K-tech

IISc

KSCST

ಸೈಬರ್ ಸೆಕ್ಯೂರಿಟಿ ಕರ್ನಾಟಕ | ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ

CySecK Cyber Security Karnataka | K-Tech CoE for Cyber Security

ಸೈಬರ್ ವಾರ್ತಿಕ

ಜುಲೈ 2022

CYBER VARTIKA

JULY 2022

ಈ ಸಂಚಿಕೆಯಲ್ಲಿ

IN THIS ISSUE

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

FOREWORD

ಸೈಬರ್ವಾರ್ತಿಕಾದ ಜುಲೈ ಸಂಚಿಕೆ ಈಗನಿಮ್ಮ ಮುಂದಿದೆ. ಹಿಂದಿನ ಸಂಚಿಕೆಗಳಹಾಗೆಯೇ, ಈ ಸಂಚಿಕೆಯುತನ್ನ ಓದುಗರಲ್ಲಿ ಸೈಬರ್‌ಸುರಕ್ಷತೆಯ ಬಗ್ಗೆ ಅರಿವು ಮೂಡಿಸುವ ಗುರಿಯನ್ನು ತಲುಪಿದೆ. ನಮ್ಮೆಲ್ಲರ ಬದುಕಿನಲ್ಲಿ ಡಿಜಿಟಲ್ ತಂತ್ರಜ್ಞಾನದ ಬಳಕೆ ಕಂಡು ಕೇಳರಿಯದ ವೇಗದಲ್ಲಿ ಹೆಚ್ಚುತ್ತಿದೆ. ಹಲವು ಬಗೆಯಲ್ಲಿ ಡಿಜಿಟಲ್ ತಂತ್ರಜ್ಞಾನ ನಮ್ಮ ಅಳವು, ಸೇರಿಕೆ ಹಾಗೂ ಶಕ್ತಿಯನ್ನು ಹೆಚ್ಚಿಸಿದೆ. ಆದರೂ ನಾವು ಹಂಚಿಕೊಳ್ಳುವ ಮಾಹಿತಿ ನಮ್ಮ ಡಿಜಿಟಲ್ ಸುರಕ್ಷತೆಗೆ ಪೂರ್ತಿಯಾಗಿ ಅಪಾಯ ತಂದೊಡ್ಡಬಹುದು ಎಂಬ ನಿಜವನ್ನು ನಾವು ಮರೆಯಬಾರದು. ಸೈಬರ್ ಅಪರಾಧಗಳು ಮೋಸಹೋದವರಿಗೆ ಬರೀ ಹಣಕಾಸಿನ ಹೊರೆಯನ್ನು ಉಂಟುಮಾಡುವುದಲ್ಲದೆ ಬಹಳಷ್ಟು ಮಾನಸಿಕ ನೋವನ್ನು ಕೂಡ ನೀಡಬಹುದು.

ಸೈಬರ್ ಅಪರಾಧಗಳ ವಿಷಯದಲ್ಲಿ ಸಕಾರಾತ್ಮಕವಾಗಿ ನೋಡುವುದಾದರೆ, ಈ ಸುದ್ದಿಯೋಲೆಯಲ್ಲಿ ಕೊಟ್ಟಿರುವಂತಹ ಹಲವಾರು ಉದಾಹರಣೆಗಳನ್ನು ನಾವು ಈಗಾಗಲೇ ನೋಡಿದ್ದೇವೆ. ಜನರು ತಮ್ಮ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವಾಗ ಇನ್ನಷ್ಟು ಎಚ್ಚರಿಕೆಯಿಂದ ನಡೆದುಕೊಂಡಿದ್ದರೆ ಅಪರಾಧಗಳನ್ನು ತಡೆಯಬಹುದಾಗಿತ್ತು. ಡಿಜಿಟಲ್ ತಂತ್ರಜ್ಞಾನ ಬಳಸುವಾಗ, ಅಂದರೆ ನಾವು ಕ್ಲಿಕ್ ಮಾಡುವ ಲಿಂಕ್‌ಗಳಿಂದ ಹಿಡಿದು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವ ಆಪ್‌ಗಳ ತನಕ, ಸೈಬರ್ ಅಪಾಯಗಳ ಬಗ್ಗೆ ಅರಿವು ಪಡೆದುಕೊಳ್ಳುವುದು ಮತ್ತು ಎಚ್ಚರಿಕೆಯಿಂದ ನಡೆದುಕೊಳ್ಳುವುದು ರಸ್ತೆ ನಿಯಮಗಳನ್ನು ಪಾಲಿಸುವಷ್ಟೇ ಮುಖ್ಯವಾಗಿದೆ. ನಾವು ಅರಿವನ್ನು ಪಡೆದುಕೊಂಡ ಬಳಿಕ, ಮಕ್ಕಳಿಂದ ಹಿಡಿದು ದೊಡ್ಡವರ ತನಕ ಈ ಅಪಾಯಗಳ ಬಗ್ಗೆ ಅವರಿಗೂ ತಿಳಿಸುವುದು ನಮ್ಮೆಲ್ಲರ ಸಾಮಾಜಿಕ ಹೊಣೆಗಾರಿಕೆಯಾಗಿದೆ. ಕೆಲವು ಬಗೆಯ ಮಾಹಿತಿ ಸೋರಿಕೆಗಳನ್ನು ತಡೆಯುವುದು ನಮ್ಮ ಕೈಯಲ್ಲಿ ಇಲ್ಲದಿದ್ದರೂ, ಸರಳ ಸುರಕ್ಷತೆಯ ಹಂತಗಳನ್ನು ಪಾಲಿಸುವುದರಿಂದ ನಾವು ನಮ್ಮ ಗೌಪ್ಯತೆಯನ್ನು ಕಾಪಾಡಿಕೊಂಡು ಸೈಬರ್ ಅಪಾಯಗಳಿಗೆ ಒಡ್ಡಿಕೊಳ್ಳುವುದನ್ನು ಕಡಿಮೆ ಮಾಡಬಹುದು. ಉದಾಹರಣೆಗೆ, ಪಿನ್ ಮತ್ತು ಓಟಿಪಿಗಳನ್ನು ಬೇರೆಯವರಿಗೆ ಕೊಡದಿರುವುದು, ಗೊತ್ತಿಲ್ಲದ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡದಿರುವುದು, ಗೊತ್ತಿಲ್ಲದ ಮೂಲಗಳಿಂದ ಕಡತ ಇಲ್ಲವೇ ಆಪ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡದಿರುವುದು ಇತ್ಯಾದಿ. "ಹವ್ಯಾಸಿಗಳು ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ ಕನ್ನಹಾಕುತ್ತಾರೆ, ವೃತ್ತಿಪರರು ಜನರ ಮನಸ್ಸಿಗೇ ಕನ್ನಹಾಕುತ್ತಾರೆ " ಎಂಬ ಹೆಸರುವಾಸಿಯಾದ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಪರಿಣತ ಬ್ರೂಸ್ ಶ್ನೇಯರ್ ಅವರ ಹೇಳಿಕೆಯನ್ನು ಎಲ್ಲ ಡಿಜಿಟಲ್ ಬಳಕೆದಾರರೂ ಯಾವಾಗಲೂ ನೆನಪಿಟ್ಟುಕೊಳ್ಳಬೇಕು.

