ಆಗಸ್ಟ್ ೨೦೨೧ | AUGUST 2021

ಸೈಬರ್ ವಾರ್ತಿಕಾ
CYBER VARTIKA

ಸೈಸೆಕ್ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ

CySecK Cyber Security Karnataka
K-Tech CoE for Cyber Security

ಮುನ್ನುಡಿ /Foreword

ತಂತ್ರಜ್ಞಾನದ ಭವಿಷ್ಯ: ಕೃತಕಮತಿಯ ಮೂಲಕ ಸ್ಮಾರ್ಟ್ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ

ಜುಲೈ 2021ರ ಕಸೇಯಾ ರ್ಯಾನ್ಸಮ್‌ವೇರ್ ದಾಳಿ, ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ದೌರ್ಬಲ್ಯಗಳಿಂದ ಉಂಟಾಗುವ ಅಗಾಧ ಹಾನಿಗಳ ಬಗ್ಗೆ ಜಗತ್ತಿನ ಎಲ್ಲಾ ದೇಶಗಳಿಗೂ ಎಚ್ಚರಿಕೆಯ ಸಂದೇಶವಾಗಿದೆ. ಸೈಬರ್ ಸುರಕ್ಷತೆಯು ಯಾವುದೇ ದೇಶದ ಅತಿಮುಖ್ಯ ಆದ್ಯತೆಗಳಲ್ಲೊಂದು ಎಂದರೆ ಉತ್ಪ್ರೇಕ್ಷೆಯಲ್ಲ. ಭಾರತದ ವಿಷಯದಲ್ಲಂತೂ ಇದು ಇನ್ನೂ ಹೆಚ್ಚು ಪ್ರಸ್ತುತ. ಯಾಕೆಂದರೆ ನಾವು ಎಲ್ಲಾ ದಿಕ್ಕುಗಳಿಂದಲೂ ನಿರಂತರವಾಗಿ ಸೈಬರ್ ಅಪಾಯಗಳಿಗೆ ತುತ್ತಾಗುತ್ತಿದ್ದೇವೆ.

ನಾವು ಹಲವಾರು ತಾತ್ಕಾಲಿಕ ಕ್ರಮಗಳ ಮೂಲಕ ಈ ಸೈಬರ್ ಅಪಾಯಗಳನ್ನು ಎದುರಿಸುತ್ತಿದ್ದೇವೆ ಎಂಬುದೇನೋ ನಿಜ. ಆದರೆ, ಒಂದು ಸಮಗ್ರ, ದೀರ್ಘಕಾಲೀನ, ಧ್ಯೇಯ-ಕೇಂದ್ರಿತ ಮತ್ತು ವೈಜ್ಞಾನಿಕ ಪರಿಹಾರ - ಈ ಹೊತ್ತಿನ ಅವಶ್ಯಕತೆ. ಇದನ್ನು ಕಂಡುಕೊಳ್ಳುವಲ್ಲಿ ಶೈಕ್ಷಣಿಕ ಸಂಶೋಧಕರು ಮತ್ತು ಮುಂಚೂಣಿ ಉದ್ದಿಮೆದಾರರು ಮಹತ್ತರ ಪಾತ್ರ ವಹಿಸಬೇಕಿದೆ.

ನಮ್ಮ ದೇಶಕ್ಕೆ ದೀರ್ಘಕಾಲೀನ ಮತ್ತು ಸದೃಢ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕಾರ್ಯತಂತ್ರ ರೂಪಿಸುವಲ್ಲಿ ಗೇಮ್ ಚೇಂಜರ್ ಆಗಬಹುದಾದ ಒಂದು ತಂತ್ರಜ್ಞಾನವೆಂದರೆ ಕೃತಕಮತಿ ಮತ್ತು ಮಶೀನ್ ಲರ್ನಿಂಗ್ (ಎಐಎಂಎಲ್). ಹಾಗಾಗಿಯೇ, ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿಗಾಗಿ ಎಐಎಂಎಲ್ ಬಳಸುವ ಕುರಿತು ಜಗತ್ತಿನ ಪ್ರಮುಖ ವಿಶ್ವವಿದ್ಯಾಲಯಗಳು ಮತ್ತು ಜಾಗತಿಕ ಉದ್ದಿಮೆಗಳಲ್ಲಿ ಸಕ್ರಿಯ ಸಂಶೋಧನೆ ನಡೆಯುತ್ತಿವೆ.

