವ ಒನ್-ಟೈಮ್ ಕೋಡ್ ವ್ಯವಸ್ಥೆಯ ಮೂಲಕ, ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಅಕೌಂಟ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿಸುತ್ತದೆ.



#### ಡೀಫಾಲ್ಟ್ ಕ್ರೆಡೆನ್ಷಿಯಲ್ ಗಳನ್ನು ಬದಲಾಯಿಸಿ

ವೈಫೈ ರೂಟರ್, IoT ಸಾಧನ ಮುಂತಾದವುಗಳನ್ನು ಡೀಫಾಲ್ಟ್ ಹಾಂಫಿಗರೇಶನ್‌ಗಳು ಅಂದರೆ ಎಲ್ಲಾ ಸಾಧನಗಳ ಸಾಮಾನ್ಯ ರೂಪುರೇಖೆ ಎನ್ನಬಹುದಾದ ಅಡ್ಡಿನ ಅಕೌಂಟ್‌ಗಳ ಪಾಸ್‌ವರ್ಡ್ ರೀತಿಯ ಮಾಹಿತಿ ಸಹಿತ ಮಾರಾಟ ಮಾಡಲಾಗುತ್ತದೆ. ಅದನ್ನು ಬದಲಾಯಿಸುವವರೆಗೂ, ಈ ಸಾಧನ ಇಂಟರ್‌ನೆಟ್‌ಗೆ ಕನೆಕ್ಟ್ ಆದಾಗ, ಹ್ಯಾಕರ್‌ಗಳು ಮುಂಚಿತವಾಗಿ ಇದ್ದಂತೆ ಅಡ್ಡಿನ ಅಕೌಂಟ್ ಕ್ರೆಡೆನ್ಷಿಯಲ್‌ಗಳೊಂದಿಗೆ ಲಾಗಿನ್ ಆಗಿ, ಆ ಸಾಧನವನ್ನು ತಮ್ಮ ನಿಯಂತ್ರಣಕ್ಕೆ ತೆಗೆದುಕೊಳ್ಳಬಹುದು. ಇಂಟರ್‌ನೆಟ್‌ಗೆ ಸಂಪರ್ಕ ಹೊಂದಿರುವ ನಿಮ್ಮ ಎಲ್ಲಾ ಸಾಧನಗಳನ್ನು ಡೀಫಾಲ್ಟ್ ಕ್ರೆಡೆನ್ಷಿಯಲ್‌ಗಳು ಬದಲಾವಣೆ ಆಗಿವೆ ಎಂಬುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.



#### ಯಾವುದೇ ಕ್ಲಿಕ್ ಮಾಡುವ ಮುನ್ನ ಯೋಚಿಸಿ

ಈಮೇಲ್ ಅಥವಾ ಎಸ್‌ಎಂಎಸ್ ಮೂಲಕ ಬರುವ ಆಕರ್ಷಕ ಸಂದೇಶಗಳಿಗೆ ಮರುಳಾಗಿ, ಬುದ್ಧಿವಂತಿಕೆ ಇಂದ ವಿಚಾರ ಮಾಡದೆ, ಕಂಡ-ಕಂಡ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ. ಅದರ ಬದಲು, ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಸ್ವತಃ ಭೇಟಿಕೊಟ್ಟು, ಅದರ ಅಸಲೀತನವನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ಸೈಬರ್ ದಾಳಿಕೋರರು ಯಾವಾಗಲೂ, ಫಿಶಿಂಗ್ ಈಮೇಲ್‌ಗಳು ಮತ್ತು ಎಸ್‌ಎಂಎಸ್ ಸಂದೇಶಗಳ ಮೂಲಕ ಜನರಿಗೆ ತಪ್ಪು ದಾರಿ ತೋರಿಸಿ, ಅವರ ಯೂಸರ್ ನೇಮ್ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್ ಹಂಚಿಕೊಳ್ಳುವಂತೆ ಅಥವಾ ಮಾಲ್ ವೇರ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿಕೊಳ್ಳುವಂತೆ ಮಾಡುತ್ತಾರೆ.



