ನವೆಂಬರ್ ೨೦೨೧ | NOVEMBER 2021

ಸೈಬರ್ ವಾರ್ತಿಕಾ
CYBER VARTIKA

ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ

CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security

ಮುನ್ನುಡಿ /Foreword

ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕ್ಷೇತ್ರದಲ್ಲಿ ಕ್ರಾಂತಿಕಾರಕ ಬೆಳವಣಿಗೆಗಳು ಸಂಭವಿಸುತ್ತಿರುವಂತೆಯೇ ನಾವು ಅನೇಕ ಚಟುವಟಿಕೆಗಳಿಗಾಗಿ ಅದರ ಸಾಧನಗಳನ್ನು ಅವಲಂಬಿಸುತ್ತಿದ್ದೇವೆ. ಇಂತಹ ಐಟಿ-ಆಧಾರಿತ ಚಟುವಟಿಕೆಗಳ ಪರಿಮಾಣ ಹಾಗೂ ವ್ಯಾಪ್ತಿ ಹೆಚ್ಚಿದಂತೆ, ಆ ಚಟುವಟಿಕೆಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ನಡೆಸಬೇಕಾದದ್ದು ಹಿಂದೆಂದಿಗಿಂತ ಹೆಚ್ಚು ಅಗತ್ಯವಾಗಿದೆ. ಅದರ ಹೆಸರನ್ನೇ ಕೇಳಿಲ್ಲದವರಿಗೂ ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ಪರಿಕಲ್ಪನೆ ಇಂದು ಪ್ರಸ್ತುತವೆನಿಸುತ್ತಿದೆ.

'ಸೈಬರ್ ವಾರ್ತಿಕಾ'ದ ಈ ಸಂಚಿಕೆಯಲ್ಲಿ ಪ್ರಸ್ತಾಪವಾಗಿರುವ ಸುದ್ದಿಗಳನ್ನೇ ನೋಡಿ. ಮಕ್ಕಳಿಂದ ದೊಡ್ಡವರವರೆಗೆ, ವ್ಯಕ್ತಿಗಳಿಂದ ಸಂಘಸಂಸ್ಥೆಗಳವರೆಗೆ ಈ ದಿನಗಳಲ್ಲಿ ಬಹುತೇಕ ಎಲ್ಲರೂ ಸೈಬರ್ ಅಪರಾಧಗಳ ಅಪಾಯವನ್ನು ಎದುರಿಸುತ್ತಿದ್ದಾರೆ. ಫೋನ್ ಕರೆಯ ಮೂಲಕ ಗಾಬರಿಹುಟ್ಟಿಸಿ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಕದಿಯುವುದಿರಲಿ, ರ್ಯಾನ್‌ಸಮ್‌ವೇರ್‌ನಂತಹ ತಾಂತ್ರಿಕ ಅಸ್ತ್ರವೇ ಇರಲಿ, ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನದ ಮೇಲಿನ ನಮ್ಮ ಅವಲಂಬನೆಯನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳುವ ಹಲವು ಮಾರ್ಗಗಳು ಇಂದು ಸೃಷ್ಟಿಯಾಗಿವೆ.

ಇದರಿಂದ ಹಲವು ಬಗೆಯ ಪರಿಣಾಮಗಳಾಗುವುದು ಸಾಧ್ಯ. ಸೈಬರ್ ಅಪರಾಧಗಳಿಂದ ಉಂಟಾಗುವ ನೇರ ಹಾನಿ - ಉದಾಹರಣೆಗೆ, ಆರ್ಥಿಕ ನಷ್ಟ - ಈ ಪರಿಣಾಮಗಳ ಒಂದು ಆಯಾಮ ಮಾತ್ರ. ಇಂತಹ ಅಪರಾಧಗಳಿಂದ ಹೆದರಿದ ಬಳಕೆದಾರರು ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನದ ಸಾಧನಗಳನ್ನು ಬಳಸಲು ಹಿಂಜರಿದರೆ ಅದು ಆ ಕ್ಷೇತ್ರದ ಬೆಳವಣಿಗೆಗೆ ಅಡ್ಡಗಾಲು ಹಾಕಬಹುದು, ಒಟ್ಟಾರೆಯಾಗಿ ನಮ್ಮ ಸಮಾಜದ ಬೆಳವಣಿಗೆಯ ಮೇಲೆಯೇ ಋಣಾತ್ಮಕ ಪರಿಣಾಮಗಳನ್ನು ಬೀರಬಹುದು. ಇದಕ್ಕೆ ವಿರುದ್ಧವಾಗಿ ಸೈಬರ್ ಅಪರಾಧಗಳ ಸಾಧ್ಯತೆಯ ಬಗ್ಗೆ ತಲೆಯನ್ನೇ ಕೆಡಿಸಿಕೊಳ್ಳದಿದ್ದರೆ? ಅಪರಾಧಗಳ ಪ್ರಮಾಣ ಇನ್ನಷ್ಟು ಹೆಚ್ಚಬಹುದು.

ಇಂತಹ ಸನ್ನಿವೇಶಗಳನ್ನು ತಪ್ಪಿಸಿ, ಸೈಬರ್ ಅಪರಾಧಗಳ ಅಪಾಯದ ಕುರಿತು ಎಚ್ಚರದಿಂದ ಇರುವಂತೆ ಬಳಕೆದಾರರನ್ನು ಪ್ರೇರೇಪಿಸಬೇಕಾದ್ದು ಇಂದಿನ ಅಗತ್ಯ. ಈ ನಿಟ್ಟಿನಲ್ಲಿ ಮಾಡಬಹುದಾದ ಪ್ರಮುಖ ಕೆಲಸವೆಂದರೆ, ಸೈಬರ್ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ಹೆಚ್ಚಿನ ಜಾಗೃತಿ ಮೂಡಿಸುವುದು. ಈ ಅಪರಾಧಗಳು ಯಾವೆಲ್ಲ ರೀತಿಯಲ್ಲಿ ಸಂಭವಿಸಬಹುದು, ನಮ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹೇಗೆ ಜೋಪಾನ ಮಾಡಿಕೊಳ್ಳಬಹುದು ಎನ್ನುವಂತಹ ವಿಷಯಗಳನ್ನು ತಿಳಿದುಕೊಂಡವರ ಸಂಖ್ಯೆ ಹೆಚ್ಚಿದಷ್ಟೂ ಸೈಬರ್ ಅಪರಾಧಗಳ ವಿರುದ್ಧದ ರಕ್ಷಣೆ ಹೆಚ್ಚುತ್ತಾ ಹೋಗುತ್ತದೆ.

