ಜೂನ್ ೨೦೨೧ | JUNE 2021

ಸೈಬರ್ ವಾರ್ತಿಕಾ
CYBER VARTIKA

ಸೈಸೆಕ್ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್ ಉನ್ನತಜಾನ ಕೇಂದ್ರ

CySecK Cyber Security Karnataka
K-Tech CoE for Cyber Security

ಮುನ್ನುಡಿ /Foreword

ನಲ್ಮೆಯ ಓದುಗರೆ,

ಸೈಸೆಕ್‌ನ ಮಾಸಿಕ ದ್ವಿಭಾಷಾ ಸುದ್ದಿಪತ್ರವಾದ ಸೈಬರ್ ವಾರ್ತಿಕಾದ ಎರಡನೆಯ ಸಂಚಿಕೆಗೆ ಸ್ವಾಗತ. ನಮ್ಮ ಓದುಗರಲ್ಲಿ ಸೈಬರ್ ತಿಳಿವು ಮೂಡಿಸಲು ಮತ್ತು ಸಮಾಜವನ್ನು ಹೆಚ್ಚು ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು, ಸೈಬರ್ ವಾರ್ತಿಕಾ ನಮ್ಮ ಪ್ರಯತ್ನವಾಗಿದೆ.

ಸಾರ್ವಜನಿಕರ ಕಣ್ಣಿಗೆ ಮಣ್ಣೆರಚಲು ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಹೊಚ್ಚಹೊಸ ದಾರಿಗಳನ್ನು ಕಂಡುಕೊಳ್ಳುತ್ತಿದ್ದಾರೆ. ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ನಕಲಿ ಆಕ್ಸಿಮೀಟರ್ ಆ್ಯಪ್‌ಗಳು ಮತ್ತು ಹಣ ಕಲೆಹಾಕುವ ಹಗರಣಗಳು ಹೆಚ್ಚಾಗುತ್ತಿವೆ. ಪ್ಲೇಸ್ಟೋರ್‌ನ ಹೆಸರುವಾಸಿಯಾದ ಆ್ಯಪ್‌ಗಳನ್ನೇ ಹೋಲುವ ನಕಲಿ ಆಂಡ್ರಾಯ್ಡ್ ಆ್ಯಪ್ ಮಾಡುವ ಅಪರಾಧಿಗಳ ಬಗೆಗಿನ ಸುದ್ದಿಯನ್ನು ನಾವು ನೀಡುತ್ತೇವೆ. ಇತ್ತೀಚಿನ CoWin ಡೇಟಾ ಸೋರಿಕೆಯ ಆರೋಪದ ಬಗ್ಗೆ ಕೂಡ ನಾವು ಸುದ್ದಿ ನೀಡುತ್ತೇವೆ. ಆದರೆ ಅದು ಸುಳ್ಳು ಸುದ್ದಿಯೆಂದು ಆಮೇಲೆ ತಿಳಿದುಬಂದಿತು. ಡಿಜಿಟಲ್ ಯುಗದಲ್ಲಿ, ತಪ್ಪು ಮಾಹಿತಿ ಕಾಡ್ಗಿಚ್ಚಿನಂತೆ ಹಬ್ಬುತ್ತದೆ. ಮಾಹಿತಿಯನ್ನು ಇತರರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವ ಮುನ್ನ, ಅದು ಸರಿ ಇದೆಯೇ ಎಂದು ಖಾತ್ರಿಪಡಿಸಿಕೊಳ್ಳಲು ನಾವು ನಮ್ಮ ಓದುಗರನ್ನು ಪ್ರೇರೇಪಿಸುತ್ತೇವೆ.

ಕರ್ನಾಟಕದ ಸಿಐಡಿ ತಂಡ, ಹವಾಲಾ ಮೋಸಕ್ಕೆ ಸಂಬಂಧಿಸಿದ 290 ಕೋಟಿ ರೂಪಾಯಿ ಹಗರಣವನ್ನು ಇತ್ತೀಚೆಗೆ ಬಯಲುಮಾಡಿತು. ನಮ್ಮ ಕಾನೂನು ಸಂಸ್ಥೆಗಳು ಹಾಗೂ ಸೈಬರ್ ಅಪರಾಧ ಇಲಾಖೆಗಳು ಚುರುಕಾಗಿವೆ. ಜವಾಬ್ದಾರಿಯುತ ನಾಗರಿಕರಾಗಿ ನಾವು ಕೂಡ ನಮ್ಮ ಕೊಡುಗೆ ನೀಡಬಹುದು!

ನಮ್ಮ ತಿಳಿವಿನ ಕೊರತೆಯಿಂದಲೇ ಸೈಬರ್ ಅಪರಾಧ ಈ ಮಟ್ಟಿಗೆ ಬೆಳೆದಿದೆ. ನಾವು ನಮ್ಮ ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ಮ್ಯಾಸ್ಕಾಟ್‌ಗಳಾದ ರಕ್ಷಕ ಮತ್ತು ಭಕ್ಷಕರನ್ನು ಹೊರತಂದಾಗ, ಸೈಬರ್ ಸುರಕ್ಷತೆಯನ್ನು ಸರಳಗೊಳಿಸಿ ಎಲ್ಲರಲ್ಲೂ ತಿಳಿವು ಮೂಡಿಸುವುದು ನಮ್ಮ ಉದ್ದೇಶವಾಗಿತ್ತು. ನಮ್ಮ ಪ್ರಯತ್ನಕ್ಕೆ ಓದುಗರು ಕೈಜೋಡಿಸಿ, ಸೈಬರ್ ಅಪರಾಧ ಮತ್ತು ಸೈಬರ್ ಬೆದರಿಕೆಗಳ ಎದುರು ಹೋರಾಡುವರು ಎಂಬ ನಂಬಿಕೆ ಮತ್ತು ಹಾರೈಕೆ ನಮಗಿದೆ. ನಮ್ಮ ಕುಟುಂಬದವರು ಮತ್ತು ಗೆಳೆಯರಿಗೆ ನಮ್ಮ ಅರಿವನ್ನು ಹಂಚುವ ಸಣ್ಣ ಕೆಲಸ ಕೂಡ ಈ ಅಪರಾಧಗಳನ್ನು ತಡೆಯುವಲ್ಲಿ ಬಹಳ ನೆರವಾಗುತ್ತದೆ.

