ಮೇ ೨೦೨೧ | MAY 2021

ಸೈಬರ್ ವಾರ್ತಿಕಾ
CYBER VARTIKA

ಮುನ್ನುಡಿ /Foreword

ಪ್ರೀತಿಯ ಬಂಧುಗಳೇ,

ಸೈಸೆಕ್-ನಿಂದ ಸವಿಹಾರೈಕೆಗಳು!

ಸೈಬರ್ ವಾರ್ತಿಕಾವನ್ನು ಸಂತೋಷದಿಂದ ನಿಮ್ಮ ಮುಂದಿಡುತ್ತಿದ್ದೇವೆ - ಇದು ಸೈಸೆಕ್-ನ ಮಾಸಿಕ ದ್ವಿಭಾಷಾ ಸುದ್ದಿಪತ್ರವಾಗಲಿದೆ. ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನದ ಎಲ್ಲಾ ಬಳಕೆದಾರರಿಗೂ ಆಸಕ್ತಿಕರವೆನಿಸುವ ಸೈಬರ್ ಭದ್ರತೆ, ಸುರಕ್ಷತೆ, ನಂಬಿಕೆ ಮತ್ತು ಗೌಪ್ಯತೆಗೆ ಸಂಬಂಧಿಸಿದ ಸುದ್ದಿಗಳನ್ನು ಇದು ಒಳಗೊಂಡಿರುತ್ತದೆ. ನಮ್ಮ ಡಿಜಿಟಲ್ ಹೆಜ್ಜೆಗುರುತು ಹೆಚ್ಚಾದಂತೆ ಮತ್ತು ನಾವು ಡಿಜಿಟಲ್ ಮಾಧ್ಯಮದಲ್ಲಿ ಹೆಚ್ಚು ಹೆಚ್ಚು ಡೇಟಾವನ್ನು ಹಂಚಿಕೊಳ್ಳುತ್ತಿದ್ದಂತೆ, ಸೈಬರ್ ಅಪಾಯಗಳು ಮತ್ತು ಆರೋಗ್ಯಕರ ಸೈಬರ್ ಅಭ್ಯಾಸಗಳ ಬಗೆಗಿನ ಅರಿವು ಪ್ರಾಮುಖ್ಯತೆ ಪಡೆದುಕೊಳ್ಳುತ್ತಿದೆ. ಸೈಬರ್ ಅಪಾಯಗಳ ಬಗ್ಗೆ ನಿಮಗೆ ಅರಿವು ಮೂಡಿಸಲು ಮತ್ತು ನಮ್ಮ ಸಮಾಜವನ್ನು ಹೆಚ್ಚು ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು, **ಸೈಬರ್ ವಾರ್ತಿಕಾ** ಸೈಸೆಕ್-ನ ಪ್ರಯತ್ನವಾಗಿದೆ.

ಅಂಟುರೋಗದ ಮಂಕು ಕವಿದಿರುವಾಗಲೇ, ಹಾಗೂ ನಮ್ಮ ಹತ್ತಿರದವರ ಆರೋಗ್ಯ ಮತ್ತು ಯೋಗಕ್ಷೇಮದ ಬಗ್ಗೆ ಹೆಚ್ಚುತ್ತಿರುವ ಕಳವಳಗಳ ನಡುವೆಯೇ, ಸೈಬರ್ ಅಪರಾಧಿಗಳು ತಮ್ಮ ಹಳೆಯ ತಂತ್ರಗಳನ್ನು ಮುಂದುವರಿಸಿದ್ದಾರೆ. ಹಲವಾರು ಸಂಸ್ಥೆಗಳು ಡೇಟಾ ಕಳ್ಳತನದ ಯಾತನೆ ಅನುಭವಿಸುತ್ತಲೇ ಇವೆ. ಇದರೊಂದಿಗೆ ಜನರು ಆಕ್ಸಿಜನ್ ನೆರವು, ಔಷಧಿ ಇಲ್ಲವೇ ಲಸಿಕೆಗಳಂತಹ ಜೀವ ಉಳಿಸುವ ಚಿಕಿತ್ಸೆಯನ್ನು ರೋಗಿಗಳು ಹುಡುಕುತ್ತಿರುವಾಗ, ಆನ್‌ಲೈನ್ ವಂಚಕರು ಅವರ ಹತಾಶೆಯನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳುತ್ತಿದ್ದಾರೆ.

ಕೊರೋನಾ ಮಹಾಮಾರಿಯ ಜೊತೆಜೊತೆಗೆ, ಮಾಹಿತಿ ಮಹಾಮಾರಿಯೂ ನಮ್ಮೆಲ್ಲರನ್ನು ಕಾಡುತ್ತಿದೆ - ಸೋಶಿಯಲ್ ಮೀಡಿಯಾದಲ್ಲಿ ತಪ್ಪು ಮಾಹಿತಿಗಳ ಮಹಾಪೂರವೇ ಹರಿದಾಡುತ್ತಿದೆ. ನಮ್ಮ ಸಮಾಜ ಸದೃಢವಾಗಿ ಇರಬೇಕೆಂದರೆ, ನಾವು ಕೊರೋನಾ ಮಹಾಮಾರಿಯ ವಿರುದ್ಧ ಮಾತ್ರವಲ್ಲದೇ ಮಾಹಿತಿ ಮಹಾಮಾರಿಯ ವಿರುದ್ಧವೂ ಹೋರಾಡಬೇಕಿದೆ. ಅದಕ್ಕಾಗಿ ನಾವು ತಪ್ಪು ಮಾಹಿತಿ ಮತ್ತು ಸುಳ್ಳು ಸುದ್ದಿಗಳನ್ನು ಹುಡುಕಿ, ಅವು ಬೇರೆಯವರಿಗೆ ಹರಡದಂತೆ ನೋಡಿಕೊಳ್ಳಬೇಕು.