ಈ ಮಾಹಿತಿಯೆಲ್ಲ ಎಲ್ಲರಿಗೂ ಅರ್ಥವಾಗುವಷ್ಟು ಸರಳವಾಗಿ, ನಮ್ಮ ಭಾಷೆಯಲ್ಲೇ ಸಿಕ್ಕಿದಾಗ ಅದು ಹೆಚ್ಚು ಬಳಕೆದಾರರನ್ನು ತಲುಪುವುದೂ ಸಾಧ್ಯವಾಗುತ್ತದೆ. ಆನ್‌ಲೈನ್ ವಂಚನೆಯ ಪ್ರಸಂಗಗಳು ದಿನನಿತ್ಯವೆನ್ನುವಂತೆ ವರದಿಯಾಗುತ್ತಿದ್ದಾಗಲೂ ಸೂಕ್ತ ಎಚ್ಚರಿಕೆ ವಹಿಸದ ಜನರು ಅಂತಹ ಅಪರಾಧಗಳಿಗೆ ಗುರಿಯಾಗುವುದು ಇನ್ನೂ ಮುಂದುವರಿದಿರುವ ಸದ್ಯದ ಪರಿಸ್ಥಿತಿಯನ್ನು ಬದಲಿಸುವುದಕ್ಕೂ ಇದು ಅತ್ಯಗತ್ಯ.

ಇಂತಹ ಅರಿವನ್ನು ಮೂಡಿಸುವ ನಿಟ್ಟಿನಲ್ಲಿ 'ಸೈಬರ್ ವಾರ್ತಿಕಾ'ದಂತಹ ಪ್ರಯತ್ನಗಳ ಪಾತ್ರ ಮಹತ್ವದ್ದು. ಅನಗತ್ಯ ಗಾಬರಿ ಮೂಡಿಸದೆ ಪ್ರಮುಖ ವಿಷಯಗಳನ್ನು ಸ್ಪಷ್ಟವಾಗಿ ತಿಳಿಸುವ ಇಂತಹ ಪ್ರಯತ್ನಗಳನ್ನು ಬೆಂಬಲಿಸುವುದು ನಮ್ಮ ಜವಾಬ್ದಾರಿ. ಅಷ್ಟೇ ಅಲ್ಲ, ಇಂತಹ ಪ್ರಯತ್ನಗಳ ಮೂಲಕ ನಾವು ಪಡೆದುಕೊಂಡ ಮಾಹಿತಿಯನ್ನು ಇತರರ ಜೊತೆಗೂ ಹಂಚಿಕೊಳ್ಳುವುದು ಹಾಗೂ ಅವರಲ್ಲೂ ಜಾಗೃತಿ ಮೂಡಿಸುವುದು ಸೈಬರ್ ಸುರಕ್ಷತೆಯನ್ನು ಹೆಚ್ಚಿಸುವ ನಿಟ್ಟಿನಲ್ಲಿ ನಾವು ಮಾಡಬಹುದಾದ ಅತ್ಯುತ್ತಮ ಕೆಲಸ.

ಟಿ. ಜಿ. ಶ್ರೀನಿಧಿ
ಸಂಪಾದಕ, ejnana.com

Digital devices are a part of almost every aspect of our daily lives, thanks to the revolutions taking place in the information and technology fields. As the volume and scope of IT-based activities increase, safe execution of those activities is more important than ever. Even the uninformed would agree that Cyber Security is very relevant today.

Check out this edition of Cyber Vaartika. From children to adults, individuals to organisations, almost everyone is at risk when it comes to cybercrime these days. Be it stealing personal information through phone call threats or using technical weapons like ransomware, there are many ways to exploit our dependency on information technology today.

This could have many consequences. Direct damage caused by cyber-crimes - for example, economic loss - is just one dimension of these consequences. Fear of such crimes can be detrimental to the growth of the sector if users are reluctant to use information technology tools, which can have a negative impact on the development of our society as a whole. Contrarily, if we stop bothering about the possibility of cyber-crimes, they will increase further.

Increasing awareness about cybercrime and encouraging users to avoid such situations is the need of the hour. The most important thing we can do in this regard is to increase awareness about cyber-crimes. Increasing awareness of how these crimes are committed and how to protect personal information will improve protection against cybercrime.

When all this information is presented in our own language, in a clear, concise and straightforward way that everyone can understand, it will reach more people. Furthermore, there is a need to change the current environment in which people are still vulnerable to online fraud, even when it is being reported on a daily basis.

Initiatives like 'Cyber Vartika' are vital in creating such awareness. We have a responsibility to support such initiatives which clarify important issues without causing unnecessary panic. In addition, the most important thing we can do is to share the information we have gathered through such efforts with others and spread awareness among them.

T. G. Srinidhi
Editor, ejnana.com

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ರ್ಯಾನ್ಸಮ್‌ವೇರ್ ಬೆದರಿಕೆಗಳುಹೆಚ್ಚಾಗಿರುವುದನ್ನು ಸೈಬರ್ ಭದ್ರತೆ ವರದಿಹೊರಗೆಡಹಿದೆ

ವರ್ಷದ ಎರಡನೇ ತ್ರೈಮಾಸಿಕದ ಆರಂಭದಿಂದ ರ್ಯಾನ್ಸಮ್‌ವೇರ್ ಗುಂಪುಗಳು ತಮ್ಮ ಕೌಶಲ್ಯ, ಎದೆಗಾರಿಕೆ ಮತ್ತು ತಂಡವನ್ನು ಹಿಗ್ಗಿಸಿಕೊಂಡು ಹೆಚ್ಚೆಚ್ಚು ದಾಳಿಗಳನ್ನು ನಡೆಸುತ್ತಿವೆ ಎಂದು ರ್ಯಾನ್ಸಮ್‌ವೇರ್ ಇಂಡೆಕ್ಸ್ ಸ್ನಾಪ್‌ಶಾಟ್ ವರದಿ ಹೊರಗೆಡಹಿದೆ. ಡ್ರಾಪರ್-ಆಸ್-ಅ-ಸರ್ವಿಸ್ ಮತ್ತು ಟ್ರೋಜನ್-ಆಸ್-ಅ-ಸರ್ವಿಸ್ ನಂತಹ ತುಂಬ ಮುಂದುವರಿದ ಹೊಸ ಬಗೆಯ ದಾಳಿಗಳನ್ನು ಕೂಡ ರ್ಯಾನ್ಸಮ್‌ವೇರ್ ಗುಂಪುಗಳು ಬಳಸಿಕೊಳ್ಳುತ್ತಿವೆ ಎಂದು ಸಂಶೋಧನೆ ಹೇಳುತ್ತದೆ.
ಡ್ರಾಪರ್-ಆಸ್-ಅ-ಸರ್ವಿಸ್ ಎಂದರೇನು?