ಮೊದಲ ಸಂಚಿಕೆಗಾಗಿ ನಮ್ಮ ತಂಡಕ್ಕೆ ಹಲವು ಸಂದೇಶಗಳು ಹಾಗೂ ಹಾರೈಕೆಗಳು ಹರಿದು ಬಂದವು. ನಾವು ನಿಮಗಾಗಿ ಪ್ರತಿ ಸಂಚಿಕೆಯಲ್ಲೂ ಇನ್ನೂ ಒಳ್ಳೆಯ ವಿಷಯಗಳನ್ನು ಹೊತ್ತು ತರಲು, ನಮ್ಮ ಓದುಗರ ಅನಿಸಿಕೆಗಳು ನಮ್ಮಲ್ಲಿ ಹುರುಪು ತುಂಬುತ್ತವೆ! ನಲ್ಮೆಯ ಓದುಗರೆ, ನಿಮ್ಮ ಹುರಿದುಂಬಿಕೆ ಮತ್ತು ಬೆಂಬಲಕ್ಕಾಗಿ ಧನ್ಯವಾದಗಳು.

ನಿಮಗೆಲ್ಲಾ ಸವಿಹಾರೈಕೆಗಳು,
ಸೈಸೆಕ್ ತಂಡದ ಪರವಾಗಿ,

ಶಿಖಾ ಪಾಠಕ್,
ಮ್ಯಾನೇಜರ್ - ಜಾಗೃತಿ, ನೀತಿ ಮತ್ತು ಸಂಪರ್ಕ

Dear Readers,

Welcome to the second edition of Cyber Vartika, CySecK's monthly, bilingual newsletter. Cyber Vartika is our humble initiative to make our readers more cyber aware and the society more cyber secure.

Cyber criminals are finding innovative ways to dupe unsuspecting masses. Fake oximeter apps, and fundraising scams are mushrooming online. We cover the news about criminals promoting malicious android apps that impersonate popular Play store apps. We also report on the alleged CoWin data leak, which was later found to be a fake story. Misinformation spreads like wildfire in the digital age. We urge our readers to develop a skeptical mind and fact-check information before forwarding to their network.

Karnataka CID team recently busted a Rs 290 Crore money laundering scam related to a hawala racket. While our law enforcement agencies and cybercrime departments are doing their best, as responsible citizens perhaps we can contribute our bit too!

Cybercrime thrives on our ignorance, and exploits our lack of awareness. When we launched our friendly cybersecurity mascots - Rakshaka & Bhakshaka - our intention was to de-jargonize cybersecurity and generate awareness for everyone. We trust and hope that our readers will also join our endeavor, and lead our crusade against cybercrime and cyber bullying! An effort as small as sharing our knowledge with our immediate family and close friends can go a long way in breaking this chain.

Our team received many messages and compliments for the first edition. The valuable feedback from our readers surely makes us work harder in each issue, and improve upon the content we bring you! Thank you, dear readers, for the encouragement and support.

Best Wishes,
On behalf of team CySecK,

Shikha Pathak,
Manager- Awareness, Policy and Communication

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ನಿಮ್ಮ ಫೋನ್‌ನಲ್ಲಿ ನೀವು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವ ಆ್ಯಪ್‌ಗಳ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ

ಪ್ಲೇಸ್ಟೋರ್‌ನ ಸೋಗಿನ ಆಕ್ಸಿಮೀಟರ್ ಆ್ಯಪ್‌ಗಳ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ!

ಕೋವಿಡ್-19 ರ ಎರಡನೇ ಅಲೆಯಿಂದಾಗಿ, ಆಕ್ಸಿಮೀಟರ್‌ಗಳಿಗೆ ಬೇಡಿಕೆ ಹೆಚ್ಚಾಗಿದೆ. ಇದರಿಂದ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಆಕ್ಸಿಮೀಟರ್ ಆ್ಯಪ್‌ಗಳು ಕೂಡ ಮಳೆಗಾಲದ ಅಣಬೆಗಳಂತೆ ತಲೆ ಎತ್ತಿವೆ. ಕ್ವಿಕ್ ಹೀಲ್ ಸೆಕ್ಯೂರಿಟಿ ಲ್ಯಾಬ್ಸ್‌ನವರು ಗೂಗಲ್ ಪ್ಲೇನಲ್ಲಿ ಕೆಲವು ಸೋಗಿನ ಆಕ್ಸಿಮೀಟರ್ ಆ್ಯಪ್‌ಗಳಿರುವುದನ್ನು ಕಂಡುಹಿಡಿದಿದ್ದಾರೆ. ಇವು ಬೆರಳಚ್ಚು ಡೇಟಾ, ಬ್ಯಾಂಕ್ ಮಾಹಿತಿ ಮುಂತಾದ ಬಳಕೆದಾರರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಕದಿಯುತ್ತವೆ.

ಸೈಬರ್ ಅಪರಾಧಿಗಳ ಬೇಟೆ ಆಂಡ್ರಾಯ್ಡ್ ಬಳಕೆದಾರರು; ಸೋಗಿನ ಆ್ಯಪ್‌ಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡುವಂತೆ ಅವರಿಗೆ ಬಲೆ ಬೀಸಿದ್ದಾರೆ!

