ಸೈಬರ್ ವಾರ್ತಿಕ | Cyber Vartika

ಸೈಸೆಕ್

ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ

ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ

CySecK

Cyber Security Karnataka

K-Tech CoE for Cyber Security

ಫೆಬ್ರವರಿ 2022 | Febraury 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

@CySecKCoE

CySecKCoE

CySecK

CySecK

CySecK

ಮುನ್ನುಡಿ /Foreword

ಪ್ರಿಯ ಓದುಗರೇ,

“ಅಂತರ್ಜಾಲವು ನಮ್ಮ ಬದುಕನ್ನು ಸುಲಭವಾಗಿಸಿದೆ” - ಇದೊಂದು ಹೇಳಿಕೆಯೋ ಅಥವಾ ನಮ್ಮ ಮುಂದಿರುವ ಒಂದು ಪ್ರಶ್ನೆಯೋ? ನಮ್ಮಂತಹ ಹೆಚ್ಚಿನ ಜನರಿಗೆ ಇದೊಂದು ಹೇಳಿಕೆಯಾಗಿಯೇ ಕಂಡರೂ, ಹಲವರಿಗೆ ಇದೊಂದು ದೊಡ್ಡ ಪ್ರಶ್ನೆಯಾಗಿಯೇ ಉಳಿದುಕೊಂಡಿದೆ. ಅಂತರ್ಜಾಲವು ಹೆಚ್ಚಿನ ಅನುಕೂಲಗಳು ಮತ್ತು ಅನಾನುಕೂಲಗಳಿರುವ ಎರಡು ಅಂಚಿನ ಕತ್ತಿಯಂತ್ತೆಯೇ ಕಾಣುತ್ತದೆ. ಇದರಿಂದಾಗಿ ಅನುಭವಿಸಬೇಕಾದ ತೊಂದರೆಗಳು, ಕೇವಲ ಅಪಾಯಕಾರಿ ಮಾತ್ರವಲ್ಲ, ಬದಲಾಗಿ ಜೀವಕ್ಕೆ ಹಾನಿಕಾರಿಯೂ ಹೌದು.

ಜಗತ್ತಿನಾದ್ಯಂತ 46,600 ಕೋಟಿಯಷ್ಟು ಆನ್‌ಲೈನ್ ಬಳಕೆದಾರರಿದ್ದಾರೆ. ನಮ್ಮನ್ನು ಗಮನಿಸುತ್ತಿರುವ ಕಣ್ಣುಗಳೆಷ್ಟು ಎಂಬ ಅಂದಾಜು ನಮಗಿಲ್ಲ. ಅದರಲ್ಲಿ ಒಳ್ಳೆಯವರೂ ಇದ್ದಾರೆ ಎನ್ನುವುದೇ ಸಮಾಧಾನ. ಅವರನ್ನು ಸಾಮಾನ್ಯವಾಗಿ ವೈಟ್ ಹ್ಯಾಟ್‌ಗಳು ಎಂದು ಕರೆಯಲಾಗುತ್ತದೆ. ಅವರು ಒಳ್ಳೆಯ ಗುರಿ ಹೊಂದಿರುವ ಎಥಿಕಲ್ ಹ್ಯಾಕರ್‌ಗಳಾಗಿದ್ದು, ನಮ್ಮನ್ನು ಸುರಕ್ಷಿತವಾಗಿಸುತ್ತಾರೆ.

ಸೈಬರ್ ಭದ್ರತೆಯ ಜಾಗೃತಿ ಅನೇಕರನ್ನು ಕಾಪಾಡಿದೆ. ಗೌಪ್ಯತೆಯ ಅರಿವಿನಿಂದ ಅದೆಷ್ಟೋ ಜನರು ತಮ್ಮ ಡೇಟಾ ಅದು ಸೈಬರ್ ಅಪರಾಧಿಗಳ ಕೈಸೇರುವುದರಿಂದ ರಕ್ಷಿಸಿಕೊಂಡಿದ್ದಾರೆ. "ಸೈಬರ್ ವಾರ್ತಿಕ”ದ ಮೂಲಕ, ಇನ್ನಷ್ಟು ವೃದ್ಧಿಸಿರುವ ಈ ಜಾಗೃತಿ ನನಗೆ ಬಹಳ ಖುಷಿಕೊಟ್ಟಿದೆ. ಕರ್ನಾಟಕ ಮಾತ್ರವಲ್ಲದೇ, ಭಾರತದ ಎಲ್ಲೆಡೆ ಇರುವ ಯುವ ಸಮೂಹ, ಸೈಬರ್ ಭದ್ರತೆಯ ಎಡೆಗೆ ಹೆಚ್ಚಿನ ಮಹತ್ವಕೊಡುವಂತೆ ಪ್ರೋತ್ಸಾಹಿಸುವ ಜೊತೆಗೆ, ಜಗತ್ತನ್ನು ಇನ್ನಷ್ಟು ಸುರಕ್ಷಿತ ತಾಣ ಆಗಿಸುವಲ್ಲಿ ಮುಂದಡಿ ಇಟ್ಟಿದೆ.

ಮಾಲ್‌ವೇರ್ ಹರಡುವಿಕೆ, ಗೇಮಿಫಿಕೇಶನ್ ಮೂಲಕ ಸೈಬರ್ ಜಾಗೃತಿ ಮೂಡಿಸಲು ಕ್ಯಾಸ್ಪರ್ಸ್ಕಿಯ ತೊಡಗಿಕೆ, ಸೈಬರ್ ಅಪರಾಧಿಗಳ ಕಾರ್ಯವಿಧಾನ ಹಾಗೂ ನೀವು ಮುದ್ರಿಸಿ, ನಿಮ್ಮ ಗೋಡೆಗೆ ಅಂಟಿಸಲು ಇಷ್ಟಪಡುವ ಭಿತ್ತಿಪತ್ರಗಳೂ ಸೇರಿದಂತೆ, ವಿವಿಧ ಆಸಕ್ತಿಕರ ವಿಷಯಗಳು ಈ ಆವೃತ್ತಿಯ ಸುದ್ದಿಪತ್ರದಲ್ಲಿ ಸೇರಿಕೊಂಡಿವೆ! ಕ್ರಿಪ್ಟೋ ಬಗ್ಗೆ ಆಸಕ್ತಿಹೊಂದಿರುವ ನಿಮ್ಮಲ್ಲಿ ಅನೇಕರು, Intel- BMZ1 ಅವರ ಇತ್ತೀಚಿನ ASIC ಬಗ್ಗೆ ಗೂಗಲ್ ಮಾಡಲು ಮರೆಯಲೇಬೇಡಿ. ಅದು 3,600 ವ್ಯಾಟ್‌ನ ಮೈನಿಂಗ್ ರಿಗ್ ಆಗಿದ್ದೂ, ಪ್ರತಿ ಸೆಕೆಂಡ್‌ಗೆ 40 ಟೆರಾ ಹ್ಯಾಶಸ್‌ನಷ್ಟು ಸಿಸ್ಟಮ್ ಹ್ಯಾಶ್ ರೇಟ್ (TH/s) ಹೊಂದಿದೆ.

ನಮನಗಳೊಂದಿಗೆ,
ಡಾ|| ಅನಂತ್ ಪ್ರಭು ಗುರ್‌ಪೂರ್
ಪ್ರೊಫೆಸರ್ ಮತ್ತು ಮುಖ್ಯ ತನಿಖಾಧಿಕಾರಿಗಳು
ಡಿಜಿಟಲ್ ಫೊರೆಂಸಿಕ್ಸ್ ಮತ್ತು ಸೈಬರ್ ಭದ್ರತೆ CoE – ಸಹ್ಯಾದ್ರಿ
LEA ಸೈಬರ್ ಕಾನೂನು ಮತ್ತು ಭದ್ರತೆ ತರಬೇರುದಾರರು

Dear Readers,

“The Internet has made our lives easier”, the million-dollar question is- is this a statement or a question? Yes for most of us it is a statement but for many others, it remains as a big question mark. Undoubtedly, it is a double-edged sword with many advantages and disadvantages! And the perils can be not only dangerous, but also life threatening.

With 4.66 billion users online across the globe, we have no idea about the number of eyes we are exposed to. Thankfully we have the good guys, The White-hat or as they are commonly called, the Ethical hackers turning their focus towards something positive, thus keeping us safe.

Cyber Security awareness has saved many lives from the threats of cyber criminals. The awareness about privacy issues has helped many lives to protect their data from the prying eyes of cybercriminals. I'm very delighted that this initiative is boosted by “Cyber Vartika” and this becomes an inspiration for the youth of Karnataka as well across the nation to head start and dive into the world cyber security and make this world a secure space.

This edition of the newsletter has many interesting topics ranging from distribution of malware , initiative of Kaspersky to spread cyber awareness by gamification, modus operandi of cyber criminals and some brilliant posters for you to print and paste on your walls! And for those of you with an interest in crypto, do google about the latest ASIC by Intel- BMZ1, a 3,600-watt mining rig with a system hash rate of 40 tera hashes per second (TH/s).