ಸುರಕ್ಷಿತವಾಗಿರಿ, ನಿಮ್ಮ ಆರೋಗ್ಯ ಕಾಪಾಡಿಕೊಳ್ಳಿ, ಆದಷ್ಟು ಬೇಗ ವ್ಯಾಕ್ಸಿನ್ ಹಾಕಿಸಿಕೊಳ್ಳಿ ಮತ್ತು ಕೋವಿಡ್ ಪರಿಸ್ಥಿತಿಗೆ ಸೂಕ್ತವಾದ ನಡವಳಿಕೆ ಅನುಸರಿಸಿ.

ಸೈಸೆಕ್ ತಂಡದ ಪರವಾಗಿ ನಿಮಗೆಲ್ಲಾ ಸವಿಹಾರೈಕೆಗಳು,
ಕಾರ್ತಿಕ್ ರಾವ್ ಬಪ್ಪನಾಡ್

Dear Friends,

Greetings from CySecK!

We are glad to bring to you Cyber Vartika – which is going to be CySecK's monthly bilingual newsletter – covering cyber security, safety, trust and privacy related stories that would be of interest to all consumers of Information Technology. As our digital footprint increases and as we share more and more data in the digital realm, awareness of cyber risks and cyber hygiene practices are also gaining increasing importance. **Cyber Vartika** is CySecK's endeavour to keep you all updated of the cyber risk landscape and make our society more cyber secure.

Amidst the gloom of the pandemic and the increasing concerns over the health and well-being of our near and dear ones, cyber criminals continue to be up to their old tricks. While several organisations continue to suffer data breaches, online fraudsters are misusing the desperation of people when looking for life saving treatment – whether it be oxygen support, medicines or vaccines.

In parallel to the pandemic, we also have an infodemic – with wrong information spread through social media channels. For the society to be strong, it is important that we display immunity to not just the pandemic, but also the infodemic by identifying and not circulating false information and fake news.

Stay safe, take care of your health, get vaccinated at the earliest possible and follow Covid Appropriate Behaviour.

With best wishes, on behalf of Team CySecK,
Karthik Rao Bappanad

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ಭಾರತೀಯ ಬಳಕೆದಾರರನ್ನು ಗುರಿಯಾಗಿಸಿಕೊಂಡು ಕೋವಿಡ್-19 ಲಸಿಕೆ ನೋಂದಣಿಗೆ ಸಂಬಂಧಿಸಿದಂತೆ ನಕಲಿ ಎಸ್‌ಎಂಎಸ್

ಭಾರತ ತನ್ನ ಲಸಿಕೆ ಅಭಿಯಾನದಲ್ಲಿ ಮುಂದೆ ಹೆಜ್ಜೆ ಹಾಕುತ್ತಿದ್ದಂತೆ, ಹೊಸ ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ಕಳವಳ ಹುಟ್ಟಿಕೊಂಡಿದೆ. ಲಸಿಕೆ ಕಾರ್ಯಕ್ರಮಕ್ಕಾಗಿ ಬಳಕೆದಾರರನ್ನು ನೋಂದಾಯಿಸುವುದಾಗಿ ಹೇಳಿಕೊಳ್ಳುವ ನಕಲಿ ಎಸ್‌ಎಂಎಸ್ ಹರಿದಾಡುತ್ತಿದೆ. ಬಳಕೆದಾರರು ಎಸ್‌ಎಂಎಸ್ ನಲ್ಲಿನ ಲಿಂಕ್ ಅನ್ನು ಕ್ಲಿಕ್ಮಾಡಿದರೆ, ಕೋವಿನ್ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಕರೆದೊಯ್ಯುವ ಬದಲು ಅಪಾಯಕಾರಿಯಾದ ಬೇರೆ ಪುಟವನ್ನು ತೋರಿಸುತ್ತದೆ.
ದಯವಿಟ್ಟು ನೆನಪಿಡಿ – ಲಸಿಕೆಗಾಗಿ ನೋಂದಾಯಿಸಿಕೊಳ್ಳಲು ಇರುವ ಒಂದೇ ಒಂದು ಅಧಿಕೃತ ಆನ್‌ಲೈನ್ ಲಿಂಕ್ ಎಂದರೆ - http://cowin.gov.in

ಕೋವಿಡ್ 19 ಎರಡನೇ ಅಲೆಯ ನಡುವೆ ರೋಗಿಗಳ ಆರೋಗ್ಯ ಮಾಹಿತಿ ಸುರಕ್ಷತೆಯ ಬಗ್ಗೆ ಕಳವಳ

ಆರೋಗ್ಯ ಸೇವೆಗಳು ಒಮ್ಮೆಗೆ ಆನ್‌ಲೈನ್ ತಾಣಗಳಲ್ಲಿ ಹೆಚ್ಚಾಗಿ ಕಾಣಿಸಿಕೊಳ್ಳುತ್ತಿದ್ದಂತೆ, ಅದು ಪರೀಕ್ಷೆಯ ಫಲಿತಾಂಶಗಳನ್ನು ಇಮೇಲ್ ಮೂಲಕ ಕಳಿಸುವುದಾಗಿರಬಹುದು ಇಲ್ಲವೇ ಆರೋಗ್ಯ ಮಾಹಿತಿಯನ್ನು ಎಸ್‌ಎಂಎಸ್ ಮೂಲಕ ಕಳಿಸುವುದಾಗಿರಬಹುದು, ಬಳಕೆದಾರರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಕೂಡಿಡುವುದು ಹೆಚ್ಚಾಗುತ್ತಿದೆ. ಆಸ್ಪತ್ರೆಗಳು ಮತ್ತು ವೈದ್ಯಕೀಯ ಕೇಂದ್ರಗಳಲ್ಲಿನ ಆರೋಗ್ಯ ಡೇಟಾವನ್ನು ಹ್ಯಾಕರ್‌ಗಳು ಕದಿಯುವುದು ಹೆಚ್ಚಾಗುತ್ತಿದೆ. ಕೆಲವು ಆಸ್ಪತ್ರೆಗಳಂತೂ ತಾವಾಗಿಯೇ ಮಾಹಿತಿಯನ್ನು ಮಾರುತ್ತಿವೆ. ರೋಗಿಗಳಿಗೆ ಗೌಪ್ಯತೆಯೇ ಇಲ್ಲದಂತಾಗಿದೆ. ಅವರ ಆರೋಗ್ಯ ಮಾಹಿತಿಯು ಇಂಟರ್‌ನೆಟ್‌ನಲ್ಲಿ ಸುಲಭವಾಗಿ ದೊರೆಯುತ್ತಿದೆ.