ಬಿಟ್‌ಡಿಫೆಂಡರ್ ಕಂಪನಿಯ ಇತ್ತೀಚಿನ ಅಧ್ಯಯನದ ಪ್ರಕಾರ, ಆಂಡ್ರಾಯ್ಡ್ ಬಳಕೆದಾರರಿಗೆ ಹೊಸ ಬೆದರಿಕೆ ಇದೆ. ಹೆಸರುವಾಸಿಯಾದ ಆ್ಯಪ್‌ಗಳ ಸೋಗಿನಲ್ಲಿ ಮೋಸಗಾರರು, ನಕಲಿ ಆಂಡ್ರಾಯ್ಡ್ ಆ್ಯಪ್‌ಗಳ ಬಲೆ ಬೀಸಿದ್ದಾರೆ. ಈ ಆ್ಯಪ್‌ಗಳಲ್ಲಿ ಬ್ಯಾಂಕರ್ ಟ್ರೋಜನ್ ವೈರಸ್ ಕುಟುಂಬಕ್ಕೆ ಸೇರಿದ ಟೀಬಾಟ್ ಮತ್ತು ಫ್ಲೂಬಾಟ್ ವೈರಸ್‌ಗಳಿವೆ.

ಹೂಡಿಕೆ ಹಗರಣ ಆ್ಯಪ್‌ಗಳ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ! ಕರ್ನಾಟಕ ಸಿಐಡಿ ಬಯಲುಮಾಡಿದ ಚೀನಾದ 'ಹವಾಲಾ' ಮೋಸಗಾರರ ನಂಟು ಹೊಂದಿರುವ 290 ಕೋಟಿ ರೂಪಾಯಿ ಹಗರಣ

ಸೈಬರ್ ಅಪರಾಧ ದಳದ ಅಧಿಕಾರಿಗಳು ಮತ್ತು ಕರ್ನಾಟಕದ ಸಿಐಡಿ ತಂಡ, ಹವಾಲಾ ಮೋಸಕ್ಕೆ ಸಂಬಂಧಿಸಿದ 290 ಕೋಟಿ ರೂಪಾಯಿ ಹಗರಣವನ್ನು ಇತ್ತೀಚೆಗೆ ಬಯಲುಮಾಡಿತು. ಇಬ್ಬರು ಚೀನೀಯರು ಮತ್ತು ಇಬ್ಬರು ಟಿಬೇಟಿಯನ್‌ರನ್ನು ಒಳಗೊಂಡು 10 ಮಂದಿಯನ್ನು ಸೆರೆಹಿಡಿಯಲಾಯಿತು. ಆನ್‌ಲೈನ್ ಪಾವತಿ ಗೇಟ್‌ವೇ ಸೇವೆ ಒದಗಿಸುವವರು ನೀಡಿದ ದೂರಿನ ಬಳಿಕ ಈ ಹಗರಣವನ್ನು ಬಯಲಿಗೆಳೆಯಲಾಯಿತು. ಅವರ ದೂರಿನ ಪ್ರಕಾರ, ಆರೋಪಿತರು ಗೇಮಿಂಗ್ ಮತ್ತು ಇ-ಕಾಮರ್ಸ್ ಒಳಗೊಂಡಂತೆ ಬೇರೆ ಬೇರೆ ಬಗೆಯ ವ್ಯಾಪಾರಗಳಲ್ಲಿ ತಾವು ತೊಡಗಿಸಿಕೊಂಡಿರುವುದಾಗಿ ಸುಳ್ಳು ಹೇಳಿ, ಅವರ ಸೇವೆಗಳ ದುರುಪಯೋಗ ಮಾಡಿಕೊಳ್ಳುತ್ತಿದ್ದರು.

ಸೋಗಿನ ಆ್ಯಪ್‌ಗಳ ಬಗ್ಗೆ ಇರಲಿ ಎಚ್ಚರ! – 5 ಲಕ್ಷಕ್ಕಿಂತ ಹೆಚ್ಚು ಭಾರತೀಯರಿಗೆ ಮೋಸ

ಬಹುದೊಡ್ಡ ಹೂಡಿಕೆ ಹಗರಣವೊಂದನ್ನು ದೆಹಲಿ ಪೊಲೀಸ್‌ನ ಸೈಬರ್ ಸೆಲ್ ಇಲಾಖೆ ಬಯಲುಮಾಡಿತು. ಇಡೀ ದೇಶದಲ್ಲಿ 5 ಲಕ್ಷಕ್ಕಿಂತ ಹೆಚ್ಚು ಜನರಿಗೆ ಮೋಸ ಮಾಡಿದ 11 ಮೋಸಗಾರರನ್ನು ಸೆರೆಹಿಡಿಯಲಾಯಿತು. ಪವರ್ ಬ್ಯಾಂಕ್, ಸನ್ ಫ್ಯಾಕ್ಟರಿ ಮತ್ತು EzPlan ಎಂಬ ಮೂರು ಆಂಡ್ರಾಯ್ಡ್ ಆ್ಯಪ್‌ಗಳ ಮೂಲಕ 150 ಕೋಟಿ ರೂಪಾಯಿಗಿಂತ ಹೆಚ್ಚಿನ ಮೊತ್ತದ ಮೋಸ ನಡೆಯಿತು. ಪವರ್ ಬ್ಯಾಂಕ್ ಆ್ಯಪ್ ಗೂಗಲ್ ಪ್ಲೇನಲ್ಲಿ ದೊರೆಯುತ್ತಿತ್ತು. ಉಳಿದೆರಡು ಆ್ಯಪ್‌ಗಳನ್ನು ವೆಬ್‌ಸೈಟ್‌ಗಳ ಮೂಲಕ ಏಪಿಕೆ ಫೈಲ್ ರೂಪದಲ್ಲಿ ಡೌನ್‌ಲೋಡ್ ಮಾಡಿಕೊಳ್ಳಬಹುದಿತ್ತು.