DaaS (ಡ್ರಾಪರ್-ಆಸ್-ಅ-ಸರ್ವಿಸ್) ಬಳಸಿ, ಸೈಬರ್ ಅಪರಾಧ ಜಗತ್ತಿಗೆ ಹೊಸದಾಗಿ ಕಾಲಿಡುತ್ತಿರುವವರು ತಮ್ಮ ಮಾಲ್‌ವೇರ್ (ಅಂದರೆ ಅಪಾಯಕಾರಿ ಸಾಫ್ಟ್‌ವೇರ್) ಅನ್ನು ಹಲವಾರು ಕಂಪ್ಯೂಟರ್‌ಗಳಿಗೆ ಡ್ರಾಪರ್ ಎಂಬ ಪ್ರೋಗ್ರಾಮ್ ಮೂಲಕ ಸಾಗಿಸುತ್ತಾರೆ. ಜನರು ನಕಲಿ ಇಲ್ಲವೇ ಅಸಲಿ ಸಾಫ್ಟ್‌ವೇರ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡುವಂತೆ ಈ ಡ್ರಾಪರ್‌ಗಳು ಬಲೆ ಬೀಸುತ್ತವೆ.

ಟ್ರೋಜನ್-ಆಸ್-ಅ-ಸರ್ವಿಸ್ ಎಂದರೇನು?
ಅಪಾಯಕಾರಿ ಸಾಫ್ಟ್‌ವೇರ್ ಇಲ್ಲವೇ ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಹಿಡಿತಕ್ಕೆ ತೆಗೆದುಕೊಳ್ಳಬಹುದಾದ ಅಸಲಿ ಸಾಫ್ಟ್‌ವೇರ್‌ನಂತೆಯೇ ಕಾಣುವ ಸಾಫ್ಟ್‌ವೇರ್ ಬಳಸಲು ಟ್ರೋಜನ್-ಆಸ್-ಅ-ಸರ್ವಿಸ್, ಮೋಸಗಾರರಿಗೆ ಅವಕಾಶ ನೀಡುತ್ತದೆ. ನಿಮ್ಮ ಡೇಟಾ ಇಲ್ಲವೇ ನೆಟ್‌ವರ್ಕ್‌ಗೆ ಕೆಡುಕು ಉಂಟುಮಾಡುವುದು, ಅಡ್ಡಿಪಡಿಸುವುದು, ಹಾನಿ ಮಾಡುವುದು ಇಲ್ಲವೇ ಅಲ್ಲಿಂದ ಕಳ್ಳತನ ಮಾಡಲು ವಿನ್ಯಾಸಗೊಳಿಸಿದ ಕಂಪ್ಯೂಟರ್ ಪ್ರೋಗ್ರಾಮ್‌ಗೆ ಟ್ರೋಜನ್ ಎನ್ನುತ್ತಾರೆ.

ಹಬ್ಬಗಳ ಕಾಲದಲ್ಲಿ 77% ಭಾರತೀಯ ಕಂಪನಿಗಳು ಸೈಬರ್ ದಾಳಿಗೆ ತುತ್ತಾಗಿವೆ: ವರದಿ

'ಸಾಂಕ್ರಾಮಿಕ ಜಗತ್ತಿನಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧ: ಕೋವಿಡ್-19 ರ ಪರಿಣಾಮ' ವರದಿಯ ಪ್ರಕಾರ, ಕಳೆದ 18 ತಿಂಗಳಲ್ಲಿ ಹಬ್ಬಗಳ ಕಾಲದಲ್ಲಿ ಉಂಟಾದ ಸೈಬರ್ ಭದ್ರತೆ ದಾಳಿಗಳಿಂದಾಗಿ 77% ಭಾರತೀಯ ವ್ಯಾಪಾರಗಳು ನಷ್ಟ ಅನುಭವಿಸಿದವು. ಅದೇ ಹೊತ್ತಿನಲ್ಲಿ 81 % ನಷ್ಟು ಜಾಗತಿಕ ಸಂಸ್ಥೆಗಳು ಸೈಬರ್ ದಾಳಿಗಳಲ್ಲಿ ಹೆಚ್ಚಳವನ್ನು ಕಂಡವು.

ಪುನೀತ್ ರಾಜ್‌ಕುಮಾರ್ ಬಗ್ಗೆ ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿ 'ಅವಹೇಳನಕಾರಿ' ಪೋಸ್ಟ್ ಹಾಕಿದ್ದಕ್ಕೆ ಬೆಂಗಳೂರಿನ ಯುವಕ ಸೆರೆ

ಕನ್ನಡದ ಸೂಪರ್‌ಸ್ಟಾರ್ ದಿವಂಗತ ಪುನೀತ್ ರಾಜ್‌ಕುಮಾರ್ ಬಗ್ಗೆ ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿ ಅವಹೇಳನಕಾರಿ ಪೋಸ್ಟ್ ಹಾಕಿದ್ದ ಯುವಕನನ್ನು ಬೆಂಗಳೂರು ನಗರ ಪೊಲೀಸ್‌ನ ಸೈಬರ್ ಅಪರಾಧ ಇಲಾಖೆ ಸೆರೆಹಿಡಿಯಿತು. ಅಕ್ಟೋಬರ್ ಕೊನೆಯ ವಾರದಲ್ಲಿ ಪುನೀತ್ ಅವರು ಹೃದಯಾಘಾತದಿಂದ ಸಾವನ್ನಪ್ಪಿದ್ದರು.
ಪೊಲೀಸ್ ಇಲಾಖೆ ಪ್ರಕಾರ, ಆರೋಪಿಯು ತನ್ನ ಇನ್ಸ್ಟಾಗ್ರಾಮ್ ಖಾತೆಯಲ್ಲಿ ಬಿಯರ್ ಬಾಟಲಿ ಇರುವ ಅವಹೇಳನಕಾರಿ ಪೋಸ್ಟ್ ಹಾಕಿದ್ದ. ಈ ಪೋಸ್ಟ್ ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿ ಮಿಂಚಿನ ವೇಗದಲ್ಲಿ ಹರಡಿ, ಹಲವಾರು ಇಂಟರ್‌ನೆಟ್ ಬಳಕೆದಾರರ ಗಮನಸೆಳೆಯಿತು. ಅವರು ಈ ಪೋಸ್ಟ್‌ಗೆ ಬೆಂಗಳೂರು ಪೊಲೀಸ್ ಇಲಾಖೆಯನ್ನು ತಳುಕಿಸಿದರು.

