K-tech

IISc

KSCST

ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ | ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ

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

ಸೈಬರ್ ವಾರ್ತಿಕ

ಆಗಸ್ಟ್ 2022

CYBER VARTIKA

AUGUST 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

ವಿಶಾಲ್ ಸಾಳ್ವಿ
ಮುಖ್ಯ ಮಾಹಿತಿ ಸುರಕ್ಷತೆ ಅಧಿಕಾರಿ (ಸಿಐಎಸ್ಒ) ಮತ್ತು
ಸೈಬರ್ ಸುರಕ್ಷತೆ ವಿಭಾಗದ ಮುಂದಾಳು, ಇನ್ಫೋಸಿಸ್ ಲಿಮಿಟೆಡ್

Vishal Salvi
Chief Information Security Officer (CISO) &
Head of Cyber Security, Infosys Limited

ಜಗತ್ತಿನಾದ್ಯಂತ ಉದ್ಯಮಗಳು ಹೆಚ್ಚೆಚ್ಚು ಹೊಸಹಮ್ಮುಗೆ, ಡಿಜಿಟೈಸೇಶನ್, ಮೊಬಿಲಿಟಿ, ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್, ತೆರೆದ ಇಂಟರ್‌ನೆಟ್, ಸ್ಮಾರ್ಟ್ ತಂತ್ರಜ್ಞಾನ ಹಾಗೂ ಇನ್ನೂ ಹಲವು ಹೊಸತನಗಳನ್ನು ಅಪ್ಪಿ ಒಪ್ಪಿಕೊಳ್ಳುತ್ತಿವೆ. ಇದರಿಂದ ಅವಕಾಶಗಳು ತಂತಾನೆ ಹೆಚ್ಚಾಗುತ್ತವೆ. ಆದರೆ, ಇದರಿಂದಾಗಿ ಉದ್ಯಮಗಳ ಡೇಟಾ, ಕಂಪ್ಯೂಟರ್ ಮತ್ತಿತರ ಸ್ವತ್ತುಗಳ ಮೇಲೆ ಹೊಚ್ಚಹೊಸ ಬಗೆಯಲ್ಲಿ ಬಂದೆರಗುವ ಸೈಬರ್ ದಾಳಿಗಳನ್ನು ತಡೆಯಲು ಹೊಸ ದಾರಿಗಳನ್ನು ಹುಡುಕುವ ಅಗತ್ಯ ಹೆಚ್ಚಾಗುತ್ತಿದೆ. ಇಂದಿನ ದಿನದಲ್ಲಿ ವ್ಯಾಪಾರ ಚೆನ್ನಾಗಿ ನಡೆಸಿಕೊಂಡು ಹೋಗಲು, ಹಣಕಾಸು ಮತ್ತು ಕಾರ್ಯನಿರ್ವಹಣೆಯ ಮೇಲಿನ ಹಿಡಿತ ಎಷ್ಟು ಮುಖ್ಯವೊ ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ಕಡೆ ಗಮನಕೊಡುವುದು ಕೂಡ ಅಷ್ಟೇ ಮುಖ್ಯವಾಗಿದೆ. ಸೈಬರ್‌ಸುರಕ್ಷತೆ ಎನ್ನುವುದು ಮುಖ್ಯವಾಹಿನಿಯಾಗಿ ಹೊರಹೊಮ್ಮಿದೆ. ಆಮೇಲೆ ನೋಡಿದರಾಯಿತು ಎಂಬ ಅಸಡ್ಡೆ ಸಲ್ಲದು.

ಕೋವಿಡ್-ಬಳಿಕದ ಜಗತ್ತಿನಲ್ಲಿ ಹೈಬ್ರಿಡ್ ಮಾದರಿ ಮತ್ತು ಎಲ್ಲಿಂದ ಬೇಕಾದರೂ ಕೆಲಸ ಮಾಡುವ ಸಂಸ್ಕೃತಿ ಹೆಚ್ಚುತ್ತಿರುವಂತೆಯೇ, ಹಲವು ಕಡೆ ಹಂಚಿಹೋಗಿರುವ ಕೆಲಸಗಾರರನ್ನು ನಿರ್ವಹಿಸಲು ಹಳೆಯ ಸುರಕ್ಷತೆ ಕ್ರಮಗಳು ಸಾಕಾಗುವುದಿಲ್ಲ ಎಂದು ಸಂಸ್ಥೆಗಳು ಅರಿತುಕೊಂಡಿವೆ. ಹೊಸ ಹೊಸ ಬಗೆಯ ಸೈಬರ್ ದಾಳಿಗಳು ಹುಟ್ಟಿಕೊಳ್ಳುತ್ತಿರುವಂತೆ, ತಪ್ಪಿಸಿಕೊಳ್ಳಲಾಗದ ಸಿಕ್ಕಲಿನ ಅಪಾಯಗಳ ಸುಳಿ ನಮ್ಮ ಕಣ್ಣೆದುರೇ ಇದೆ. ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ಉಲ್ಲಂಘನೆಯ ಪರಿಣಾಮ ಬರೀ ಹಣಕಾಸಿನ ನಷ್ಟಕ್ಕೆ ಸೀಮಿತವಾಗಿಲ್ಲ. ಅಂತಹ ಒಂದು ಘಟನೆಯಿಂದ ಐಟಿ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಕೆಲಹೊತ್ತು ಕೆಲಸ ಮಾಡುವುದನ್ನು ನಿಲ್ಲಿಸಬಹುದು. ಇದರಿಂದ ಬಳಕೆದಾರರಿಗೆ ತೊಂದರೆ ಆಗುತ್ತದೆ ಹಾಗೂ ಸಂಸ್ಥೆಯ ಹೆಸರು ಹಾಳಾಗಿ, ಕೊಳ್ಳುಗರು ಸಂಸ್ಥೆಯ ಮೇಲಿನ ನಂಬಿಕೆ ಕಳೆದುಕೊಳ್ಳಬಹುದು. ಸೈಬರ್ ದಾಳಿಗಳಿಂದಾಗಿ ಮಾಡಬೇಕಾದ ಕೆಲಸ ಇಲ್ಲವೇ ನೀಡಬೇಕಾದ ಸೇವೆಯಲ್ಲಿ ಏರುಪೇರಾದರೆ ಕಾನೂನು ಕ್ರಮಗಳನ್ನು ಎದುರಿಸಲು ಕೂಡ ಅಣಿಯಾಗಿರಬೇಕು.

ಜನರು, ಸಿಸ್ಟಮ್ ಇಲ್ಲವೇ ಪ್ರಕ್ರಿಯೆಗಳಿಂದ ಅಪಾಯಗಳು ಬರಬಹುದಾದ್ದರಿಂದ, ಒಂದು ಸಂಸ್ಥೆಯಲ್ಲಿ ಸೈಬರ್ ಸುರಕ್ಷತೆಯನ್ನು ಎಲ್ಲಾ ಹಂತದಲ್ಲೂ ಪಾಲಿಸಬೇಕು. ಸಂಸ್ಥೆಗಳು ಎಲ್ಲಾ ಹೊತ್ತಿನಲ್ಲೂ ಎಚ್ಚರಿಕೆಯಿಂದಿರಬೇಕು ಹಾಗೂ ತಮ್ಮದೇ ಸಂಸ್ಥೆಯ, ಕೊಳ್ಳುಗರ ಮತ್ತು ಬಳಕೆದಾರರ ಮಾಹಿತಿ, ಡೇಟಾ ಮತ್ತು ಸ್ವತ್ತುಗಳನ್ನು ಕಾಪಾಡಿಕೊಳ್ಳಲು ಬೇಕಾದ ಸರಿಯಾದ ಸಾಧನಗಳು, ತಂತ್ರಜ್ಞಾನ, ಪ್ರಕ್ರಿಯೆ, ಸಿಸ್ಟಮ್, ಕೌಶಲ್ಯ, ಅನುಭವ, ಅರಿವು ಮತ್ತು ಪರಿಣತಿಯಲ್ಲಿ ಹೂಡಿಕೆ ಮಾಡಿ ಅವನ್ನು ಜಾರಿಗೆ ತರಬೇಕು.