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ – ಮೋಸದ ಆ್ಯಪ್‌ಗಳ ಬಲೆಗೆ ಸಿಕ್ಕಿಬೀಳುವುದನ್ನು ತಪ್ಪಿಸಲು, ಬಳಕೆದಾರರು ಗೂಗಲ್ ಪ್ಲೇ ಹಾಗೂ ಆ್ಯಪಲ್‌ನ ಆ್ಯಪ್ ಸ್ಟೋರ್‌ಗಳಂತಹ ನಂಬುಗೆಯ ಮೂಲಗಳಿಂದ ಮಾತ್ರ ಪ್ರೋಗ್ರಾಮ್‌ಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಬೇಕು.ಎಸ್‌ಎಮ್‌ಎಸ್ ಇಲ್ಲವೇ ವಾಟ್ಸಾಪ್‌ನಲ್ಲಿ ಬರುವ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಿ ಯಾವ ಆ್ಯಪ್‌ಗಳನ್ನೂ ಡೌನ್‌ಲೋಡ್ ಮಾಡಬೇಡಿ.

OTP ಮೋಸಕ್ಕೆ ಗುರಿಯಾದ ನಿವೃತ್ತ ಬಿಎಸ್‌ಎನ್‌ಎಲ್ ಸಿಬ್ಬಂದಿ

ನಿವೃತ್ತ ಬಿಎಸ್‌ಎನ್‌ಎಲ್ ಉದ್ಯೋಗಿಯಾದ ಬೆಳಗಾವಿಯ ಒಬ್ಬ ವ್ಯಕ್ತಿ ಆನ್‌ಲೈನ್ ಮೋಸಕ್ಕೆ ಒಳಗಾದರು. ಮೋಸಗಾರನು 102 ಸಾಲು ಸಾಲು ಆನ್‌ಲೈನ್ ವಹಿವಾಟುಗಳ ಮೂಲಕ ಒಟ್ಟು 10 ಲಕ್ಷ ರೂಪಾಯಿ ಮೋಸ ಮಾಡಿದ ಎಂಬ ಆರೋಪವಿದೆ. ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕರ್‌ಗಳ ಸೋಗಿನಲ್ಲಿ ಮೋಸಗಾರರು ಇವರಿಂದ ದಾಖಲೆಗಳು ಮತ್ತು ವನ್ ಟೈಮ್ ಪಾಸ್‌ವರ್ಡ್ (OTP) ಗಳನ್ನು ಪಡೆದಿದ್ದರು.

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ – ಈಗ ಎದುರಾಗಿರುವ ಕೋವಿಡ್-19 ಬಿಕ್ಕಟ್ಟಿನಿಂದಾಗಿ, ಸೈಬರ್ ಅಪರಾಧ ಹೆಚ್ಚಾಗಿದೆ! ಸದ್ಯದ ತುರ್ತು ಪರಿಸ್ಥಿತಿಯ ಲಾಭ ಪಡೆದು ಮೋಸಗಾರರು ಹೆದರಿಕೆ ಹುಟ್ಟಿಸುತ್ತಿದ್ದಾರೆ. ಯಾವುದೇ ಸಂದರ್ಭದಲ್ಲೂ, ಯಾರಿಗೇ ಆದರೂ ನಿಮ್ಮ OTP ಕೊಡಬೇಡಿ. ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿರಿ.

ಹೆಸರುವಾಸಿಯಾದ ಆಸ್ಪತ್ರೆಯ ಸೋಗಿನಲ್ಲಿ ಅಕ್ರಮ ಅಂಗಾಂಗ ವ್ಯಾಪಾರ ನಡೆಸುತ್ತಿದ್ದ ನಕಲಿ ವೆಬ್‌ಸೈಟ್

ಅಕ್ರಮ ಅಂಗಾಂಗ ವ್ಯಾಪಾರ ನಡೆಸಲು ಮೋಸಗಾರರು, ಮಣಿಪಾಲ್ ಆಸ್ಪತ್ರೆಯ ವೆಬ್‌ಸೈಟನ್ನೇ ಹೋಲುವ ನಕಲಿ ವೆಬ್‌ಸೈಟ್ ಮಾಡಿ, ಅವರ ಲೋಗೊ ಮತ್ತು ಫೋಟೊ ಬಳಸಿದ್ದರು. ಮೋಸಗಾರರು, 5 ಕೋಟಿ ರೂಪಾಯಿಗೆ ಕಿಡ್ನಿ ಕೊಳ್ಳುವುದಾಗಿ ಮತ್ತು ಅದು ಬೇರೆಯವರಿಗೆ ಮಾರಾಟವಾದ ಕೂಡಲೇ ಕಿಡ್ನಿ ದಾನ ಮಾಡಿದವರಿಗೆ ಹಣ ನೀಡುವುದಾಗಿ ಜಾಹೀರಾತು ನೀಡಿದರು. ಅವರು ಫೋನ್ ನಂಬರ್ ನೀಡಿ, ಆಸಕ್ತಿಯಿರುವವರು ಕರೆ ಮಾಡಬೇಕೆಂದು ಮನವಿ ಮಾಡಿಕೊಂಡಿದ್ದರು.

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ – ಅಕ್ರಮ ವ್ಯಾಪಾರದ ಜಾಹೀರಾತುಗಳ ಬಲೆಗೆ ಬೀಳಬೇಡಿ. ಒಂದು ವೆಬ್‌ಸೈಟನ್ನು ನಂಬುವ ಮುನ್ನ ಎಚ್ಚರಿಕೆಯಿರಲಿ. ಅದು ನಕಲಿ ಇರಬಹುದು ಎಂದು ನಿಮಗೆ ಅನಿಸಿದರೆ, ಆ ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ಮುಂದುವರಿಯಬೇಡಿ ಇಲ್ಲವೇ ಅದರ ಬಗ್ಗೆ ರಿಪೋರ್ಟ್ ಮಾಡಿ.