2020 ರಲ್ಲಿ ಮಕ್ಕಳ ವಿರುದ್ಧದ ಸೈಬರ್ ಅಪರಾಧ ಪ್ರಕರಣಗಳಲ್ಲಿ 400% ಗೂ ಮೀರಿದ ಹೆಚ್ಚಳ: NCRB ಡೇಟಾ

ಇತ್ತೀಚಿನ NCRB ಡೇಟಾ ಪ್ರಕಾರ, 2019 ಕ್ಕೆ ಹೋಲಿಸಿದರೆ 2020 ರಲ್ಲಿ ಮಕ್ಕಳನ್ನು ಒಳಗೊಂಡ ಸೈಬರ್ ಅಪರಾಧ ಪ್ರಕರಣಗಳಲ್ಲಿ 400% ಏರಿಕೆಯಾಗಿತ್ತು. ಅವುಗಳಲ್ಲಿ ಹೆಚ್ಚಿನವು, ಮಕ್ಕಳು ಲೈಂಗಿಕ ಕ್ರಿಯೆಯಲ್ಲಿ ತೊಡಗಿರುವಂತೆ ಚಿತ್ರಿಸಿರುವ ಪ್ರಕಟಣೆಗಳು ಇಲ್ಲವೇ ಚಿತ್ರ/ವಿಡಿಯೊಗಳನ್ನು ಹಂಚುವುದಾಗಿತ್ತು.
ಮಕ್ಕಳ ವಿರುದ್ಧ ಸೈಬರ್ ಅಪರಾಧಗಳನ್ನು ವರದಿ ಮಾಡುವ ಮೊದಲ ಐದು ರಾಜ್ಯಗಳೆಂದರೆ ಉತ್ತರ ಪ್ರದೇಶ (170), ಕರ್ನಾಟಕ (144), ಮಹಾರಾಷ್ಟ್ರ (137), ಕೇರಳ (107), ಮತ್ತು ಒಡಿಶಾ (71).

ಗೋಡ್ಯಾಡಿ ಡೇಟಾ ಸೋರಿಕೆಯಿಂದ ಹತ್ತು ಲಕ್ಷಕ್ಕಿಂತ ಹೆಚ್ಚು ವರ್ಡ್‌ಪ್ರೆಸ್ ಬಳಕೆದಾರರ ಡೇಟಾ ಬಯಲು

ವೆಬ್ ಹೋಸ್ಟಿಂಗ್ ಕಂಪನಿಯಾದ ಗೋಡ್ಯಾಡಿ, ತನ್ನ ಡೇಟಾ ಸೋರಿಕೆಯಾಗಿದೆ ಎಂದು ಸೋಮವಾರ ಘೋಷಿಸಿತು. ಸುಮಾರು 12 ಲಕ್ಷ ಸಕ್ರಿಯ ಮತ್ತು ನಿಷ್ಕ್ರಿಯ ಬಳಕೆದಾರರ ಡೇಟಾಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ ದೊರಕಿತು. 2018 ರಿಂದ ಬೆಳಕಿಗೆ ಬಂದ ಇಂತಹ ಮೂರನೆಯ ಪ್ರಕರಣ ಇದಾಗಿದೆ. 12 ಲಕ್ಷದಷ್ಟು ವರ್ಡ್‌ಪ್ರೆಸ್‌ನ ಸಕ್ರಿಯ ಮತ್ತು ನಿಷ್ಕ್ರಿಯ ಬಳಕೆದಾರರ ಇಮೇಲ್ ವಿಳಾಸಗಳು ಮತ್ತು ಕಸ್ಟಮರ್ ನಂಬರ್‌ಗಳು ಕಳ್ಳರ ಕೈಸೇರಿವೆ. ಇದರಲ್ಲಿ ಸಕ್ರಿಯ ಬಳಕೆದಾರರಿಗೆ ಹೊಂದಿಕೊಂಡ ಡೇಟಾಬೇಸ್ ಯೂಸರ್‌ನೇಮ್ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್‌ಗಳೂ ಸೇರಿವೆ.

ಒಂದು ವರ್ಷಕ್ಕಿಂತ ಕಡಿಮೆ ಸಮಯದಲ್ಲಿ, ಮೋಸದ ವಹಿವಾಟುಗಳಿಂದ 66.5 ಕೋಟಿ ರೂಪಾಯಿಗಳನ್ನು ಪೊಲೀಸ್ ಮರಳಿಪಡೆದಿದ್ದಾರೆ

ಎರಡು ತಿಂಗಳ ಹಿಂದೆ, ಭಾರತೀಯ ರಕ್ಷಣಾ ಪಡೆಗೆ ಸೇರಿದ ಬೆಂಗಳೂರಿನಲ್ಲಿ ನೆಲೆಸಿರುವ ವ್ಯಕ್ತಿಯೊಬ್ಬರು ಸೈಬರ್ ಮೋಸದಲ್ಲಿ 7.2 ಲಕ್ಷ ಕಳೆದುಕೊಂಡರು. ತಾವು ಮೋಸ ಹೋದುದು ಗೊತ್ತಾದ ಕೆಲವೇ ನಿಮಿಷಗಳಲ್ಲಿ, ಅವರು ಕೂಡಲೇ ಪೊಲೀಸ್ ಕಂಟ್ರೋಲ್ ರೂಮ್‌ಗೆ ಕರೆ ಮಾಡಿದರು. ಆಮೇಲೆ ಪೊಲೀಸ್ ಸಿಬ್ಬಂದಿ ಬ್ಯಾಂಕ್‌ನ ಸೈಬರ್ ಸೆಲ್ ತಂಡಕ್ಕೆ ಎಚ್ಚರಿಕೆ ನೀಡದರು. ಅವರು 20 ನಿಮಿಷಗಳ ಒಳಗೆ ಚುರುಕಿನಿಂದ ಕೆಲಸ ಮಾಡಿ, 7.2 ಲಕ್ಷದಲ್ಲಿ 6.5 ಲಕ್ಷ ಮರಳಿಪಡೆದರು.
ಸೈಬರ್ ಅಪರಾಧಗಳು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸೆಕೆಂಡುಗಳ ಒಳಗೆ ನಡೆಯುವುದರಿಂದ, ಎಷ್ಟು ಬೇಗ ಸಾಧ್ಯವೊ ಅಷ್ಟು ಬೇಗ ತಮಗೆ ತಿಳಿಸಬೇಕೆಂದು ಪೊಲೀಸ್ ಇಲಾಖೆ ಹೇಳುತ್ತದೆ. ದಿನದ 24 ಗಂಟೆಯೂ ಸ್ಪಂದಿಸುವ ಸೈಬರ್ ಅಪರಾಧ ಸೆಲ್ ಅನ್ನು ತೆರೆಯಲಾಯಿತು. ದೂರು ನೀಡುವವರು '100' ಇಲ್ಲವೇ '112' ಡಯಲ್ ಮಾಡಿ ಈ ತಂಡವನ್ನು ತಲುಪಬಹುದು.