ಬಗೆಬಗೆಯ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಪರಿಹಾರಗಳನ್ನು ಒಂದಾಗಿಸಿ ಬಲ ತುಂಬಲು "zero trust approach" ಅಂದರೆ ಯಾರನ್ನೂ ನಂಬದಿರುವ ದಾರಿಯೇ ಸರಿಯಾದುದು ಎಂಬುದು ನನ್ನ ಬಲವಾದ ವಾದ. ಎಲ್ಲಾ ಬಳಕೆದಾರರು ಪಾಸ್‌ವರ್ಡ್ ಬಳಸಬೇಕು. ಎಲ್ಲಾ ಬಗೆಯ ಅಪ್ಲಿಕೇಶನ್ ಮತ್ತು ಡೇಟಾವನ್ನು ಸರಿಯಾದ ಪರಿಶೀಲನೆ ಇಲ್ಲದೆ ಯಾರೂ ನೋಡುವಂತಿರಬಾರದು ಮತ್ತು ನೆಟ್‌ವರ್ಕ್ ಒಳಗಿದ್ದ ಮಾತ್ರಕ್ಕೆ ಯಾರಿಗೂ ಉಚಿತ ಪ್ರವೇಶ ನೀಡಬಾರದು. ವ್ಯಾಪಾರದ ಪ್ರತಿಯೊಂದು ಹಂತದಲ್ಲೂ, secure-by-design ಅಂದರೆ ಕಟ್ಟುವಾಗಲೇ ಸುರಕ್ಷಿತವಾಗಿರುವಂತೆ ನೋಡಿಕೊಳ್ಳುವುದನ್ನು ಅಳವಡಿಸಿಕೊಂಡರೆ, ಸೈಬರ್ ಅಪಾಯಗಳನ್ನು ಆದಷ್ಟೂ ತಗ್ಗಿಸಬಹುದು. ಇಂದು, ಸಂಸ್ಥೆಗಳು ತಮ್ಮ ಈಗಿನ ಮತ್ತು ನಾಳೆಯ ವ್ಯಾಪಾರದ ಅಗತ್ಯಗಳಿಗೆ ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ವಿಷಯದಲ್ಲಿ ಎಚ್ಚರಿಕೆಯ ತೀರ್ಮಾನಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳುತ್ತಿದ್ದಾರೆ. ಸೈಬರ್ ಸುರಕ್ಷತೆ ಚರ್ಚೆಯಲ್ಲಿ ಸಕ್ರಿಯವಾಗಿ ತೊಡಗಿಸಿಕೊಳ್ಳುವ ಅಗತ್ಯವಿದೆ ಹಾಗೂ ಜೇಡರ ಬಲೆಯಂತೆ ಕೂಡಿಕೊಂಡಿರುವ ಇಂದಿನ ಜಗತ್ತಿನಲ್ಲಿ ಉಳಿದು ಬೆಳೆಯಲು, ವ್ಯಾಪಾರದ ಪ್ರತಿಯೊಂದು ಹಂತದಲ್ಲೂ ಸುರಕ್ಷತೆಯನ್ನು ಅಳವಡಿಸಬೇಕು.

ಸೈಬರ್ ಸುರಕ್ಷತೆ ಎನ್ನುವುದು ಒಂದು ಸಂಸ್ಥೆಯೊಳಗಿನ ಭದ್ರತೆ ಅಧಿಕಾರಗಳ ಹೊಣೆ ಮಾತ್ರವಲ್ಲ, ಎಲ್ಲಾ ಕೆಲಸಗಾರರು ಮತ್ತು ಪಾಲುದಾರರ ಒಟ್ಟಾರೆ ಹೊಣೆಗಾರಿಕೆಯಾಗಿದೆ. ಸುರಕ್ಷತೆಯ ಮನಸ್ಥಿತಿ ಬೆಳೆಸಿಕೊಳ್ಳಲು ಅನುವು ಮಾಡಿಕೊಡಬೇಕು ಹಾಗೂ ಸಕಾರಾತ್ಮಕ ಮತ್ತು ಬಾಳಿಕೆ ಬರುವ ಸುರಕ್ಷತೆಯ ಸಂಸ್ಕೃತಿಗೆ ನೀರೆರೆಯಬೇಕು. ಎಲ್ಲಾ ಸಂಬಂಧಪಟ್ಟವರು ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ನೀತಿ ನಿಯಮಗಳನ್ನು ತಿಳಿದುಕೊಂಡು ಅದರಂತೆ ನಡೆದುಕೊಳ್ಳುವುದು, ಒಂದು ಸಂಸ್ಥೆಯ ಸುರಕ್ಷತೆಯ ನಿಲುವನ್ನು ಎತ್ತಿಹಿಡಿಯುವಲ್ಲಿ ಮಹತ್ವದ ಪಾತ್ರ ವಹಿಸುತ್ತದೆ.

Enterprises worldwide are increasingly embracing innovation, digitization, mobility, cloud computing, open internet, smart technology and more, which organically leads to amplified opportunities. However, this also entails an increasing need for sophistication in handling the ever evolving cyberattacks on enterprise assets. Today, one cannot deny that cyber security has taken the center stage, along with financial and operations controls when it comes to upholding the health of a business. Cybersecurity has clearly emerged as mainstream and is no more an afterthought.

With hybrid and work from anywhere culture emerging as the new reality in the post-pandemic world, organizations have realized that the conventional security architecture is not enough to deal with a distributed workforce. And then, there is the threat landscape that is becoming more complex and inescapable, with cyberattacks getting more deceptive by the day. The impact of cybersecurity breach is not just limited to financial losses. A single incident can trigger downtime of IT applications, thereby impacting customer experience, and can also lead to loss of reputation and client trust. Non-compliance with regulatory mandates caused due to security breaches can also lead to legal actions.

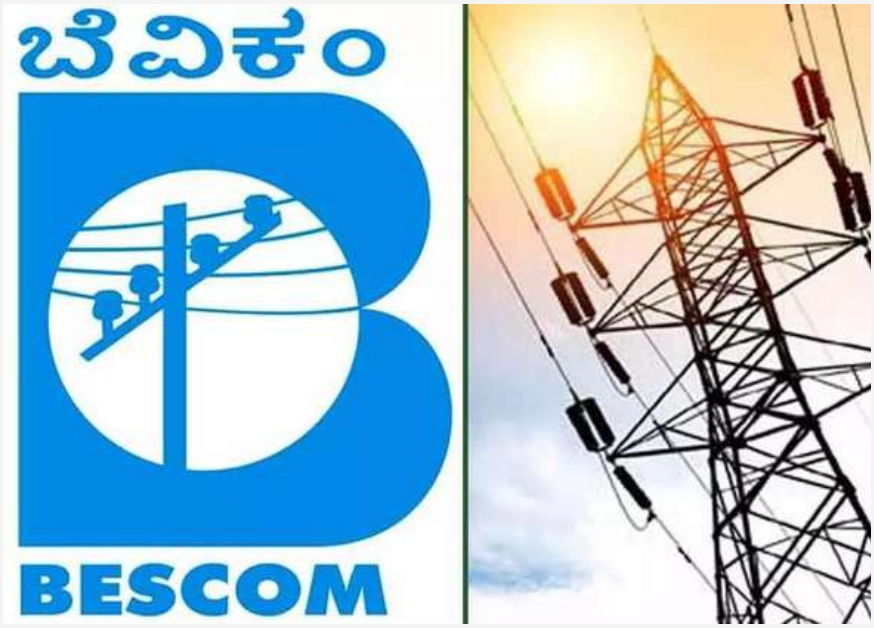
Cybersecurity thus needs to be all-pervasive within an organization as threats could arise from people, systems, or processes. Businesses need to be cyber vigilant round the clock and implement and invest in the right tools, technology, processes, systems, skills, experience, knowledge, and expertise in order to guard their organizational, clients, and the end customers' information, data, and assets.