ಎಐಎಂಎಲ್ ಮತ್ತು ಅದಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ಇತರ ತಂತ್ರಜ್ಞಾನಗಳು ಅಗಾಧ ಪ್ರಮಾಣದ ಡೇಟಾವನ್ನು ಮಿಂಚಿನ ವೇಗದಲ್ಲಿ ವಿಶ್ಲೇಷಿಸುವ ಸಾಮರ್ಥ್ಯ ಹೊಂದಿರುವುದರಿಂದ, ಸೈಬರ್ ಸುರಕ್ಷತೆಗೆ ಬರುವ ಯಾವುದೇ ಅಪಾಯವನ್ನು ತಕ್ಷಣವೇ ಅಂದಾಜಿಸಿ, ಪತ್ತೆಹಚ್ಚಿ, ಸರಿಪಡಿಸಲು ಸಾಧ್ಯವಾಗುತ್ತದೆ. ಈ ಆಶಾದಾಯಕ ತಂತ್ರಜ್ಞಾನವನ್ನು ಕಾರ್ಯರೂಪಕ್ಕೆ ತರಬೇಕಿದೆ ಹಾಗೂ ಅದನ್ನು ಮುಂದೆ ನಿಂತು ನಡೆಸಬಲ್ಲ ಪ್ರತಿಭಾನ್ವಿತ ವಿದ್ಯಾರ್ಥಿಗಳು, ಸಂಶೋಧಕರು ಮತ್ತು ವೃತ್ತಿಪರರ ಹೊಸ ಪೀಳಿಗೆಯೊಂದನ್ನು ಸೃಷ್ಟಿಸಲು ಗಣನೀಯ ಹೂಡಿಕೆಯ ಅಗತ್ಯವಿದೆ. ಜೊತೆಗೆ, ಸರ್ಕಾರ, ಶೈಕ್ಷಣಿಕ ಸಂಸ್ಥೆಗಳು ಮತ್ತು ಸ್ಟಾರ್ಟ್‌ಅಪ್‌ಗಳನ್ನು ಒಳಗೊಂಡ ಬೃಹತ್ ಸಹಯೋಗ ವೇದಿಕೆಯನ್ನೂ ಸೃಷ್ಟಿಸಬೇಕಿದೆ.

ಕೃತಕಮತಿ ಹಾಗೂ ಸಂಬಂಧಿತ ತಂತ್ರಜ್ಞಾನಗಳ ಮೂಲಕ ಸ್ಮಾರ್ಟ್ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಸಾಧಿಸುವುದರ ಮೇಲೆ ದೇಶದ ಸೈಬರ್ ಭವಿಷ್ಯ ನಿಂತಿದೆ. ಈ ನಿಟ್ಟಿನಲ್ಲಿ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಸರ್ಕಾರ ಹಾಗೂ ಭಾರತ ಸರ್ಕಾರ ಸ್ಫೂರ್ತಿದಾಯಕ ಹೆಜ್ಜೆಗಳನ್ನು ಇಡುತ್ತವೆ ಹಾಗೂ ಕರ್ನಾಟಕ ಮತ್ತು ಭಾರತವನ್ನು ಸಂಪೂರ್ಣವಾಗಿ ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿಸಲು ಅಗತ್ಯವಿರುವ ಸಂಪನ್ಮೂಲಗಳನ್ನು ಒದಗಿಸಲಿವೆ ಎಂದು ನಮಗೆ ಭರವಸೆಯಿದೆ.

ಪ್ರೊಫೆಸರ್ ವೈ. ನರಹರಿ
ಕಂಪ್ಯೂಟರ್ ಸೈನ್ಸ್ ಮತ್ತು ಆಟೋಮೇಶನ್ ವಿಭಾಗ
ಭಾರತೀಯ ವಿಜ್ಞಾನ ಸಂಸ್ಥೆ

The Future: Smart Cyber Security using Artificial Intelligence

The devastation caused by viruses such as Kaseya in July 2021 serves as a grim reminder for any nation in the world about the boundless damage that can be caused by cyber security loopholes. Needless to say, cyber security is one of the highest priorities for any nation. This is even more true in the case of India since we are under increasing cyber threat from all directions.

While we continue to fight cyber threats through various short term measures, there is a need for a comprehensive, long term, mission oriented, scientific approach to counter cyber threats. Academic researchers and industry leaders have a key role to play here.

One technology that promises to be a game changer for evolving a long-term robust cyber security strategy for our country is Artificial Intelligence and Machine Learning (AIML). It is no surprise that AIML for Cyber Security has emerged as an active area of research in leading universities and the global industry all over the world.

The capability of AIML and other associated technology innovations to analyze massive amounts of data at high speed will enable any security threat to be predicted, detected, and fixed in real-time. It is important to transform this promise into a reality and this calls for substantial investments in preparing a new generation of brilliant students, researchers, and professionals who will be at the forefront of this transformation. It will also call for a grand collaborative platform involving the Government, the academic institutions, the industry, and the startup ecosystem.

The future is in achieving smart cyber security through artificial intelligence and other associated technology innovations. Hope the Karnataka State Government and the Indian Government launch an inspirational initiative in this direction and invest the resources required to make Karnataka and India completely cyber safe.

Professor Y. Narahari
Department of Computer Science and Automation
Indian Institute of Science

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ಐಫೋನ್ ಮತ್ತು ಐಪ್ಯಾಡ್ ಬಳಕೆದಾರರು 'ಕೂಡಲೇ' ತಮ್ಮ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್ ಅಪ್‌ಡೇಟ್ ಮಾಡತಕ್ಕದ್ದು: ಸೆರ್ಟ್-ಇನ್