With respectful regards,
Dr. Ananth Prabhu Gurpur
Professor and Principal Investigator
Digital Forensics and Cyber Security CoE-Sahyadri
Cyber Law and Security Trainer for LEA

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ಹ್ಯಾಕರ್‌ಗಳು ಮೈಕ್ರೋಸಾಫ್ಟ್ ಚಾಟ್ಸ್ ಬಳಸಿಕೊಂಡು ಮಾಲ್‌ವೇರ್ ಹರಡುತ್ತಿದ್ದಾರೆ ಎಂದು ಸಾವಿರಾರು ಪ್ರಕರಣಗಳು ವರದಿಯಾಗುತ್ತಿವೆ.

ಮಾಲ್‌ವೇರ್ ಹರಡುವ ಸಲುವಾಗಿ, ಒಂದೇ ಸಲಕ್ಕೆ ಹೆಚ್ಚಿನ ಬಳಕೆದಾರರಿಗೆ ಮಾಲ್‌ವೇರ್ ಇರುವ ಫೈಲ್‌ಗಳನ್ನು ಕಳುಹಿಸಲು, ಹ್ಯಾಕರ್‌ಗಳು ಸತತವಾಗಿ ಮೈಕ್ರೋಸಾಫ್ಟ್ ಟೀಮ್ಸ್ ಚಾಟ್‌ಗಳನ್ನು ಬಳಸಿಕೊಳ್ಳುತ್ತಿದ್ದಾರೆ. ಟೀಮ್ಸ್ ಚಾಟ್ ಮುಖಾಂತರ ಮಾಲ್‌ವೇರ್ ಇರುವ ಫೈಲ್‌ಗಳನ್ನು ಕಳುಹಿಸುವ ಪ್ರಯತ್ನ ಇತ್ತೀಚಿಗೆ ನಡೆದಿತ್ತು. ಒಂದು ಸಲ ಸಕ್ರಿಯವಾದರೆ, ಮಾಲ್‌ವೇರ್ ಯಾವುದೇ ಸಿಸ್ಟಮ್‌ಗೆ DLL ಫೈಲ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುತ್ತದೆ ಮತ್ತು ಸ್ವತಃ ತಾನೇ ಸಿಸ್ಟಮ್ ನಿರ್ವಹಣೆ ಮಾಡುವಂತೆ ಶಾರ್ಟ್‌ಕಟ್ ಲಿಂಕ್‌ಗಳನ್ನು ರಚಿಸುತ್ತದೆ.

ಈ ವರ್ಷದ ಜನವರಿಯಿಂದ ಮೈಕ್ರೋಸಾಫ್ಟ್ ಟೀಮ್ಸ್ ಚಾಟ್‌ಗಳ ಮುಖಾಂತರ ಅಟ್ಯಾಕ್ ಪ್ರಾರಂಭವಾಗಿದ್ದು 'ಅವನನ್' ಕಂಪನಿ ಕಂಡುಹಿಡಿದಿದೆ.

ಭಾರತವು 54 ಚೈನಿಸ್ ಆ್ಯಪ್‌ಗಳನ್ನು ನಿಷೇಧಿಸಿದೆ

ಭಾರತೀಯ ನಾಗರೀಕರ ಗೌಪ್ಯತೆ ಮತ್ತು ಭದ್ರತೆಗೆ ಹಾನಿಕರ ಎಂಬ ಅನುಮಾನದ ಮೇರೆಗೆ, ಕೇಂದ್ರ ಸರ್ಕಾರ 54 ಚೈನಿಸ್ ಆ್ಯಪ್‌ಗಳನ್ನು ನಿಷೇಧಿಸಿ ಹೊಸ ಆದೇಶ ಹೊರಡಿಸಿದೆ. ಇದರಲ್ಲಿ ಹೆಚ್ಚಿನ ಆ್ಯಪ್‌ಗಳು 2020 ರಲ್ಲಿ ಭಾರತ ನಿಷೇಧಿಸಿದ್ದ ಆ್ಯಪ್‌ಗಳದ್ದೇ ರೀಬ್ರ್ಯಾಂಡೆಂಡ್ ಆವೃತ್ತಿಗಳಾಗಿವೆ.

ಕೇಂದ್ರ ಸರ್ಕಾರದ ಪ್ರಕಾರ, "ಈ 54 ಆ್ಯಪ್‌ಗಳು ವಿವಿಧ ಮುಖ್ಯ ಅನುಮತಿಗಳನ್ನು ಕಾನೂನಿಗೆ ವಿರುದ್ಧ ಪಡೆದುಕೊಂಡು, ಬಳಕೆದಾರರ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಗಳನ್ನು ಕಲೆಹಾಕುತ್ತವೆ". ಸರ್ಕಾರವು, ಗೂಗಲ್ ಪ್ಲೇ ಸ್ಟೋರ್ ಸೇರಿದಂತೆ ಪ್ರಮುಖ ಆ್ಯಪ್ ಸ್ಟೋರ್‌ಗಳಿಗೂ ಭಾರತದಲ್ಲಿ ಈ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬ್ಲಾಕ್ ಮಾಡುವಂತೆ ನಿರ್ದೇಶಿಸಿದೆ.

ಸೈಬರ್ ಭದ್ರತೆಯ ಜಾಗೃತಿ ಹೆಚ್ಚಿಸಲು ಕ್ಯಾಸ್ಪರ್ಸ್ಕಿ ಮೊಬೈಲ್ ಗೇಮ್ ಬಿಡುಗಡೆ ಮಾಡಿದೆ

ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ತರಬೇತಿಯನ್ನು ಇನ್ನಷ್ಟು ರಂಜನೀಯವಾಗಿಸಿ, ಕೆಲಸಗಾರರಿಗೆ ಮಾಹಿತಿ ಭದ್ರತೆಯ ಬಗ್ಗೆ ಆಸಕ್ತಿ ಹೆಚ್ಚಿಸಲು, ಕ್ಯಾಸ್ಪಸ್ಕಿ [ಡಿಸ್]ಕನೆಕ್ಟೆಡ್ ಎಂಬ ಹೆಸರಿನ ಒಂದು ಹೊಸ ಮೊಬೈಲ್ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಗೇಮ್ ಸೃಷ್ಟಿಸಿದೆ. ಕಂಪನಿಯ ಪ್ರಕಾರ, ವ್ಯಕ್ತಿಯ ದೈನಂದಿನ ಚಟುವಟಿಕೆಗಳ ಮೇಲೆ ಈ ಇಂಟರ‍್ಯಾಕ್ಟಿವ್ ಅಡ್ವೆಂಚರ್ ಆ್ಯಪ್ ಕಣ್ಣಿಡುತ್ತದೆ. ಭವಿಷ್ಯದಲ್ಲಿ, ಕೆಲಸ ಮತ್ತು ಆರೋಗ್ಯದಲ್ಲಿ ಸಮತೋಲನ ಕಾಪಾಡಿಕೊಳ್ಳುವುದರ ಜೊತೆಗೆ, ಕೆಲಸದಲ್ಲಿ ಮತ್ತು ಕೌಟುಂಬಿಕವಾಗಿ ವ್ಯಕ್ತಿಯು ಯಶಸ್ಸು ಸಾಧಿಸುವಂತೆ ಮಾಡುವುದು ಆ್ಯಪ್‌ನ ಗುರಿಯಾಗಿದೆ. ಬಿಸಿನೆಸ್‌ಗೆ ಅವಶ್ಯಕತೆ ಇರುವ ಭದ್ರತೆಯ ಜಾಗೃತಿ ಕಾರ್ಯಕ್ರಮಗಳನ್ನು, ನಡವಳಿಕೆ ಸುಭದ್ರವಾಗಿಸುವ ಪ್ರಯೋಜನಗಳ ಮೂಲಕ ತೋರಿಸಿವುದು ಮತ್ತು ತಮ್ಮಲ್ಲಿ ಕೆಲಸ ಮಾಡುವ ಸಿಬ್ಬಂದಿ ಕಲಿತದ್ದನ್ನು ತಕ್ಕಮಟ್ಟಿಗೆ ಬಳಸುವಂತೆ ನೋಡಿಕೊಳ್ಳುವುದು ಈ ಗೇಮ್‌ನ ಗುರಿಯಾಗಿದೆ. ಕೇವಲ ಕಾರ್ಪೊರೇಟ್ ಗ್ರಾಹಕರಿಗೆ ಈಗ [ಡಿಸ್]ಕನೆಕ್ಟೆಡ್ ಲಭ್ಯವಿದೆ. ಅದು ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಮತ್ತು iOS ಸ್ಮಾಟ್‌ಫೋನ್‌ಗಳಲ್ಲಿ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತದೆ.