I strongly believe that today a Zero Trust approach is imperative to consolidate different security solutions: with security framework necessitating authentication of all users, authorization, and validation of all access to applications and data, and systematic checks to eliminate access by default. Also, by adopting a secure-by-design approach at every phase of the business lifecycle, security risks can be minimized to a great extent. Today, organizations are making strategic decisions in terms of cyber security investments for their current and future business needs. There is indeed a need to proactively engage in the cyber security dialogue and embed security at every stage of the business in order to survive and thrive in the hyper-connected world.

Cyber Security is no more the sole responsibility of the security practitioners within an organization, it is a collective responsibility of the employees and the different stakeholders. Driving security mindset, and nurturing a positive and sustainable security culture, where all the relevant stakeholders are aware of, and abide by the policy, rules and regulations is critical for upholding the security posture of an organization.

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ಸೈಬರ್ ಪೊಲೀಸರ ಬಳಿ ದೂರು ದಾಖಲಿಸಿದ ಬೆಸ್ಕಾಮ್



ಇತ್ತೀಚೆಗೆ ಹಲವು ಬಳಕೆದಾರರು, ಬಿಲ್ ಕಟ್ಟುವಂತೆ ಅವರಿಗೆ ಬರುತ್ತಿರುವ ಎಸ್ಎಮ್ಎಸ್‌ಗಳ ಬಗ್ಗೆ ದೂರು ನೀಡಲು ಬೆಸ್ಕಾಮ್ ಸಹಾಯವಾಣಿ1912 ಕ್ಕೆ ಕರೆ ಮಾಡಿದ ಬಳಿಕ ಅಧಿಕಾರಿಗಳು ದೂರು ದಾಖಲಿಸಿದ್ದಾರೆ . ವಿದ್ಯುತ್ ಬಿಲ್‌ಗಳನ್ನು ಕಟ್ಟಲು ಬೆಸ್ಕಾಮ್ ಬಿಲ್ಲಿಂಗ್ ಕೌಂಟರ್‌ಗಳು, ಬೆಸ್ಕಾಮ್ ಮಿತ್ರ ಆಪ್ ಇಲ್ಲವೇ ಬೆಸ್ಕಾಮ್ ಆನ್‌ಲೈನ್ ಪೋರ್ಟಲ್‌ಗಳನ್ನು ಮಾತ್ರ ಬಳಸಬೇಕು ಎಂದು ಬೆಸ್ಕಾಮ್ ತನ್ನ ಬಳಕೆದಾರರನ್ನು ಕೇಳಿಕೊಳ್ಳುತ್ತದೆ.

ಆನ್‌ಲೈನ್ ಮೋಸದಲ್ಲಿ 1 ಲಕ್ಷಕ್ಕಿಂತ ಹೆಚ್ಚು ಕಳೆದುಕೊಂಡ ಹೆಂಗಸು

ಮೋಸಹೋದ ಹೆಂಗಸಿಗೆ ತಮ್ಮ ಪ್ಯಾನ್ ಕಾರ್ಡ್ ಅಪ್‌ಡೇಟ್ ಮಾಡುವಂತೆ ಮೂರು ಓಟಿಪಿಗಳು ಒಟ್ಟೊಟ್ಟಿಗೆ ಬಂದವು. ಸಂದೇಶದಲ್ಲಿಸೂಚಿಸಿದಂತೆ ಓಟಿಪಿ ಸಲ್ಲಿಸಿದ ಬಳಿಕ, ಮೂರು ವಹಿವಾಟುಗಳಲ್ಲಿ ಅವರು 1.24 ಲಕ್ಷ ಕಳೆದುಕೊಂಡರು.

ಇತ್ತೀಚಿನ ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್ ಮೋಸಗಳ ಮಾಹಿತಿ ಹಂಚಿಕೊಂಡ ಸರ್ಕಾರ

ಆಗಸ್ಟ್ ಆರಂಭದಲ್ಲಿ ರಾಜ್ಯ ಸಭೆಗೆ ಕೊಡಲಾದ ಮಾಹಿತಿಯಂತೆ, ಹಿಂದಿನ ಹಣಕಾಸು ವರ್ಷಕ್ಕೆ ಹೋಲಿಸಿದರೆ 2022ರ ಹಣಕಾಸು ವರ್ಷದಲ್ಲಿಆನ್‌ಲೈನ್ ಮೋಸದ ಪ್ರಕರಣಗಳ ಎಣಿಕೆ ಸುಮಾರು 17.5% ನಷ್ಟು ಅಂದರೆ 160 ಕೋಟಿಯಿಂದ 128 ಕೋಟಿಗೆ ಇಳಿದಿದೆ.

ಕೆವೈಸಿ ಅಪ್‌ಡೇಟ್ ಮಾಡುವ ಲಿಂಕ್ ಕ್ಲಿಕ್ ಮಾಡಿ ₹93,804 ಕಳೆದುಕೊಂಡ ವ್ಯಕ್ತಿ

ಉಡುಪಿಯ ಒಬ್ಬ ವ್ಯಕ್ತಿಗೆ ಕೆವೈಸಿ ಅಪ್‌ಡೇಟ್ ಮಾಡುವಂತೆ ಸಂದೇಶ ಬಂದಿತು. ಅದರಲ್ಲಿದ್ದ ಲಿಂಕ್ ಕ್ಲಿಕ್ ಮಾಡಿದ ಬಳಿಕ, ಅವರು ತಮಗೆ ಬಂದಓಟಿಪಿ ಸಲ್ಲಿಸಿದರು. ಚಿಟಿಕೆ ಹೊಡೆಯುವಷ್ಟರಲ್ಲಿ ಕಳ್ಳರು ಅವರ ಎರಡು ಬ್ಯಾಂಕ್ ಖಾತೆಗಳಿಂದ ಸಾವಿರಾರು ರೂಪಾಯಿ ದೋಚಿದರು.

'ಸುಳ್ಳು ಮಾಹಿತಿ' ಹರಡಿದ್ದಕ್ಕಾಗಿ ಎಂಟು ಯೂಟ್ಯೂಬ್ ಚಾನಲ್‌ಗಳನ್ನು ತಡೆಹಿಡಿದ ಸರ್ಕಾರ

ತಡೆಹಿಡಿಯಲಾದ ಯೂಟ್ಯೂಬ್ ಚಾನಲ್‌ಗಳನ್ನು 114 ಕೋಟಿಗಿಂತ ಹೆಚ್ಚು ಮಂದಿ ನೋಡುತ್ತಿದ್ದರು ಹಾಗೂ 85 ಲಕ್ಷಕ್ಕಿಂತ ಹೆಚ್ಚು ಮಂದಿ ಅವುಗಳಿಗೆ ಸಬ್‌ಸ್ಕೈಬ್ ಆಗಿದ್ದರು. ಭಾರತದಲ್ಲಿನ ಧಾರ್ಮಿಕ ಸಮುದಾಯಗಳ ನಡುವೆ ಹಗೆತನವ ಬಿತ್ತಲು ಈ ಯೂಟ್ಯೂಬ್ ಚಾನಲ್‌ಗಳನ್ನು ಹುಟ್ಟುಹಾಕಲಾಗಿತ್ತು. ಈ ಚಾನಲ್‌ಗಳು ನಕಲಿ ಮತ್ತು ಕೆರಳಿಸುವ ಚಿತ್ರಗಳು, ನ್ಯೂಸ್ ಓದುವವರ ಚಿತ್ರಗಳು ಹಾಗೂ ಕೆಲವು ಟೀವಿ ಸುದ್ದಿ ಚಾನಲ್‌ಗಳ ಗುರುತುಗಳನ್ನು ಬಳಸಿ ಸುದ್ದಿ ಸರಿಯಾಗಿದೆ ಎಂದು ನೋಡುಗರನ್ನು ನಂಬಿಸುವ ಕೆಲಸ ಮಾಡುತ್ತಿದ್ದವು.