ಭಾರತದ ಅತ್ಯುನ್ನತ ಸೈಬರ್ ಭದ್ರತಾ ಸಂಸ್ಥೆಯಾದ ಸೆರ್ಟ್-ಇನ್, ಆಪಲ್‌ನ ಹಳೆಯ ಮೊಬೈಲ್ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ಗಳಲ್ಲಿರುವ ದೌರ್ಬಲ್ಯಗಳ ಬಗ್ಗೆ ಎಚ್ಚರಿಸುತ್ತಾ, ಬಳಕೆದಾರರು ಆದಷ್ಟು ಬೇಗ ಇತ್ತೀಚಿನ ಆವೃತ್ತಿಗಳಾದ iOS 14.7.1 ಮತ್ತು iPadOS 14.7.1 ಗಳಿಗೆ ಅಪ್‌ಡೇಟ್ ಮಾಡಿಕೊಳ್ಳಬೇಕೆಂದು ಸೂಚಿಸಿದೆ.
"ಆಪಲ್‌ನ ಐಓಎಸ್ ಮತ್ತು ಐಪ್ಯಾಡ್ ಓಎಸ್‌ನಲ್ಲಿ ಕೆಲವು ದೌರ್ಬಲ್ಯಗಳು ಕಂಡುಬಂದಿದ್ದು, ದೂರದಲ್ಲಿರುವ ಆಕ್ರಮಣಕಾರರು ಇದರ ಲಾಭ ಪಡೆದುಕೊಂಡು ತಮ್ಮಿಚ್ಛೆಯ ಕೋಡ್‌ಗಳನ್ನು ಕಾರ್ಯಗತಗೊಳಿಸಿ, ಬೇರೊಬ್ಬರ ಸಿಸ್ಟಮ್ ಗಳನ್ನು ಗುರಿ ಮಾಡಿ ಆ ಸಿಸ್ಟಮ್ ಗಳ ಅಡ್ಮಿನ್ ಆಕ್ಸೆಸ್ ಪಡೆದುಕೊಳ್ಳುವ ಸಾಧ್ಯತೆಯಿದೆ." ಎಂದು ಸೆರ್ಟ್-ಇನ್ ಎಚ್ಚರಿಸಿದೆ.

ವೊಡಾಫೋನ್-ಐಡಿಯಾ, ಏರ್‌ಟೆಲ್ ಮತ್ತು ಜಿಯೋ ಚಂದಾದಾರರೇ, ಕೆವೈಸಿ ಮೋಸಜಾಲದ ಬಗ್ಗೆ ಎಚ್ಚರ ವಹಿಸಿ!

ನಿಮ್ಮ ಕೆವೈಸಿ ವಿವರಗಳು ಅಪೂರ್ಣವಾಗಿರುವ, ತಡವಾಗಿರುವ ಅಥವಾ ಅವಧಿ ಮೀರಿರುವ ಕಾರಣ ನಿಮ್ಮ ಸಿಮ್ ಕಾರ್ಡನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲಾಗುತ್ತಿದೆ ಎಂದು ಹೆದರಿಸುವ ವಂಚಕ ಎಸ್ಎಂಎಸ್‌ಗಳು ಮತ್ತು ಫೋನ್ ಕರೆಗಳ ಬಗ್ಗೆ ಎಚ್ಚರ ವಹಿಸುವಂತೆ ವೊಡಾಫೋನ್-ಐಡಿಯಾ, ಭಾರ್ತಿ ಏರ್‌ಟೆಲ್ ಮತ್ತು ರಿಲಾಯನ್ಸ್ ಜಿಯೋ ಕಂಪನಿಗಳು ತಮ್ಮ ಗ್ರಾಹಕರಿಗೆ ಸೂಚಿಸಿವೆ.

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ: ಸೈಬರ್ ವಂಚಕರು ಕಂಪನಿ ಪ್ರತಿನಿಧಿಗಳ ಸೋಗು ಹಾಕಿಕೊಂಡು, ಈ ಕೂಡಲೇ ನಿಮ್ಮ ಕೆವೈಸಿ ಅಪ್‌ಡೇಟ್ ಮಾಡದಿದ್ದರೆ ನಿಮ್ಮ ಸಿಮ್ ಕಾರ್ಡನ್ನು ಬ್ಲಾಕ್ ಮಾಡುತ್ತೇವೆಂದು ಬೆದರಿಸುತ್ತಾರೆ. ಪರಿಶೀಲನೆಯ ನೆಪದಲ್ಲಿ ಅವರು ಬಳಕೆದಾರರ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವಂತೆಯೂ ಕೇಳಬಹುದು. ನಿಮ್ಮ ಕೆವೈಸಿ ಮಾಹಿತಿಯನ್ನು ಯಾರಿಗೂ ಬಿಟ್ಟುಕೊಡಬೇಡಿ, ಓಟಿಪಿ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ ಹಾಗೂ ಎಸ್ಎಂಎಸ್‌ನಲ್ಲಿರುವ ಯಾವುದೇ ಲಿಂಕನ್ನು ಒತ್ತಬೇಡಿ.