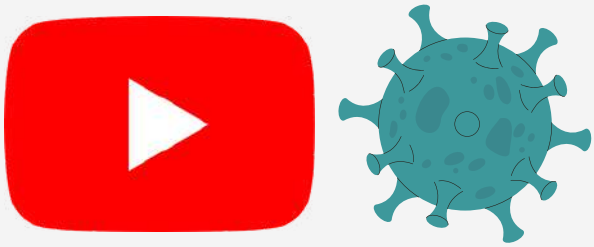
ಪ್ರೊಫೆಸರ್ ಭಾವನಾ ಕಾನುಕುರ್ತಿ
ಕಂಪ್ಯೂಟರ್ ವಿಜ್ಞಾನ ಮತ್ತು ಆಟೊಮೇಶನ್ ವಿಭಾಗ
ಐಐಎಸ್‌ಸಿ

Cyber Vartika's July edition is now here. Much like the previous editions, this edition serves the much-needed goal of educating its readers about cybersecurity. Digital technology has proliferated our lives at an unprecedented rate. It is a fact that digital technology has made us, in many ways, more efficient, more connected and more empowered. However, we must be cognizant of the fact that the information that we share can potentially compromise our digital security entirely. Cybercrimes cause not just financial burden to its victims but also a great deal of mental agony.

On the positive side, when we look at cyber-crimes, history is replete with examples – such as the ones highlighted in this magazine -- where the crime could have been avoided if the victim had been more careful with their information. Educating ourselves on cyberthreats and exhibiting caution while using digital technology – from the links we click to the apps we download – is as important as following road rules. Once we educate ourselves, we also have a social responsibility to make those around us – from children to aged people alike – aware of these threats. While certain breaches are outside our control, we can protect our privacy and minimise the risk of a cyberthreat by applying simple safeguards: for example, never share PINs and OTPs, never click unknown links, never download files or apps from unknown sources etc. The following quote by renowned cyber-security expert, Bruce Schneier, "Amateurs hack systems, professionals hack people", is one that every user of digital technology must always remember.

Prof. Bhavana Kanukurthi
Department of Computer Science and Automation, IISc

ಸುಳ್ಳು ಸುದ್ದಿ ಹರಡಿದ್ದಕ್ಕಾಗಿ 94 ಯೂಟ್ಯೂಬ್ ಚಾನಲ್ ಹಾಗೂ 747 ಯುಆರ್‌ಎಲ್‌ಗಳನ್ನು ಸರ್ಕಾರ ತಡೆಹಿಡಿಯಿತು



2020 ರ ಮಾರ್ಚ್ 31 ರಂದು, ಕೋವಿಡ್-19 ಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ಸುಳ್ಳು ಸುದ್ದಿ ಹರಡುವಿಕೆಯನ್ನು ತಡೆಯಲು, ಪತ್ರಿಕಾ ಮಾಹಿತಿ ಬ್ಯೂರೋದ (ಪಿಐಬಿ) ಸತ್ಯ ತಪಾಸಣೆ ಘಟಕದ ವಿಶೇಷ ತಂಡವೊಂದನ್ನು ಸ್ಥಾಪಿಸಲಾಯಿತು. ಪಿಐಬಿಯ ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಖಾತೆಗಳಲ್ಲಿ ಕೋವಿಡ್-19 ಇಲ್ಲವೇ ಯಾವುದೇ ಸುದ್ದಿಯನ್ನು ಜನರು ಪರಿಶೀಲಿಸಬಹುದು.

ಬೆಸ್ಕಾಮ್ ವಿದ್ಯುತ್ ಬಿಲ್ ಪಾವತಿ ಮೋಸ: 2 ವ್ಯಕ್ತಿಗಳಿಗೆ ₹2.3 ಲಕ್ಷಗಳ ಮೋಸ

ಸುಳ್ಳು ಸಂದೇಶಗಳನ್ನೇ ಬೆಸ್ಕಾಮ್‌ನ ಅಧಿಕೃತ ಸಂದೇಶಗಳು ಎಂಬಂತೆ ನಂಬಿಸಿ ಇಬ್ಬರು ವ್ಯಕ್ತಿಗಳನ್ನು ಮೋಸಗೊಳಿಸಲಾಯಿತು. ಬಿಲ್ ಪಾವತಿ ಮಾಡದಿದ್ದರೆ ವಿದ್ಯುತ್ ಕಡಿತ ಮಾಡಲಾಗುವುದು ಎಂಬ ಎಚ್ಚರಿಕೆಯ ಎಸ್‌ಎಮ್‌ಎಸ್‌ಗಳನ್ನು ಕಡೆಗಣಿಸುವಂತೆ ಬೆಸ್ಕಾಮ್ ತನ್ನ ಬಳಕೆದಾರರಿಗೆ ಮನವಿ ಮಾಡಿದೆ. ಇವು ಸುಳ್ಳು ಸಂದೇಶಗಳು. ಬಿಲ್ ಪಾವತಿಯ ಬೇಡಿಕೆ ಇಡುವಂತಹ ಸಂದೇಶಗಳನ್ನು ಬೆಸ್ಕಾಮ್ ತನ್ನ ಬಳಕೆದಾರರಿಗೆ ಕಳುಹಿಸುವುದಿಲ್ಲ.