ಪ್ಲೇ ಸ್ಟೋರ್‌ನಲ್ಲಿ 2000 ಕ್ಕಿಂತ ಹೆಚ್ಚು ಆಪ್‌ಗಳಿಗೆ ಗೂಗಲ್‌ನಿಂದ ತಡೆ

ತಡೆಹಿಡಿಯಲಾದ ಆಪ್‌ಗಳು ಭಾರತೀಯ ಮಾರುಕಟ್ಟೆಗೆಂದೇ ಇನ್‌ಸ್ಟಂಟ್ ಲೋನ್ ಸೇವೆಗಳನ್ನು ಒದಗಿಸುತ್ತಿದ್ದವು.
ಆಗಸ್ಟ್ 11 ರಂದು, ಡಿಜಿಟಲ್ ಸಾಲ ನೀಡುವ ಸಂಸ್ಥೆಗಳಿಗೆ ಆರ್‌ಬಿಐ ಹೊಸ ಸೂಚನೆಗಳನ್ನು ನೀಡಿತು. ಅದರಲ್ಲಿ ಎಲ್ಲಾ ಮರೆಮಾಚಿದ ವೆಚ್ಚಗಳನ್ನುಬಯಲುಮಾಡಬೇಕು, ಕಂತಿನ ರಸೀತಿಯ ಬ್ಯಾಂಕ್ ವರ್ಗಾವಣೆಗಳಲ್ಲಿ ಇಲ್ಲವೇ ಬಳಕೆದಾರರ ಖಾತೆಗಳಿಗೆ ಆಗುವ ಹಣದ ಹಂಚಿಕೆಯಲ್ಲಿಹೊರಗಿನವರು ಶಾಮೀಲಾಗುವಂತಿಲ್ಲ ಹಾಗೂ ಇನ್ನೂ ಮುಂತಾದ ಸೂಚನೆಗಳು ಸೇರಿವೆ.

ಭಾರತದ 85% ಮಕ್ಕಳು ಸೈಬರ್ ಬೆದರಿಕೆಗೆ ಒಳಗಾಗುತ್ತಾರೆ: ಮೆಕಫಿ ವರದಿ

ಸೈಬರ್ ಬೆದರಿಕೆಗೆ ಒಳಗಾದ ಭಾರತದ ಮಕ್ಕಳ ಅಳತೆ ಜಾಗತಿಕ ಸರಾಸರಿಯ ಎರಡು ಪಟ್ಟಿಗಿಂತ ಹೆಚ್ಚಿದೆ. ಭಾರತದಲ್ಲಿ, ವರದಿಯಾದ ಸೈಬರ್ ಬೆದರಿಕೆಯ ಪ್ರಮುಖ ಮೂರು ಬಗೆಗಳೆಂದರೆ ಸುಳ್ಳು ಸುದ್ದಿ ಹರಡುವುದು (39%), ಗುಂಪುಗಳು ಇಲ್ಲವೇ ಮಾತುಕತೆಗಳಿಂದ ಹೊರಗಿಡುವುದು(35%) ಹಾಗೂ ಬಯ್ಯುವುದು (34%)

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ಆಕಾಶ ಏರ್‌ಲೈನ್ಸ್‌ನಲ್ಲಿ ಡೇಟಾ ಕಳ್ಳತನ: ಪ್ರಯಾಣಿಕರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಸೋರಿಕೆ

ಇದೇ ತಿಂಗಳು ಕೆಲಸ ಶುರುಮಾಡಿದ ಆಕಾಶ ಏರ್ ಎಂಬ ಭಾರತದ ಏರ್‌ಲೈನ್ಸ್ ಕಂಪನಿಯಲ್ಲಿ ಡೇಟಾ ಕಳ್ಳತನವಾಯಿತು. ಹೆಸರು, ಲಿಂಗ, ಫೋನ್ ನಂಬರ್ ಮತ್ತು ಇಮೇಲ್ ವಿಳಾಸದಂತಹ ಪ್ರಯಾಣಿಕರ ಮಾಹಿತಿ ಸೋರಿಕೆಯಾಗಿದೆ ಎಂದು ಏರ್‌ಲೈನ್ಸ್ CERT-In ಗೆ ತಿಳಿಸಿತ್ತು.

ಕಳ್ಳತನದ ವರದಿ ಮಾಡಿದ ಲಾಸ್ಟ್‌ಪಾಸ್ ಎಂಬ ಪಾಸ್‌ವರ್ಡ್ ಮ್ಯಾನೇಜರ್, ಪಾಸ್‌ವರ್ಡ್ ಕದ್ದೊಯ್ದಿಲ್ಲ ಎಂಬ ಸ್ಪಷ್ಟನೆ

ಲಾಸ್ಟ್‌ಪಾಸ್ ಎಂಬ ಹೆಸರುವಾಸಿಯಾದ ಪಾಸ್‌ವರ್ಡ್ ಮ್ಯಾನೇಜರ್ ಸ್ಟೋರೇಜ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗೆ ಕಳ್ಳರು ಕನ್ನ ಹಾಕಿದ್ದರು ಎಂದು ಕಂಪನಿಯುಖಚಿತಪಡಿಸಿದೆ. ಇತ್ತೀಚೆಗೆ ಕಳ್ಳರು ಕಂಪನಿಯ ಸೋರ್ಸ್ ಕೋಡ್ ಮತ್ತು ಬೇರೆ ಗುಟ್ಟಿನ ಮಾಹಿತಿಯನ್ನು ಕದ್ದರು. ಆದರೆ ಬಳಕೆದಾರರಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಅವರು ಕದ್ದಿಲ್ಲ ಎಂದು ಕಂಪನಿಯ ಸಿಇಒ ಖಚಿತಪಡಿಸಿದರು.

ಹೋಮ್ ಡೆಲಿವರಿಯ ಸೋಗಿನಲ್ಲಿ ನಿವೃತ್ತ ಐಎಎಸ್ ಅಧಿಕಾರಿಗೆ ₹2 ಲಕ್ಷ ಮೋಸ

ಮೋಸಹೋದವರು jagdishwineshopgurgaon.co ನಿಂದ ಮದ್ಯ ಆರ್ಡರ್ ಮಾಡಿದ್ದರು. ಗಡಿಬಿಡಿಯಲ್ಲಿ ಆಕೆ ಕಾಲ್ ಮಾಡಿದವರನ್ನು ನಂಬಿಓಟಿಪಿ ಜೊತೆ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ನಂಬರ್ ಹಂಚಿಕೊಂಡರು. ಆಕೆಯ ಕಾರ್ಡ್‌ನಿಂದ ₹630 ಮೊದಲಿಗೆ ಕಡಿತವಾಯಿತು. ಆದರೆ ಆಮೇಲೆ₹1,92,477.50 ಕಡಿತವಾಗಿರುವುದು ತಿಳಿಯಿತು.

ಕೆಆನ್‌ಲೈನ್ ಮೋಸದಲ್ಲಿ ₹3.53 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ ಹೆಂಗಸು

ಇತ್ತೀಚೆಗೆ 43 ರ ಹರೆಯದ ಒಬ್ಬ ಹೆಂಗಸಿಗೆ ಒಂದು ಸಂದೇಶ ಬಂದಿತು. ಅದರಲ್ಲಿ ಆನ್‌ಲೈನ್ ಕಮಾಡಿಟಿ ಮಾರಾಟದ ಮೂಲಕ ದಿನವೂ 5000 ರೂಪಾಯಿಗಿಂತ ಹೆಚ್ಚಿನ ಮೊತ್ತ ದುಡಿಯುವ ಅವಕಾಶವಿದೆ ಎಂದು ಬರೆದಿತ್ತು. ಹೂಡಿಕೆಯ ಬಳಿಕ, ಆ ಹೆಂಗಸು ತಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಯಲ್ಲಿ ಸಣ್ಣಮೊತ್ತ ಪಡೆದರು. ಅವರು ದೊಡ್ಡ ವಹಿವಾಟು ಮಾಡುವುದನ್ನು ಮುಂದುವರಿಸಿದರು. ಕೊನೆಗೆ ಮೋಸದಲ್ಲಿ ₹3.53 ಲಕ್ಷದಷ್ಟು ಕಳೆದುಕೊಂಡರು.