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ಆನ್‌ಲೈನ್ ಮೋಸಗಳು

ಬೆಂಗಳೂರಿನ ಹ್ಯಾಕರ್ ಒಬ್ಬ ಸರ್ಕಾರದ ಇ-ಸಂಗ್ರಹಣ ವೆಬ್‌ಸೈಟ್ ಒಳನುಗ್ಗಿ ಹಣ ಕದ್ದಿದ್ದಾನೆ

ಸೈಬರ್ ಮೋಸ ಪ್ರಕರಣ: 3.38 ಲಕ್ಷ ರೂಪಾಯಿ ಕಳೆದುಕೊಂಡ 70 ವರ್ಷ ವಯಸ್ಸಿನ ನಿವೃತ್ತ ಆರ್‌ಬಿಐ ಉದ್ಯೋಗಿ

ಹ್ಯಾಕ್ ಆದ ಓಸಿಎಸಿ ಸಿಇಒ ಅವರ ವಾಟ್ಸಾಪ್ ನಂಬರ್: ಪ್ರಕರಣದ ಹಿಂದೆ ನೈಜೀರಿಯಾದ ಸೈಬರ್ ಮೋಸಗಾರರ ತಂಡದ ಕೈವಾಡವಿರುವ ಶಂಕೆ

ಮುಂಬೈ: 2.99 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ, ಕೆವೈಸಿ ಮೋಸದ ಬಲೆಗೆ ಬಿದ್ದ 80 ರ ಹರೆಯದ ಡಾಕ್ಟರ್

3.02 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ, ನಕಲಿ ಕೊರಿಯರ್ ಸೈಬರ್ ಮೋಸದ ಬಲೆಗೆ ಬಿದ್ದ ಮುಂಬೈನ ಮೂರು ಮಂದಿ

ಸೈಬರ್ ಮೋಸ: ವ್ಯಕ್ತಿಯೊಬ್ಬರಿಗೆ 45 ಲಕ್ಷ ಮೋಸ ಮಾಡಿದ್ದಕ್ಕಾಗಿ 7 ಮಂದಿ ಸೆರೆ; 6.5 ಲಕ್ಷ ಮರಳಿಪಡೆಯಲಾಗಿದೆ

ಸೈಬರ್ ಮೋಸದಲ್ಲಿ 7.48 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ 42 ರ ಹರೆಯದ ಹೆಂಗಸು

ಸೈಬರ್ ಮೋಸದಲ್ಲಿ 1.17 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ, ಮನೆಯಿಂದ ಮಾಡುವ ಕೆಲಸ ಹುಡುಕುತ್ತಿದ್ದ ವಿದ್ಯಾರ್ಥಿ

ವಿಮೆ ಪಾಲಿಸಿ ವಿವರಗಳ ಸೋರಿಕೆ ಮಾಡಿದ ಸೈಬರ್ ಮೋಸಗಾರ, ವ್ಯಕ್ತಿಯೊಬ್ಬರಿಗೆ 1.5 ಲಕ್ಷ ಮೋಸ ಮಾಡಿದ

ಸೈಬರ್ ಮೋಸದ ಆರೋಪದಲ್ಲಿ ಬೆಂಗಳೂರಿನ ಏಟಿಎಮ್‌ನಲ್ಲಿ ಸೆರೆಯಾದ ನೈಜೀರಿಯಾದ ಪ್ರಜೆ

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ: ನೀವು ಆನ್‌ಲೈನ್ ಮೋಸಕ್ಕೆ ಒಳಗಾಗಿದ್ದರೆ, ಮೋಸ ನಡೆದ ಎರಡು ಗಂಟೆಗಳ ಒಳಗೆ ಅಧಿಕಾರಿಗಳನ್ನು ಸಂಪರ್ಕಿಸಿ. ಈ ಸಮಯಕ್ಕೆ ತುಂಬ ಮಹತ್ವವಿದೆ. ಏಕೆಂದರೆ ಈ ಸಮಯದಲ್ಲಿ ಖಾತೆಗಳನ್ನು ತಡೆಹಿಡಿಯುವುದು, ಮುಂದಿನ ವಹಿವಾಟುಗಳನ್ನು ನಿಲ್ಲಿಸುವುದು ಮತ್ತು ಹಣವನ್ನು ಮರಳಿ ಪಡೆಯುವ ಸಾಧ್ಯತೆ ಹೆಚ್ಚಿದೆ. ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹಣದ ವಹಿವಾಟು ನಡೆಸುವಾಗ ಯಾವಾಗಲೂ ಹುಶಾರಾಗಿರಿ. ಸೈಬರ್ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ.

Top Cyber News

Cyber security report reveals increase in ransomware threats

The Ransomware Index Spotlight Report reveals that ransomware groups are continuing to increase in "sophistication, boldness, and volume," with numbers up across the board since the second quarter of the year. The research says, Ransomware groups are also employing newer, more advanced approaches in attacks, such as dropper-as-a-service and trojan-as-a-service.

What is Dropper-as-a-Service?
DaaS allows inexperienced threat actors to use droppers to deploy their malware to targets. The victims are duped into downloading pirated or real software by these droppers.