ಅಧ್ಯಯನದ ಪ್ರಕಾರ, ಭಾರತೀಯ ಮೊಬೈಲ್ ವ್ಯಾಲೆಟ್, ಬ್ಯಾಂಕಿಂಗ್ ಮತ್ತು ಸಂಪರ್ಕ ಕಲ್ಪಿಸುವ ಆ್ಯಪ್‌ಗಳಿಗೆ ನೀಡುವ ಅನುಮತಿಗಳು ಬಹಳ ಅಪಾಯಕಾರಿ ಎಂದು ಕಂಡುಬಂದಿವೆ

ಭಾರತೀಯ ಮೊಬೈಲ್ ಆ್ಯಪ್ ಮತ್ತು ವೆಬ್‌ಸೈಟ್‌ಗಳು ಸಾಕಷ್ಟು ಅತೀ ಸೂಕ್ಷ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸುತ್ತವೆ. ಆ ರೀತಿ ಸಂಗ್ರಹ ಆಗುವ ಮಾಹಿತಿ ದುರ್ಬಳಕೆ ಆಗಬಹುದು ಮತ್ತು ಬಳಕೆದಾರರಿಗೆ ಹಾನಿ ಉಂಟುಮಾಡಬಹುದು. ಆರ್ಕಾ ಅವರ 2021 ರ ವಾರ್ಷಿಕ ಗೌಪ್ಯತೆ ಸರ್ವೇ ಪ್ರಕಾರ, ಆಶ್ಚರ್ಯ ಎನ್ನಿಸುವಂತೆ ಶೇಕಡ 74ರಷ್ಟು ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಅಪ್ಲಿಲೇಶನ್‌ಗಳು ಬಳಕೆದಾರರ ನಿರ್ದಿಷ್ಟ ಲೊಕೇಶನ್ ಮಾಹಿತಿ ಪಡೆದುಕೊಳ್ಳುವಷ್ಟು ಆಕ್ಸೆಸ್ ಹೊಂದಿವೆ. ಶೇಕಡ 56 iOS ಆ್ಯಪ್‌ಗಳು ಮೊಬೈಲ್‌ನಲ್ಲಿ ಬಳಕೆಯಲ್ಲಿ ಇಲ್ಲದಿದ್ದರೂ, ಈ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸುತ್ತಿವೆ. ಸುಮಾರು 68 ಪರ್ಸೆಂಟ್ ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಅಪ್ಲಿಲೇಶನ್‌ಗಳು ಮತ್ತು 69 ಪರ್ಸೆಂಟ್ iOS ಆ್ಯಪ್‌ಗಳು ಕ್ರಮವಾಗಿ, ಬಳಕೆದಾರರ ಕ್ಯಾಮರಾಗೆ ಆಕ್ಸೆಸ್ ಹೊಂದಿರುವುದಲ್ಲದೇ, ಅಂದಾಜು 46 ಪರ್ಸೆಂಟ್ ಆ್ಯಂಡ್ರಾಯ್ಡ್ ಆ್ಯಪ್‌ಗಳು ಮತ್ತು 41 ಪರ್ಸೆಂಟ್ iOS ಆ್ಯಪ್‌ಗಳು ಬಳಕೆದಾರರ ಸಂಪರ್ಕಗಳ ವಿವರಗಳನ್ನು ಓದುವಷ್ಟು ಪ್ರಬಲವಾಗಿವೆ.

CERT-In ಗೂಗಲ್ ಕ್ರೋಮ್ ಬಳಕೆದಾರರಿಗೆ 'ಹೆಚ್ಚು ತೀವ್ರತೆ'ಯ ಸಲಹೆ ನೀಡಿದೆ

CERT-In ಪ್ರಕಾರ, ನಿರ್ದಿಷ್ಟ ಅಟ್ಯಾಕ್‌ಗಳನ್ನು ತಡೆಯುವ ಸಲುವಾಗಿ, ಗೂಗಲ್ ಕ್ರೋಮ್ ಬಳಕೆದಾರರು ತಮ್ಮ ಬ್ರೌಸರ್‌ಗಳನ್ನು ತಕ್ಷಣ ಅಪ್‌ಗ್ರೇಡ್ ಮಾಡಿಕೊಳ್ಳಬೇಕು. ಕಂಪ್ಯೂಟರ್ ಎಮರ್ಜೆನ್ಸಿ ರೆಸ್ಪಾನ್ಸ್ ಟೀಮ್ (CERT-In) ಪ್ರಕಾರ, ಗೂಗಲ್ ಕ್ರೋಮ್‌ನ ಹೆಚ್ಚಿನ ದೌರ್ಬಲ್ಯದಿಂದ, ಅದು ಸೈಬರ್-ಅಟ್ಯಾಕ್ಗಳಿಗೆ ಗುರಿಯಾಗುತ್ತದೆ. ಹ್ಯಾಕರ್‌ಗಳು ಗೂಗಲ್ ಕ್ರೋಮ್ OS ಅನ್ನು ಅಟ್ಯಾಕ್ ಮಾಡಿ, "ಅದರ ಮಿತಿಗಳನ್ನು ದಾಟಿ, ಅರ್ಬಿಟ್ರರಿ ಕೋಡ್ ರನ್ ಮಾಡಿ, ಬ್ರೌಸರ್‌ಗೆ ಪೂರ್ಣ ಆಕ್ಸೆಸ್ ಪಡೆದುಕೊಳ್ಳಬಹುದಾಗಿದೆ."

ಸಂಸ್ಥೆಯ ಪ್ರಕಾರ, ದೌರ್ಬಲ್ಯಗಳು 98.0.4758.80 ಗೂ ಹಿಂದಿನ ಕ್ರೋಮ್ ಆವೃತ್ತಿಗಳನ್ನು ಬಾಧಿಸುತ್ತವೆ. ಇದೇ ತಿಂಗಳ ಶುರುವಿನಲ್ಲಿ ಈ ದೌರ್ಬಲ್ಯವನ್ನು ಗೂಗಲ್ ಪ್ಯಾಚ್ ಮಾಡಿತ್ತು. ಈ ತೊಂದರೆಯ ತೀವ್ರತೆಯನ್ನು "ಹೆಚ್ಚು" ಎಂಬ ವರ್ಗದಲ್ಲಿ ಗೂಗಲ್ ಸಲಹೆ ಮೇರೆಗೆ ನೋಡಲ್ ಏಜೆನ್ಸಿ ವರ್ಗೀಕರಿಸಿದೆ.

Top Cyber News

Hackers are using Microsoft Teams chats to spread malware, thousands of incidents getting reported

Hackers are constantly targeting Microsoft Teams chats in order to use a malicious file to spread malware to several recipients in one go. The latest attacks try to send a malicious file through Teams chat. Once activated, the malware downloads DLL files on any system and creates self-administering shortcut links.
The attacks on Microsoft Teams chats started in January this year and have now been spotted by Avanan, a Check Point company that secures such collaboration platforms.

India bans 54 Chinese Apps

The union government has issued new orders banning over 54 Chinese apps, seeing them as a threat to Indian citizens' privacy and security. A number of these apps are rebranded versions of apps that India banned in 2020.
According to the centre, “These 54 apps allegedly obtain various critical permissions and collect sensitive user data”. The government has also directed top app stores including Google’s Playstore to block these applications in India.

Kaspersky launches mobile game to enhance cybersecurity awareness

To make cybersecurity training more entertaining and enhance employees' interest in information security, Kaspersky has created [Dis]connected, a new mobile cybersecurity game. As per the company, the interactive adventure is a look into the everyday routine of a person in the near future who is trying to strike a healthy work-life balance while still succeeding in their job and relationships. The game is aimed to complement typical business security awareness training programmes by demonstrating the benefits of secure conduct and can be used to reinforce what employees have learnt.[Dis]connected is currently only available for corporate customers. It runs on Android and iOS smartphones.

According to a study, Indian Mobile wallets, banking & comms apps access maximum dangerous permissions

Indian mobile apps and websites collect a considerable amount of very sensitive personal data, which could be misused and cause harm to users. According to Arrka's annual privacy survey for 2021, a staggering 74 74 percent of Android applications have access to the user's exact precise location, with a 56 percent of iOS apps doing so even when the app is not in use. Around 68 percent of Android applications and 69 percent of iOS apps can access the user's camera, respectively, and around 46 percent of Android apps and 41 percent of iOS apps can read the user's contacts.

CERT-In issues ‘high severity’ advisory for Google Chrome users

According to CERT-In, in order to avoid target attacks, Google Chrome users should upgrade their browsers immediately. According to Computer Emergency Response Team (CERT-In), Google Chrome is particularly vulnerable to cyber-attacks due to several vulnerabilities in the browser. Hackers might attack Google Chrome OS to "bypass many limitations, run arbitrary code, and get full access to the browser."
The vulnerabilities affect only Chrome versions previous to 98.0.4758.80, according to the organisation.Though Google patched the flaws in Chrome 98 earlier this month. The severity of the issues was classified as "high" by the nodal agency in its advisory.