ಸಾವಿರಾರು ಫೇಸ್‌ಬುಕ್ ಖಾತೆಗಳನ್ನು ಹ್ಯಾಕ್ ಮಾಡಿದ ಹೊಸ ಆಂಡ್ರಾಯ್ಡ್ ಮಾಲ್‌ವೇರ್

ಮಾರ್ಚ್ 2021ರಿಂದ ಈಚೆಗೆ, ಗೂಗಲ್ ಪ್ಲೇಸ್ಟೋರ್ ಮತ್ತಿತರ ಥರ್ಡ್ ಪಾರ್ಟಿ ಆಪ್ ಮಾರುಕಟ್ಟೆಗಳ ಮೂಲಕ ಹಂಚಿಕೆಯಾದ ವಂಚಕ ಆಪ್‌ಗಳಿಂದ ಕನಿಷ್ಟ 144 ದೇಶಗಳಿಗೆ ಸೇರಿದ 10,000ಕ್ಕೂ ಹೆಚ್ಚು ಜನರ ಫೇಸ್‌ಬುಕ್ ಖಾತೆಗಳಲ್ಲಿ ಒಂದು ಹೊಚ್ಚಹೊಸ ಆಂಡ್ರಾಯ್ಡ್ ಮಾಲ್‌ವೇರ್ ನುಸುಳಿದೆಯೆಂದು ವರದಿಯಾಗಿದೆ. ಈ ದಾಳಿಗೆ ತುತ್ತಾದ ಖಾತೆಗಳನ್ನು ಪೇಜ್‌ಗಳು, ವೆಬ್‌ಸೈಟ್‌ಗಳು ಮತ್ತು ಉತ್ಪನ್ನಗಳ ಜನಪ್ರಿಯತೆ ಹೆಚ್ಚಿಸುವುದು, ಸುಳ್ಳುಸುದ್ದಿ ಹರಡುವುದು ಮತ್ತು ರಾಜಕೀಯ ಪ್ರಚಾರ ಸೇರಿದಂತೆ ಹಲವಾರು ದುರುದ್ದೇಶಗಳಿಗೆ ಬಾಟ್‌ನೆಟ್ ರೀತಿಯಲ್ಲಿ ಬಳಸಬಹುದಾಗಿದೆ.

ಭಾರತದ ಬ್ಯಾಂಕಿಂಗ್ ಬಳಕೆದಾರರಿಗೆ ಕುತ್ತು ತರಲಿರುವ ಹೊಸ ಫಿಶಿಂಗ್ ದಾಳಿ

ಭಾರತದ ಸೈಬರ್ ವಂಚಕರು ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಪೋರ್ಟಲ್‌ಗಳನ್ನು ನಕಲು ಮಾಡುವ ಹೊಸದೊಂದು ಫಿಶಿಂಗ್ ದಾಳಿಯ ಮೂಲಕ ಭಾರತೀಯ ಬ್ಯಾಂಕಿಂಗ್ ಬಳಕೆದಾರರನ್ನು ಗುರಿ ಮಾಡಿದ್ದಾರೆ ಎಂದು ದೇಶದ ಸೈಬರ್ ಭದ್ರತಾ ಸಂಸ್ಥೆ ತಿಳಿಸಿದೆ. ಭಾರತೀಯ ಕಂಪ್ಯೂಟರ್ ತುರ್ತುಸ್ಥಿತಿ ನಿರ್ವಹಣಾ ತಂಡ (ಸೆರ್ಟ್-ಇನ್) ಪ್ರಕಾರ, ಮೊಬೈಲ್ ಸಂಖ್ಯೆ, ಓಟಿಪಿ ಮತ್ತು ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಪಾಸ್‌ವರ್ಡ್‌ನಂತಹ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಕದಿಯುವ ಉದ್ದೇಶದಿಂದ ವಂಚಕರು ಈ ಫಿಶಿಂಗ್ ವೆಬ್‌ಸೈಟ್‌ಗಳನ್ನು ಎನ್‌ಗ್ರೋಕ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮಿನಲ್ಲಿ ಶೇಖರಿಸಿದ್ದಾರೆ

ಭಾರತದ ಅತಿದೊಡ್ಡ ಬಿ2ಬಿ ಮಾರುಕಟ್ಟೆ ಇಂಡಿಯಾಮಾರ್ಟ್‌ನಲ್ಲಿ ಡೇಟಾ ಸೋರಿಕೆ, ಹ್ಯಾಕರ್‌ಗಳ ಪಾಲಾಯ್ತು 3.8 ಕೋಟಿ ಸದಸ್ಯರ ಗೌಪ್ಯ ಮಾಹಿತಿ