15 ಕೋಟಿ ಜನರ CoWin ಡೇಟಾ ಸೋರಿಕೆಯಾಗಿದೆ ಎಂದು ನಕಲಿ ವೆಬ್‌ಸೈಟ್ ಹೇಳಿಕೆ, ಸುಳ್ಳು ಸುದ್ದಿಯೆಂದು ಖಚಿತಪಡಿಸಿದ ಕೇಂದ್ರ ಸರ್ಕಾರ

ಜೂನ್ ಪ್ರಾರಂಭದಲ್ಲಿ ಡೇಟಾ ಸೋರಿಕೆ ಮಾರುಕಟ್ಟೆಯು, ಕೋವಿಡ್-19 ಅನ್ನು ತಡೆಗಟ್ಟಲು ಲಸಿಕೆ ಪಡೆದ 15 ಕೋಟಿ ಭಾರತೀಯರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಇರುವ CoWin ಡೇಟಾಬೇಸ್ ಅನ್ನು 800 ಡಾಲರ್‌ಗಳಿಗೆ ಮಾರುತ್ತಿದೆ ಎಂಬ ವರದಿ ಹಬ್ಬಿತ್ತು.
ಲಸಿಕೆ ಪಡೆಯಲು ನೋಂದಾಯಿಸಿಕೊಂಡಿದ್ದ ಜನರ ಹೆಸರು, ಆಧಾರ್ ನಂಬರ್, ಸ್ಥಳ, ಫೋನ್ ನಂಬರ್‌ಗಳು ನಕಲಿ ಡೇಟಾಬೇಸ್‌ನಲ್ಲಿ ಇದ್ದವು ಎಂಬ ಆರೋಪ ಕೇಳಿಬಂದಿತ್ತು. ಮಾಹಿತಿ ಸೋರಿಕೆಯ ವರದಿಗಳು ಸುಳ್ಳು ಎಂದು ಆರೋಗ್ಯ ಮತ್ತು ಕುಟುಂಬ ಕಲ್ಯಾಣ ಮಂತ್ರಾಲಯ ಈಗ ಖಚಿತಪಡಿಸಿದೆ.

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ – ಗಾಳಿಸುದ್ದಿಗಳಿಗೆ ಕಿವಿಗೊಡಬೇಡಿ. ಆದಷ್ಟು ಬೇಗ ಲಸಿಕೆ ಪಡೆದುಕೊಳ್ಳಿ. ಲಸಿಕೆಗೆ ಸಂಬಂಧಿಸಿದ ಎಲ್ಲಾ ಡೇಟಾವನ್ನು CoWin ಸುರಕ್ಷಿತ ಮತ್ತು ಭದ್ರವಾದ ಡಿಜಿಟಲ್ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಕೂಡಿಡುತ್ತದೆ.

ಆ್ಯಪಲ್‌ನ ಹೊಸ ಗೌಪ್ಯತೆಯು ಬೇರೆ ಕಂಪನಿಗಳಿಗೆ ಮಾನದಂಡವಾಗಲಿದೆ

iOS 14.5 ಅಪ್‌ಡೇಟ್, ಹೆಚ್ಚುವರಿ ಗೌಪ್ಯತೆಯ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಒಳಗೊಂಡಿದೆ. ಭದ್ರತೆ ಮತ್ತು ಗೌಪ್ಯತೆಯ ಪರಿಣತರು ಇದನ್ನು ಮೆಚ್ಚಿಕೊಂಡಿದ್ದಾರೆ. ಈ ವೈಶಿಷ್ಟ್ಯಕ್ಕೆ "ಆ್ಯಪ್ ಟ್ರ್ಯಾಕಿಂಗ್ ಟ್ರಾನ್ಸ್‌ಪರೆನ್ಸಿ" ಎಂದು ಹೆಸರಿಡಲಾಗಿದೆ. ಇದರಿಂದಾಗಿ ಬಳಕೆದಾರರು ತಮ್ಮ ವೈಯಕ್ತಿಕ ಡೇಟಾದ ಮೇಲೆ ಹೆಚ್ಚಿನ ಹಿಡಿತವನ್ನು ಹೊಂದಬಹುದು.

ಆ್ಯಪ್ ಟ್ರ್ಯಾಕಿಂಗ್ ಟ್ರಾನ್ಸ್‌ಪರೆನ್ಸಿ ಹೇಗೆ ಕೆಲಸ ಮಾಡುತ್ತದೆ?

ಹಲವಾರು ಆ್ಯಪ್‌ಗಳಲ್ಲಿ ಬಳಕೆದಾರರು ನಡೆಸುವ ಚಟುವಟಿಕೆಗಳ ಮೇಲೆ ಒಂದು ಕಣ್ಣಿಡಲು ನೆರವಾಗುವ ವಿಶಿಷ್ಟವಾದ ಡಿವೈಸ್ ಐಡೆಂಟಿಫಯರ್ ಅನ್ನು ಮೊಬೈಲ್ ಫೋನ್‌ನ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್ ಜಾಹೀರಾತುದಾರರಿಗೆ ಒದಗಿಸುತ್ತದೆ. ಇದು ಬಹಳಷ್ಟು ಬಳಕೆದಾರರಿಗೆ ತಿಳಿದಿಲ್ಲ. ಆ್ಯಪಲ್ ಸಿಸ್ಟಮ್‌ಗಳಲ್ಲಿ ಇದನ್ನು "ಐಡೆಂಟಿಫಯರ್ ಫಾರ್ ಅಡ್ವರ್ಟೈಸರ್ಸ್" (IDFA) ಎಂದು ಕರೆಯುತ್ತಾರೆ.