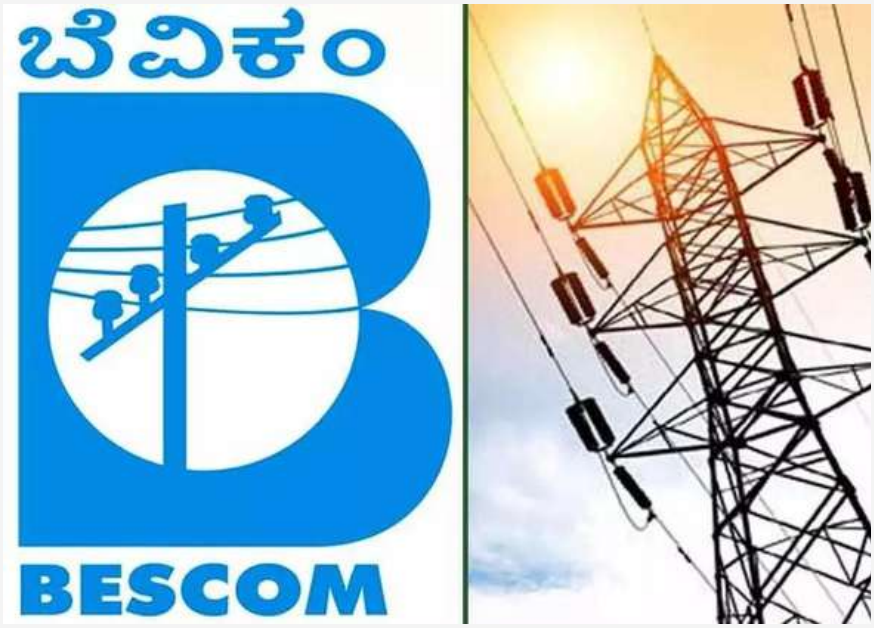
ಉಡುಪಿಯ ಹೆಂಗಸಿಗೆ ₹15.33 ಲಕ್ಷದ ಆನ್‌ಲೈನ್ ಮೋಸ

ಮೋಸಹೋದವರಿಗೆ ನಾಪ್‌ತೋಲ್‌ನಿಂದ ಗೀರೆಲೆ (ಸ್ಕ್ರ್ಯಾಚ್ ಕಾರ್ಡ್) ಇರುವ ಪತ್ರ ಅಂಚೆಯ ಮೂಲಕ ಬಂದಿತು. ಲಾಟರಿಯನ್ನು ಗೀರಿದಾಗ,ಅವರು ₹14.08 ಲಕ್ಷ ಗೆದ್ದಿರುವುದು ತಿಳಿಯಿತು. ಅವರು ಯಾವುದೇ ಮೊತ್ತ ಗೆದ್ದರೆ, ಕರೆ ಮಾಡಲು ನಂಬರ್ ನೀಡಲಾಗಿತ್ತು. ಅವರು ನಂಬಿ ಕರೆಮಾಡಿದಾಗ, ತಾವು ಗೆದ್ದ ಹಣ ಪಡೆಯಲು ಹಲವು ಹಂತಗಳಲ್ಲಿ ಹಣ ಕಳುಹಿಸುವಂತೆ ಅವರನ್ನು ಮರುಳು ಮಾಡಲಾಯಿತು.

ALWAYS BE CAREFUL

TOP CYBER NEWS

BESCOM FILES A COMPLAINT WITH CYBER POLICE



The officials filed a complaint after several customers recently dialled 1912, Bescom's helpline number, to complain about receiving the SMS asking them to pay bills. Bescom urges customers to pay their electricity bills only at Bescom billing counters, the Bescom Mitra App, or the Bescom online portal.

ONLINE SCAM COSTS A WOMAN MORE THAN ₹1 LAKH

The victim received three continuous OTP's requesting her PAN card update. After entering the OTP as instructed in the message, the woman lost 1.24 lakh in three transactions.

GOVT SHARES DATA ON ONLINE BANKING FRAUDS IN RECENT TIMES

According to information provided to the Rajya Sabha in early August, online fraud cases decreased by about 17.5% in FY22, from 160 crores to 128 crores, compared to the previous fiscal's record.

MAN LOSES ₹93,804 BY CLICKING ON KYC UPDATING LINK

The victim from Udupi received the message on KYC updation, and after clicking the link- he submitted the OTP received. The fraudsters, in no time, transacted thousands of rupees from his two bank accounts.

GOVT BANS EIGHT YOUTUBE CHANNELS FOR SPREADING 'DISINFORMATION'

The blocked YouTube channels had a cumulative viewership of over 114 crores and were subscribed to by over 85 lakh users. These YouTube channels were created to stir up hatred among religious communities in India.

The blocked channels were found to be using fake and sensational thumbnails, images of news anchors, and logos of certain TV news channels to mislead viewers into believing the news was genuine.

GOOGLE BANS OVER 2000 APPS FROM PLAY STORE

The banned apps were offering instant loan services that were specifically catering to the Indian market itself.

On August 11, the RBI issued new guidelines for digital lending firms to follow, including full disclosure of all hidden costs, no third-party involvement in bank transfers of installment receipts or disbursals to user accounts, and so on.

85% OF INDIAN CHILDREN EXPERIENCE CYBERBULLYING: MCAFEE REPORT

Indian children reported experiencing cyberbullying at rates that were higher than twice the global average. In India, the top three forms of cyberbullying reported were spreading false rumors (39%), being excluded from groups or conversations (35%), and name calling (34%).

TOP CYBER NEWS

AKASA AIRLINES SUFFERS DATA BREACH: PASSENGERS' PERSONAL INFORMATION EXPOSED

Akasa Air, an Indian domestic airline that started operations this month, experienced a data breach. The airline notified CERT-In that passenger information such as name, gender, phone number, and email address had been leaked.

PASSWORD MANAGER LASTPASS REPORTS BREACH, SAYS NO CREDENTIALS STOLEN

LastPass, one of the most popular password storage platforms, has confirmed that it was hacked. The hackers recently stole parts of the company's source code and other sensitive information. The company's CEO confirmed that its users' passwords had not been compromised.

RETIRED IAS OFFICER DUPED OF ₹2 LAKH ON THE PRETEXT OF HOME DELIVERY

The victim had ordered liquor from jagdishwineshopgurgaon.co and, in hurry, trusted the caller and shared the credit card number with the OTP. Initially, ₹630 was debited through her card but later found a transaction of ₹1,92,477.50.

WOMAN LOSES RS 3.53 LAKH IN ONLINE FRAUD

A 43-year-old woman recently received a text message offering an opportunity to earn over Rs 5000 per day through online commodity sales. After investing, the woman received a small sum of money in her bank account, and she continued to make larger transactions, eventually losing Rs 3.53 lakh to the fraud.

UDUPI WOMAN DUPED OF ₹15.33 LAKH IN ONLINE FRAUD

The victim received a letter that had a scratch card from Naaptol via post. Upon scratching the lottery, she realized that she had won ₹14.08 lakh. She was guided to call on a number if she had won any amount; upon calling she was asked to transfer money in phases to receive her prize money.