Online frauds
ಆನ್‌ಲೈನ್ ಮೋಸಗಳು

Two held in Odisha for links to password sale over Telegram for online fraud
ಆನ್‌ಲೈನ್ ವಂಚನೆಗೆ ಟೆಲಿಗ್ರಾಮ್‌ನಲ್ಲಿ ಪಾಸ್‌ವರ್ಡ್ ಮಾರಾಟ ಮಾಡುತ್ತಿದ್ದ ಇಬ್ಬರನ್ನು ಒಡಿಸಾದಲ್ಲಿ ಬಂಧಿಸಲಾಗಿದೆ.

2 residents in Chandigarh lose Rs 6 lakh in online frauds, c ..
ಇಬ್ಬರು ಚಂದೀಗಢ್ ನಿವಾಸಿಗಳು ಆನ್‌ಲೈನ್ ವಂಚನೆಯಲ್ಲಿ 6 ಲಕ್ಷ ರೂಪಾಯಿಗಳನ್ನು ಕಳೆದುಕೊಂಡರು.

Two arrested for a novel online fraud
ಹೊಸ ರೀತಿಯ ಆನ್‌ಲೈನ್ ವಂಚನೆಯಲ್ಲಿ ಇಬ್ಬರನ್ನು ಬಂಧಿಸಲಾಗಿದೆ

Cyber frauds: 33 fraudsters arrested from Thalaposh village in Bihar's Nawada
ಸೈಬರ್ ವಂಚನೆಗಳು: ಬಿಹಾರದ ನವಾಡದಲ್ಲಿನ ತಾಲಪೋಶ್ ಗ್ರಾಮದಲ್ಲಿ 33 ವಂಚಕರನ್ನು ಸೆರೆಹಿಡಿಯಲಾಯಿತು

74-year-old loses life's savings to cyber fraud
ಸೈಬರ್ ವಂಚನೆಯಲ್ಲಿ 74-ವರ್ಷದ ವ್ಯಕ್ತಿಯೊಬ್ಬರು ತಮ್ಮ ಉಳಿತಾಯದ ಹಣವನ್ನೆಲ್ಲ ಕಳೆದುಕೊಂಡಿದ್ದಾರೆ

Pilot duped by cyber frauds in Hyderabad
ಹೈದರಬಾದ್‌ನಲ್ಲಿ ಪೈಲಟ್ ಒಬ್ಬರು ಸೈಬರ್ ವಂಚಕರಿಂದ ಮೋಸ ಹೋಗಿದ್ದಾರೆ

Casual dumping of mobile number proves costly for woman in Kollam
ಕೋಲಂನ ಮಹಿಳೆಯೊಬ್ಬರಿಗೆ ಕಸ ಎಂದು ಬಿಸಾಡಿದ ತಮ್ಮ ಹಳೆಯ ಮೊಬೈಲ್ ಫೋನ್ ಶತ್ರುವಾಯಿತು.

Delhi man held in cyber fraud case
ಸೈಬರ್ ವಂಚನೆ ಪ್ರಕರಣದಲ್ಲಿ ದೆಹಲಿಯ ವ್ಯಕ್ತಿಯನ್ನು ಬಂಧಿಸಲಾಗಿದೆ

21-year-old youth held in cyber fraud case
21-ವರ್ಷದ ಯುವಕನನ್ನು ಸೈಬರ್ ವಂಚನೆಯ ಅಡಿ ಬಂಧಿಸಲಾಯಿತು

Bank manager loses Rs 60,000 in KYC fraud
KYC ವಂಚನೆಯಲ್ಲಿ ಬ್ಯಾಂಕ್ ಮ್ಯಾನೇಜರ್ ಒಬ್ಬರು 60,000 ರೂಪಾಯಿಗಳನ್ನು ಕಳೆದುಕೊಂಡಿದ್ದಾರೆ

Fraudsters use 'PM loan' scheme to dupe vendor of Rs 71,000
'PM ಲೋನ್' ಯೋಜನೆ ಬಳಸಿಕೊಂಡು, ವಂಚಕರು ವ್ಯಾಪಾರಿಯೊಬ್ಬರಿಗೆ 71,000 ಟೋಪಿ ಹಾಕಿದ್ದಾರೆ

Man booked for promising jobs, duping 85 from Bhor
ಬಿಹಾರದ 85 ಜನರಿಗೆ ಕೆಲಸದ ಆಸೆ ಹುಟ್ಟಿಸಿ ವಂಚಿಸಿದವನನ್ನು ವಂಚನೆ ಪ್ರಕರಣದಲ್ಲಿ ದಸ್ತಗಿರಿ ಮಾಡಲಾಯಿತು

Brothers from Delhi Dupe Senior Citizen of Rs 14 Lakh Using Woman's Identity, Voice on WhatsApp
ಮಹಿಳೆಯ ಗುರುತು, ದನಿ ಮತ್ತು ವಾಟ್ಸ್‌ಅಪ್ ಬಳಸಿಕೊಂಡು, ದೆಹಲಿಯ ಸೋದರರಿಬ್ಬರು ಹಿರಿಯ ನಾಗರೀಕರಿಗೆ 14 ಲಕ್ಷ ರೂಪಾಯಿಗಳನ್ನು ವಂಚಿಸಿದ್ದಾರೆ

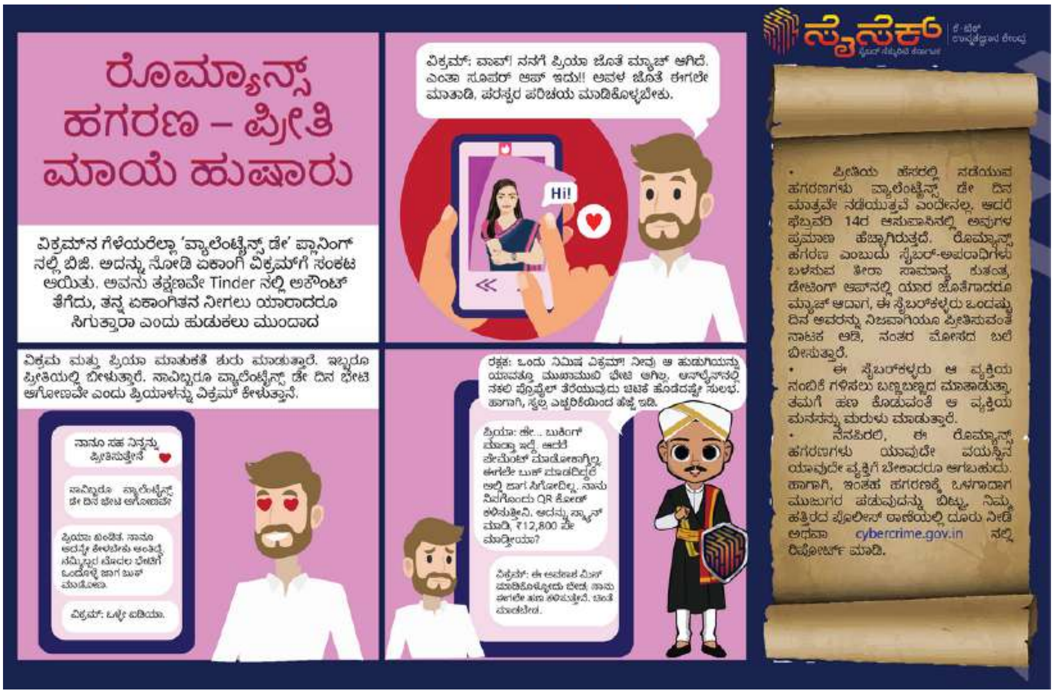
Man nabbed from Bengaluru for 'duping teacher over bitcoin'
'ಶಿಕ್ಷಕನಿಗೆ ಬಿಟ್‌ಕಾಯಿನ್ ವಂಚನೆ ಮಾಡಿರುವ ಪ್ರಕರಣದಲ್ಲಿ' ವ್ಯಕ್ತಿಯೊಬ್ಬರನ್ನು ಬೆಂಗಳೂರಿನಲ್ಲಿ ಸೆರೆಹಿಡಿಯಲಾಯಿತು

Woman Held In Tilak Nagar For Swindling Men Online
ಪುರುಷರನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ವಂಚಿಸುತ್ತಿದ್ದ ಮಹಿಳೆಯೊಬ್ಬಳನ್ನು ತಿಲಕ್ ನಗರದಲ್ಲಿ ಬಂಧಿಸಲಾಯಿತು