ಬೆಂಗಳೂರಿನವೈಟ್‌ಫೀಲ್ಡ್‌ನಲ್ಲಿ ನಕಲಿ ಕಾಲ್ ಸಂಟರ್‌ಗಳಿಗೆ ಬೀಗ; 72 ಮಂದಿ ಸೆರೆ ಮತ್ತು 138 ಕಂಪ್ಯೂಟರ್‌ಗಳು ವಶಕ್ಕೆ

ಮೋಸಗಾರರುಪ್ರಮುಖವಾಗಿ ಯೂಎಸ್‌ನ ಬಳಕೆದಾರರಿಗೆಬಲೆ ಬೀಸುತ್ತಿದ್ದರು. ಅವರ ಖಾತೆಗಳಲ್ಲಿ (ಬ್ಯಾಂಕ್, ಅಮೇಜಾನ್, ಇತ್ಯಾದಿ) ಮೋಸ ನಡೆದಿದೆ ಎಂದು ಎಸ್‌ಎಮ್‌ಎಸ್ ಮತ್ತುವಾಯ್ಸ್‌ಮೇಲ್ ಮೂಲಕ ಸುಳ್ಳು ಎಚ್ಚರಿಕೆಗಳನ್ನು ನೀಡುತ್ತಿದ್ದರು.

ಆ ಬಳಕೆದಾರರು ಇದನ್ನು ನಂಬಿ, ತೊಂದರೆಯನ್ನು ಸರಿಪಡಿಸಲು ಕೋರಿಕೊಂಡಾಗ, ಅವರ ಖಾಸಗಿ ಮತ್ತು ಗುಟ್ಟಾದ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಲಾಗುತ್ತಿತ್ತು. ಅವರ ಖಾತೆಗಳಿಂದ ಹಣ ಕದಿಯಲು, ಆರೋಪಿಗಳು ಅಮೇಜಾನ್ ಉಡುಗೊರೆ ಕಾರ್ಡ್, ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿ ಮತ್ತು ವೈರ್ ಟ್ರಾನ್ಸ್‌ಫರ್‌ನಂತಹ ಕಂಡುಹಿಡಿಯಲಾಗದ ಹಣ ವರ್ಗಾವಣೆ ಆಪ್‌ಗಳನ್ನು ಬಳಸುತ್ತಿದ್ದರು.

ಫ್ಲಿಪ್‌ಕಾರ್ಟ್ ಒಡೆತನದ ಕ್ಲಿಯರ್‌ಟ್ರಿಪ್‌ನಲ್ಲಿ ಬಳಕೆದಾರರ ಡೇಟಾ ಸೋರಿಕೆ

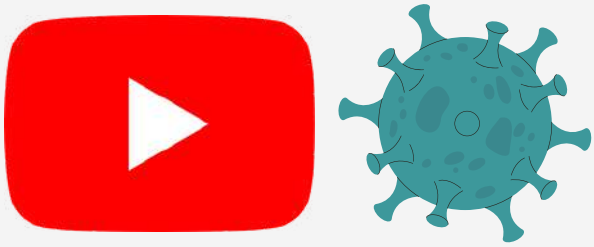
ಕಂಪನಿಯು ತನ್ನ ಗ್ರಾಹಕರಿಗೆ ಇಮೇಲ್ ಮೂಲಕ ಸುದ್ದಿ ಮುಟ್ಟಿಸಿತು.
ಕೆಲವುಪ್ರೊಫೈಲ್-ಸಂಬಂಧಿತ ಮಾಹಿತಿ ಸೋರಿಕೆಯಾಗಿರುವುದನ್ನುಒಪ್ಪಿಕೊಂಡ ಫ್ಲಿಪ್‌ಕಾರ್ಟ್ ಒಡೆತನದಕಂಪನಿ, ಯಾವ ಗುಟ್ಟಾದ ಮಾಹಿತಿಯೂ ಸೋರಿಕೆಯಾಗಿಲ್ಲ ಎಂದು ಭರವಸೆ ಕೊಟ್ಟಿದೆ. ಮುನ್ನೆಚ್ಚರಿಕೆ ಕ್ರಮವಾಗಿ, ಪಾಸ್‌ವರ್ಡ್ ಬದಲಾಯಿಸುವಂತೆ ಅದು ತನ್ನ ಬಳಕೆದಾರರನ್ನು ಕೇಳಿಕೊಂಡಿತು.

ಭದ್ರತೆಯ ಕಾರಣಗಳಿಗಾಗಿ ಅಪಾಯಕಾರಿ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಗೂಗಲ್ ತಡೆಹಿಡಿದಿದೆ

Google Play

Quick Text SMS, Voice Languages Translator, Blood Pressure Monitor, ಹಾಗೂ Smart SMS Messages ಎಂಬ ನಾಲ್ಕು ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಗೂಗಲ್‌ನ ಪ್ಲೇ ಸ್ಟೋರ್‌ನಿಂದ ತೆಗೆದುಹಾಕಲಾಗಿದೆ. ಬಳಕೆದಾರರು ತಮಗರಿವಿಲ್ಲದಂತೆ ದುಬಾರಿ ಸದಸ್ಯತ್ವ ತೆಗೆದುಕೊಳ್ಳುವಂತೆ ಮಾಡಿ, ಆ ಮೂಲಕ ಹಣ ದೋಚುವ ಸ್ಪೈವೇರ್ ಈ ಆಪ್‌ಗಳಲ್ಲಿ ಇದ್ದವು.