ALWAYS BE CAREFUL

ತಪ್ಪು ಮಾಹಿತಿ VS ಸುಳ್ಳು ಮಾಹಿತಿ

- ತಪ್ಪು ಮಾಹಿತಿ ಎಂದರೆ ನಿಜವಲ್ಲದ, ತಪ್ಪುದಾರಿಗೆ ಎಳೆಯುವ ಇಲ್ಲವೇ ಗೊತ್ತಿಲ್ಲದೆ ಹಂಚುವ ಬೇರೊಂದು ಹಿನ್ನೆಲೆಯ ವಿಷಯವಾಗಿದೆ.
- ತಪ್ಪು ಮಾಹಿತಿ ಜನರು ಸರಿಯಾದ ತೀರ್ಮಾನ ತೆಗೆದುಕೊಳ್ಳುವುದನ್ನು ತಡೆಯುತ್ತದೆ ಹಾಗೂ ಅವರು ತಮ್ಮ ಬಾಳಿಗೇ ಮುಳ್ಳಾಗುವಂತಹತೀರ್ಮಾನಗಳನ್ನು ಮಾಡುವ ಹಂತಕ್ಕೂ ಅದು ಕರೆದೊಯ್ಯಬಹುದು.
- ಎರಡೇ ದಿನದಲ್ಲಿ ಡಯಾಬಿಟಿಸ್ ಗುಣಪಡಿಸಬಹುದು ಎಂಬ ಸಂದೇಶ ಇಲ್ಲವೇ ರಾಜಕೀಯ ಸಂಚುಗಳ ಸಂದೇಶಗಳು ಕುಟುಂಬದವಾಟ್ಸಾಪ್ ಗುಂಪುಗಳಲ್ಲಿ ಹೊಳೆಯಂತೆ ಉಕ್ಕಿ ಹರಿಯುತ್ತಿದ್ದರೆ, ಅವರು ನಿಮ್ಮನ್ನು ಮರುಳು ಮಾಡುತ್ತಿದ್ದಾರೆ ಎಂದು ಅರ್ಥವಲ್ಲ. ತಾವುಸರಿಯಾದ ಸುದ್ದಿಯನ್ನೇ ದಾಟಿಸುತ್ತಿದ್ದೇವೆ ಎಂದು ಪಾಪ ಅವರು ಅಂದುಕೊಂಡಿರುತ್ತಾರೆ. ಆದರೆ, ಅವರು ತಪ್ಪುಸುದ್ದಿ ಹರಡುತ್ತಿರುತ್ತಾರೆ.
- ನೀವು ಹರಡುತ್ತಿರುವ ಸುದ್ದಿ ತಪ್ಪಾಗಿದ್ದು, ಆದರೆ ಅದು ತಪ್ಪೆಂದು ನಿಮಗೆ ಗೊತ್ತಿಲ್ಲದಿದ್ದರೆ, ನೀವು ತಪ್ಪು ಮಾಹಿತಿ ಹರಡುತ್ತಿದ್ದೀರ

- ಸುಳ್ಳು ಮಾಹಿತಿ ಎಂದರೆ ಮೋಸಮಾಡಲು ಇಲ್ಲವೇ ಕೆಡುಕುಂಟುಮಾಡಲು ಬೇಕೆಂದೇ ಸುಳ್ಳು ಇಲ್ಲವೇ ಅಡ್ಡದಾರಿಗೆ ಎಳೆಯುವ ಸುದ್ದಿಗಳನ್ನುಹಂಚುವುದು.
- ಸಾಮಾನ್ಯವಾಗಿ ರಾಜಕೀಯ ಶಕ್ತಿ, ಪ್ರಭಾವ, ಲಾಭ ಇಲ್ಲವೇ ಗೊಂದಲವೆಬ್ಬಿಸಿ ಜನರನ್ನು ತತ್ತರಿಸುವ ಬಯಕೆ ಸುಳ್ಳು ಮಾಹಿತಿ ಹರಡುವಂತೆಮಾಡುತ್ತದೆ.
- ಸುಳ್ಳು ಮಾಹಿತಿ ಜನರ ನೆಮ್ಮದಿಯನ್ನು ಕದಡಿ, ಅವರು ಗುಂಪುಗಳಾಗಿ ಒಡೆದುಹೋಗುವಂತೆ ಮಾಡಬಹುದು. ಸಿಟ್ಟು, ಹಗೆತನಕ್ಕೆ ಮರುಳಾಗಿಜನರು ಕೊಲ್ಲುವ ಹಂತಕ್ಕೂ ಹೋಗಬಹುದು.
- ಮೋಸದ ಸಂದೇಶಗಳು, "ನಂಬಲು ಕಷ್ಟವೆನಿಸುವ ಕೊಡುಗೆ"ಗಳು ನಿಮ್ಮನ್ನು ಹುಡುಕಿಕೊಂಡು ಬಂದರೆ - ಅದು ಸುಳ್ಳು ಮಾಹಿತಿ. ಮೋಸಮಾಡಲೆಂದೇ ಬಳಕೆದಾರರನ್ನು ಗುರಿಯಾಗಿಸಿದ ಸಂದೇಶಗಳು ಅವು.
- ಬೇಕೆಂದೇ ಹರಡುವ ತಪ್ಪುಸುದ್ದಿಯೇ ಸುಳ್ಳು ಮಾಹಿತಿ.

MISINFORMATION VS DISINFORMATION

•Misinformation is content that is false, misleading, or out of context that is shared unknowingly.

•Misinformation prevents people from making truly informed decisions and may even lead them to make decisions that are detrimental to their best interests.

•When the family WhatsApp groups are flooded with messages that help you cure diabetes in two days or political conspiracy theories, they're not trying to trick you—they're under the impression that they're passing along legit information. In reality, they're spreading misinformation.

•If you are spreading information that is wrong but don't know it is wrong, then you are spreading misinformation.

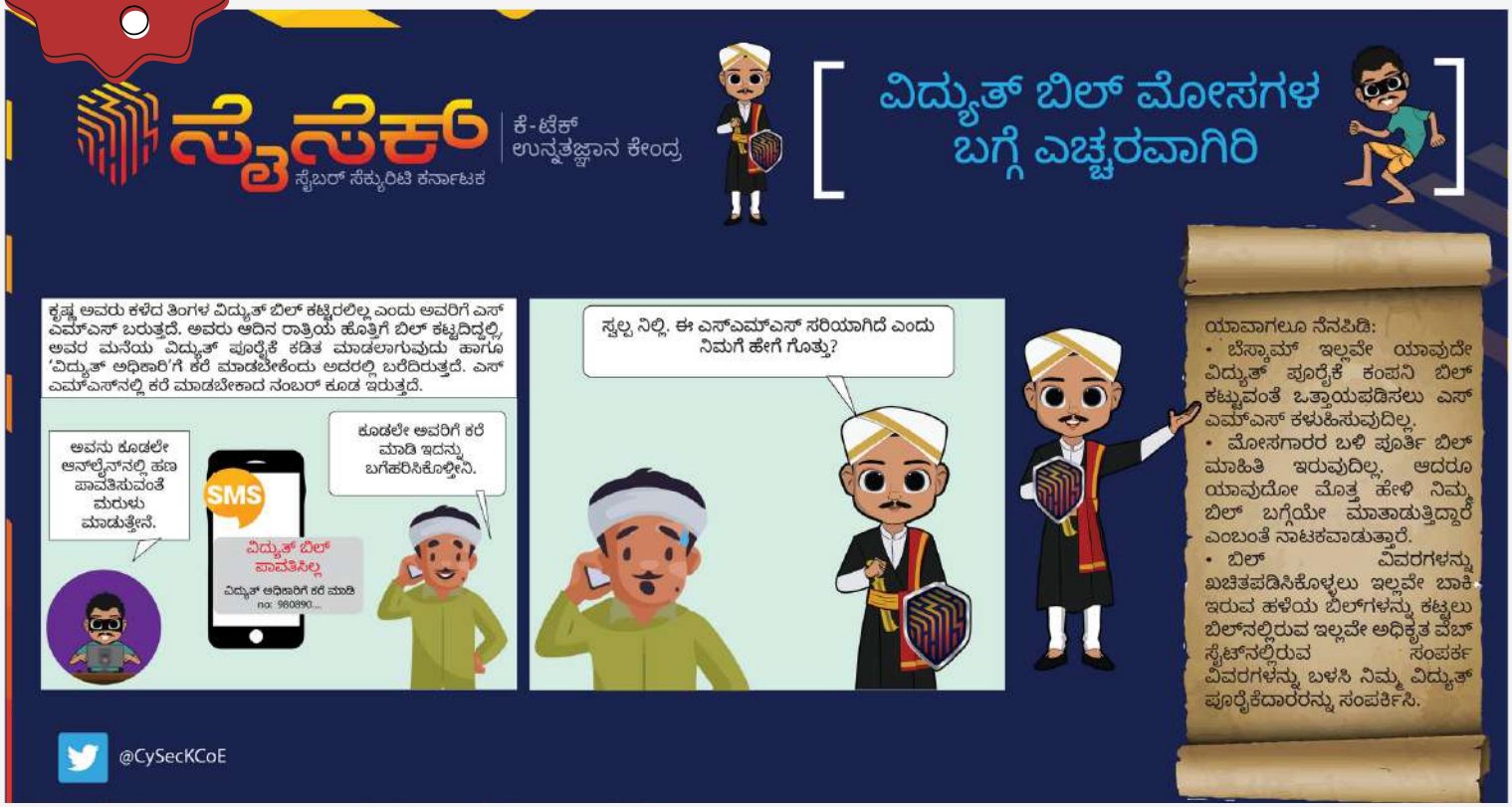
•Disinformation is intentionally false or misleading content that is shared with the intent to deceive or cause harm.