ಬಳಕೆದಾರರನ್ನು ಮರುಳುಮಾಡಿ ಅವರು ನಕಲಿ ಆ್ಯಪ್‌ಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡುವಂತೆ ಹ್ಯಾಕರ್‌ಗಳು ಹೊಂಚುಹಾಕಿದ್ದಾರೆ!

iOS ಮತ್ತು ಆಂಡ್ರಾಯ್ಡ್ ಪ್ಲಾಟ್‌ಫಾರಂಗಳಲ್ಲಿ, ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿ, ಟ್ರೇಡಿಂಗ್ ಮತ್ತು ಬ್ಯಾಂಕಿಂಗ್ ಆ್ಯಪ್‌ಗಳ ವೇಷದಲ್ಲಿ ಹಲವಾರು ಆ್ಯಪ್‌ಗಳು ಅಡಗಿ ಕುಳಿತಿರುವುದನ್ನು ಸೋಫೋಸ್ ಕಂಪನಿ ಕಂಡುಹಿಡಿದಿದೆ. ಗುಟ್ಟಾದ ಮಾಹಿತಿ ಮತ್ತು ಹಣವನ್ನು ಕದಿಯಲೆಂದೇ ಈ ಆ್ಯಪ್‌ಗಳನ್ನು ಡಿಸೈನ್ ಮಾಡಲಾಗಿದೆ. ಅವು ಸರಿಯಾದ ಆ್ಯಪ್‌ಗಳಂತೆಯೇ ಕಾಣುವಂತೆ ಬಹಳ ಜಾಣ್ಮೆಯಿಂದ ಡಿಸೈನ್ ಮಾಡಲಾಗಿದೆ. ನಂಬುಗೆಯ ಆ್ಯಪ್ ಸ್ಟೋರ್‌ಗಳಾದ ಆ್ಯಪಲ್‌ನ ಆ್ಯಪ್ ಸ್ಟೋರ್ ಇಲ್ಲವೇ ಗೂಗಲ್‌ನ ಪ್ಲೇ ಸ್ಟೋರ್‌ಗಳಲ್ಲಿ ಈ ಆ್ಯಪ್‌ಗಳು ದೊರೆಯುವುದಿಲ್ಲ.

ಏರ್ ಇಂಡಿಯಾ ಮತ್ತು ಡೊಮಿನೊಸ್ ಪಿಜ್ಜಾ ಡೇಟಾ ಸೋರಿಕೆ; ಗ್ರಾಹಕರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಅಪಾಯದ ಸುಳಿಯಲ್ಲಿ

ಏರ್ ಇಂಡಿಯಾದ ಕಸ್ಟಮರ್ ಡೇಟಾಬೇಸ್ ಭಾರೀ ಪ್ರಮಾಣದ ಡೇಟಾ ಸೋರಿಕೆಗೆ ತುತ್ತಾಗಿದೆ. ಆಗಸ್ಟ್ 2011ರಿಂದ ಫೆಬ್ರವರಿ 2021ರ ನಡುವೆ ನೋಂದಾಯಿಸಿಕೊಂಡ ಲಕ್ಷಾಂತರ ಪ್ರಯಾಣಿಕರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಕಳುವಾಗಿದೆ. ಹುಟ್ಟಿದ ದಿನಾಂಕ, ಸಂಪರ್ಕಮಾಹಿತಿ, ಪಾಸ್‌ಪೋರ್ಟ್ ಮತ್ತು ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳು, ಮುಂತಾದ ಪಯಣಿಗರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಗಳು ಒಂದು ಸಂಕೀರ್ಣ ಸೈಬರ್ ದಾಳಿಯಲ್ಲಿ ಸೋರಿಕೆಯಾಗಿವೆ.
ಮತ್ತೊಂದು ಸಂದರ್ಭದಲ್ಲಿ, ಡಾಮಿನೋಸ್ ಪಿಜ್ಜಾ ಇಂಡಿಯಾ- ಒಂದು ಬೃಹತ್ ಡೇಟಾ ಸೋರಿಕೆಗೆ ತುತ್ತಾಗಿದ್ದು, ಅದೆಷ್ಟೋ ಅತಿಮುಖ್ಯ ವಿವರಗಳು ಈಗ ಡಾರ್ಕ್ ವೆಬ್‌ನಲ್ಲಿ ಹರೆದಾಡುತ್ತಿವೆ. 18 ಕೋಟಿ ಆರ್ಡರ್ ವಿವರಗಳು ಹಾಗೂ ಗ್ರಾಹಕರು ಮತ್ತು ನೌಕರರಿಗೆ ಸಂಬಂಧಿಸಿದ 13 ಟಿಬಿಯಷ್ಟು ಅಗಾಧ ಮಾಹಿತಿ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಕಾಣಿಸಿಕೊಂಡಿದೆ. ಬಳಕೆದಾರರ ಮೊಬೈಲ್ ಸಂಖ್ಯೆ, ಹೆಸರು, ಇಮೇಲ್ ವಿಳಾಸ ಮತ್ತು ಜಿಪಿಎಸ್ ಲೊಕೇಶನ್ ತರಹದ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಗಳು ಇದರಲ್ಲಿಸೇರಿವೆ.