#### ಪ್ರತಿ ಸೇವೆ ಪಡೆದುಕೊಳ್ಳುವಾಗಲೂ ಭಿನ್ನವಾದ, ಸ್ಟ್ರಾಂಗ್ ಪಾಸ್‌ವರ್ಡ್ ಬಳಸಿ

ಪ್ರತಿ ಸರ್ವಿಸ್ ಅಥವಾ ಇಂಟರ್‌ನೆಟ್ ಸೇವೆ ಪಡೆದುಕೊಳ್ಳುವಾಗ, ನೀವು ಒಂದೇ ಪಾಸ್‌ವರ್ಡ್ ಮರುಬಳಕೆ ಮಾಡುತ್ತಿದ್ದರೆ, ಒಂದು ಡೇಟಾಬೇಸ್ ಹ್ಯಾಕ್ ಮಾಡಿ ಹ್ಯಾಕರ್‌ಗಳು ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಪಡೆದುಕೊಂಡಾಗ, ನೀವು ಬಳಸುತ್ತಿರುವ ಬೇರೆ-ಬೇರೆ ಸರ್ವಿಸ್‌ಗಳನ್ನು ಹ್ಯಾಕರ್‌ಗಳು ಆಕ್ಸೆಸ್ ಪಡೆದುಕೊಳ್ಳಲು ದಾರಿ ಮಾಡಿಕೊಟ್ಟಂತೆ ಆಗುತ್ತದೆ. ಆ ಕಾರಣದಿಂದ, ಊಹಿಸಲು ಕಷ್ಟವಾಗುವಂತೆ ಭಿನ್ನವಾದ, ಸ್ಟ್ರಾಂಗ್ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಪ್ರತಿ ಸೇವೆಗೂ ಸೆಟ್ ಮಾಡಿಕೊಳ್ಳುವುದು ಅತ್ಯಂತ ಅವಶ್ಯಕವಾಗುತ್ತದೆ. ಹೆಚ್ಚಿನ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ನೆನಪಿಟ್ಟುಕೊಳ್ಳಲು ನಿಮಗೆ ಕಷ್ಟವಾಗುತ್ತಿದ್ದರೆ, ಆಗ ನಂಬಬಲ್ಲ ಪಾಸ್‌ವರ್ಡ್ ಮ್ಯಾನೇಜರ್ ಬಳಸಬಹುದು.

# CySecK Awareness Repository

## Identity Management Day

12 April 2022

Identity Management Day is observed on second Tuesday of April to educate about the necessity of maintaining and securing digital identities.

### Why is Identity Management important?

Everyone has a digital identity, which is made up of a vast amount of personal information. Your information is crucial to hackers, whether it originates from your social media profiles, search engine histories, or email accounts. Fortunately, there are ways to increase the security of your online identities by following a few practices:



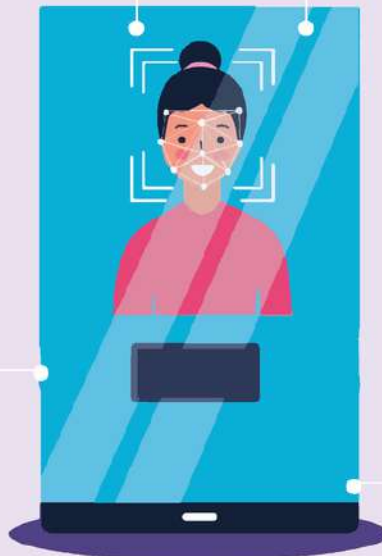
#### Multifactor Authentication

Multifactor Authentication will protect your online accounts by allowing the most secure authentication methods, such as biometrics or a one-time code sent to your phone or mobile device.