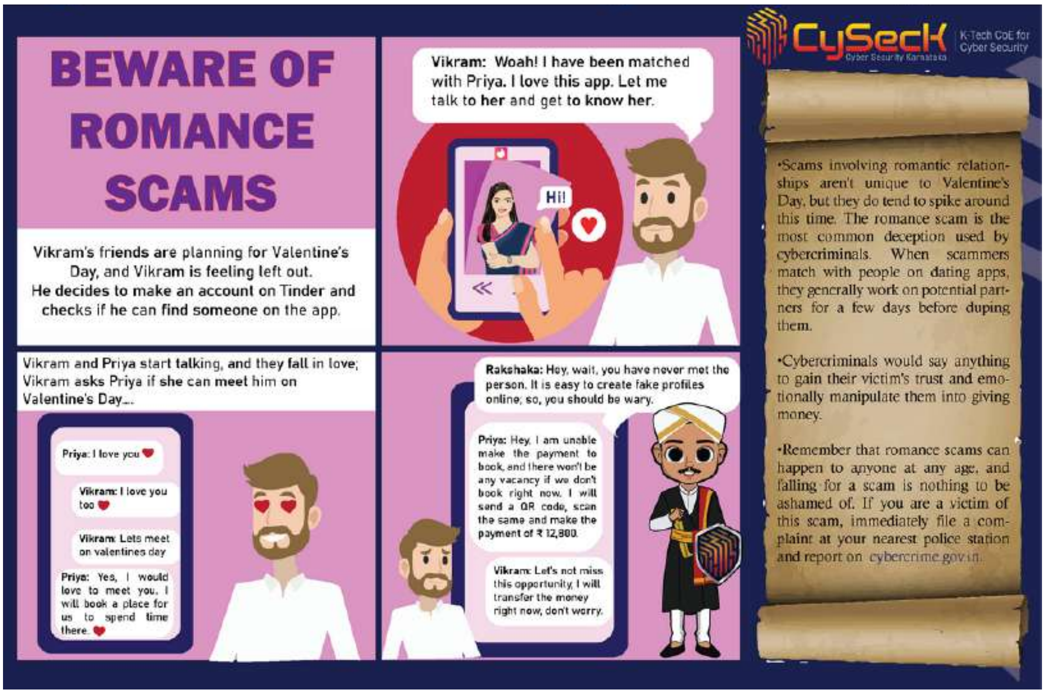
ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು

Awareness Posters

ರೊಮ್ಯಾನ್ಸ್ ಹಗರಣ – ಪ್ರೀತಿ ಮಾಯೆ ಹುಷಾರು



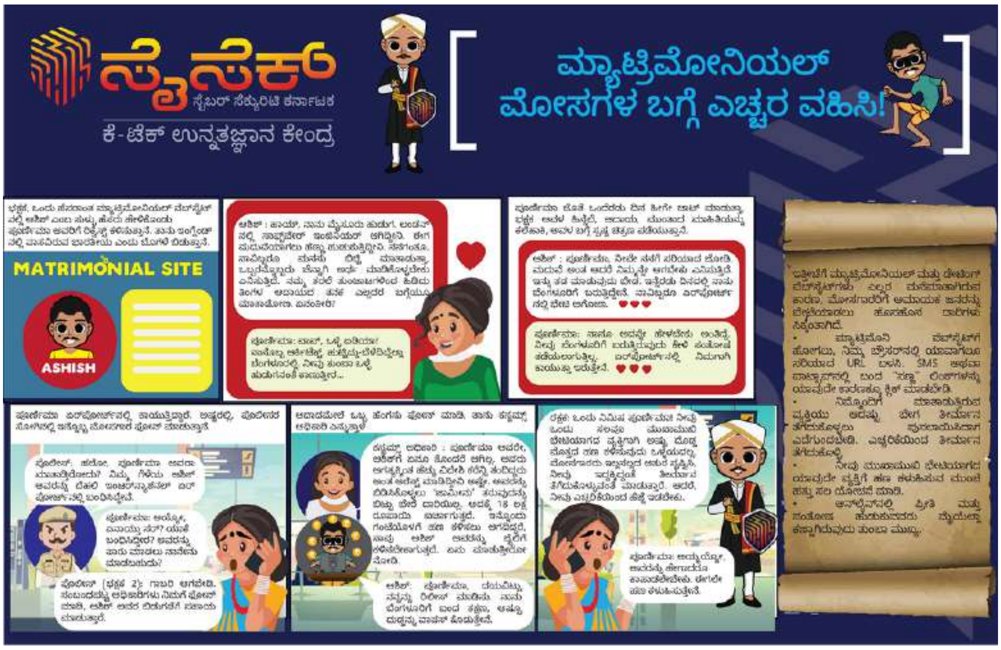
Beware of Romance Scams



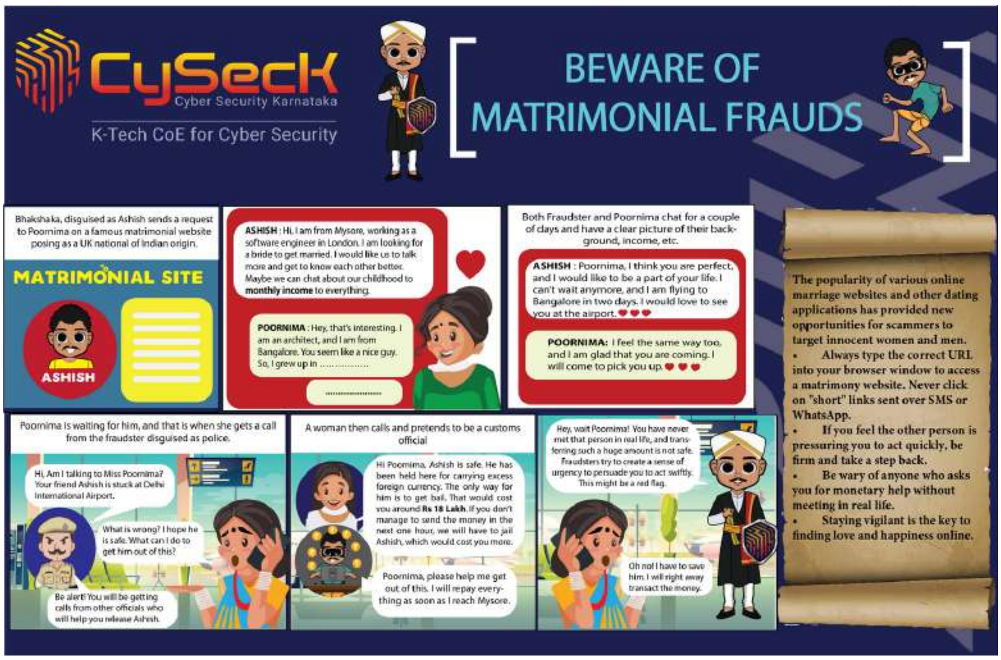
ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು

Awareness Posters

ಮ್ಯಾಟ್ರಿಮೋನಿಯಲ್ ಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರ ವಹಿಸಿ!



Beware of Matrimonial Frauds



ಸೈಸೆಕ್ ಜಾಗೃತಿ ಭಂಡಾರ

ಬ್ಲೂಟೂತ್ ಕನೆಕ್ಷನ್‌ಗಳನ್ನು ಸರಿಯಾಗಿ ಕಾನ್‌ಫಿಗರ್ ಮಾಡಲು ಮರೆಯದಿರಿ

ಬ್ಲೂಟೂತ್ ಇಲ್ಲದ ಜಗತ್ತು ಹೇಗಿರುತ್ತಿತ್ತು?

ಹಾಡು ಕೇಳುವ ಮುಂಚೆ ಇಯರ್‌ಫೋನ್ ಮತ್ತು ಹೆಡ್ ಫೋನ್‌ಗಳ ಸಿಕ್ಕುಗಟ್ಟಿದ ವೈರ್‌ಗಳನ್ನು ಬಿಡಿಸುವುದೇ ಒಂದು ದೊಡ್ಡ ತಲೆನೋವಿನ ಕೆಲಸವಾಗುತ್ತಿತ್ತು. ಲ್ಯಾಪ್ ಟಾಪ್ ಮತ್ತು ಫೋನ್ ನಡುವೆ ಫೈಲ್ ಟ್ರಾನ್ಸ್‌ಫರ್ ಮಾಡಲು ಒಂದು ಅನುಕೂಲಕರ ವಿಧಾನದ ಕೊರತೆ ಕಾಡುತ್ತಿತ್ತು. ನಿಮ್ಮ ಫೋನನ್ನು ಕಾರಿನ ಸ್ಪೀಕರ್‌ಗೆ ಕನೆಕ್ಟ್ ಮಾಡುವುದು ಬಹಳ ಕಷ್ಟ ಆಗುತ್ತಿತ್ತು. ಅಲ್ಲವೇ?