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ - ಯಾವ ಪ್ರಯಾಣಿಕರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಸೋರಿಕೆಯಾಗಿದೆಯೋ, ಅವರು ತಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಹಾಗೂ ಪಿನ್ ನಂಬರ್ ಬದಲಿಸುವ ಮೂಲಕ ಮುನ್ನೆಚ್ಚರಿಕೆ ವಹಿಸಬೇಕಾಗಿ ಮನವಿ. ಇಮೇಲ್ ಅಥವಾ ಎಸ್‌ಎಂಎಸ್ ಮೂಲಕ ಬರುವ ಯಾವ್ಯಾವುದೋ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.

ಕೋವಿಡ್ ವ್ಯಾಕ್ಸಿನೇಷನ್‌ನಿಂದ ಪಾರಾಗಲು ಗ್ರಾಮಸ್ಥರು ಯುಪಿಯ ಸರಾಯು ನದಿಗೆ ಹಾರಿದ್ದಾರೆ

ಲಸಿಕೆ ಹಿಂಜರಿಕೆಯ ಉದಾಹರಣೆಯಲ್ಲಿ, ಗ್ರಾಮಸ್ಥರು ಕೋವಿಡ್-19 ವಿರುದ್ಧದ ಲಸಿಕೆಯಿಂದ ತಪ್ಪಿಸಿಕೊಳ್ಳಲು ಸರಾಯು ನದಿಗೆ ಹಾರಿದ ಘಟನೆ ಯುಪಿಯ ಬಾರಾಬಂಕಿಯಲ್ಲಿ ನಡೆದಿದೆ. ಇದು ಲಸಿಕೆ ಅಲ್ಲ, ವಿಷಕಾರಿ ಚುಚ್ಚುಮದ್ದು ಎಂದು ತಿಳಿಸಿದ್ದರಿಂದ ಅವರು ನದಿಗೆ ಹಾರಿದ್ದಾರೆ ಎಂದು ಗ್ರಾಮಸ್ಥರು ತಿಳಿಸಿದ್ದಾರೆ.
ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಮತ್ತು ಮೆಸೇಜಿಂಗ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳ ಮೂಲಕ ಹರಡುವ ಕೋವಿಡ್-19 ಬಗ್ಗೆ ನಕಲಿ ಸುದ್ದಿಗಳಿಂದ ಜೀವವನ್ನು ಕಳೆದುಕೊಳ್ಳಬಹುದು. ತಪ್ಪು ಮಾಹಿತಿಯ ವಿರುದ್ಧ ಸಾರ್ವಜನಿಕರನ್ನು ಪ್ರತಿರಕ್ಷಿಸುವುದು ಸಹ ಬಹುಮುಖ್ಯ.

Top Cyber News

Fake SMS regarding COVID-19 vaccine registrations targeting Indian users.

New cybersecurity concerns have emerged as India moves forward with its vaccination drive. A fake SMS is being circulated among the users that claims to register users for the vaccination program. The link in the SMS is redirecting the users to a malicious page instead of leading to the CoWIN portal.

Please remember- The only official online link for vaccination is - http://cowin.gov.in.

Concerns about the security of patients' health data rise amidst Covid19 second wave

With sudden shift of health services to online platforms, whether for providing test results on mail or sending health related information via SMS, users personal data is increasingly being stored online. Hackers are now gaining access to health data from hospitals and medical centres in large quantities. Some hospitals are even voluntarily selling data. Patients are therefore facing massive privacy breach, where their health data is openly available on the dark web.

Hackers target users to lure them into installing fake apps!

Sophos discovered multiple apps disguised as cryptocurrency, trading, and banking apps on iOS and Android platforms, designed specifically to steal sensitive information and money. These apps are cleverly designed to look like the legitimate ones. These apps bypass trustable app stores like Apple's App Store or Google's Play Store.

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.

Air India and Domino's Pizza suffer data leaks; personal data of consumers compromised

Air India's customer database suffered a massive data breach. Personal data of millions of passengers registered between August 2011 and February 2021 was stolen. Flyers personal information, including date of birth, contact information, passport and credit card information, has been leaked as a result of a sophisticated cyberattack.
In another story, Domino's Pizza India was also at the receiving end of a massive data breach in which 18 crore order records, along with 13TB of customer and employee details has resurfaced on the dark web. Users' mobile numbers, names, e-mail addresses, and GPS locations are among the sensitive data released.

Please remember- Customers whose data has been compromised should consider taking precautionary measures by changing their passwords and PINs. Never click on random URL links that you receive via email or SMS.

Villagers jump into Sarayu river in UP to escape Covid vaccination

In an extreme example of vaccine hesitancy, Villagers in Barabanki jumped into Sarayu river to escape from vaccination against Covid-19. The villagers said they jumped into the river because they were told that this was not a vaccine, but a poisonous injection.
Fake news about COVID-19 spread through social media and messaging apps can cost lives. Immunizing the public against misinformation is also important.

ಸೈಸೆಕ್ ಜಾಗೃತಿ ಭಂಡಾರ

ಫಿಶಿಂಗ್ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ

ಫಿಶಿಂಗ್‌ಎಂದರೇನು?