ಇತ್ತೀಚೆಗೆ ಬಿಡುಗಡೆಯಾಗಿರುವ ಅಪ್‌ಡೇಟ್‌ನಲ್ಲಿ, IDFA ಟ್ರ್ಯಾಕಿಂಗ್‌ನಿಂದ ಹೊರಗುಳಿಯುವ ಆಯ್ಕೆಯನ್ನು ಬಳಕೆದಾರರಿಗೆ ನೀಡಲಾಗಿದೆ. ಬೇರೆ ಆ್ಯಪ್‌ಗಳಲ್ಲಿ ಬಳಕೆದಾರರು ನಡೆಸುವ ಚಟುವಟಿಕೆಗಳ ಮೇಲೆ ಕಣ್ಣಿಡುವ ಪ್ರತಿಯೊಂದು ಕಂಪನಿಯೂ ಕೂಡ, ಮೊದಲು ಬಳಕೆದಾರರ ಒಪ್ಪಿಗೆ ಪಡೆಯಬೇಕು. ಇದರಿಂದ ಬಳಕೆದಾರರು ಪ್ರತಿಯೊಂದು ಆ್ಯಪ್‌ಗೂ ಒಪ್ಪಿಗೆ ನೀಡುವ ಬಗ್ಗೆ ಸರಿಯಾದ ತೀರ್ಮಾನಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳಲು ನೆರವಾಗುತ್ತದೆ.

IDFA ನಂತಹ ವ್ಯವಸ್ಥೆಯನ್ನು ಆಂಡ್ರಾಯ್ಡ್ ಡಿವೈಸ್‌ಗಳಲ್ಲಿ AAID (ಗೂಗಲ್/ಆಂಡ್ರಾಯ್ಡ್ ಅಡ್ವರ್ಟೈಸಿಂಗ್ ಐಡಿ) ಎಂದು ಕರೆಯಲಾಗುತ್ತದೆ. ಆ್ಯಪಲ್‌ನ ಹೊಸ ವೈಶಿಷ್ಟ್ಯದಿಂದಾಗಿ, ಬಳಕೆದಾರರ ಆನ್‌ಲೈನ್ ಚಟುವಟಿಕೆಗಳ ಗೌಪ್ಯತೆಯನ್ನು ಕಾಪಾಡಲು ಬೇರೆ ಕಂಪನಿಗಳು ಕೂಡ ಪೈಪೋಟಿಗೆ ಬಿದ್ದು ಇನ್ನಷ್ಟು ಆಯ್ಕೆಗಳನ್ನು ನೀಡುವಂತಾದರೆ ಚೆನ್ನ.

Top Cyber News

Beware of what you install on your phone

Beware of fake oximeter apps on play store!
The second wave of the COVID-19 has created huge demand for Oximeters, which has led to a proliferation of oximeter apps online. Quick Heal Security Labs have found some fake Oximeter apps on Google Play store that steal user's personal information like fingerprint data, bank credentials, etc.

Cybercriminals target Android users; lure them into installing fake apps!
According to Bitdefender's recent study, there is a new threat for Android users. Fake Android apps disguised as popular apps are being offered by fraudsters. These apps are infected with TeaBot and Flubot which are from banker trojan families.

Beware of investment scam apps! -Karnataka CID busts Rs 290 crore scam with links to Chinese 'Hawala' operators
Cybercrime officials with the CID of Karnataka busted a Rs 290 crore money laundering scam linked to a hawala racket. Ten people were arrested, including two Chinese and two Tibetans. The scam was discovered after a well-known payment gateway provider received a complaint that the accused were abusing its services by falsely claiming that they were running businesses in several categories including gaming and e-commerce.

Beware of fake apps! – Over 5 lakh Indians lured
The Cyber Cell department of Delhi Police busted a big investment scam and arrested 11 fraudsters for luring over 5 lakh people throughout the country. The total amount over INR 150 crore was duped via three Android apps—Power Bank, Sun Factory, and EzPlan—The Power Bank app was available on Google Play, and the other two apps were available for download through websites in the form of APK files.

Please remember- To prevent falling prey to fraudulent apps, users should only install applications from trusted sources, such as Google Play and Apple's App Store. Never download apps by clicking on links you get over email, SMS or WhatsApp.

Retired BSNL staff falls prey to OTP fraud

A man from Belagavi, a retired BSNL employee fell prey to an online fraud after a fraudster allegedly managed to make transactions totalling INR 10 lakh, in a series of 102 shocking, online transactions. Fraudsters disguised as online bankers got him to share his documents and One Time Passwords (OTPs).

Please remember- The ongoing COVID-19 crisis has witnessed a surge in cybercrime! Fraudsters take advantage of the current emergency, and create fear. Do not share your OTP with anyone, under any circumstance. Stay cyber secure.

Fake website disguised as famous hospital offers illegal organ trade

Fraudsters created a website disguised as Manipal Hospital and allegedly used their logo, pictures to facilitate illegal organ trade. The fraudsters advertised that they are buying a kidney for Rs 5 crore and that the money would be handed to the donors shortly after the organ was sold. They provided a phone number and requested individuals who were interested to call on that number.

Top Cyber News

Please remember- Don't fall prey to Advertisements that promote illegal trade. Be vigilant while you trust a website, if the website seems fake, avoid surfing through that website or report it.

Fake website claims CoWin data of 150 million leaked, Centre Govt confirms the news is fake.

In the beginning of June there were reports spreading that Data Leak Market was selling a database of CoWin, carrying personal details of 150 million Indians who had got vaccinated against Covid-19 for $800.
The fake database allegedly included names, Aadhaar numbers, location, phone numbers of people who had registered for the vaccines. The Ministry of Health and Family Welfare has now confirmed, that the reports about the leak are fake.

Please remember- Do not fall for baseless rumours, get yourself vaccinated at the earliest. CoWin stores all the vaccination data in a safe and secure digital environment.