ಇಂಡಿಯಾ ಮಾರ್ಟ್ ವೆಬ್‌ಸೈಟ್‌ನಿಂದ ಅಗಾಧ ಪ್ರಮಾಣದ ಮಾಹಿತಿಯನ್ನು ತೆಗೆದು, ಅದನ್ನು ಹ್ಯಾಕಿಂಗ್ ಫೋರಮ್‌ಗಳಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳಲಾಗಿದೆ ಎಂದು ಖ್ಯಾತ ಡೇಟಾ ಸೋರಿಕೆ ಮಾಹಿತಿಜಾಲ 'ಹ್ಯಾವ್ ಐ ಬೀನ್ ಪ್ವೆನ್ಡ್'ನ (Have I Been Pwned) ಸೃಷ್ಟಿಕರ್ತ ಟ್ರಾಯ್ ಹಂಟ್ ತಿಳಿಸಿದ್ದಾರೆ. ಕದ್ದಿರುವ ಮಾಹಿತಿಯಲ್ಲಿ ಸುಮಾರು 3.8 ಕೋಟಿ ಬಳಕೆದಾರರ ಫೋನ್ ನಂಬರ್, ಇಮೇಲ್ ವಿಳಾಸ, ಕಂಪನಿ ಹೆಸರುಗಳು ಮತ್ತು ಸಂಪರ್ಕ ವಿಳಾಸದಂತಹ ಮಾಹಿತಿಯೂ ಸೇರಿದೆ.
ನಿಮ್ಮ ಇಮೇಲ್ ಖಾತೆ ಅಥವಾ ಫೋನ್ ಸಂಖ್ಯೆ ಇಂತಹ ದಾಳಿಗೆ ತುತ್ತಾಗಿದೆಯೇ ಎಂದು ನೋಡಲು https://haveibeenpwned.com/ ಗೆ ಭೇಟಿ ನೀಡಿ.
ದಾಳಿಗೆ ತುತ್ತಾಗಿದ್ದಲ್ಲಿ, ಕೂಡಲೇ ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು (ಅದರಲ್ಲೂ, ದಾಳಿಗೆ ತುತ್ತಾದ ಖಾತೆಗಳ ಪಾಸ್‌ವರ್ಡನ್ನು) ಬದಲಾಯಿಸಿ. ಸಂಬಂಧಪಟ್ಟ ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ಮಲ್ಟಿಫ್ಯಾಕ್ಟರ್ ಅಥೆಂಟಿಕೇಶನ್ ಸೌಲಭ್ಯವಿದ್ದರೆ, ಅದನ್ನು ತಪ್ಪದೇ ಬಳಸಿ.

ವಾಟ್ಸಾಪ್‌ನ ಮಾರ್ಪಡಿಸಿದ ಆವೃತ್ತಿಯಲ್ಲಿತ್ತು ಟ್ರಯಾಡಾ ಟ್ರೋಜನ್

ಆಂಡ್ರಾಯ್ಡ್ ಬಳಕೆದಾರರಿಗೆ ಟ್ರೋಜನ್ ಸೋಂಕಿತ ವಾಟ್ಸಾಪ್ ಆವೃತ್ತಿಯೊಂದು ಲಭ್ಯವಿದ್ದು, ಇದು ಚಾಟ್‌ಗಳನ್ನು ಕದ್ದು ನೋಡುತ್ತದೆ, ದುರುದ್ದೇಶಪೂರಿತ ಪೇಲೋಡ್‌ಗಳನ್ನು ಪಸರಿಸುತ್ತದೆ, ಫುಲ್-ಸ್ಕ್ರೀನ್ ಜಾಹೀರಾತುಗಳನ್ನು ಪ್ರಕಟಿಸುತ್ತದೆ ಮತ್ತು ಬಳಕೆದಾರರನ್ನು ಅವರಿಗೆ ಅರಿವಿಲ್ಲದೆಯೇ ಅನವಶ್ಯಕ ಪ್ರೀಮಿಯಂ ಸದಸ್ಯತ್ವಗಳಿಗೆ ಸೈನ್-ಅಪ್ ಮಾಡಿಸುತ್ತದೆ. ಕ್ಯಾಸ್ಪರ್ಸ್ಕಿ ಸಂಸ್ಥೆ ಪತ್ತೆಹಚ್ಚಿರುವ ಈ ಮಾರ್ಪಡಿಸಿದ ಆವೃತ್ತಿಯು ಡಿವೈಸ್‌ನ ವಿಶೇಷ ಗುರುತುಗಳನ್ನು ಸಂಗ್ರಹಿಸಿ, ಅವನ್ನು ರಿಮೋಟ್ ಸರ್ವರ್ ಜೊತೆ ಹಂಚಿಕೊಳ್ಳುತ್ತದೆ. ಇದಕ್ಕೆ ಬದಲಾಗಿ ಆ ಸರ್ವರ್, ಒಂದು ಪೇಲೋಡ್ ಲಿಂಕ್ ಕಳುಹಿಸುತ್ತದೆ. ಟ್ರಯಾಡಾ ಟ್ರೋಜನ್, ಈ ಲಿಂಕ್ ಮೂಲಕ ಪೇಲೋಡನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ, ಡಿಕ್ರಿಪ್ಟ್ ಮಾಡಿ, ಕಾರ್ಯಾಚರಣೆ ಆರಂಭಿಸುತ್ತದೆ.

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ: ಇಂತಹ ನಯವಂಚಕ ಆಪ್‌ಗಳ ದಾಳಿಯಿಂದ ತಪ್ಪಿಸಿಕೊಳ್ಳಲು, ಬಳಕೆದಾರರು ಗೂಗಲ್ ಪ್ಲೇಸ್ಟೋರ್ ಮತ್ತು ಆಪಲ್ ಆಪ್ ಸ್ಟೋರ್‌ನಂತಹ ನಂಬಿಕಸ್ಥ ಮೂಲಗಳಿಂದ ಮಾತ್ರವೇ ಆಪ್‌ಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಿಕೊಳ್ಳತಕ್ಕದ್ದು.

Top Cyber News

iPhone and iPad users must update their operating systems 'immediately', says CERT-In

India's top cyber agency has issued a warning about a vulnerability in older versions of Apple's mobile operating software, urging users to update to the most recent version, iOS 14.7.1 and iPad OS 14.7.1, as soon as possible.