Govt blocked 94 YouTube channels, and 747 URLs in FY21 for spreading fake news



On March 31, 2020, a special cell of the Press Information Bureau's (PIB) fact-checking unit was established to stop the spread of fake news linked to COVID-19. People can verify COVID-19-related or any news on PIB's social media accounts.

Bescom electricity bill payment fraud: 2 persons cheated of ₹2.3 lakh

Victims were deceived into believing the fraud messages as Bescom official messages.
Bescom has urged its customers to disregard any SMS warning that their electricity would be cut off for failure to pay their bills. These texts are fraudulent. Bescom doesn't send messages to customers demanding to pay their bills.

Fake call centers busted in Whitefield, Bengaluru; 72 arrested and 138 computers seized

The fraudsters primarily targeted victims in the US. The callers alerted the victims that fraudulent activity had been discovered in their accounts (Bank, Amazon, etc.) using SMS and voice mail.
Private and sensitive information was stolen from the victims when they wanted to solve the problem. The accused used untraceable money transfer apps like Amazon gift cards, cryptocurrency, and wire transfers to siphon funds from the victims.

Flipkart-owned Cleartrip suffers customer data breach

The company notified its clients through email.
The Flipkart-owned company said that certain profile-related information was exposed, but it assured that no sensitive data was compromised. As a precaution, it requested that its users update their passwords.

Google bans harmful applications over security concerns

Four applications - Quick Text SMS, Voice Languages Translator, Blood Pressure Monitor, and Smart SMS Messages - have been removed from Google's Play Store. These apps had spyware that would steal money by tricking users into signing up for pricey memberships without their knowledge.

- **ಆನ್‌ಲೈನ್ ಮೋಸದಲ್ಲಿ ₹1 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ ಉಡುಪಿಯ ವ್ಯಕ್ತಿ**

ಮೋಸಹೋದವ್ಯಕ್ತಿಗೆ ಈ ಸಂದೇಶಬಂದಿತ್ತು, "ಕೆವೈಸಿ ಅಪ್‌ಡೇಟ್‌ನಿಂದಾಗಿ ನಿಮ್ಮ ಖಾತೆಬ್ಲಾಕ್ ಆಗಿದೆ. ನಿಮ್ಮ ಸೇವೆಯನ್ನು ಮುಂದುವರಿಸಲು, 24 ಗಂಟೆಗಳ ಒಳಗೆ 9593983124 ನಲ್ಲಿ ಕಸ್ಟಮರ್ ಕೇರ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ." ಅವರು ಈ ನಂಬರಿಗೆ ಕರೆ ಮಾಡಿದಾಗ, ಅವರ ಫೋನಿಗೆ ಬಂದ ಓಟಿಪಿ ಅನ್ನು ಹೇಳುವಂತೆ ಅವರನ್ನು ಮರುಳು ಮಾಡಲಾಯಿತು.

- **ಆನ್‌ಲೈನ್ ಮೋಸದಲ್ಲಿ ₹1.16 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ ಗೃಹಿಣಿ**

ಯಾವುದೇಹೂಡಿಕೆಯನ್ನು ಕೂಡಲೇ ಎರಡು ಪಟ್ಟುಮಾಡುವುದಾಗಿ ಗೃಹಿಣಿಯೊಬ್ಬರಿಗೆ ಒಂದು ವಾಟ್ಸಾಪ್ ಸಂದೇಶಬಂದಿತ್ತು. ಆ ಸಂದೇಶದಲ್ಲೇ ಹೂಡಿಕೆ ಮಾಡಲು ಒಂದು ಲಿಂಕ್ ಅನ್ನೂ ಕೊಡಲಾಗಿತ್ತು. ಅವರು ಕುತೂಹಲಕ್ಕೆ 100 ರೂಪಾಯಿ ಕಳುಹಿಸಿದಾಗ, 190 ರೂಪಾಯಿ ವಾಪಸ್ ಬಂದಿತು. ಎರಡನೇ ಬಾರಿ ₹760 ಹೂಡಿಕೆ ಮಾಡಿದಾಗ ಅವರ ಖಾತೆಯಲ್ಲಿ ₹1,115 ಕೂಡಲೇ ಬಂದಿತು. ಆಮೇಲೆ ಅವರು ತಮ್ಮ ಗಂಡನ ಖಾತೆಯಿಂದ ₹1 ಲಕ್ಷ ಹೂಡಿಕೆ ಮಾಡಿದಾಗ, ಏನೂ ವಾಪಸ್ ಬರಲಿಲ್ಲ. ಆ ನಂಬರ್‌ಗೆ ಕರೆ ಮಾಡಿದಾಗ, ತಾವು ಮೋಸಹೋದುದು ಅವರಿಗೆ ತಿಳಿಯಿತು.

- **ಸರಕು ಸಾಗಣೆಯಲ್ಲಿ ಜನರಿಗೆ ಮೋಸ ಮಾಡುತ್ತಿದ್ದ ಗುಂಪಿನ ಸೆರೆ**

ಹುಸೇನ್‌ಎಂಬುವವರ ಬಳಿ, ಒಬ್ಬ ವ್ಯಕ್ತಿಯು ತಾನು ಸಂದೀಪ್ ಎಂದುಪರಿಚಯ ಮಾಡಿಕೊಂಡು, 4,000 ರೂಪಾಯಿಗೆ ಬೈಕ್ ಸಾಗಿಸುವುದಾಗಿ ಹೇಳಿದಾಗ ಈ ಮೋಸ ಬೆಳಕಿಗೆ ಬಂದಿತು. ಹೇಳಿದ ಜಾಗಕ್ಕೆ ಬೈಕ್ ಬಂದು ತಲುಪದಿದ್ದಾಗ, ಹುಸೇನ್ ಅವರು ಸಂದೀಪ್‌ಗೆ ಕರೆ ಮಾಡಿದರು. ಬೈಕ್ ಸಾಗಿಸಲು ಅವನು ಇನ್ನಷ್ಟು ಹಣದ ಬೇಡಿಕೆ ಇಟ್ಟ.