Apple's new privacy feature raises the bar for other companies

iOS 14.5 update has introduced an additional privacy feature which is being appreciated by the security & privacy experts. The feature is called "App Tracking transparency", and is broadly a mechanism that will allow the users to be in better control of their personal data.

How does App tracking transparency work?

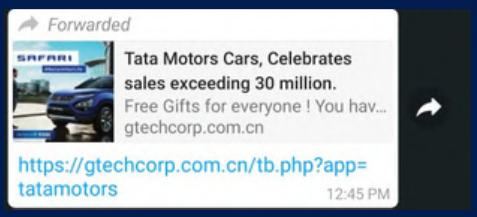
Most users have no idea that the phone's operating system provides a unique device identifier to advertisers for tracking their activities across multiple apps. This tool, for the Apple system specifically, is called "Identifier for Advertisers" (IDFA).

Now with the latest update, users can opt out of IDFA based tracking. Every single company tracking users' data across apps will have to first seek explicit permission from the users. This helps users to make informed choices about the permissions they grant to each app.

The equivalent of IDFA on Android devices is called AAID (Google/Android Advertising ID). Hopefully Apple's new feature will raise the bar for others to provide more options for protecting privacy of user's online activities.

ಸೈಸೆಕ್ ಜಾಗೃತಿ ಭಂಡಾರ

ಮೋಸದ ವೆಬ್‌ಸೈಟ್‌ಗಳ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ



ಇಲ್ಲಿನ ಕೊಡುಗೆಗಳು ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗಳಿಂದಲೇ ಬಂದಿರುವ ಹಾಗೆ ತೋರುತ್ತದೆ. ಆದರೆ ಇವು ಟಾಟಾ ಮೋಟರ್ಸ್ ಇಲ್ಲವೇ ಬಿಗ್ ಬಜಾರ್ ಗಳ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗಳ ಬದಲಿಗೆ, ಮೋಸದ ಡೊಮೈನ್‌ಗಳಲ್ಲಿರುವ ವೆಬ್‌ಸೈಟ್‌ಗಳಾಗಿವೆ.

ಮೋಸದ ಲಿಂಕ್‌ಗಳನ್ನು ಗುರುತಿಸುವುದು ಹೇಗೆ?

- ಲಿಂಕ್‌ಗಳ ವೆಬ್ ವಿಳಾಸದಲ್ಲಿ ಏನೋ ಮೋಸವಿರುವಂತೆ ತೋರುತ್ತದೆ. ಏಕೆಂದರೆ ಟಾಟಾ ಮೋಟರ್ಸ್ ಮತ್ತು ಬಿಗ್ ಬಜಾರ್ ಗಳ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಬೇರೆ ಬಗೆಯಲ್ಲಿವೆ.
- URL ಅನ್ನು ಗಮನವಿಟ್ಟು ನೋಡಿ – ಅದರಲ್ಲಿ ತುಂಬ ಅಕ್ಷರ ಮತ್ತು ಗುರುತುಗಳಿವೆ. ಇದು ಮೋಸದ ವೆಬ್‌ಸೈಟ್‌ನ ಗುರುತಾಗಿದೆ.
- ಈ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಬಳಕೆದಾರರನ್ನು ಹಲವಾರು ಜಾಹೀರಾತು ಪುಟಗಳಿಗೆ ಕರೆದುಕೊಂಡು ಹೋಗುತ್ತವೆ.
- ನಂಬಲು ಕಷ್ಟವೆನಿಸುವ ಕೊಡುಗೆಗಳಿಂದ ದೂರವಿರಿ.

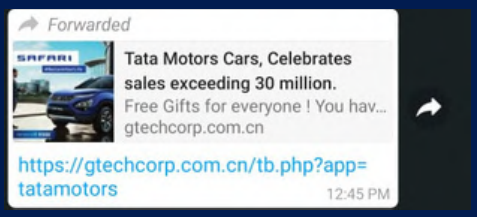
- ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ಯಾರೋ ಬರೆದಿರುವ ಪ್ರತಿಕ್ರಿಯೆಗಳನ್ನು ನಂಬಬೇಡಿ. ಅವು, ಮೋಸದ ಕೊಡುಗೆಗಳ ಬಲೆಗೆ ಜನರನ್ನು ಬೀಳಿಸಲೆಂದು, ಬೇಕೆಂದೇ ನಕಲಿ ಖಾತೆಗಳಿಂದ ಬರೆಸಲಾಗಿರುವ ಮರುಳು ಮಾಡುವ ಮಾತುಗಳಾಗಿರಬಹುದು.

ಇಮೇಲ್ ಇಲ್ಲವೇ ಎಸ್‌ಎಮ್‌ಎಸ್ ಮೂಲಕ ಬಂದಿರುವ ಗೊತ್ತಿಲ್ಲದ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವ ಬಗ್ಗೆ ಬಳಕೆದಾರರು ಎಚ್ಚರಿಕೆಯಿಂದಿರಬೇಕು.

CySeck
Cyber Security Karnataka
K-Tech CoE for Cyber Security

CySecK Awareness Repository

Beware of Phishing Sites



The campaigns here pretend to be an offer from official sites but hosted on the third-party domain instead of the official websites of Tata Motors or Big Bazaar.

How to identify fraudulent links?

- The web address of the links is seen to be fraudulent because the official websites of Tata Motors and Big Bazaar are different.
- Pay attention to the URL- It consists many characters, showing signs of a fake website.
- These sites simply keeps redirecting the user to multiple advertisements webpages.
- Walk away from deals that are too good to be true.

- Do not trust the comments on the website, they might be from fake accounts and deliberately written to make people believe in fake offers.

Users should be cautious about clicking on any unknown links sent via email or SMS.