#### Change default credentials

Many devices – like WiFi routers, IoT devices, etc - are sold with default configurations like password for admin accounts. Unless you change this, when this device gets connected to the internet hackers can login with the admin credentials and take control of the device. Ensure that the default credentials are changed for all your internet-connected devices.



#### Think Before You Click!

Don't click on the link right away if you get an attractive offer by email or SMS. Instead, go straight to the official website to ensure it's genuine. Attackers frequently use phishing emails and SMS to deceive people into giving up personal information like usernames and passwords or downloading malware.



#### Use unique, strong passwords for each service

If you have reused passwords across multiple services, if the hackers are able to obtain the password from hacking one database, they will be able to access other services as well. Hence it is critical that you set a unique, strong password that is not easy to guess for each service. If you are finding it difficult to remember multiple passwords, use a reliable password manager.



# ಸೈಸಿಕ್ ಜಾಗೃತಿ ಭಂಡಾರ



## ಕುಟುಂಬದ ಇಂಟರ್‌ನೆಟ್ ಸುರಕ್ಷತೆ ಸಲಹೆಗಳು ಯುವಕರಿಗೆ

ಡಿಜಿಟಲ್ ಜಗತ್ತಿನಲ್ಲಿ ಯುವಕರನ್ನು ವಂಚಿಸುವ ಆನ್‌ಲೈನ್ ಮೋಸಗಾರರು, ಬೇರೆ-ಬೇರೆ ರೀತಿಯ ಸೈಬರ್ ಕ್ರಿಮಿನಲ್‌ಗಳು ಹೆಚ್ಚಾಗಿದ್ದಾರೆ



### ನೀವು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳುತ್ತಿರುವ ಮಾಹಿತಿಯ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ

ಅಂತರ್ಜಾಲಕ್ಕೆ ಯಾವುದೇ ಮಿತಿಗಳಿಲ್ಲ. ನೀವು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಮಾಡಿಕೊಳ್ಳುವ ಸ್ನೇಹಿತರು, ಹಂಚಿಕೊಳ್ಳುವ ಚಿತ್ರಗಳು ಮತ್ತು ಮಾಹಿತಿಯ ಮೇಲೆ ತುಂಬಾ ಜಾಗೃತರಾಗಿರಬೇಕು. ಅಷ್ಟೇ ಅಲ್ಲ, ಎಲ್ಲರೂ ಜವಾಬ್ದಾರಿಯುತ ಬಳಕೆದಾರರಾಗಬೇಕು. ಇಂಟರ್‌ನೆಟ್‌ನಲ್ಲಿ ಟ್ರಾಲ್ ಮಾಡುವುದನ್ನು ಅಥವಾ ಯಾವುದೇ ರೀತಿಯ ಕೆಟ್ಟ ಕಾಮೆಂಟ್‌ಗಳನ್ನು ಹಾಕುವುದನ್ನು ಮಾಡಬಾರದು. ನೀವು ಮಾಡುವ ಪ್ರತಿಯೊಂದು ಪೋಸ್ಟ್ ಅಥವಾ ಕಾಮೆಂಟ್ ನಿಮ್ಮ ಮೇಲೆ ಪರಿಣಾಮ ಬೀರುವುದಂತು ಕಂಡಿತ.



### ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಸ್ನೇಹಿತರನ್ನು ಭೇಟಿಯಾಗುವಾಗ ತುಂಬಾ ಜಾಗೃತರಾಗಿರಿ.

ನೀವು ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಸ್ನೇಹಿತರನ್ನು ಮೊದಲನೇ ಬಾರಿ ಎದುರುಗೊಳ್ಳಲು, ಸುರಕ್ಷಿತವಾದ, ಸಾರ್ವಜನಿಕ ಸ್ಥಳವನ್ನು ಆರಿಸಿಕೊಳ್ಳಿ. ಬಹಳ ಜಾಗೃತಿ ವಹಿಸಬೇಕು ಅಥವಾ ಗೊತ್ತಿರುವವರನ್ನು ಜೊತೆಯಲ್ಲಿ ಕರೆದುಕೊಂಡು ಹೋಗಬೇಕು.