What is Trojan-as-a-Service?
Trojan-as-a-Service allows hackers to use malicious malware or software that appears to be legal yet has the ability to take control of your computer. A Trojan is a computer programme that is designed to damage, disrupt, steal, or otherwise harm your data or network.

77% of Indian companies hit by cyber threat during festive season: Report

According to the report, 'Cybercrime in a Pandemic World: The Impact of Covid-19', 77% of Indian businesses faced downtime owing to cybersecurity risks during the festive season in the previous 18 months. 81 percent of worldwide organisations observed an increase in cyber risks during the same time period.

Bengaluru youth held for 'offensive' social media post on Puneeth Rajkumar

A youth was arrested by Bengaluru city police's Cyber Crime Department for reportedly posting an offensive remark on social media about late Kannada superstar Puneeth Rajkumar. The actor died in late October after suffering a cardiac arrest.
The accused allegedly posted a derogatory post of a beer bottle on his Instagram account, according to the police. The post quickly went viral on social media, attracting the attention of netizens who tagged the Bengaluru police department.

Over 400% rise in cybercrime cases against children in 2020: NCRB data

According to the latest NCRB data, there was a 400% increase in cybercrime cases involving juveniles in 2020 compared to 2019, with the majority of them involving the publication or transmission of materials depicting children in sexually explicit acts.
The top five states reporting cyber-crimes against children are Uttar Pradesh (170), Karnataka (144), Maharashtra (137), Kerala (107), and Odisha (71).

GoDaddy Data Breach Exposes Over 1 million WordPress Customers' Data

GoDaddy, the web hosting company, announced a data breach on Monday that resulted in unauthorised access to data belonging to 1.2 million active and inactive customers, making it the third security incident to surface since 2018. The hacker has access to Email addresses and customer numbers of up to 1.2 million, both active and inactive Managed WordPress customers and database usernames and passwords associated with its active customers

In less than a year, police recover ₹66.5 crore from fraudulent transactions

Two months ago, an Indian armed forces person based out of Bengaluru lost ₹7.2 lakh in a cyber fraud scam. Minutes after realization, he immediately called the police control room, following which the staff alerted the bank's cyber cell team, who responded within 20 minutes. They managed to recover ₹6.5 lakh of the total ₹7.2 lakh.
Since cybercrimes are committed online within seconds, the police initiate a response akin to the 'golden hour' concept. A 24/7 cybercrime cell was set up for quick response, which complainants can access by dialling '100' or '112'.

Top Cyber News

ONLINE FRAUDS

Bengaluru hacker broke into state's e-procurement site and 'stole' funds

Cyber fraud case: ₹3.38 lakhs loss for 70-years old retired RBI employee

WhatsApp number of OCAC CEO hacked: Nigerian cyber fraud gang suspected behind the case

Mumbai: 80-year-old doctor falls for KYC cyber-fraud, loses Rs 2.99 lakh

Three from Mumbai fell prey to fake courier cyber-fraud, lose Rs 3.02 lakh

Cyber fraud: 7 held for duping man of Rs 45L; Rs 6.5L recovered

42-year-old woman loses Rs 7.48 lakh in cyber fraud

Student looking for WFH job loses ₹1.17 lakh in cyber fraud

Cyber fraudster leaks insurance policy details, dupes man of Rs 1.5 lakh

Nigerian held in Bengaluru ATM for cyber fraud

Please remember: If you are a victim of online fraud, contact the authorities during the first two hours of the fraud, also known as the "golden hour". Chances of freezing the accounts, stopping future transactions, and recovering the funds are high during that period. Always be careful while transacting money online, stay cautious and remain cyber alert.

ಸೈಸೆಕ್ ಜಾಗೃತಿ ಭಂಡಾರ

ಮಕ್ಕಳು ಮತ್ತು ವಿಡಿಯೊಗೇಮ್‌ಗಳು

ಮಕ್ಕಳು ಆನ್‌ಲೈನ್ ವಿಡಿಯೊಗೇಮ್‌ಗಳನ್ನು ಆಡುವುದು ತುಂಬ ಸಾಮಾನ್ಯ. ಅವುಗಳಲ್ಲಿ ಯಾವುದು ಮಕ್ಕಳಿಗೆ ತುಂಬ ಒಳ್ಳೆಯದು ಎಂದು ಹೆತ್ತವರು ಯೋಚಿಸುತ್ತಾರೆ. ನಿಮ್ಮ ಮಕ್ಕಳು ಆಡುವ ಗೇಮ್‌ಗಳ ಬಗ್ಗೆ ಇನ್ನಷ್ಟು ತಿಳಿಯಲು ಮತ್ತು ಅವರು ಸರಿಯಾದ ದಾರಿಯಲ್ಲೇ ಇರುವಂತೆ ನೋಡಿಕೊಳ್ಳಲು, ಗೇಮ್ ರೇಟಿಂಗ್ ಮತ್ತು ಪೇರೆಂಟಲ್ ಕಂಟ್ರೋಲ್‌ಗಳಂತಹ ಸಾಧನಗಳು ನಿಮಗೆ ನೆರವಾಗುತ್ತವೆ.

ನಿಮ್ಮ ಮಕ್ಕಳೊಂದಿಗೆ ಮಾತನಾಡಿ:

ಪೇರೆಂಟಲ್ ಕಂಟ್ರೋಲ್‌ನಂತಹ ಸಾಧನಗಳು ನೆರವಾಗುತ್ತವೆ ನಿಜ, ಆದರೆ ಅದರೊಂದಿಗೆ, ಈ ಕೆಳಗಿನ ವಿಷಯಗಳ ಬಗ್ಗೆ ನಿಮ್ಮ ಮಕ್ಕಳೊಂದಿಗೆ ಮಾತನಾಡುವುದು ಕೂಡ ಮುಖ್ಯವಾಗುತ್ತದೆ:

ಅವರು ಯಾವ ಆಟಗಳು ಮತ್ತು ಆಪ್‌ಗಳನ್ನು ಆಡುತ್ತಾರೆ ಇಲ್ಲವೇ ಬಳಸುತ್ತಾರೆ?

ಅವರು ಯಾವ ಆಟಗಳನ್ನು ಆಡಬಹುದು, ಯಾವಾಗ ಆಡಬಹುದು ಇಲ್ಲವೇ ಎಷ್ಟು ಹೊತ್ತು ಆಡಬಹುದು ಎಂಬ ಯಾವುದೇ ಕಟ್ಟುಪಾಡುಗಳಿವೆಯೇ?