ಫಿಶಿಂಗ್ ಒಂದು ವಂಚನೆಯ ರೂಪವಾಗಿದ್ದು, ಇದರಲ್ಲಿ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕದಿಯುವ ಉದ್ದೇಶದಿಂದ ಆಕ್ರಮಣಕಗಾರರು ಮೋಸದ ಸಂವಹನಗಳನ್ನು ಕಳುಹಿಸುತ್ತಾರೆ. ಜನರ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಸಂಖ್ಯೆಗಳು, ಜೀವನಚರಿತ್ರೆಯ ಮಾಹಿತಿ, ಖಾತೆ ಮಾಹಿತಿ ಇತ್ಯಾದಿಗಳನ್ನು ಪಡೆಯುವುದು ಅವರ ಗುರಿಯಾಗಿರುತ್ತದೆ . ಈ ದಾಳಿಯನ್ನು ಸಾಮಾನ್ಯವಾಗಿ ಇಮೇಲ್, ಎಸ್‌ಎಂಎಸ್, ಫೋನ್ ಕರೆಗಳ ಮೂಲಕ ಮಾಡಲಾಗುತ್ತದೆ.

ಫಿಶಿಂಗಿನ ಹಲವು ಪ್ರಕಾರಗಳು

1. ಡಿಸೆಪ್ಟಿವ್ ಫಿಶಿಂಗ್- ಜನರ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಲು ದಾಳಿಕೋರರು ಒಂದು ನಿಜವಾದ ಸಂಸ್ಥೆಯಂತೆ ನಟಿಸುತ್ತಾರೆ.
2. ಸ್ಪಿಯರ್ ಫಿಶಿಂಗ್- ಆಕ್ರಮಣಗಾರರು ತಮ್ಮ ಗುರಿಯ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಗಳನ್ನು ಬಳಿಸಿ ಮೇಲ್-ಳನ್ನು ಹೆಚ್ಚು ನೈಜ ಮತ್ತು ಅವರನ್ನು ತಿಳಿದಿರುವಂತೆ ಕಸ್ಟಮೈಸ್ಮಾಡುತ್ತಾರೆ.
3. ವ್ಹೆಲಿಂಗ್ - ದಾಳಿಕೋರರ ಗುರಿಯು ಕಂಪನಿಯ ಸಿಇಒ ಅಥವಾ ಉನ್ನತ ಶ್ರೇಣಿಯ ಅಧಿಕಾರಿಗಳಾಗಿರುತ್ತಾರೆ, ಅವರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಮತ್ತು ಅವರ ಕಂಪನಿಯ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯಲು ಈ ದಾಳಿಯನ್ನು ನಡಿಸುತ್ತಾರೆ.

ಫಿಶಿಂಗ್ ದಾಳಿ ನಡೆಸಲು ಬಳಸುವ ಸಂಪರ್ಕ ಮಾಧ್ಯಮಗಳು

1. ಇಮೇಲ್ ಫಿಶಿಂಗ್- ಜನರ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯಲು ಒಂದು ನಕಲಿ ಲಿಂಕನ್ನು ಮೇಲ್ ಮುಖಾಂತರ ಜನರಿಗೆ ಕಳಿಸಲಾಗುತ್ತದೆ. ಕೆಲವೊಮ್ಮೆ ಈ ಲಿಂಕಗಳು ಗುರಿಯ ಕಂಪ್ಯೂಟರ್‌ನಲ್ಲಿ ದುರುದ್ದೇಶಪೂರಿತ ಸಾಫ್ಟ್‌ವೇರ್ ಡೌನ್‌ಲೋಡ್ ಆಗಲು ಕಾರಣವಾಗುತ್ತದೆ.
2. ಸ್ಮಿಶಿಂಗ್ / ವಿಶಿಂಗ್- ಎಸ್‌ಎಂಎಸ್ ಮೂಲಕ ಫಿಶಿಂಗ್ ಮಾಡಿದಾಗ ಅದಕ್ಕೆ ಸ್ಮಿಶಿಂಗ್ ಎನ್ನುತ್ತಾರೆ. ಧ್ವನಿ ಕರೆ ಮೂಲಕ ಅಪ್ಲಿಕೇಶನ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ಅಥವಾ ತಮ್ಮ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಗುರಿಯನ್ನು ಮನವರಿಕೆ ಮಾಡಿದಾಗ ಅದಕ್ಕೆ ವಿಶಿಂಗ್ ಎನ್ನುತ್ತಾರೆ.

ಫಿಶಿಂಗನಿಂದ ನಿಮ್ಮನ್ನು ರಕ್ಷಿಸಿಕೊಳ್ಳಿ

1. ಸ್ವೀಕರಿಸಿದ ಮೇಲ್ ಅಥವಾ ಎಸ್‌ಎಂಎಸ್ನಲ್ಲಿ ವ್ಯಾಕರಣದ ತಪ್ಪುಗಳಿವೆಯೇ ಎಂದು ಪರಿಶೀಲಿಸಿ.
2. URL ಅನ್ನು ಕ್ಲಿಕ್ ಮಾಡ ಬೇಡಿ; ಸಂದೇಹವಿದ್ದಲ್ಲಿ, ಮೂಲ ಸೈಟ್‌ಗೆ ನೇರವಾಗಿ ಹೋಗಿ ಲಾಗಿನ್ ಮಾಡಿ.
3. ಅಪೇಕ್ಷಿಸದ ಮೇಲ್ ಅಟ್ಯಾಚಮೆಂಟಗಳ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ.
4. ಬಂದಿರುವ ಕರೆ, ಎಸ್‌ಎಂಎಸ್ ಅಥವಾ ಇಮೇಲ್‌ಗಳು ನಿಮ್ಮನ್ನು ತುರ್ತಾಗಿ ಪ್ರತಿಕ್ರಿಯಿಸಲು ಪ್ರಯತ್ನಿಸುತ್ತಿದ್ದರೆ, ಅದರ ಬಗ್ಗೆ ಜಾಗರೂಕತೆ ಇರಲಿ.

ಆನ್‌ಲೈನ್ ಹಗರಣಗಳನ್ನು ವರದಿ ಮಾಡಲು ಇಲ್ಲಿ ಕ್ಲಿಕ್ ಮಾಡಿ

CySecK Awareness Repository

Beware of Phishing

WHAT IS PHISHING?