### ಅಪ್ಪ-ಅಮ್ಮನ ಮಾರ್ಗದರ್ಶನ ಪಡೆಯಿರಿ.



ಯಾರಾದರೂ ನಿಮಗೆ ತಾವು ಹೇಳಿದ ಕೆಲಸವನ್ನು ಮಾಡಲೇಬೇಕು ಎಂದು ಒತ್ತಡ ಹೇರುತ್ತಿದ್ದರೇ, ಅಥವಾ ಸಹಾಯ ಕೇಳುತ್ತಿದ್ದರೇ, ನಿಮಗೆ ಅನುಮಾನ ಬರುವಂತೆ ನಡೆದುಕೊಳ್ಳುತ್ತಿದ್ದರೇ, ಅಂತಹ ಕೆಲಸವನ್ನು ಮಾಡಲೇಬೇಡಿ. ಆಗ್ಗಿಂದಾಗಿ ಅವರ ಜೊತೆ ಮಾತುಕತೆ ನಿಲ್ಲಿಸಿ, ಅಂತವರನ್ನು ಬ್ಲಾಕ್ ಮಾಡಿ. ಸೈಬರ್ ತಂಟೆಕೋರರು ಯಾರಿಗೆ ಬೇಕಾದರು, ಎಲ್ಲಿ ಬೇಕಾದರು ಕಾಟ ಕೊಡಬಹುದು. ಈ ರೀತಿ ಘಟನೆಗಳು ನಡೆದಾಗ, ತುಂಬಾ ಜಾಗೃತಿ ವಹಿಸುವುದಷ್ಟೇ ಅಲ್ಲ, ನಿಮ್ಮ ತಂದೆ-ತಾಯಿಯ ಗಮನಕ್ಕೆ ತನ್ನಿ.



# CySecK Awareness Repository



## INTERNET SAFETY TIPS FOR FAMILIES FOR TEENAGERS

There are online predators and plenty of other cyber criminals waiting to prey on teenagers in the digital world.



### **Be mindful of what you share on the Internet**

The Internet has no boundaries. Be cautious about the friends you make, pictures you post, and information you share on social media. On the other hand, be a responsible user and avoid trolling or posting nasty comments on the Internet. You may have to live with what you publish about yourself or others.



### **Be cautious while you meet your online friend in person.**

When meeting your online friend for the first time, ensure it is in a safe place, like a public place. Be cautious or take someone along.



### **Talk to your parents**

If someone forces you to do certain activities or ask favours, be very suspicious and avoid doing it. Stop the conversation and block such accounts right away. Cyberbullying can happen to anyone anywhere. Be careful and alert your parents in such instances.



# ಉಪಯುಕ್ತ ಲಿಂಕ್‌ಗಳು Useful links



ಸೈಬರ್ ಜಾಗೃತಿ ಮತ್ತು ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿರಲು ಕೆಲವು ಉಪಯುಕ್ತ ಲಿಂಕ್‌ಗಳು ಇಲ್ಲಿವೆ-