ಆನ್‌ಲೈನ್ ಆಟಗಳನ್ನು ಯಾವುದೇ ತೊಂದರೆಯಾಗದಂತೆ ಯಾರೊಂದಿಗೆ ಆಡಬಹುದು?

ವಿಳಾಸ, ಶಾಲೆಯ ಮಾಹಿತಿ ಇಲ್ಲವೇ ಫೋನ್ ನಂಬರ್‌ಗಳಂತಹ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ನೀಡದೆ ಇರುವುದು ಏಕೆ ಮುಖ್ಯವಾಗುತ್ತದೆ?

ಹೆತ್ತವರು ಕೆಳಗಿನವುಗಳನ್ನು ಯಾವಾಗಲೂ ನೋಡಬೇಕು:

<u>ವಯಸ್ಸಿನ ರೇಟಿಂಗ್‌ಗಳು:</u> ತೆರೆಯ ಮೇಲೆ ಇಲ್ಲವೇ ಹೆಚ್ಚಿನ ಗೇಮ್ ಬಾಕ್ಸ್‌ಗಳ ಮೇಲೆ ವಯಸ್ಸಿನ ರೇಟಿಂಗ್ ಸೂಚಿಸುವ ಗುರುತುಗಳು ಕಾಣಬಹುದು (ಚಿಕ್ಕ ಮಕ್ಕಳಿಂದ ಹಿಡಿದು ವಯಸ್ಕರಿಗೆ ಮಾತ್ರ 18+). ಗೇಮ್ ಯಾವ ವಯಸ್ಸಿನವರಿಗೆ ಸರಿಹೊಂದುತ್ತದೆ ಎಂದು ಈ ಗುರುತುಗಳು ಸೂಚಿಸುತ್ತವೆ.

<u>ವಿಷಯದ ವಿವರಣೆಗಳು:</u> ಗೇಮ್ ಬಾಕ್ಸ್‌ನ ಹಿಂಭಾಗದಲ್ಲಿ ಇಲ್ಲವೇ ಆನ್‌ಲೈನ್ ವಿವರಣೆಯಲ್ಲಿ, ಆಟವನ್ನು ಯಾವ ಗುಂಪಿಗೆ ಸೇರಿಸಲಾಗಿದೆ ಎಂಬ ಮಾಹಿತಿ ಇರುತ್ತದೆ. ಉದಾಹರಣೆ: ಕ್ರೌರ್ಯ, ಕಾಮ, ಕಟುವಾದ ಭಾಷೆ ಹಾಗೂ ಜೂಜಾಟ.

ಇನ್ನೊಬ್ಬ ಆಟಗಾರನ ಆನ್‌ಲೈನ್ ನಡವಳಿಕೆ ಸರಿಯಿಲ್ಲದಿರುವಾಗ ಹೇಗೆ ನಿಭಾಯಿಸಬೇಕು? ನಿಮ್ಮ ಮಕ್ಕಳಿಗೆ ತೊಂದರೆಯಾಗುತ್ತಿದ್ದರೆ, ಅವರು ನಿಮ್ಮೊಂದಿಗೆ ಹೇಳಿಕೊಳ್ಳಬೇಕು.

ಪ್ರಮುಖವಾದ ಸಲಹೆಗಳಲ್ಲಿ ಒಂದು, ಕಂಪ್ಯೂಟರ್ ಇಲ್ಲವೇ ವಿಡಿಯೊ ಗೇಮ್ ಸಿಸ್ಟಮ್ ಅನ್ನು ಎಲ್ಲರಿಗೂ ಕಾಣುವಂತೆ ಇಡಬೇಕು. ಇದರಿಂದ, ಮಕ್ಕಳು ಏನು ಆಡುತ್ತಿದ್ದಾರೆ ಎಂದು ಕಣ್ಣಿಡಬಹುದು ಹಾಗೂ ಅನುಮಾನ ಬಂದರೆ, ಪ್ರಶ್ನೆಗಳನ್ನು ಕೇಳಿ, ಕೂಡಲೇ ಮಾತುಕತೆ ನಡೆಸಿ ಬಗೆಹರಿಸಿಕೊಳ್ಳಬಹುದು.

CySeck
Cyber Security Karnataka
K-Tech CoE for Cyber Security

CySecK Awareness Repository

CHILDREN AND VIDEOGAMES

Children playing online videogames is very common. When they do, parents have thoughts about what is the best for them. Fortunately, tools like game ratings and parental controls can help you learn more about the games your children are playing– and ensure that they are on the right track.

TALK TO YOUR CHILDREN

Parental controls are useful, but in addition, it is important to talk to your children about the following topics:

PARENTS SHOULD ALWAYS CHECK FOR

Age Ratings:
Age rating icons (Early Childhood to Adults Only 18+) may be found on the screen or front of most game boxes and indicate which ages the game is appropriate for.

Content Descriptors:
On the back of the game box or in the description (if it is online), the content descriptors list game components that may have caused a certain classification, such as violence, sex, language and gambling.

- What games and apps do they play or use?
- Are there any restrictions on what they can play, when they can play, or how long they can play?
- How to cope with another player's improper online behaviour? And share if they feel trapped.
- With whom is it okay to play online games?
- Why it is important not to provide personal information such as their address, school, or phone numbers?

One of the most important tips is to keep the computer or video game system in a shared space. This allows you to ask questions and have spontaneous conversations.

CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security

ಜಾಗೃತಿ ವೇದಿಕೆ

ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು

ಪಾವತಿವಂಚನೆಗಳ ವಿರುದ್ಧ ನಿಮ್ಮ ವ್ಯಾಪಾರವನ್ನು ರಕ್ಷಿಸಿ

ಪೇಜ್‌ಜಾಕಿಂಗ್ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ 

ಲಾಟರಿಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ

ಲೋನ್ ಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರಿಕೆ 

ಸೈಸೆಕ್ ಸ್ಪರ್ಧೆ #7

ಟ್ವಿಟರ್ ನಲ್ಲಿ ಸೈಬರ್ ಭದ್ರತೆಯನ್ನು ಕಾಪಾಡಲು ಮೂರು ಪ್ರಮುಖ ಸಲಹೆಗಳನ್ನು ನೀಡಿ.