ಬ್ಲೂಜಾಕಿಂಗ್

ಆದರೆ ಇದೇ ಬ್ಲೂಟೂತ್ ಮೂಲಕ ಸೈಬರ್ -ಕಳ್ಳರು ಹಲವಾರು ದಾಳಿಗಳನ್ನು ಮಾಡಬಹುದು. ಹ್ಯಾಕರ್‌ಗಳು ಬ್ಲೂಟೂತ್ ಕನೆಕ್ಷನ್ ಮೂಲಕ ನಿಮ್ಮ ಫೋನ್‌ಗೆ ಆಕ್ಸೆಸ್ ಪಡೆದು, ಸುತ್ತಮುತ್ತಲಿನ ಇತರ ಡಿವೈಸ್ ಗಳಿಗೆ ಬೇನಾಮಿ ಮೆಸೇಜ್ ಕಳಿಸಬಹುದು. ಇದಕ್ಕೆ ಬ್ಲೂಜಾಕಿಂಗ್ ಎನ್ನುತ್ತಾರೆ. ಬ್ಲೂಜಾಕಿಂಗ್ ದಾಳಿಯಲ್ಲಿ ನಮ್ಮ ಡಿವೈಸ್ ನಿಂದ ಇನ್ನೊಬ್ಬರಿಗೆ ಡೇಟಾ ಕಳಿಸಲಾಗುತ್ತದೆ.

ತಂತ್ರಜ್ಞಾನದ ಬಳಕೆ ಹೆಚ್ಚುತ್ತಿರುವ ಈ ಹೊತ್ತಿನಲ್ಲಿ, ಬ್ಲೂಟೂತ್ ಡಿವೈಸ್ ಸೆಕ್ಯುರಿಟಿ ಬಗ್ಗೆ ಬಳಕೆದಾರರು ಗಮನ ನೀಡಬೇಕಿದೆ. ಆದ್ದರಿಂದ, ಬ್ಲೂಟೂತ್ ಗೆ ಸಂಬಂಧಿಸಿದ ಸೆಕ್ಯುರಿಟಿ ಅಪಾಯಗಳನ್ನು ನಾವು ಸರಿಯಾಗಿ ತಿಳಿದುಕೊಂಡರೆ, ಈ ಅದ್ಭುತ ವೈರ್ ಲೆಸ್ ತಂತ್ರಜ್ಞಾನದಿಂದ ಹೆಚ್ಚೆಚ್ಚು ಅನುಕೂಲ ಪಡೆದು, ಅಪಾಯಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಬಹುದು.

ಬ್ಲೂಸ್ನಾರ್ಫಿಂಗ್

ಅದೇ ರೀತಿ ಬ್ಲೂಸ್ನಾರ್ಫಿಂಗ್ ಎಂಬ ಇನ್ನೊಂದು ದಾಳಿಯಲ್ಲಿ ಇನ್ನೊಬ್ಬರಿಂದ ಡೇಟಾ ಕದಿಯಲಾಗುತ್ತದೆ. ನಿಮ್ಮ ಫೋನ್ ಅಥವಾ ಲ್ಯಾಪ್‌ಟಾಪ್ ನಲ್ಲಿರುವ ಮೆಸೇಜ್‌ಗಳು, ಇಮೇಲ್, ಫೋಟೋಗಳು ಮತ್ತು ವಿಶಿಷ್ಟ ಗುರುತಿನ ಮಾಹಿತಿಗಳು ಬ್ಲೂಸ್ನಾರ್ಫಿಂಗ್ ಮೂಲಕ ಸೈಬರ್‌ಕಳ್ಳರ ಕೈಸೇರಿದರೆ, ಅಪಾಯ ಕಟ್ಟಿಟ್ಟ ಬುತ್ತಿ.

ಬ್ಲೂಟೂತ್ ಸೆಕ್ಯುರಿಟಿ ಸಲಹೆಗಳು

- ನಿಮ್ಮ ಫೋನ್‌ನಲ್ಲಿರುವ ಹೊಸ ಆ್ಯಪ್ ಅಥವಾ ಅಪ್ಡೇಟೆಡ್ ಆ್ಯಪ್‌ನ ಪರ್ಮಿಶನ್ ಪಟ್ಟಿಯನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಗಮನಿಸಿ. ಹೀಗೆ ಮಾಡುವುದರಿಂದ ಅನಿರೀಕ್ಷಿತ ಮತ್ತು ಹಠಾತ್ ಕನೆಕ್ಟಿವಿಟಿಯನ್ನು ತಪ್ಪಿಸಬಹುದು.
- ಬಹುತೇಕ ಬ್ಲೂಟೂತ್ ದಾಳಿಗಳನ್ನು ಹತ್ತಿರದಿಂದ ಮಾತ್ರವೇ ಮಾಡಲು ಸಾಧ್ಯ. ಹಾಗಾಗಿ, ನಿಮ್ಮ ಸುತ್ತಮುತ್ತಲ ಜಾಗದ ಮತ್ತು ಜನರ ಬಗ್ಗೆ ಎಚ್ಚರಿಕೆ ವಹಿಸಿ.
- ಪಾಸ್‌ವರ್ಡ್‌ನಂತಹ ಗುಟ್ಟಾದ ಮಾಹಿತಿಯನ್ನು ಯಾವುದೇ ಕಾರಣಕ್ಕೂ ಬ್ಲೂಟೂತ್ ಮೂಲಕ ಕಳಿಸಬೇಡಿ. ಒಂದು ವೇಳೆ ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್‌ನಿಂದ ಅಗತ್ಯ ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳನ್ನು ಕಳಿಸಲು ಬ್ಲೂಟೂತ್ ಬಳಸಲೇಬೇಕಾದ ಪರಿಸ್ಥಿತಿ ಬಂದರೆ, ಅಂತಹ ಫೈಲ್‌ಗಳನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ ನಂತರವಷ್ಟೇ ಕಳಿಸಿ.
- ನಿಮ್ಮ ಫೋನ್, ಟ್ಯಾಬ್ಲೆಟ್ ಅಥವಾ ಲ್ಯಾಪ್‌ಟಾಪ್‌ನಲ್ಲಿ ಬ್ಲೂಟೂತ್ ಬಳಕೆ ಅಗತ್ಯವಿರದ ಸಮಯದಲ್ಲಿ ಅದನ್ನು "ಆಫ್" ಮಾಡಿ. ಇದರ ಮೂಲಕ, ನೀವು ಬಹುತೇಕ ಬ್ಲೂಟೂತ್-ಸಂಬಂಧಿತ ಸೈಬರ್ ದಾಳಿಗಳನ್ನು ತಪ್ಪಿಸಬಹುದು.

ಸೈಸೆಕ್
ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ

CySecK Awareness Repository

Always configure Bluetooth connections securely.

What would we do if we did not have Bluetooth?

We would spend most of our time untangling the wires of our earphones and headphones, which would be inconvenient. We would have one less method of transferring files between your laptop and phone. And what about connecting your phone to your car?

Bluejacking

There are multiple attacks cybercrooks can carry via Bluetooth. A hacker utilizes a Bluetooth connection to gain access to your phone and send anonymous messages to other nearby devices, known as Bluejacking. Bluejacking attack sends data;

Bluetooth device security has become a concern for users due to the widespread use of technology in our daily lives. It is imperative to understand the security dangers associated with Bluetooth so you can make use of all of the benefits of the widely used wireless technology while minimizing the risks.

BlueSnarfing

There is BlueSnarfing attack which steals data. Text messages, emails, images, and the unique identifying information that your phone or laptop uses are all examples of data that might be deadly in the hands of cyber attackers via Bluesnarfing.

BLUETOOTH SECURITY TIPS

TIP 1 :

It is essential to read the permissions lists of new or updated apps on your phone to avoid being surprised by unexpected connectivity features.

TIP 2 :

Never use Bluetooth to send sensitive information such as passwords. If you absolutely must utilize Bluetooth to send your essential documents from your phone to your PC, don't forget to encrypt your files beforehand.

TIP 3 :

Most Bluetooth attacks can only be carried out at close range; always be mindful of your surroundings, i.e., shoulder surfers, if you are doing something susceptible to Bluetooth

TIP 4 :

There is no reason to keep Bluetooth turned on if you are not using/ don't use it on your phone, tablet, or laptop. By doing this, you will be able to eliminate a potential cyber-attack.