- **ಮುಂಬೈ ವ್ಯಾಪಾರಿಗೆ ಬಲೆ ಬೀಸಿದ ಸುಲಿಗೆಕೋರರು; ₹8 ಲಕ್ಷ ಸುಲಿಗೆ**

ಹಿರಿಯನಾಗರಿಕರಾದ ಘಾಟ್‌ಕೋಪರ್‌ನ ಒಬ್ಬ ಬಟ್ಟೆ ವ್ಯಾಪಾರಿಯನ್ನು ಒಂದು ಹೆಂಗಸು ವಿಡಿಯೊಕಾಲ್‌ಗೆ ಬರುವಂತೆಸೆಳೆದು ರೆಕಾರ್ಡ್ ಮಾಡಿದಳು. ಆಮೇಲೆ ದೊಡ್ಡ ಮೊತ್ತ ನೀಡುವಂತೆ ವ್ಯಾಪಾರಿಗೆ ಹಲವು ಬಾರಿ ಬೆದರಿಕೆ ಕರೆಗಳು ಬಂದವು. ಹಣ ಕಳೆದುಕೊಂಡದ್ದು ತಿಳಿದ ಬಳಿಕ, ಅವರು ಪೊಲೀಸ್ ಸ್ಟೇಶನ್‌ಗೆ ಹೋಗಿ ದೂರು ದಾಖಲಿಸಿದರು.

- **ಆರು ಮಂದಿಗೆ ₹3.82 ಲಕ್ಷದಷ್ಟು ಮೋಸ ಮಾಡಿದ ರಿಮೋಟ್ ಅಕ್ಸೆಸ್ ಆಪ್**

ಬಾಕಿ ಉಳಿಸಿಕೊಂಡ ವಿದ್ಯುತ್ ಬಿಲ್‌ಗಳನ್ನು ಒಂದು ವಾರದಒಳಗೆ ಕಟ್ಟುವಂತೆ ಮೋಸಗಾರರು ಆರುಮಂದಿಗೆ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸಿದರು. ಮೋಸಗಾರರು ನೀಡಿದ ನಂಬರ್‌ಗೆ ಇವರು ಕರೆಮಾಡಿದಾಗ, ಸಾಫ್ಟ್‌ವೇರ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡುವಂತೆ ಅವರಿಗೆ ಸೂಚನೆ ಸಿಕ್ಕಿತು. ಇದರಿಂದ ಆರೋಪಿಗಳಿಗೆ ಈ ಆರು ಮಂದಿಯ ಬ್ಯಾಂಕ್ ಖಾತೆಗಳ ಅಕ್ಸೆಸ್ ಸಿಕ್ಕಿ, ಅವುಗಳಿಂದ ಹಣ ದೋಚಲು ಸಾಧ್ಯವಾಯಿತು.

- **Udupi man duped of ₹1 lakh in online fraud**

The victim received a message saying "your account has been blocked due to KYC update. Within 24 Hrs, Please contact customer care 9593983124 to continue your service." Upon calling the number to confirm, the victim was deceived into giving the OTP he received on his phone.

- **Online scam costs a homemaker ₹1.16 lakh**

The victim received an unexpected WhatsApp message offering to double any investments she made instantly. A link to the investment was also included in the message.
The victim curiously transferred ₹100 and received ₹190. She invested a second time for ₹760 and immediately received ₹1,115 back in her account. She then transferred ₹ 1 lakh from her husband's account and received nothing. Upon calling the number, she realized that she was duped.

- **A gang was busted for defrauding people via movers and packers scam**

The fraud came to light when Mr. Hussain was approached by a man who introduced himself as Sandeep and offered to deliver the bike for 4,000 rupees. When the bike did not arrive at the intended location, Mr. Hussain called Sandeep, who began requesting more money to transport the vehicle.

- **Sextortionists trap Mumbai businessman, and force him to fork out Rs 8 lakh**

The senior citizen, a textile merchant from Ghatkopar, was lured into video calling by a woman and recorded. The victim then got threat calls to transfer hefty amounts multiple times. Upon realizing the loss, the victim filed a complaint at the police station

- **A remote access app defrauded six people of Rs. 3.82 lakh**

Fraudsters used texts to trick six victims into paying their past-due electricity bills within a week. When the victims called a number provided by the scammers, they were instructed to download software, which allowed the accused to access the victims' bank accounts and transfer the money out of them.

ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಕಾಪಾಡುವ ದಾರಿಗಳು

ಊಹಿಸಲು ಸಾಧ್ಯವಾಗದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಇರಿಸಿ

ಮಾಹಿತಿ ಸುರಕ್ಷತೆಯ ಹಾದಿಯಲ್ಲಿ ಊಹಿಸಲು ಸಾಧ್ಯವಾಗದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಇರಿಸುವ ಅಭ್ಯಾಸ ಮಾಡಿಕೊಳ್ಳುವುದು ಮೊದಲ ಹೆಜ್ಜೆಯಾಗಿದೆ. ಪಾಸ್‌ವರ್ಡ್ ಆರಿಸುವಾಗ, ನಿಮ್ಮ ಹುಟ್ಟಿದ ದಿನಾಂಕದಂತಹ, ಕಳ್ಳರಿಂದ ಸುಲಭವಾಗಿ ಊಹಿಸಲು ಸಾಧ್ಯವಾಗುವ ಪದಗಳನ್ನು ಇಲ್ಲವೇ ಅಂಕಿಗಳನ್ನು ಇರಿಸಬೇಡಿ. ಸಣ್ಣ ಮತ್ತು ದೊಡ್ಡ ಗುರುತು, ಅಂಕಿ ಹಾಗೂ ಅಕ್ಷರಗಳನ್ನು ಬಳಸಿ ಹಾಗೂ ನಿಯಮಿತವಾಗಿ ಇವುಗಳನ್ನು ಆಚೀಚೆ ಮಾಡಿ ಪಾಸ್‌ವರ್ಡ್ ಬದಲಾಯಿಸುತ್ತಿರಿ.