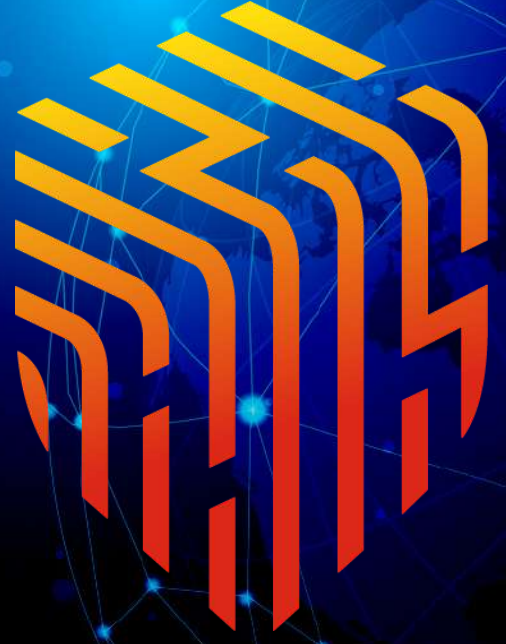
- ಸೈಬರ್ ವಂಚನೆಗಳ ಬಗ್ಗೆ ದೂರು ದಾಖಲಿಸಲು [cybercrime.gov.in](https://cybercrime.gov.in)
- ತಪ್ಪು ಮಾಹಿತಿ ಗುರುತಿಸಲು -<https://factcheck.ksp.gov.in>
- ಆನ್‌ಲೈನ್ ವಂಚನೆಗೆ ಸಂಬಂಧಿಸಿದ ದೂರುಗಳನ್ನು ನೋಂದಾಯಿಸಲು ಬೆಂಗಳೂರು ಜನರು 112ಗೆ ಕರೆ ಮಾಡಬಹುದು

Some useful links for staying cyber aware and cyber safe -

- To lodge complaint against a cyber-crime - [cybercrime.gov.in](https://cybercrime.gov.in)
- To identify fake information: <https://factcheck.ksp.gov.in>
- Bangalorians can call 112 for registering complaints related to online frauds.



# ಸೈಸೆಕ್ ಬಗ್ಗೆ About CySecK



ಸೈಸೆಕ್ (CySecK) ಎಂಬುದು ಸೈಬರ್ ಸೆಕ್ಯೂರಿಟಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಸರ್ಕಾರದ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರವಾಗಿದೆ (ಸೆಂಟರ್ ಆಫ್ ಎಕ್ಸಲೆನ್ಸ್ ,ಸಿಒಇ). ಇದು ಐಐಎಸ್ಸಿ (ಇಂಡಿಯನ್ ಇನ್ಸ್ಟಿಟ್ಯೂಟ್ ಆಫ್ ಸೈನ್ಸ್) ಸಂಸ್ಥೆಯ ಆವರಣದಲ್ಲಿದೆ. ಐಐಎಸ್ಸಿಯು ಇದರ ಆಂಕರ್ ಸಂಸ್ಥೆಯಾಗಿದ್ದು , ಕೆಎಸ್ಸಿಎಸ್ಸಿ (ಕರ್ನಾಟಕ ಸ್ಟೇಟ್ ಕೌನ್ಸಿಲ್ ಫಾರ್ ಸೈನ್ಸ್ ಅಂಡ್ ಟೆಕ್ನಾಲಜಿ) ಇದರ ಅನುಷ್ಠಾನ ಸಂಸ್ಥೆಯಾಗಿರುತ್ತದೆ. ಸೈಸೆಕ್ ಅನ್ನು ಕರ್ನಾಟಕ ಸರ್ಕಾರದ ಐಟಿ, ಬಿಟಿ ಎಸ್ ಟಿ ವಿಭಾಗದ ಕರ್ನಾಟಕ ಸೃಜನಶೀಲತೆ ಮತ್ತು ತಂತ್ರಜ್ಞಾನ ಸೊಸೈಟಿ (ಕರ್ನಾಟಕ ಇನ್ನೋವೇಶನ್ ಅಂಡ್ ಟೆಕ್ನಾಲಜಿ ಸೊಸೈಟಿ) ಸ್ಥಾಪಿಸಿದೆ.

CySecK is the Karnataka state government's K-tech Centre of Excellence in Cybersecurity, housed in the IISc (Indian Institute of Science) campus, with IISc as the anchor institute and KSCST (Karnataka State Council for Science and Technology) as the implementation agency. CySecK was setup by KITS (Karnataka Innovation and Technology Society) of the Department of IT, BT and S&T.