CySecK Cyber Security Karnataka
K-Tech CoE for Cyber Security

ಸೈಸೆಕ್ ಸ್ಪರ್ಧೆ #8
ಉತ್ತರ ಕೀಗಳು

1. ಈ ಕೆಳಗಿನ ಪಾಸ್‌ವರ್ಡ್‌ಗಳಲ್ಲಿ ಯಾವುದು ಹೆಚ್ಚು ಸುರಕ್ಷಿತವಾಗಿದೆ?
a. instagram94
b. Ka$@T4Se ✓
c. Krishna1998
d. Officepwd1

2. ಸೈಬರ್ ಬೆದರಿಕೆಯಿಂದ ನಿಮ್ಮನ್ನು ನೀವು ಕಾಪಾಡಿಕೊಳ್ಳುವುದು ಹೇಗೆ?
a. ನಿಮ್ಮ ಪ್ರೊಫೈಲ್ ಅನ್ನು ಖಾಸಗಿಯಾಗಿಸಿ
b. ಇಂಟರ್‌ನೆಟ್‌ನಲ್ಲಿ ಗೊತ್ತಿಲ್ಲದವರೊಂದಿಗೆ ಮಾತುಕತೆ ನಡೆಸದಿರಿ
c. ನಿಮಗೆ ಬೆದರಿಕೆ ಹಾಕುವವರನ್ನು ಬ್ಲಾಕ್ ಮತ್ತು ರಿಪೋರ್ಟ್ ಮಾಡಿ
d. ಮೇಲಿನ ಎಲ್ಲವೂ ✓

3. ಈ ಕೆಳಗಿನವುಗಳಲ್ಲಿ ಯಾವುದು "ಫಿಶಿಂಗ್" ದಾಳಿಗೆ ಸಾಮಾನ್ಯ ಉದಾಹರಣೆಯಾಗಿದೆ?
a. ನೀವು ಅಪರೂಪಕ್ಕೊಮ್ಮೆ ಮಾತನಾಡುವ ದೂರದ ನೆಂಟರಿಂದ ನಿಮಗೆ ಲಿಂಕ್ ಇರುವ ಇಮೇಲ್ ಬರುತ್ತದೆ.
b. ನಿಮ್ಮ ಖಾತೆ ನಂಬರ್ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್ ಬರೆಯಲು ನಿಮ್ಮನ್ನು ಕೋರಿ, ನಿಮ್ಮ ಬ್ಯಾಂಕ್‌ನಿಂದ ಇಮೇಲ್ ಬರುತ್ತದೆ, ಆದರೆ ಬ್ಯಾಂಕ್ ವೆಬ್‌ಸೈಟ್ URL ಬೇರೆಯಾಗಿರುತ್ತದೆ.
c. ನೀವು ಒಂದು ಸ್ಪರ್ಧೆಯಲ್ಲಿ ಗೆದ್ದಿರುವಿರಿ ಎಂದೂ ಹಾಗೂ ಬಹುಮಾನ ಪಡೆಯಲು ಒಂದು URL ಗೆ ಹೋಗಬೇಕೆಂದೂ ನಿಮಗೊಂದು ಸಂದೇಶ ಬರುತ್ತದೆ.
d. ಮೇಲಿನ ಎಲ್ಲವೂ ✓

4. ಸ್ಪೈವೇರ್ ಎಂದರೆ, ಬಳಕೆದಾರರ ಒಪ್ಪಿಗೆಯಿಲ್ಲದೆ ಕಂಪ್ಯೂಟರ್‌ನಲ್ಲಿ ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಲಾಗುವ ಸಾಫ್ಟ್‌ವೇರ್ ಹಾಗೂ ಇದು ಕಂಪ್ಯೂಟರ್‌ನ ಬಳಕೆಯ ಮೇಲೆ ಒಂದು ಕಣ್ಣಿಟ್ಟಿರುತ್ತದೆ.
a. ಸರಿ ✓
b. ತಪ್ಪು

5. ಸ್ಮಿಶಿಂಗ್ ಎಂಬ ದಾಳಿಯನ್ನು, ಈ ಕೆಳಗಿನ ಯಾವುದರ ಮೂಲಕ ಮಾಡಲಾಗುತ್ತದೆ?
a. ಇಮೇಲ್
b. ಎಸ್‌ಎಮ್‌ಎಸ್ ✓
c. ವೈ-ಫೈ
d. ಪೆನ್ ಡ್ರೈವ್

6. ಒಂದು ಉತ್ಪನ್ನದ ರಿಯಾಯಿತಿ ಕೊಡುಗೆಯ ಬಗ್ಗೆ ತಿಳಿಸುವ ಲಿಂಕ್ ಇರುವ ಇಮೇಲ್, ಫ್ಲಿಪ್‌ಕಾರ್ಟ್‌ನಿಂದ ನಿಮಗೆ ಬಂದಂತೆ ತೋರುತ್ತಿದೆ. ಈಗ ನೀವೇನು ಮಾಡಬೇಕು?

a. ಈ ಕೊಡುಗೆಯ ಲಾಭ ಪಡೆಯಲು, ಕೂಡಲೇ ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಕು.

b. ಇಮೇಲ್ ಕಳುಹಿಸಿದವರ ಹೆಸರನ್ನು ಪರಿಶೀಲಿಸಿ, ಅದು ಸರಿಯಾಗಿದೆ ಎಂದು ಖಚಿತವಾದರೆ ಮಾತ್ರ, ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಕು.

c. ಇಮೇಲ್ ಕಳುಹಿಸಿದವರ ಇಮೇಲ್ ಐಡಿ ಪರಿಶೀಲಿಸಿ, ಅದು ಸರಿಯಾಗಿದೆ ಎಂದು ಖಚಿತವಾದರೆ ಮಾತ್ರ, ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಕು.

d. ನೇರವಾಗಿ ಫ್ಲಿಪ್‌ಕಾರ್ಟ್ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಹೋಗಿ, ಅಲ್ಲಿ ಕೊಡುಗೆಯನ್ನು ಹುಡುಕಿ. ✅

7. ಬ್ಯಾಂಕ್ ಇಲ್ಲವೇ ಬೇರೆ ಯಾವುದೇ ನೆರವು ತಂಡದಿಂದ ಮಾತಾಡುತ್ತಿರುವುದಾಗಿ ನಿಮಗೆ ಕರೆ ಬಂದಾಗ, ಫೋನಿನಲ್ಲಿ ಕೆಳಗಿನ ಯಾವ ವಿಷಯಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬಹುದು?

a. ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ನಂಬರ್

b. CVV ನಂಬರ್

c. ಕಾರ್ಡ್ ಮುಕ್ತಾಯದ ವಿವರಗಳು

d. ಮೇಲಿನ ಯಾವುದೂ ಅಲ್ಲ ✅

8. ನಿಮ್ಮ ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಖಾತೆಗಳನ್ನು ಸುರಕ್ಷಿತ ಮತ್ತು ಸುಭದ್ರವಾಗಿ ಇರಿಸಲು, ______ ನೆರವಾಗುತ್ತದೆ

a. ಎರಡು ಬಗೆಯ ದೃಢೀಕರಣ ಬಳಸುವುದು

b. ಊಹಿಸಲು ಕಷ್ಟವಾಗುವ ಪಾಸ್‌ವರ್ಡ್ ಬಳಸುವುದು

c. ವಿಶಿಷ್ಟವಾದ ಪಾಸ್‌ವರ್ಡ್ ಬಳಸುವುದು

d. ಮೇಲಿನ ಎಲ್ಲವೂ ✅

9. ನಿಮ್ಮ ಸಹೋದ್ಯೋಗಿಯೊಂದಿಗೆ ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಹಂಚಿಕೊಳ್ಳಬಹುದಾದ ಸನ್ನಿವೇಶಗಳು ಯಾವುವು?

a. ನೀವು ರಜೆಯಲ್ಲಿರುವಾಗ

b. ನಿಮ್ಮ ಮೇಲ್ವಿಚಾರಕರು ಸೂಚಿಸಿದಾಗ

c. ಸಹೋದ್ಯೋಗಿ ನಂಬುಗೆಯವರಾಗಿದ್ದಾಗ

d. ಮೇಲಿನ ಎಲ್ಲವೂ

e. ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳದಿರಿ ✅

10. ಈ ಕೆಳಗಿನವುಗಳಲ್ಲಿ ಯಾವುದು, ಹಲವು ಬಗೆಯ ದೃಢೀಕರಣದ ಸರಿಯಾದ ಉದಾಹರಣೆಯಲ್ಲ?

a. ಪಾಸ್‌ವರ್ಡ್ + ಎಸ್‌ಎಮ್‌ಎಸ್ OTP

b. ಪಾಸ್‌ವರ್ಡ್ + ಪಿನ್ ✅

c. ಪಾಸ್‌ವರ್ಡ್ + ಮುಖ ಗುರುತಿಸುವಿಕೆ

d. ಏಟಿಎಮ್‌ನಲ್ಲಿ ಹಣ ಹಿಂಪಡೆಯಲು ಕಾರ್ಡ್ ಬಳಸುವಾಗ, ಪಿನ್ ಒತ್ತುವುದು

11. ಟಾರೆಂಟ್ ಹಾಗೂ ಅಂತಹ ಬೇರೆ ಉಚಿತ ವೆಬ್‌ಸೈಟ್‌ಗಳಿಂದ, ಸಿನೆಮಾಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವುದು ಸುರಕ್ಷಿತವೇ?
a. ಹೌದು, ಬಹಳ ಮಂದಿ ಅದನ್ನು ಬಳಸುತ್ತಾರೆ. ಹಾಗಾಗಿ ಅದು ಸುರಕ್ಷಿತವೇ ಇರಬೇಕು.
b. ಇಲ್ಲ, ಅಂತಹ ಫೈಲ್‌ಗಳಲ್ಲಿ, ನಮ್ಮ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಕೆಡುಕುಂಟು ಮಾಡುವ ಮಾಲ್‌ವೇರ್ ಇರಬಹುದು.✅