Phishing is a form of fraud wherein the attacker sends deceitful communications with the intent to steal personal information and sensitive data- like credit card numbers, biographical information, account information, etc. This attack is commonly done via email, SMS, phone calls, pop-up windows or other communication channels.

COMMON TYPES OF PHISHING

1. **Deceptive phishing- Attackers impersonate a genuine organization in order to steal one's information.**
2. **Spear phishing- Attacker customizes mails with their target's personal information to seem more genuine and known.**
3. Whaling- Attackers target a company's CEO or high ranking official to obtain their personal information and the sensitive data of their company

CHANNELS USED TO CARRY OUT PHISHING ATTACKS

1. Email phishing- A fraud link will be attached to the mail in order to obtain information or sometimes it leads to downloading of malicious software on the target's computer.
2. Smishing/Vishing- Smishing is when phishing is done through SMS and Vishing is convincing the target to share their information or perceiving them to download an application via voice call.

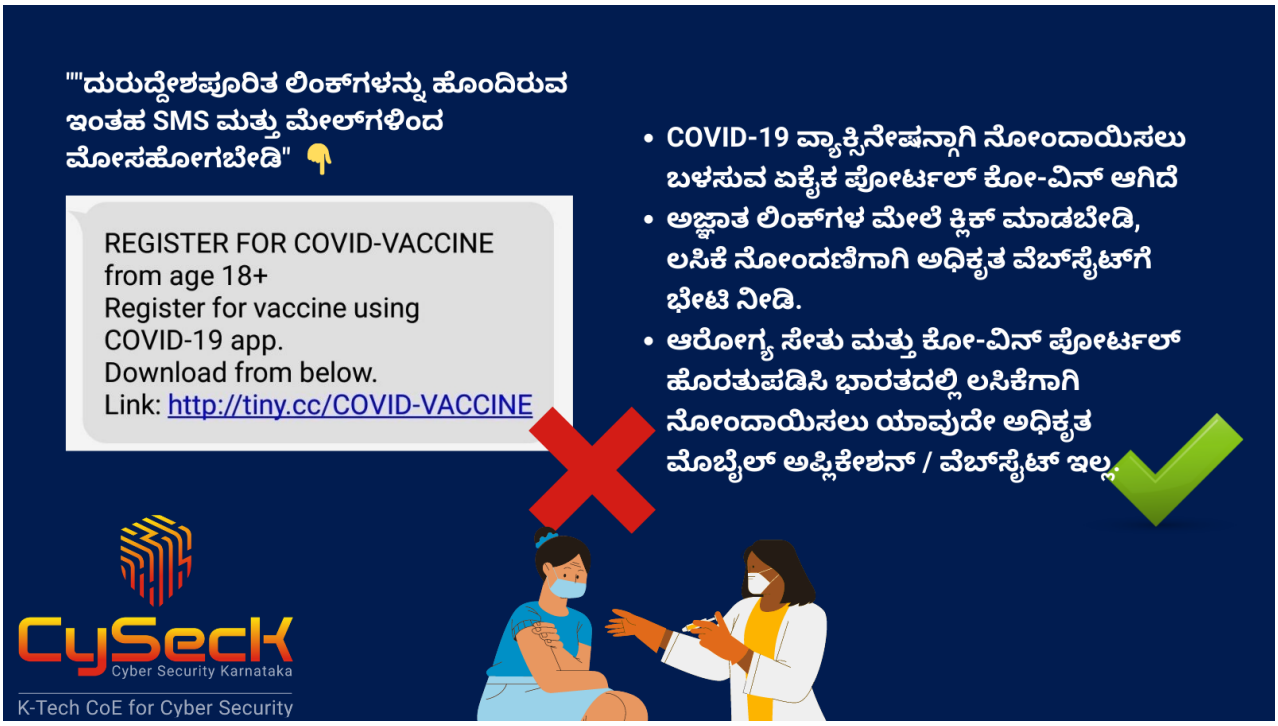
PROTECT YOURSELF FROM PHISHING ATTACKS

1. **Check if there are spelling / grammatical mistakes in the mail/message received.**
2. **Do not click on the URL; if in doubt, login to the legitimate site directly.**
3. **Be aware of unsolicited attachments.**
4. **Check if the mail/SMS/person is trying to bait you with urgency.**