"A Vulnerability has been detected in Apple iOS and iPad OS that might be exploited by a remote attacker to execute arbitrary code and gain elevated privileges on a targeted system," according to a CERT-In advisory that was recently released.

Subscribers of Vodafone Idea, Airtel, and Jio are warned against KYC fraud

Vodafone Idea, Bharti Airtel, and Reliance Jio have warned their customers to be wary of fraudulent SMS and phone calls from fraudsters threatening to deactivate SIM cards by falsely stating that the subscriber's KYC credentials are incomplete, delayed, or expired.

Please remember: Cyber crooks pose as company representatives and threaten users with a SIM block if KYC is not updated then and there. They may also ask the users to share confidential information in the name of verification. Never give out your KYC information over the phone, share your OTP, or click on any link in an SMS.

New android malware hacks thousands of Facebook accounts

Since March 2021, a new Android malware has been reported to have infiltrated Facebook accounts of over 10,000 people in at least 144 countries via fraudulent apps distributed through the Google Play Store and other third-party app marketplaces. The accounts compromised can be used as a botnet for a variety of purposes, including increasing the popularity of pages, sites, and products, as well as spreading disinformation and political propaganda.

This latest phishing attack may target banking users in India.

Scammers in India are targeting banking users with a new sort of phishing assault that imitates internet banking portals, according to the country's cybersecurity agency. Scammers are hosting phishing websites on the ngrok platform to acquire sensitive information such as mobile numbers, OTP's and internet banking passwords, according to the Indian Computer Emergency Response Team, or CERT-In.

IndiaMART, India's largest B2B marketplace, appears to have had a data breach, with over 38 million records of its members available on a forum.

Troy Hunt, the author of the data-breach record database Have I Been Pwned, said he discovered a massive data dump being extracted from the website IndiaMART and disseminated on hacking forums. The data set included information such as phone numbers, e-mail addresses, company names, and contact addresses of 38 million users.
Check https://haveibeenpwned.com/ to see whether your email account or phone number has been compromised.
If you discover you've been pwned, reset your passwords immediately (especially for those affected accounts). Set up multi-factor authentication if the website offers that option.

Triada Trojan was discovered in a modified version of WhatsApp for Android.

A trojanized version of the WhatsApp messaging programme is available for Android that can intercept text conversations, serve malicious payloads, display full-screen advertising, and sign up users for unwanted premium memberships without their knowledge. The altered version of the software found by Kaspersky has the ability to collect unique device identifiers, which are provided to a remote server, followed by answering with a link to a payload, and then Triada trojan downloads, decrypts, and launches.

Please remember: To prevent falling prey to fraudulent apps, users should only install programmes from trusted sources, such as Google Play and Apple's App Store.

ಸೈಸೆಕ್ ಜಾಗೃತಿ ಭಂಡಾರ

KYC ಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ

KYC ಎಂದರೇನು?

ಗುರುತಿಗಾಗಿ ಬ್ಯಾಂಕ್ ಇಲ್ಲವೇ ಬೇರೆ ಹಣಕಾಸು ಸಂಸ್ಥೆಗಳಿಗೆ, ಬಳಕೆದಾರರು ತಮ್ಮ ಪರಿಶೀಲಿಸಲ್ಪಟ್ಟ ಮಾಹಿತಿಯನ್ನು ಒದಗಿಸುವ ಪ್ರಕ್ರಿಯೆಯೇ ನೋ ಯುವರ್ ಕಸ್ಟಮರ್ (KYC) ಅಂದರೆ ನಿಮ್ಮ ಬಳಕೆದಾರರನ್ನು ತಿಳಿಯಿರಿ. ಕಪ್ಪು ಹಣವನ್ನು ಬಿಳಿಮಾಡುವ ಕೆಲಸದಲ್ಲಿ ಮತ್ತು ಮೋಸದ ಯೋಜನೆಗಳಲ್ಲಿ ತೊಡಗಿಸಿಕೊಂಡಿರುವ ಜನರ ಜೊತೆ, ಹಣಕಾಸು ಸಂಸ್ಥೆಯೊಂದು ಯಾವ ವ್ಯವಹಾರವನ್ನೂ ಇಟ್ಟುಕೊಳ್ಳದಂತೆ KYC ನೋಡಿಕೊಳ್ಳುತ್ತದೆ.

KYC ಮೋಸಗಳು ಯಾವುವು?

ನಿಮಗೆ ಒಂದು SMS ಬರುತ್ತದೆ. ಅದರಲ್ಲಿ ಈ ಕೆಳಗಿನ ಮಾಹಿತಿ ಇರುತ್ತದೆ:
1. ನಿಮ್ಮ KYC ಗಡುವು ಮುಗಿದಿದೆ
2. KYC ಅನ್ನು ಹೊಸದಾಗಿಸಬೇಕು
3. ನಿಮ್ಮ KYC ಅಪ್‌ಡೇಟ್ ಮಾಡಿ, ಇಲ್ಲವಾದರೆ, ನಿಮ್ಮ ಖಾತೆಯನ್ನು 24 ಗಂಟೆ ನಿಲ್ಲಿಸಲಾಗುತ್ತದೆ.