ಪ್ರಮುಖ ಸೈಬರ್ ಭದ್ರತೆ ಸಲಹೆಗಳನ್ನು ನೀಡಿ ಬಹುಮಾನವನ್ನು ನಿಮ್ಮದಾಗಿಸಿಕೊಳ್ಳಿ. ನಿಮ್ಮ ಟ್ವಿಟರ್ ಖಾತೆಯಿಂದ ನಿಮ್ಮ ಉತ್ತರವನ್ನು @CySecKCoE ಎಂದು ಟ್ಯಾಗ್ ಮಾಡಿ #CySecK #CyberVartika ಬಳಸಿ ಕಮೆಂಟ್ ಮಾಡಿ.

ಬಹುವಿಧದ ಉತ್ತರಗಳಿಗೆ ಅನುಮತಿಯಿದೆ.

ಕೊನೆಯ ದಿನಾಂಕ: 10 ಡಿಸೆಂಬರ್ 2021

Awareness Corner

Awareness Posters

Protect your business against payment frauds

Beware of pagejacking! 

Beware of fake lottery scams

Beware of Loan Scams! 

CySecK Contest #7

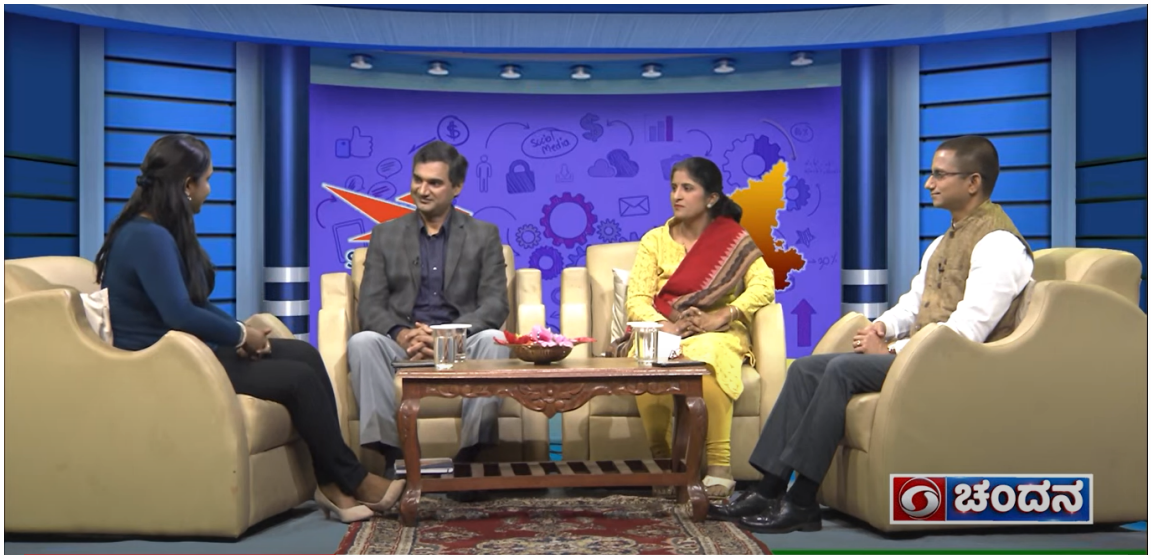
Provide three important tips to stay cybersecure on Twitter.

Put the thinking cap on and tell us the important tips, goodies await the winners. Comment your answer from your Twitter account, tag us @CySecKCoE and use the hashtags #CySecK #CyberVartika

Multiple entries allowed.

Last date: 10 December 2021

ಸೈಸೆಕ್ ವರದಿ/CySecK Update



ಸೈಸೆಕ್-ನ ಕೇಂದ್ರದ ಮುಖ್ಯಸ್ಥ, ಶ್ರೀ ಕಾರ್ತಿಕ್ ರಾವ್ ಬಪ್ಪನಾಡ್ ಅವರು DD ಚಂದನ ದೂರದರ್ಶನದಲ್ಲಿ ಬರುವ ನವಭಾರತದ ಶಿಲ್ಪಿಗಳು ಕಾರ್ಯಕ್ರಮದಲ್ಲಿ ಭಾಗಿಯಾಗಿದ್ದರು.
ಈ ಸಂಚಿಕೆಯನ್ನು ನವೆಂಬರ್ 20, ಶನಿವಾರ 7:30 PM IST ರಂದು DD ಚಂದನ ಟೆಲಿವಿಷನ್‌ನಲ್ಲಿ ಪ್ರಸಾರ ಮಾಡಲಾಯಿತು.
ಸಂಚಿಕೆಯ ಲಿಂಕ್: **https://www.youtube.com/watch?v=3KgDcG0wSIo**

CySecK's Centre Head, Mr. Karthik Rao Bappanad was on DD Chandana Television for a talk on the Karnataka Start-up Champion show.
The episode was telecasted on 20th November, Saturday 7:30 PM IST on DD Chandana Television.
Link for the episode: **https://www.youtube.com/watch?v=3KgDcG0wSIo**

ಸೈಬರ್ ಜಾಗೃತಿ ಮತ್ತು ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿರಲು ಕೆಲವು ಉಪಯುಕ್ತ ಲಿಂಕ್‌ಗಳು ಇಲ್ಲಿವೆ-
Some useful links for staying cyber aware and cyber safe -
1. ಸೈಬರ್ ವಂಚನೆಗಳ ಬಗ್ಗೆ ದೂರು ದಾಖಲಿಸಲು / To lodge complaint against a cyber-crime - cybercrime.gov.in
2. ತಪ್ಪು ಮಾಹಿತಿ ಗುರುತಿಸಲು /To identify fake information: https://factcheck.ksp.gov.in/
3. ಆನ್‌ಲೈನ್ ವಂಚನೆಗೆ ಸಂಬಂಧಿಸಿದ ದೂರುಗಳನ್ನು ನೋಂದಾಯಿಸಲು ಬೆಂಗಳೂರು ಜನರು 112ಗೆ ಕರೆ ಮಾಡಬಹುದು / 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.

Our social media handles

CySeck CoE

@CySecKCoE

CySecKCoE

CySecK

CySecK

CySecKCoE

ಸೈಬರ್ ವರ್ತಿಕಾನ್ನು ನಿಮ್ಮ ಸ್ನೇಹಿತರು ನಿಮಗೆ ಕಳಿಸಿದ್ದಲ್ಲಿ, ಪ್ರತಿ ತಿಂಗಳು ಅದನ್ನು ನೇರವಾಗಿ ಪಡೆಯಲು, ನಮ್ಮ ಸುದ್ಧಿಪತ್ರಿಕೆಯ 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