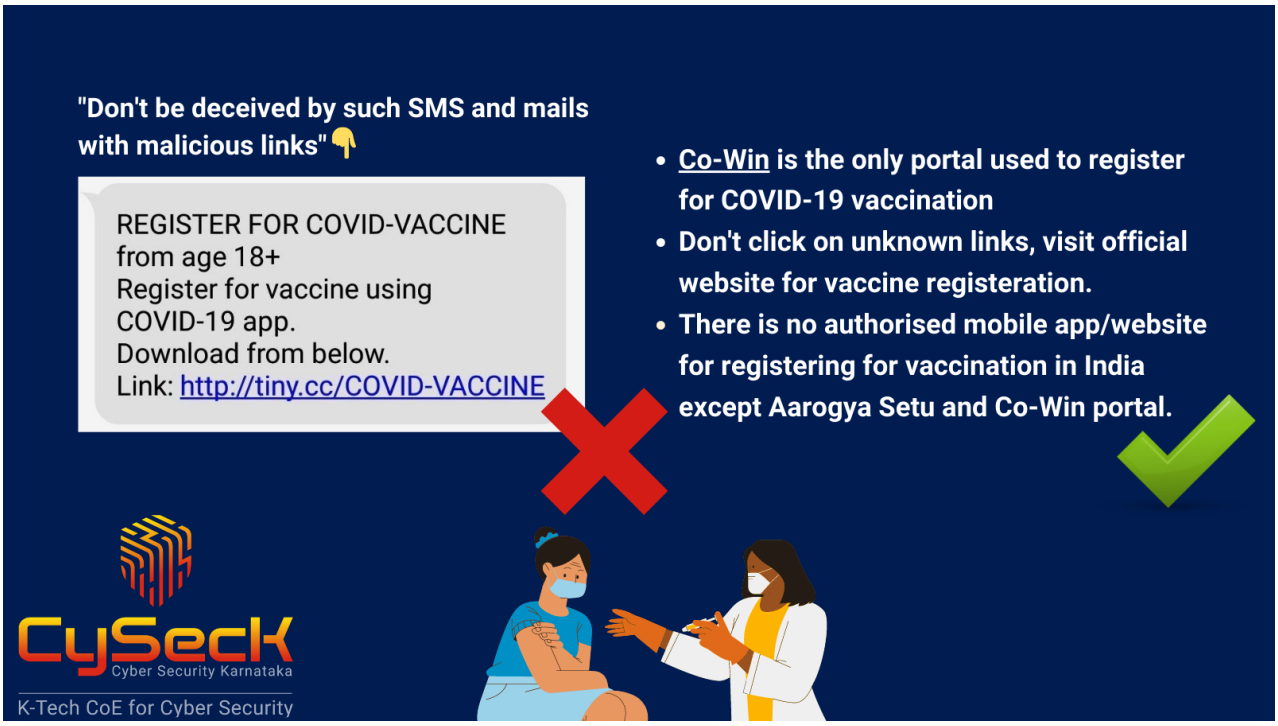
Click here to report online scams

ಜಾಗೃತಿ ವೇದಿಕೆ

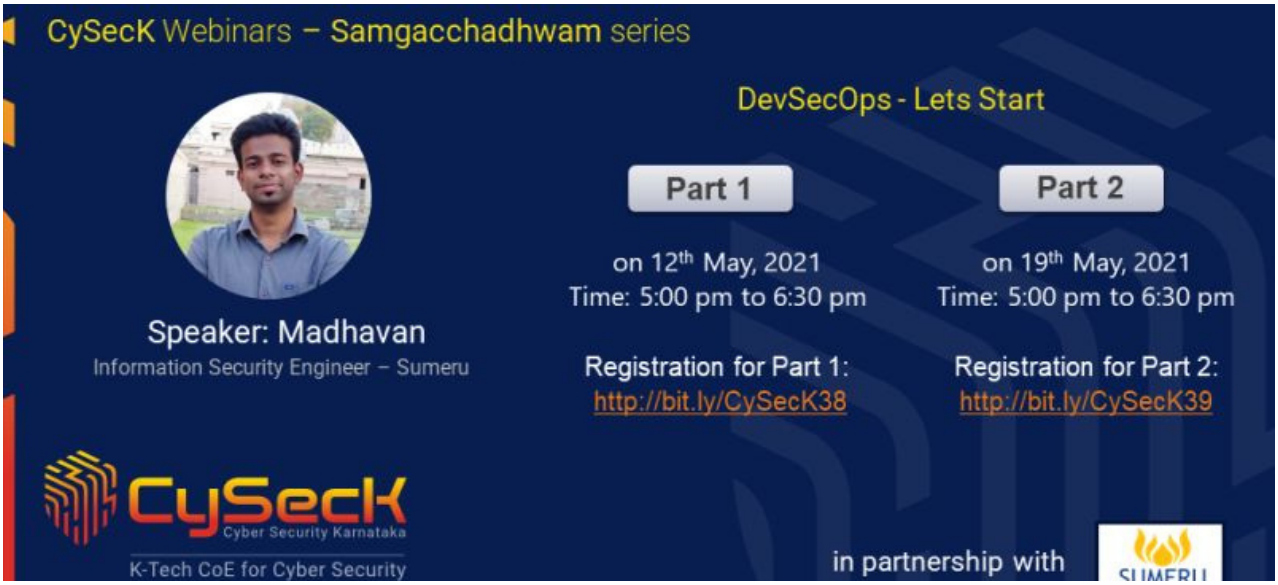
CySeck
Cyber Security Karnataka
K-Tech CoE for Cyber Security
ಸ್ಮಿಶಿಂಗ್ ಹಗರಣಗಳ ಬಗ್ಗೆ ಎಚ್ಚರ ವಹಿಸಿ!
ಒಬ್ಬ ಉದ್ಯೋಗಿಯ ಫೋನಿಗೆ ಆತನ ಬ್ಯಾಂಕಿನಿಂದ ಒಂದು ಅಭಿನಂದನೆಯ ಎಸ್‌ಎಂಎಸ್ ಬಂದಿದೆ.
ABC ಬ್ಯಾಂಕಿನ ಆಮೂಲ್ಯ ಗ್ರಾಹಕರಾದ ನಿಮಗೆ ಅಭಿನಂದನೆಗಳು!!
ನಿಮಗೆ 0 EMI ಸಾಲ ಸೌಲಭ್ಯವಿರುವ DIAMOND Credit Card ಸಿದ್ಧವಿದೆ ಸ್ವೀಕರಿಸಲು ಕೂಡಲೇ ಅದರ ಪ್ರಯೋಜನ ಪಡೆಯಲು ಇಲ್ಲಿ ಒತ್ತಿ bit.ly/xyz.
ಬಾರೆ ಬಾ! ನಾನು ಈ ವೆಬ್ಸೈಟಿಗೆ ಹೋಗಿ, ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಮೂಲಕ ಲಾಗಿನ್ ಆದರೆ ಈ ಆಫರ್ ನನ್ನದಾಗುತ್ತದೆ.
ಹೇ, ಈ URL ನಿಜವಾಗಿಯೂ ನಿನ್ನನ್ನು ಬ್ಯಾಂಕಿನ ಅಸಲಿ ವೆಬ್ಸೈಟ್ಗೆ ಕರೆದೊಯ್ಯುತ್ತದೆಯೇ? ಇಂತಹ ಶಾರ್ಟ್ URLಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವಾಗ ಹುಷಾರಾಗಿರಬೇಕು!
1. ಎಸ್‌ಎಂಎಸ್ ಮೂಲಕ ನಡೆಯುವ ಫಿಶಿಂಗ್ ಅನ್ನು ಸ್ಮಿಶಿಂಗ್ ಎನ್ನುತ್ತಾರೆ.
2. ಶಾರ್ಟ್ URLಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವಾಗ ಜಾಗ್ರತೆ ವಹಿಸಿ. ಅವು ನಿಮ್ಮನ್ನು ಬ್ಯಾಂಕಿನ ಅಸಲಿ ವೆಬ್ಸೈಟ್ಗಿಂತಲೇ ಕಾಣುವ ಮೋಸದ ವೆಬ್ಸೈಟ್ಗೆ ಕರೆದೊಯ್ಯಬಹುದು. ಅದು ಸುರಕ್ಷಿತವೋ ಅಲ್ಲವೋ ಎಂದು ಗೊತ್ತಿರದಿದ್ದರೆ, ಅದನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ!
3. ಅಗತ್ಯ ಬಿದ್ದರೆ, ಶಾರ್ಟ್ URLಗಳ ಪೂರ್ತಿ ವಿವರ ತೋರಿಸುವ ವೆಬ್ಸೈಟ್ಗಳ ನೆರವು ಪಡೆಯಿರಿ. ಉದಾ: http://getlinkinfo.com/.
4. ಸ್ಮಿಶಿಂಗ್ ಹಗರಣಗಳು ಆಫರ್, ಡೀಲ್ ಅಥವಾ ಎಚ್ಚರಿಕೆಗಳ ಮೂಲಕ ನೀವು ಕೂಡಲೇ ಅದನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವಂತೆ ಪ್ರೇರೇಪಿಸುತ್ತದೆ. ದಯವಿಟ್ಟು ಎಚ್ಚರ ವಹಿಸಿ!
@CySecKCoE