ಹಲವು ಬಗೆಯ ದೃಢೀಕರಣ ಬಳಸಿ

ಹಲವು ಬಗೆಯ ದೃಢೀಕರಣದಿಂದಾಗಿ, ಒಂದು ಅಪ್ಲಿಕೇಶನ್ ಇಲ್ಲವೇ ಆನ್‌ಲೈನ್ ಖಾತೆಯ ಒಳಹೋಗಲು ಬಳಕೆದಾರರು ಎರಡು ಇಲ್ಲವೇ ಹೆಚ್ಚಿನ ಪರಿಶೀಲನೆಯನ್ನು ಸಲ್ಲಿಸಬೇಕು. ಹಲವು ಬಗೆಯ ದೃಢೀಕರಣದಿಂದಾಗಿ, ಅನಧಿಕೃತ ವ್ಯಕ್ತಿಗಳಿಗೆ ಯಾವುದೇ ವ್ಯಕ್ತಿಯ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಪಡೆಯುವುದು ಬಹಳ ಕಷ್ಟವಾಗುತ್ತದೆ.

ಸಾರ್ವಜನಿಕ ವೈ-ಫೈ ಬಳಸದಿರಿ

ಹೆಚ್ಚಿನ ಉಚಿತ ಸಾರ್ವಜನಿಕ ವೈ-ಫೈ ನೆಟ್‌ವರ್ಕ್‌ಗಳಲ್ಲಿ ಸುರಕ್ಷತೆಯ ತಡೆಗೋಡೆಗಳು ಬಹಳ ಕಡಿಮೆಯಿರುತ್ತವೆ ಹಾಗೂ ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಇರುವುದಿಲ್ಲ. ಇದರಿಂದಾಗಿ ಅದೇ ನೆಟ್‌ವರ್ಕ್‌ನಲ್ಲಿರುವ ಬೇರೆ ಬಳಕೆದಾರರು ಸುಲಭವಾಗಿ ನಿಮ್ಮ ಚಟುವಟಿಕೆಯನ್ನು ನೋಡಬಹುದು. ಆನ್‌ಲೈನ್ ಪಾವತಿಗಳನ್ನು ಮಾಡಲು, ನಿಮ್ಮ ಮನೆ ತಲುಪುವವರೆಗೂ ಕಾಯಿರಿ ಇಲ್ಲವೇ ಸುರಕ್ಷಿತವಾದ, ಪಾಸ್‌ವರ್ಡ್ ಇರುವ ನೆಟ್‌ವರ್ಕ್‌ನಲ್ಲಿ ಮಾಡಿರಿ.

ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿ ತುಂಬ ಮಾಹಿತಿ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ

ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಹೊತ್ತು ಕಳೆಯುವುದು ನಿಮಗೆ ಬಹಳ ಇಷ್ಟವಾಗಿರಬಹುದು, ಆದರೆ ಅದರಿಂದ ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಬಟಾಬಯಲಾಗುವ ಅಪಾಯ ಕೂಡ ಇದೆ. ನಿಮ್ಮ ಗೌಪ್ಯತೆ ಸೆಟಿಂಗ್‌ಗಳನ್ನು ರೀಸೆಟ್ ಮಾಡಿ ಹಾಗೂ ನಿಮ್ಮ ಪೋಸ್ಟ್‌ಗಳನ್ನು ಯಾರೆಲ್ಲಾ ನೋಡಬಲ್ಲರು ಎಂಬುದರ ಅರಿವಿರಲಿ. ನಿಮ್ಮ ಲೊಕೇಶನ್, ಹುಟ್ಟಿದ ದಿನಾಂಕ, ಸ್ಕೂಲ್/ಕಾಲೇಜ್/ಕೆಲಸದ ಸ್ಥಳ ಇಲ್ಲವೇ ಬೇರೆ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವಾಗ ಎಚ್ಚರಿಕೆ ವಹಿಸಿ.

Ways to Protect Personal Information Online

Create reliable passwords

Good password hygiene is the first step in information security. While choosing a password, avoid using words or numbers that a hacker may easily decipher, such as your birthdate. Select mixtures of symbols, numerals, and letters in lowercase and uppercase, and switch them up regularly.

Set up Multi Factor Authentication

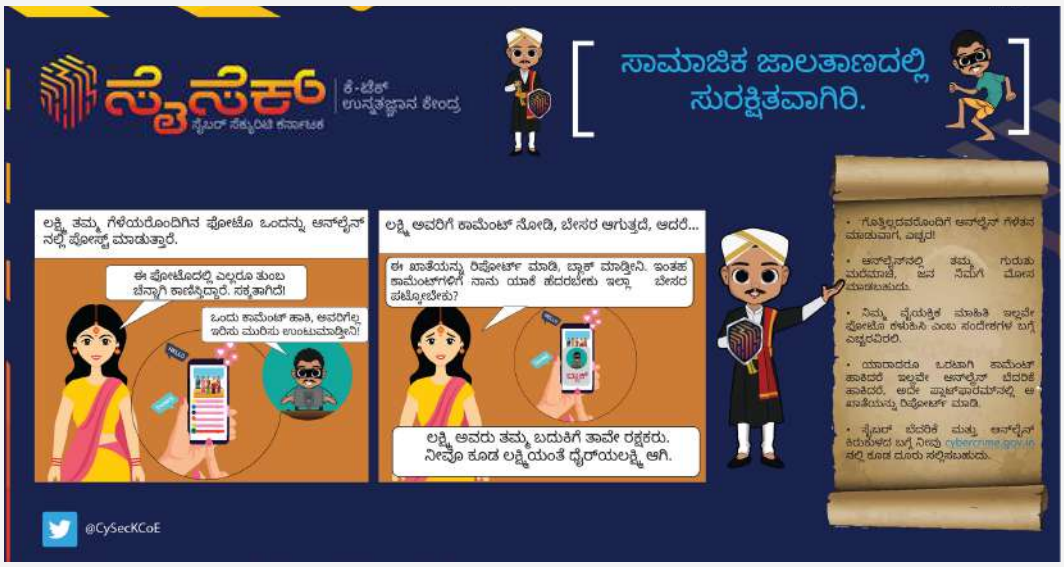
With **multi-factor authentication** (MFA), a user must submit two or more verification factors in order to access a resource like an application or an online account. MFA is like super strong shield that makes it more difficult for an unauthorized person to access one's personal information.