ಇಂತಹ ಸಂದೇಶಗಳನ್ನು ನಂಬಬಿರಿ. ನೀವು ಬೆವರು ಹರಿಸಿ ದುಡಿದ ಹಣವನ್ನು ದೋಚುವುದಕ್ಕಾಗಿ ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯಲು ಮೋಸಗಾರರು ಇಂತಹ ದಾರಿಗಳನ್ನು ಬಳಸುತ್ತಾರೆ. ನಿಮಗೆ ಯಾರಾದರೂ ಕರೆ ಮಾಡಿ, ನಿಮ್ಮ KYC ಕೆಲಸ ಮುಗಿಸಲು ಇಲ್ಲವೇ ಹೊಸದಾಗಿಸಲು, Any desk ಇಲ್ಲವೇ Quick Support ನಂತಹ ಆ್ಯಪ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ಹೇಳಿದರೆ, ಅವರ ಮಾತಿನಂತೆ ನಡೆದುಕೊಳ್ಳಬೇಡಿ. ಯಾಕೆಂದರೆ, ಇಂತಹ ಆ್ಯಪ್‌ಗಳಿಂದ ಮೋಸಗಾರರು ದೂರದಿಂದಲೇ ನಿಮ್ಮ ಡಿವೈಸ್‌ಗಳನ್ನು ಅವರ ಹಿಡಿತಕ್ಕೆ ತೆಗೆದುಕೊಳ್ಳುತ್ತಾರೆ.

KYC ಮೋಸಗಳಿಂದ ನಿಮ್ಮನ್ನು ನೀವು ಕಾಪಾಡಿಕೊಳ್ಳುವುದು ಹೇಗೆ?

ಇಂತಹ ನುರಿತ ಸೈಬರ್ ಅಪರಾಧಗಳು ಕೂಡ ಇವೆ ಎಂದು ತಿಳಿದುಕೊಳ್ಳಲು, ಬಳಕೆದಾರರು ಇಂಟರ್‌ನೆಟ್, ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಮತ್ತು ಮೊಬೈಲ್‌ಗಳಂತಹ ಡಿಜಿಟಲ್ ತಂತ್ರಜ್ಞಾನಗಳ ಬಳಕೆಯ ಬಗ್ಗೆ ಹೆಚ್ಚೆಚ್ಚು ಅರಿವು ಮೂಡಿಸಿಕೊಳ್ಳಬೇಕು. ಯಾವುದೇ ಬ್ಯಾಂಕ್ ಇಲ್ಲವೇ ಡಿಜಿಟಲ್ ಇ-ವಾಲೆಟ್, SMS ಇಲ್ಲವೇ ವಾಟ್ಸಾಪ್ ಮೂಲಕ KYC ನಡೆಸುವುದಿಲ್ಲ ಎಂಬುದನ್ನು ಬಳಕೆದಾರರು ನೆನಪಿಟ್ಟುಕೊಳ್ಳಬೇಕು.

- KYC ಪ್ರಕ್ರಿಯೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಕೂಡ ನಡೆಯಬಹುದಾದರೂ, ಯಾವುದೇ ಬ್ಯಾಂಕ್ ಇಲ್ಲವೇ ಹಣಕಾಸು ಸಂಸ್ಥೆ Any desk ನಂತಹ ಹೊರಗಿನ ಆ್ಯಪ್‌ಗಳನ್ನು ಬಳಸಿ ನಿಮಗೆ KYC ಮಾಡಲು ಹೇಳುವುದಿಲ್ಲ.
- ಬ್ಯಾಂಕ್ ಒಳಗೊಂಡಂತೆ ಯಾರಿಗೂ ಕೂಡ, ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆ ಮಾಹಿತಿ, ಕ್ರೆಡಿಟ್ ಇಲ್ಲವೇ ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಮಾಹಿತಿ, UPI ಪಿನ್ ಇಲ್ಲವೇ OTP ಕೊಡಬೇಡಿ.
- ಕೂಡಲೇ ನಿಮ್ಮ ಬ್ಯಾಂಕಿಗೆ ತಿಳಿಸಿ. ಹತ್ತಿರದ ಪೊಲೀಸ್ ಸ್ಟೇಶನ್‌ಗೆ ಹೋಗಿ ದೂರು ಸಲ್ಲಿಸಿ ಹಾಗೂ ನ್ಯಾಶನಲ್ ಸೈಬರ್ ಕ್ರೈಮ್ ರಿಪೋರ್ಟಿಂಗ್ ಪೋರ್ಟಲ್ ಆದ cybercrime.gov.in ನಲ್ಲಿ ಆನ್‌ಲೈನ್ ದೂರು ಸಲ್ಲಿಸಿ.

CySeck
Cyber Security Karnataka
K-Tech CoE for Cyber Security

CySecK Awareness Repository

Beware of KYC frauds

What is KYC?

Know Your Customer (KYC) is a process in which customers provide verified information to banks or other financial institutions in order to be identified. KYC ensures that a financial institution isn't doing business with people who are involved in money laundering and fraud schemes.

What are KYC frauds?

If you receive an SMS that says:

1. Your KYC has expired
2. Or it needs to be renewed
3. Update your KYC, otherwise, your account will be suspended for 24 hours.