""ದುರುದ್ದೇಶಪೂರಿತ ಲಿಂಕ್‌ಗಳನ್ನು ಹೊಂದಿರುವ ಇಂತಹ SMS ಮತ್ತು ಮೇಲ್‌ಗಳಿಂದ ಮೋಸಹೋಗಬೇಡಿ" 👇
REGISTER FOR COVID-VACCINE
from age 18+
Register for vaccine using
COVID-19 app.
Download from below.
Link: http://tiny.cc/COVID-VACCINE
• COVID-19 ವ್ಯಾಕ್ಸಿನೇಷನ್‌ಗಾಗಿ ನೋಂದಾಯಿಸಲು ಬಳಸುವ ಏಕೈಕ ಪೋರ್ಟಲ್ ಕೋ-ವಿನ್ ಆಗಿದೆ
• ಅಜ್ಞಾತ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ, ಲಸಿಕೆ ನೋಂದಣಿಗಾಗಿ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಭೇಟಿ ನೀಡಿ.
• ಆರೋಗ್ಯ ಸೇತು ಮತ್ತು ಕೋ-ವಿನ್ ಪೋರ್ಟಲ್ ಹೊರತುಪಡಿಸಿ ಭಾರತದಲ್ಲಿ ಲಸಿಕೆಗಾಗಿ ನೋಂದಾಯಿಸಲು ಯಾವುದೇ ಅಧಿಕೃತ ಮೊಬೈಲ್ ಅಪ್ಲಿಕೇಶನ್ / ವೆಬ್‌ಸೈಟ್ ಇಲ್ಲ.
CySeck
Cyber Security Karnataka
K-Tech CoE for Cyber Security

Awareness Corner



ಸೈಸೆಕ್ ವರದಿ/CySecK Update



ಸಮ್‌ಗಚ್ಚದ್ವಮ್ ಸರಣಿಯ ವೆಬಿನಾರ್‌ಗಳ ಒಂದು ಭಾಗವಾಗಿ- **"DevSecOps - Lets Start"** ಎಂಬ ವಿಷಯದ ಕುರಿತು ವಿದ್ಯಾರ್ಥಿಗಳು / ಅಧ್ಯಾಪಕರು / ಕೆಲಸ ಮಾಡುವ ವೃತ್ತಿಪರರಿಗೆ ಉಚಿತ ವೆಬಿನಾರ್ ನಡೆಸಲಾಯಿತು. ಸುಮೇರು ಸೊಲ್ಯೂಷನ್ಸ್‌ನ ಶ್ರೀ ಮಾಧವನ್ -ಸಂಪನ್ಮೂಲ ವ್ಯಕ್ತಿಯಾಗಿದ್ದರು. ನಡೆದ ವೆಬಿನಾರ್ ಎರಡು ಭಾಗಗಳನ್ನು ಹೊಂದಿದ್ದು , ಎರಡು ಬೇರೆ ಬೇರೆ ದಿನಗಳಲ್ಲಿ ನಡೆಸಲಾಯಿತು.

ಭಾಗ 1- https://youtu.be/mldevII45Xk
ಭಾಗ 2- https://youtu.be/HbfbrDYpelo

As part of Samgacchadhwam series of webinars- a free webinar was conducted for students / faculty / working professionals on the topic "DevSecOps - Lets Start". Mr. Madhavan from Sumeru Solutions was the speaker. There were two parts to this webinar held on two different days.

Link for the Part 1- https://youtu.be/mldevII45Xk
Link for the Part 2- https://youtu.be/HbfbrDYpelo

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 ಸುದ್ಧಿಪತ್ರಿಕೆಯ ಮುಕ್ತ ಚಂದಾದಾರರಾಗಿ!
http://bit.ly/CyberVartikaSubscribe1
If Cyber Vartika was forwarded to you by a friend, get it directly every month by SUBSCRIBING HERE!
http://bit.ly/CyberVartikaSubscribeNow