ಜಾಗೃತಿ ವೇದಿಕೆ

ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು

ವಿಶಿಂಗ್ ಬಗ್ಗೆ ಹುಷಾರಾಗಿರಿ

ಆನ್‌ಲೈನ್ ಶಾಪಿಂಗ್ ಹಗರಣಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ

ವೆಬ್‌ಕ್ಯಾಮ್ ಸುಲಿಗೆಗಳ ಬಗ್ಗೆ ಜಾಗ್ರತೆ ವಹಿಸಿ

ಮಕ್ಕಳ ಮತ್ತು ಹದಿಹರೆಯದವರ ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆ

CONTEST ALERT

ಸೈಸೆಕ್ ಸ್ಪರ್ಧೆ #2

ಒಂದೇ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಅನೇಕ ಆನ್‌ಲೈನ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳಲ್ಲಿ ಬಳಸದಿರುವುದು ಉತ್ತಮ ಡಿಜಿಟಲ್ ಅಭ್ಯಾಸವಾಗಿದೆ. ಒಂದೇ ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ಏಕೆ ಮರುಬಳಕೆ ಮಾಡಬಾರದೆಂದು ನಮಗೆ ಸಂಕ್ಷಿಪ್ತವಾಗಿ ಹೇಳಿ.

ನಿಮ್ಮ ಪ್ರತಿಕ್ರಿಯೆಯನ್ನು ನೀವು ಒಂದು ಟ್ವೀಟ್‌ನಲ್ಲಿ ಬರೆದು ನಮಗೆ ಪ್ರತಿಕ್ರಿಯಿಸಬಹುದು. ನಿಮ್ಮ ಉತ್ತರವನ್ನು ಟ್ವಿಟ್ಟರ್‌ನಲ್ಲಿ ಪೋಸ್ಟ್ ಮಾಡಿ. ನಮ್ಮನ್ನು @CySecKCoE ಟ್ಯಾಗ್ ಮಾಡಲು ಮತ್ತು ಹ್ಯಾಶ್‌ಟ್ಯಾಗ್‌ಗಳನ್ನು #CySecKCoE #CyberVartika. ಬಳಸಲು ಮರೆಯಬೇಡಿ.
ಸ್ಪರ್ಧೆಯು 5 ಜುಲೈ 2021 ರಂದು ಕೊನೆಗೊಳ್ಳುತ್ತದೆ.

Awareness Corner

Awareness Posters

Beware of vishing

Beware of online shopping scams

Beware of webcam blackmail

Child and Adolescent online safety

CONTEST ALERT

Cyseck Contest #2

It is good digital hygiene practice to not use the same password across multiple online services. Tell us briefly why passwords should not be reused.

You can write your response within one tweet, and respond only in text. Post your answer on twitter. Do not forget to tag us @CySecKCoE and use hashtags #CySecKCoE #CyberVartika.
Contest ends on 5 July 2021.

ಸೈಸೆಕ್ ವರದಿ/CySecK Update

Congratulations to the following faculty from Karnataka for completing Cyber Crime Intervention Officer certification

1. **Sapna S**- NMAM Institute of Technology
2. **Chandrika Prasad**- Ramaiah Institue of Technology
3. **Shwetha KB**- RRIT
4. **Ambika V**- Vidyavardhaka College of Engineering
5. **Sanjeev Kumar Hatture**- Basaveshwar Engineering College
6. **Santoshi M Pujai**- Poojaya dodappa appa college of engineering
7. **Prof.Prashantha**- Moodlakatte Institute of Technology.
8. **Bhargava R**- Nagarjuna College of Engineering and Technology
9. **Dr.P.karthik**- K S School of Engineering and Management
10. **Anand Pasupathimath**- S.D.M. College of Engineering and Technology
11. **Shivachalesh Guddodagi**- KLS Vishwanathrao Deshpande Institute of Technology
12. **Veena Desai**- KLS Vishwanathrao Deshpande Institute of Technology
13. **Jayanthi MG**- Cambridge Institute of Technology
14. **Shruthi SV**- T JOHN College
15. **M Shanmugam**- Government Engineering College, Mandya
16. **Dr.Bhagyashri Hanji**- Global Academy of Technology
17. **Sushma Ethadi**- PES University , RR Campus
18. **Andhe Pallavi**- RNS Institute of Technology
19. **Shylesh BC**- Dr. B. B. Hegde First Grade College, Kundapura
20. **Murthy DHR**- Presidency University
21. **L.Sri Ramachandra**- Govt. Engineering College, Ramanagara
22. **Dr.Kiran**- Kalpataru Institute of Technology
23. **Raghu Nandan**- Navkis college of Engineering

Announcing winners of CySecK Cyber Vartika Contest #1

1. Earliest correct response- Ajay Kumar (**@AjayKum07606332** on twitter)
2. Best Kannada response- mwc ind (**@mwcindia** on twitter)
3. Best English response- Knows nothing (**@adnan_khan2601** on twitter)

ಸೈಸೆಕ್ ಬಗ್ಗೆ /About CySecK

ಸೈಸೆಕ್ (CySecK) ಎಂಬುದು ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಸರ್ಕಾರದ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರವಾಗಿದೆ (ಸೆಂಟರ್ ಆಫ್ ಎಕ್ಸಲೆನ್ಸ್ ,ಸಿಒಇ). ಇದು ಐಐಎಸ್ಸಿ (ಇಂಡಿಯನ್ ಇನ್ಸ್ಟಿಟ್ಯೂಟ್ ಆಫ್ ಸೈನ್ಸ್) ಸಂಸ್ಥೆಯ ಆವರಣದಲ್ಲಿದೆ. ಐಐಎಸ್ಸಿಯು ಇದರ ಆಂಕರ್ ಸಂಸ್ಥೆಯಾಗಿದ್ದು , ಕೆಎಸ್ಸಿಎಸ್ಟಿ (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.

Our social media handles

CySeck CoE

@CySecKCoE

CySecKCoE

CySecK

CySecK

CySecKCoE

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