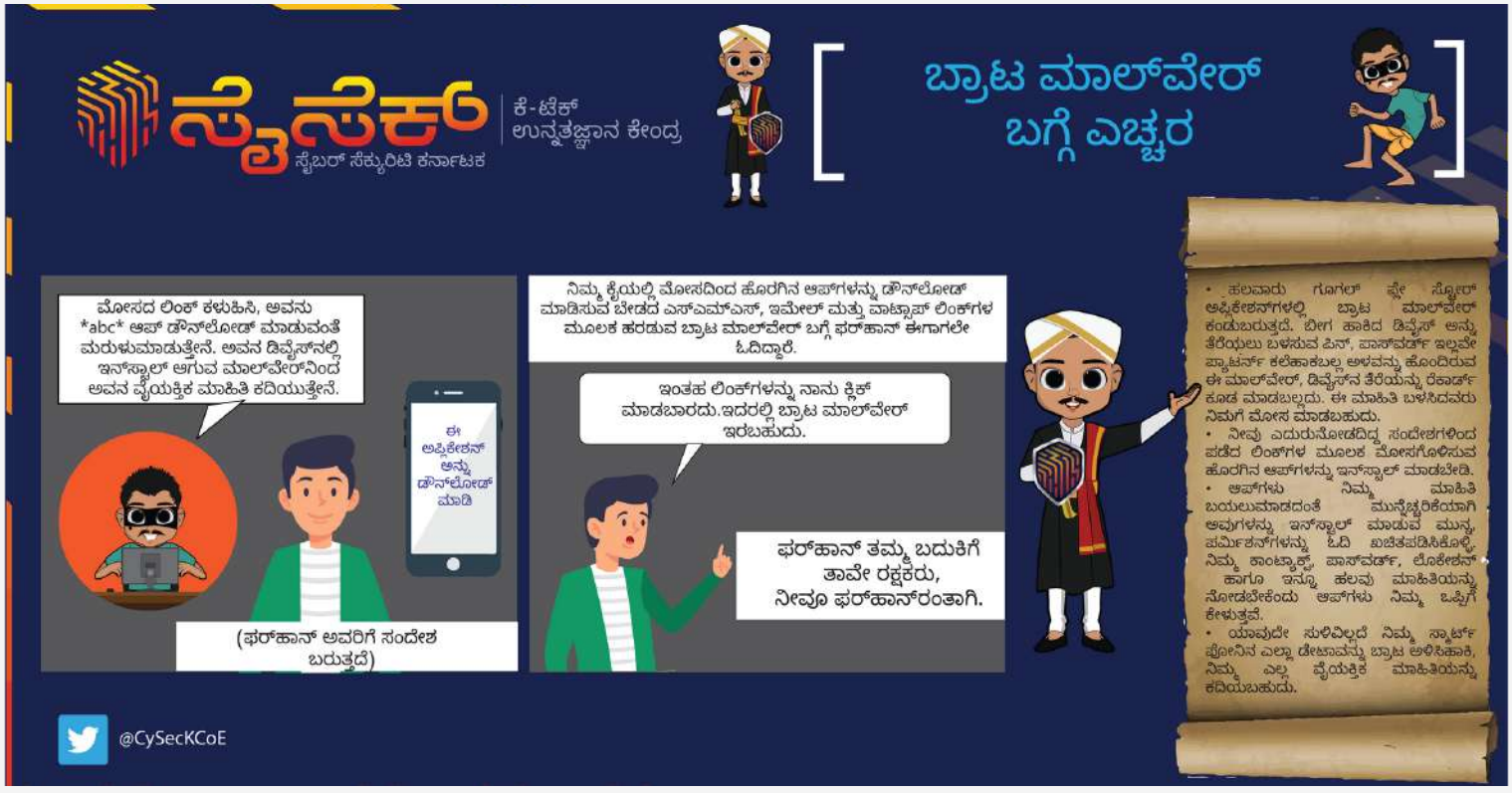
•Disinformation frequently stirs up strong emotions like anger and polarisation. It can lead to people expressing extreme views or getting lured.

•It is usually motivated by political power, influence, profit, or the desire to stir up chaos and confusion.

•When you get phishing messages, phone scams, or forward messages with "too good to be true offers,"- it's disinformation. These messages are aimed at consumers with the intent to harm.

•Disinformation is misinformation that is intentionally spread.


ಸೈಸೆಕ್
ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್
ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ
ವಿದ್ಯುತ್ ಬಿಲ್ ಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರವಾಗಿರಿ
ಕೃಷ್ಣ ಅವರು ಕಳೆದ ತಿಂಗಳ ವಿದ್ಯುತ್ ಬಿಲ್ ಕಟ್ಟಿರಲಿಲ್ಲ ಎಂದು ಅವರಿಗೆ ಎಸ್ ಎಮ್ಎಸ್ ಬರುತ್ತದೆ. ಅವರು ಆದಿನ ರಾತ್ರಿಯ ಹೊತ್ತಿಗೆ ಬಿಲ್ ಕಟ್ಟದಿದ್ದಲ್ಲಿ, ಅವರ ಮನೆಯ ವಿದ್ಯುತ್ ಪೂರೈಕೆ ಕಡಿತ ಮಾಡಲಾಗುವುದು ಹಾಗೂ 'ವಿದ್ಯುತ್ ಅಧಿಕಾರಿ'ಗೆ ಕರೆ ಮಾಡಬೇಕೆಂದು ಅದರಲ್ಲಿ ಬರೆದಿರುತ್ತದೆ. ಎಸ್ ಎಮ್ಎಸ್‌ನಲ್ಲಿ ಕರೆ ಮಾಡಬೇಕಾದ ನಂಬರ್ ಕೂಡ ಇರುತ್ತದೆ.
ಅವನು ಕೂಡಲೇ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹಣ ಪಾವತಿಸುವಂತೆ ಮರುಳು ಮಾಡುತ್ತೇನೆ.
SMS
ವಿದ್ಯುತ್ ಬಿಲ್ ಪಾವತಿಸಿಲ್ಲ
ವಿದ್ಯುತ್ ಅಧಿಕಾರಿಗೆ ಕರೆ ಮಾಡಿ no: 980890...
ಕೂಡಲೇ ಅವರಿಗೆ ಕರೆ ಮಾಡಿ ಇದನ್ನು ಬಗೆಹರಿಸಿಕೊಳ್ಳೀನಿ.
ಸ್ವಲ್ಪ ನಿಲ್ಲಿ. ಈ ಎಸ್ಎಮ್ಎಸ್ ಸರಿಯಾಗಿದೆ ಎಂದು ನಿಮಗೆ ಹೇಗೆ ಗೊತ್ತು?
ಯಾವಾಗಲೂ ನೆನಪಿಡಿ:
• ಬೆಸ್ಕಾಮ್ ಇಲ್ಲವೇ ಯಾವುದೇ ವಿದ್ಯುತ್ ಪೂರೈಕೆ ಕಂಪನಿ ಬಿಲ್ ಕಟ್ಟುವಂತೆ ಒತ್ತಾಯಪಡಿಸಲು ಎಸ್ ಎಮ್ಎಸ್ ಕಳುಹಿಸುವುದಿಲ್ಲ.
• ಮೋಸಗಾರರ ಬಳಿ ಪೂರ್ತಿ ಬಿಲ್ ಮಾಹಿತಿ ಇರುವುದಿಲ್ಲ. ಆದರೂ ಯಾವುದೋ ಮೊತ್ತ ಹೇಳಿ ನಿಮ್ಮ ಬಿಲ್ ಬಗ್ಗೆಯೇ ಮಾತಾಡುತ್ತಿದ್ದಾರೆ ಎಂಬಂತೆ ನಾಟಕವಾಡುತ್ತಾರೆ.
• ಬಿಲ್ ವಿವರಗಳನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಇಲ್ಲವೇ ಬಾಕಿ ಇರುವ ಹಳೆಯ ಬಿಲ್‌ಗಳನ್ನು ಕಟ್ಟಲು ಬಿಲ್‌ನಲ್ಲಿರುವ ಇಲ್ಲವೇ ಅಧಿಕೃತ ವೆಬ್ ಸೈಟ್‌ನಲ್ಲಿರುವ ಸಂಪರ್ಕ ವಿವರಗಳನ್ನು ಬಳಸಿ ನಿಮ್ಮ ವಿದ್ಯುತ್ ಪೂರೈಕೆದಾರರನ್ನು ಸಂಪರ್ಕಿಸಿ.
@CySecKCoE