12. ನೀವು ಆಂಡ್ರಾಯ್ಡ್ ಬಳಕೆದಾರರಾಗಿದ್ದಲ್ಲಿ, ಈ ಕೆಳಗಿನ ಯಾವ ಮೂಲಗಳು, ಆ್ಯಪ್/ಗೇಮ್ ಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಲು ಸುರಕ್ಷಿತವಾಗಿವೆ?
a. UC ಬ್ರೌಸರ್
b. ಗೂಗಲ್ ಪ್ಲೇ ಸ್ಟೋರ್ ✅
c. ವಾಟ್ಸಾಪ್‌ನಲ್ಲಿ ಹಂಚಿದ ಲಿಂಕ್‌ಗಳು
d. ಮೇಲಿನ ಎಲ್ಲವೂ

13. ನಿಮಗೆ ದಾರಿಯಲ್ಲಿ ಸಿಕ್ಕಿದ ಪೆನ್ ಡ್ರೈವ್ ಅನ್ನು ನೇರವಾಗಿ ನಿಮ್ಮ ಸಿಸ್ಟಮ್‌ನಲ್ಲಿ ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡುವುದು ಸುರಕ್ಷಿತವೇ?
a. ಹೌದು, ಯಾವಾಗಲೂ
b. ಸಿಸ್ಟಮ್‌ನ ಆ್ಯಂಟಿ-ವೈರಸ್ ಅಪ್‌ಡೇಟ್ ಆಗಿದ್ದರೆ ಮಾತ್ರ
c. ಎಂದಿಗೂ ಇಲ್ಲ ✅
Ans: c. ಎಂದಿಗೂ ಇಲ್ಲ

14. ಒಮಿಕ್ರಾನ್ ಕೊರೋನ ವೈರಸ್ ಬಗ್ಗೆ ಇತ್ತೀಚಿನ ಅಪ್‌ಡೇಟ್ ಅನ್ನು ನಿಮ್ಮ ವಾಟ್ಸಾಪ್‌ನಲ್ಲಿ ಪಡೆಯುವಿರಿ ಹಾಗೂ ನೀವು ______________
a. ಅದನ್ನು ಕೂಡಲೇ ನಿಮ್ಮ ಕುಟುಂಬದವರು ಮತ್ತು ಗೆಳೆಯರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವಿರಿ.
b. ದಿಗಿಲುಗೊಳ್ಳುವಿರಿ.
c. ಬೇರೆ ಕೆಲವು ಮೂಲಗಳನ್ನು ನೋಡಿ, ಹಂಚುವ ಮುನ್ನ ಸುದ್ದಿ ಸರಿ ಇದೆಯೇ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳುವಿರಿ.✅
d. ಮೇಲಿನ ಯಾವುದೂ ಅಲ್ಲ.

15. ನಿಮ್ಮ ಇಮೇಲ್ ಖಾತೆ ಹ್ಯಾಕ್ ಆದರೆ, ನೀವು __________
a. ನಿಮ್ಮ ಸೋಗಿನಲ್ಲಿರುವ ಯಾವುದೇ ಖಾತೆಗೂ, ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ನೀಡದಂತೆ ಇಲ್ಲವೇ ಹಣ ಕಳುಹಿಸದಂತೆ ನಿಮ್ಮ ಗೆಳೆಯರನ್ನು ಎಚ್ಚರಿಸಬೇಕು.
b. ನಿಮ್ಮ ಲಾಗಿನ್ ಐಡಿ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್ ಬದಲಾಯಿಸಿ; ಊಹಿಸಲು ಕಷ್ಟವಾಗುವ ವಿಶಿಷ್ಟವಾದ ಪಾಸ್‌ವರ್ಡ್ ಬಳಸಿ.
c. ಇದೇ ಪಾಸ್‌ವರ್ಡ್ ಇರುವ ಬೇರೆ ಖಾತೆಗಳ ಪಾಸ್‌ವರ್ಡ್ ಬದಲಾಯಿಸಿ.
d. ಮೇಲಿನ ಎಲ್ಲವೂ.✅

CySecK Contest #8

Answer Keys

1. Which of the following passwords is more secure?

a. instagram94
b. Ka$@T4Se ✔
c. Krishna1998
d. Officepwd1

2. How to protect yourself from cyber bullying?

a. Turn your profile private
b. Never respond to strangers on the internet
c. Block and report the bully
d. All of the above ✔

3. Which of the following is a common example of a "phishing" attack?

a. You get an email with link from a distant relative with whom you rarely communicate.
b. You receive an email from your bank requesting you to enter your account number and password, but the online site URL appears different.
c. You receive a text message informing you that you have won a contest and directs you to a URL to claim the prize.
d. All of the above ✔

4. Spyware is software that is installed on a computer without the consent of the user and monitors usage.

a. True ✔
b. False

5. Smishing is a type of attack done over

a. Email
b. SMS ✔
c. Wi-Fi
d. Pen drive

6. You have received an email purportedly from Flipkart regarding a discount offer for a product with a link provided. What should you do about it?
a. Click on the link immediately so that you do not miss out on the opportunity.
b. Verify the display name of the sender and proceed to click on the link if it looks genuine.
c. Verify the email id of the sender and proceed to click on the link if it looks genuine.
d. Go directly to Flipkart website and look for the offer there. ✔

7. Which of the following details can be shared over phone whenever you receive calls stating from banks or any other support team?
a. Credit card number
b. CVV number
c. Card expiry details
d. None of the above ✔

8. _____ helps to keep your social media accounts safe and secure
a. Enabling two factor authentication
b. Using strong password
c. Using unique password
d. All of the above ✔

9. What are the scenarios where it is acceptable to share your password with a colleague?
a. When you are on leave
b. When directed by your supervisor
c. When the colleague is trustworthy
d. All of the above
e. Never ✔

10. Which among the below is not a correct example of multi-factor authentication?
a. Password + SMS OTP
b. Password + PIN ✔
c. Password + Face recognition
d. Entering PIN for a card transaction while withdrawing money at ATM

11. Is it safe to download movies from the torrent and other such free sites?
a. Yes, many people use it. So it should be safe.
b. No, such files can contain malware that can infect our systems. ✓

12. If you are an Android user, which of these sources are safe to install apps / games?
a. UC Browser
b. Google Play Store ✓
c. Links shared on WhatsApp
d. All of the above

13. Is it safe to install a pen drive that you find on the roadside directly in your system?
a. Yes, always
b. Only if the system's anti-virus is updated
c. Never ✓

14. You receive a latest update about Omicron Corona Virus on WhatsApp and you ______
a. Share it with your friends and family immediately
b. Start panicking
c. Check a few other sources and confirm the news before sharing ✓
d. None of the above

15. If your email account is hacked, you _______
a. Alert your friends to not share credit card details or send money to any account impersonating you.
b. Change your credentials; use a complex and a unique password that cannot be cracked easily.
c. Change the password on other accounts that use the same password.
d. All of the above ✓

WINNERS OF ENGLISH QUIZ

Congrats!

- Bhargav K N
- Ashit.D
- Soumya

- Elaine M Paily
- Impana
- Dileep P
- Sanjurani Panda
- Janani B
- Mohith C Shekar

- Deepanshu Raj
- Vinay
- Manjushree
- Rebecca Judaist
- Krutik Raut
- Karthik Gowda D
- Yashas M N
- Vicky
- Ramakrishna HN

ಕನ್ನಡ ರಸಪ್ರಶ್ನೆ ವಿಜೇತರು

ಅಭಿನಂದನೆಗಳು!

- Keerthana R
- Rakshit N
- Niharika Darur

- Deepashree V
- Akash Mishra
- Ashish J D Souza

ಸೈಸೆಕ್ ಅಪ್‌ಡೇಟ್
CySecK Update

ಸೈಸೆಕ್ ಸೆಂಟರ್ ಮುಖ್ಯಸ್ಥ, ಕಾರ್ತಿಕ್ ಬಪ್ಪನಾಡ್ ಅವರು 5 ಫೆಬ್ರವರಿ 2022 ರಂದು HKBK ಕಾಲೇಜ್‌ನಲ್ಲಿ ಸೈಬರ್ ಭದ್ರತೆಯ ಜಾಗೃತಿ ಕುರಿತು ಒಂದು ಕಾರ್ಯಕ್ರಮದಲ್ಲಿ ಮಾತನಾಡಿದರು.

CySecK's Center Head, Mr. Karthik Bappanad conducted a session on cybersecurity awareness for HKBK College on 5th February 2022.

ಉಪಯುಕ್ತ ಲಿಂಕ್‌ಗಳು
Useful links

ಸೈಬರ್ ಜಾಗೃತಿ ಮತ್ತು ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿರಲು ಕೆಲವು ಉಪಯುಕ್ತ ಲಿಂಕ್‌ಗಳು ಇಲ್ಲಿವೆ-

- **ಸೈಬರ್ ವಂಚನೆಗಳ ಬಗ್ಗೆ ದೂರು ದಾಖಲಿಸಲು 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
- 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 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.