Avoid public Wi-Fi

Most free **public Wi-Fi networks** have very few security safeguards in place and lack encryption, making it possible for other users of the same network to view your activity readily. Before making online payments, you should wait until you are at home or on a secure, password-protected network.

Don't overshare on social media

Social media can be your favourite pass time, but it can also put your personal information at risk. Reset your privacy settings and be aware of who has access to your posts, and be cautious when you are sharing your location, birthday, school/college/workplace, or other personal details.


ಸೈಸೆಕ್
ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್
ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ
ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿ ಸುರಕ್ಷಿತವಾಗಿರಿ.
ಲಕ್ಷ್ಮಿ ತಮ್ಮ ಗೆಳೆಯರೊಂದಿಗಿನ ಫೋಟೊ ಒಂದನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪೋಸ್ಟ್ ಮಾಡುತ್ತಾರೆ.
ಈ ಫೋಟೊದಲ್ಲಿ ಎಲ್ಲರೂ ತುಂಬ ಚೆನ್ನಾಗಿ ಕಾಣಿಸ್ತಿದ್ದಾರೆ. ಸಕ್ಕತಾಗಿದೆ!
ಒಂದು ಕಾಮೆಂಟ್ ಹಾಕಿ, ಅವರಿಗೆಲ್ಲ ಇರಿಸು ಮುರಿಸು ಉಂಟುಮಾಡ್ತೀನಿ!
ಲಕ್ಷ್ಮಿ ಅವರಿಗೆ ಕಾಮೆಂಟ್ ನೋಡಿ, ಬೇಸರ ಆಗುತ್ತದೆ, ಆದರೆ...
ಈ ಖಾತೆಯನ್ನು ರಿಪೋರ್ಟ್ ಮಾಡಿ, ಬ್ಲಾಕ್ ಮಾಡ್ತೀನಿ. ಇಂತಹ ಕಾಮೆಂಟ್‌ಗಳಿಗೆ ನಾನು ಯಾಕೆ ಹೆದರಬೇಕು ಇಲ್ಲಾ ಬೇಸರ ಪಟ್ಕೋಬೇಕು?
ಲಕ್ಷ್ಮಿ ಅವರು ತಮ್ಮ ಬದುಕಿಗೆ ತಾವೇ ರಕ್ಷಕರು. ನೀವೂ ಕೂಡ ಲಕ್ಷ್ಮಿಯಂತೆ ಧೈರ್ಯಲಕ್ಷ್ಮಿ ಆಗಿ.
• ಗೊತ್ತಿಲ್ಲದವರೊಂದಿಗೆ ಆನ್‌ಲೈನ್ ಗೆಳೆತನ ಮಾಡುವಾಗ, ಎಚ್ಚರ!
• ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ತಮ್ಮ ಗುರುತು ಮರೆಮಾಚಿ, ಜನ ನಿಮಗೆ ಮೋಸ ಮಾಡಬಹುದು.
• ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಇಲ್ಲವೇ ಫೋಟೊ ಕಳುಹಿಸಿ ಎಂಬ ಸಂದೇಶಗಳ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ.
• ಯಾರಾದರೂ ಒರಟಾಗಿ ಕಾಮೆಂಟ್ ಹಾಕಿದರೆ ಇಲ್ಲವೇ ಆನ್‌ಲೈನ್ ಬೆದರಿಕೆ ಹಾಕಿದರೆ, ಅವೇ ಪ್ಲಾಟ್‌ಫಾರಮ್‌ನಲ್ಲಿ ಆ ಖಾತೆಯನ್ನು ರಿಪೋರ್ಟ್ ಮಾಡಿ.
• ಸೈಬರ್ ಬೆದರಿಕೆ ಮತ್ತು ಆನ್‌ಲೈನ್ ಕಿರುಕುಳದ ಬಗ್ಗೆ ನೀವು cybercrime.gov.in ನಲ್ಲಿ ಕೂಡ ದೂರು ಸಲ್ಲಿಸಬಹುದು.
@CySecKCoE