ಸೈಸೆಕ್
ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್
ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ
ಬ್ಯಾಟ ಮಾಲ್‌ವೇರ್ ಬಗ್ಗೆ ಎಚ್ಚರ
ಮೋಸದ ಲಿಂಕ್ ಕಳುಹಿಸಿ, ಅವನು *abc* ಆಪ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡುವಂತೆ ಮರುಳುಮಾಡುತ್ತೇನೆ. ಅವನ ಡಿವೈಸ್‌ನಲ್ಲಿ ಇನ್‌ಸ್ಟಾಲ್ ಆಗುವ ಮಾಲ್‌ವೇರ್‌ನಿಂದ ಅವನ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಕದಿಯುತ್ತೇನೆ.
ಈ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ
(ಫರ್‌ಹಾನ್ ಅವರಿಗೆ ಸಂದೇಶ ಬರುತ್ತದೆ)
ನಿಮ್ಮ ಕೈಯಲ್ಲಿ ಮೋಸದಿಂದ ಹೊರಗಿನ ಆಪ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿಸುವ ಬೇಡದ ಎಸ್ಎಮ್ಎಸ್, ಇಮೇಲ್ ಮತ್ತು ವಾಟ್ಸಾಪ್ ಲಿಂಕ್‌ಗಳ ಮೂಲಕ ಹರಡುವ ಬ್ಯಾಟ ಮಾಲ್‌ವೇರ್ ಬಗ್ಗೆ ಫರ್‌ಹಾನ್ ಈಗಾಗಲೇ ಓದಿದ್ದಾರೆ.
ಇಂತಹ ಲಿಂಕ್‌ಗಳನ್ನು ನಾನು ಕ್ಲಿಕ್ ಮಾಡಬಾರದು.ಇದರಲ್ಲಿ ಬ್ಯಾಟ ಮಾಲ್‌ವೇರ್ ಇರಬಹುದು.
ಫರ್‌ಹಾನ್ ತಮ್ಮ ಬದುಕಿಗೆ ತಾವೇ ರಕ್ಷಕರು, ನೀವೂ ಫರ್‌ಹಾನ್‌ರಂತಾಗಿ.
• ಹಲವಾರು ಗೂಗಲ್ ಪ್ಲೇ ಸ್ಟೋರ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಲ್ಲಿ ಬ್ಯಾಟ ಮಾಲ್‌ವೇರ್ ಕಂಡುಬರುತ್ತದೆ. ಬೀಗ ಹಾಕಿದ ಡಿವೈಸ್ ಅನ್ನು ತೆರೆಯಲು ಬಳಸುವ ಪಿನ್, ಪಾಸ್‌ವರ್ಡ್ ಇಲ್ಲವೇ ಪ್ಯಾಟರ್ನ್ ಕಲೆಹಾಕಬಲ್ಲ ಅಳವನ್ನು ಹೊಂದಿರುವ ಈ ಮಾಲ್‌ವೇರ್, ಡಿವೈಸ್‌ನ ತೆರೆಯನ್ನು ರೆಕಾರ್ಡ್ ಕೂಡ ಮಾಡಬಲ್ಲದು. ಈ ಮಾಹಿತಿ ಬಳಸಿದವರು ನಿಮಗೆ ಮೋಸ ಮಾಡಬಹುದು.
• ನೀವು ಎದುರುನೋಡದಿದ್ದ ಸಂದೇಶಗಳಿಂದ ಪಡೆದ ಲಿಂಕ್‌ಗಳ ಮೂಲಕ ಮೋಸಗೊಳಿಸುವ ಹೊರಗಿನ ಆಪ್‌ಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಬೇಡಿ.
• ಆಪ್‌ಗಳು ನಿಮ್ಮ ಮಾಹಿತಿ ಬಯಲುಮಾಡದಂತೆ ಮುನ್ನೆಚ್ಚರಿಕೆಯಾಗಿ ಅವುಗಳನ್ನು ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡುವ ಮುನ್ನ ಪರ್ಮಿಶನ್‌ಗಳನ್ನು ಓದಿ ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ನಿಮ್ಮ ಕಾಂಟ್ಯಾಕ್ಟ್, ಪಾಸ್‌ವರ್ಡ್, ಲೊಕೇಶನ್ ಹಾಗೂ ಇನ್ನೂ ಹಲವು ಮಾಹಿತಿಯನ್ನು ನೋಡಬೇಕೆಂದು ಆಪ್‌ಗಳು ನಿಮ್ಮ ಒಪ್ಪಿಗೆ ಕೇಳುತ್ತವೆ.
• ಯಾವುದೇ ಸುಳಿವಿಲ್ಲದೆ ನಿಮ್ಮ ಸ್ಮಾರ್ಟ್ ಫೋನಿನ ಎಲ್ಲಾ ಡೇಟಾವನ್ನು ಬ್ಯಾಟ ಅಳಿಸಿಹಾಕಿ, ನಿಮ್ಮ ಎಲ್ಲ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಬಹುದು.
@CySecKCoE


CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security
Beware of Electricity Bill Scams
Krishna receives an SMS that he had not paid the electricity bill for the previous month. And if he does not pay the bill by tonight, the electricity supply to his house will be cut. He was instructed to call the 'electricity officer' and talk. The number was attached with the SMS.
Let me call and clarify this as soon as possible.
I will manipulate him to pay the money online immediately.
SMS
ELECTRICITY BILL NOT PAID!!
CALL ELECTRICITY OFFICER NO: 980890.....
Hey, wait. How do you know that this SMS is legitimate?
Always remember:
• Bescom or any electricity supply company does not send text messages to insist on payment of bills.
• Scammers will not have all the billing information, but they will throw in a random but specific amount to make it look legitimate.
• The best option is to contact your electricity provider using the official contact details on the bill or the official website to confirm billing details or pay past-due electricity bills.
@CySecKCoE


CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security
Beware of BRATA Malware
Let me send a phishing link and provoke him to download the *abc* app; the malware installed on his device will help me access his personal information.
DOWNLOAD THIS APP NOW!
(Farhan gets a message)
Farhan has already read about BRATA malware being spread through unsolicited links via SMS, Email, and WhatsApp, that make you download third-party apps.
I should not click on such links; this could contain BRATA malware.
Farhan is the Rakshaka of his life, be like Farhan.
• The BRATA malware can be found in several Google Play Store applications. The malware combines full device control capabilities with the capacity to collect screen lock credentials (PIN, password, or pattern) and record the infected device's screen. The information can be utilised to conduct fraudulent transactions.
• Do not install shady third-party apps via links received from messages you were not expecting.
• Always verify the app's permissions before installing it to be sure they won't expose your information. Access to contacts, passwords, locations, and many more things are among this permission.
• BRATA may erase all the data on your smartphone and steal all of your personal information without leaving any traces.
@CySecKCoE

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.**

CYSECK UPDATES

- ಸೈಸೆಕ್ -ಸಿಸಾ ಸಹಯೋಗದೊಂದಿಗೆ ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ಜಾಗೃತಿಯನ್ನು ಹರಡಲು ಸಹಾಯ ಮಾಡುವ ವೀಡಿಯೊವನ್ನು ಬಿಡುಗಡೆ ಮಾಡಿದೆ.
- CySecK in collaboration with SISA released a video aiding in spreading cybersecurity awareness.

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.