Never trust these messages. These are scammers aiming to obtain your personal information in order to cheat you of your hard-earned money. If someone calls you and asks you to download an app like Any desk or Quick Support to complete or renew your KYC, do not do so because these apps give remote access of your device to the scammers.

How to protect from KYC frauds

Customers will need to become more digitally literate in order to be aware of these sophisticated cybercrimes. Customers should keep in mind that no bank or digital e-wallet will conduct KYC over SMS or WhatsApp.

Regardless of the fact that the KYC procedure can be digital, no bank institution requires you to complete it via third-party apps such as Any desk.

Never give out bank account information, credit or debit card information, UPI pin or OTP to anyone, including the bank.

Notify your bank right away and file a complaint in the nearest police station. Report online via cybercrime.gov.in, the National Cyber Crime Reporting Portal.

CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security

ಜಾಗೃತಿ ವೇದಿಕೆ

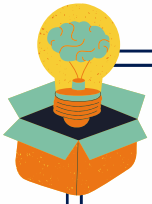
ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು

ಇಮೇಲ್ ನಲ್ಲಿ ಬರುವ ನಕಲಿ ಉದ್ಯೋಗ ಕೊಡುಗೆಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ

ಉಚಿತ ಉಡುಗೊರೆಯ ಮೋಸದ ಬಗ್ಗೆ ಎಚ್ಚರವಾಗಿರಿ

ರಿಮೋಟ್ ಆ್ಯಕ್ಸೆಸ್ ಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ

ಸುಳ್ಳು ಸುದ್ದಿಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ



ಸೈಸೆಕ್ ಸ್ಪರ್ಧೆ #4

ಶೀರ್ಷಿಕೆ ಸ್ಪರ್ಧೆ

ಇದೋ ಇಲ್ಲಿದೆ ನಿಮ್ಮ ಬುದ್ಧಿಮತ್ತೆಗೊಂದು ಸವಾಲು.... ಈ ಮೇಲಿನ ಚಿತ್ರಕ್ಕೆ ಅತ್ಯುತ್ತಮವಾದ ಶೀರ್ಷಿಕೆಯನ್ನು ತಿಳಿಸಿ ಬಹುಮಾನವನ್ನು ನಿಮ್ಮದಾಗಿಸಿಕೊಳ್ಳಿ. ನಮ್ಮ ಟ್ವಿಟರ್ **@CySecKCoE** ಖಾತೆಯಲ್ಲಿರುವ ಸೈಸೆಕ್ ಸ್ಪರ್ಧೆ #4 ನ ಪೋಸ್ಟರ್ ಮೇಲೆ ನಿಮ್ಮ ಉತ್ತರವನ್ನು ಕಮೆಂಟ್ ಮಾಡಿ.
ಬಹುವಿಧದ ಉತ್ತರಗಳಿಗೆ ಅನುಮತಿಯಿದೆ.

ಕೊನೆಯ ದಿನಾಂಕ: 08 ಸೆಪ್ಟೆಂಬರ್ 2021

Awareness Corner

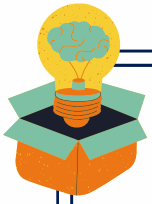
Awareness Posters

Beware of fake job offers through email

Beware of free gift scams

Beware of Remote Access Scams

Beware of Fake News



CySecK Contest #4

Caption contest

Put the thinking cap on and tell us the best caption for the image, goodies await the winners. Comment your answer on our latest post titled CySecK Contest #4 on our twitter @CySecKCoE.
Multiple enteries allowed.

Last date: 08 September 2021

ಸೈಸೆಕ್ ವರದಿ/CySecK Update

ಸಮ್‌ಗಚ್ಚದ್ವಮ್ ಸರಣಿಯ ವೆಬಿನಾರ್‌ಗಳ ಒಂದು ಭಾಗವಾಗಿ- **"Importance of Security During Cloud Migration"** ಎಂಬ ವಿಷಯದ ಕುರಿತು ವಿದ್ಯಾರ್ಥಿಗಳು / ಅಧ್ಯಾಪಕರು / ಕೆಲಸ ಮಾಡುವ ವೃತ್ತಿಪರರಿಗೆ ಉಚಿತ ವೆಬ್‌ನಾರ್ ನಡೆಸಲಾಯಿತು. ಪ್ರಾಫೇಜ್ ಟೆಕ್ನಾಲಜೀಸ್ ಸಂಸ್ಥೆಯ ಶ್ರೀ ವೈಶಾಖ್ ಮತ್ತು ಶ್ರೀಮತಿ ಲಕ್ಷ್ಮಿ ದಾಸ್ ಇವರು ಸಂಪನ್ಮೂಲ ವ್ಯಕ್ತಿಗಳಾಗಿದ್ದರು.

ವೆಬಿನಾರ್‌ನ ಲಿಂಕ್- https://www.youtube.com/watch?v=BNpjyNQ9QgI

As a part of Samgacchadhwam series of webinars- a free webinar was conducted for students / faculty / working professionals on the topic "**Importance of Security During Cloud Migration**". Mr. Vaisakh & Ms. Lakshmi Das from Prophaze Technologies, were the speakers.

Link of the webinar- https://www.youtube.com/watch?v=BNpjyNQ9QgI

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 / Bengalorians 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 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