ಸೈಸೆಕ್
ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್
ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ
ಜ್ಯೂಸ್ ಜ್ಯಾಕಿಂಗ್ ಬಗ್ಗೆ ಎಚ್ಚರ
ಸುಶ್ಮಾ ಮತ್ತು ಪ್ರತೀಕ್ ಒಂದು ಮಾಲ್‌ನಲ್ಲಿದ್ದಾರೆ. ಸುಶ್ಮಾ ಅವರ ಫೋನಿನ ಬ್ಯಾಟರಿ ಚಾರ್ಜ್ ಮುಗಿಯುತ್ತಾ ಬಂದಿದೆ. ಅವರು ತಮ್ಮ ಹತ್ತಿರದಲ್ಲೇ ಇರುವ ಚಾರ್ಜಿಂಗ್ ಕೇಬಲ್‌ಗಳನ್ನು ನೋಡುತ್ತಾರೆ.
ಹೇಯ್, ನನ್ ಫೋನ್ ಚಾರ್ಜ್ ಮಾಡೋಕೆ ಕೇಬಲ್ ಸಿಕ್ತು; ಫೋನ್ ಇನ್ನೇನ್ ಆಫ್ ಆಗ್ಲಿಕ್ಕಿತ್ತೆ.
ಸಾರ್ವಜನಿಕರಿಗೆ ಇಟ್ಟಿರುವ ಚಾರ್ಜಿಂಗ್ ಪೋರ್ಟ್‌ಗಳಲ್ಲಿರುವ ಕೇಬಲ್‌ನಿಂದ ನಿಮ್ಮ ಫೋನ್ ಚಾರ್ಜ್ ಮಾಡುವ ಮುನ್ನ ಎರಡು ಬಾರಿ ಯೋಚಿಸಿ – ಕಳ್ಳರು ಬಲೆ ಬೀಸಿರುತ್ತಾರೆ.
• ಬಳಕೆದಾರರು ತಮ್ಮ ಡಿವೈಸ್‌ಗಳನ್ನು ಯುಎಸ್‌ಬಿ ಪೋರ್ಟ್‌ಗಳ ಪ್ಲಗ್ ಮಾಡಿದಾಗ ಇಲ್ಲವೇ ಮಾಲ್‌ವೇರ್ ತುಂಬಿರುವ ಯುಎಸ್‌ಬಿ ಕೇಬಲ್ ಬಳಸಿದಾಗ ಜ್ಯೂಸ್ ಜ್ಯಾಕಿಂಗ್ ಆಗುತ್ತದೆ.
• ಯುಎಸ್‌ಬಿ ಚಾರ್ಜರ್‌ನ ಡೇಟಾ ಪಿನ್‌ನಿಂದ ಕಳ್ಳರು ಡೇಟಾ ಹೊರತೆಗೆಯುತ್ತಾರೆ. ಇದರರ್ಥ ಡಿವೈಸ್ ಚಾರ್ಜ್ ಆಗುವುದರ ಜೊತೆಗೆ, ತನ್ನೊಳಗಿನ ಡೇಟಾವನ್ನು ಹೊರಗಿನವರಿಗೆ ನೋಡಲು ಬಿಡುತ್ತದೆ.
• ಆಗ ಕಳ್ಳರು ನಿಮ್ಮ ಡೇಟಾ ನೋಡಿ, ಕಾಪಿ ಮಾಡಿಕೊಳ್ಳಬಹುದು ಹಾಗೂ ನೀವು ಬಳಸಲು ಆಗದಂತೆ ಡಿವೈಸ್‌ಗಳಿಗೆ ಬೀಗ ಹಾಕಬಹುದು.
• ಯಾವಾಗಲೂ ನಿಮ್ಮದೇ ಚಾರ್ಜಿಂಗ್ ಕೇಬಲ್‌ಗಳನ್ನು ಬಳಸಿ.
@CySecKCoE


ಸೈಸೆಕ್
ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್
ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ
ಆನ್‌ಲೈನ್ ಶಾಪಿಂಗ್ ಮಾಡುವಾಗ ಎಚ್ಚರ!
ಪ್ರೇಮ ಅವರು ಹೊಸ ಬ್ರ್ಯಾಂಡೆಡ್ ಬ್ಯಾಗ್ ಕೊಳ್ಳಲು ತುಂಬ ದಿನಗಳಿಂದ ಕಾಯುತ್ತಿದ್ದಾರೆ. ಅದನ್ನು ಅರ್ಧ ಬೆಲೆಗೆ ಮಾರುತ್ತಿರುವ ಇನ್ಸ್ಟಾಗ್ರಾಮ್ ಅಂಗಡಿಯೊಂದು ಅವರ ಕಣ್ಣಿಗೆ ಬೀಳುತ್ತದೆ.
ಆಹಾ! ಎಷ್ಟು ಕಡಿಮೆ ಬೆಲೆಗೆ ಸಿಕ್ತಿದೆ. ಖಾಲಿ ಆಗೋಕೂ ಮುಂಚೆ ನಾನ್ ಬೇಗ ಕೊಂಡುಕೊಳ್ತೀನಿ.
ಕೆಲವು ಬಳಕೆದಾರರು ಹಣ ಕಳುಹಿಸಿದ ಮೇಲೆ, ಖಾತೆಯನ್ನೇ ಅಳಿಸಿ ಹಾಕ್ತೀನಿ.
ಸ್ವಲ್ಪ ನಿಲ್ಲಿ. ಈ ಇನ್ಸ್ಟಾಗ್ರಾಮ್ ಖಾತೆಯಲ್ಲಿ ತುಂಬ ಕಡಿಮೆ ಫೋಸ್ಟ್‌ಗಳಿವೆ. ಇದು ಮೋಸದ ಅಂಗಡಿ ಆಗಿರಬಹುದಲ್ಲಾ? ಅವರ ಬಳಿ ಸರಿಯಾದ ವೆಬ್‌ಸೈಟ್ ಇದೆಯಾ?
• ಆನ್‌ಲೈನ್ ಮೂಲಕ ಕೊಳ್ಳುವಾಗ ಎಚ್ಚರವಾಗಿರಿ.
• ವೆಬ್‌ಸೈಟ್ / ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಖಾತೆ ಸರಿಯಾಗಿದೆಯೇ ನೋಡಿ. ಬಹಳಷ್ಟು ಬಾರಿ ಸರಿಯಾಗಿ ಇರುವಂತೆಯೇ ಕಾಣುವ ವೆಬ್‌ಸೈಟ್ /ಖಾತೆಗಳನ್ನು ಮೋಸಗಾರರು ಹುಟ್ಟುಹಾಕುತ್ತಾರೆ.
• ನಿಮಗೆ ಖಾತ್ರಿಯಿಲ್ಲದಿದ್ದರೆ, ಆರ್ಡರ್ ಮಾಡುವಾಗ ಕ್ಯಾಶ್ ಆನ್ ಡೆಲಿವರಿ ಆಯ್ಕೆಮಾಡಿ.
@CySecKCoE

AWARENESS POSTERS

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.**

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.