Cyber Security Basics: Keeping Your Data Safe

(For Class- 9th and 10th

JAGDAMBA PRASAD DOBHAL

Key words: Data Global Village Stakeholders Hackers/Crackers IoTs
Media Ethic Encryption Alpha-Numeric Pattern OTT platform Log-Out
Two-Way Verification Mirroring/ Screen-Cast 3-2-1 Back-up Rule Access Control Third Party Links Digital Literacy
Cyber-Space Virus/ Anti-Virus Digital-Ethics IITBM
Cyber-Safe Zone 22-Digital arresting Digital Arresting ITAct 2000/2008

प्रोजेक्ट का शीर्षक: **Cyber Security Basics: Keeping Your Data Safe** (For Class 9th n 10th)

प्रोजेक्ट बैकग्राउंड**: -** आज के इस समय में हर एक व्यक्ति के पास मोबाइल फोन है और digital literacy के संदर्भ में हर उपयोगकर्ता लगभग निपुण है। उपयोगकर्ता अपना हर एक काम मोबाइल फोन से या लैपटॉप आदि से करता है। रोजमर्रा के काम में लेन-देन हो या घरों/कार्यालय से संबंधित किसी भी प्रकार के बिल जमा करने हों या आपस में पैसों का लेन-देन करना हो या बैंक से संबंधित कोई भी कार्य हो या फीस भरनी हो या ऑनलाइन शॉपिंग करनी हो या मेल भेजनी हो... हमारे सभी काम फोन की सहायता से बहुत ही आसानी से हो जाते हैं।
आजकल के तकनीकी आधारित समय में से पूरी दुनिया भर में हर एक व्यक्ति internet के माध्यम से जुड़ा हुआ है। आजकल चाहे वह खरीदारी की बात हो, चाहे धन के लेनदेन की बात हो या किसी भी प्रकार का संदेश देने की बात हो, हर काम को करने वाला user, internet का प्रयोग कर रहा है। यह स्थिति केवल भारत की ही नहीं बल्कि पूरी दुनिया भर की है। Internet के माध्यम से अपने हर प्रकार के काम को करने के पीछे समय की बचत करना है, अपनी

सुरक्षा करना है और एक दूसरे से संदेश भेज कर विभिन्न प्रकार की जानकारी का आदान-प्रदान करना है।

Internet के प्रयोग के बाद से समाज में कुछ ऐसी विकृतियों भी आई हैं जिनसे कि लोगों ने internet का दुरुपयोग करके दूसरे user/stakeholder को सामाजिक, आर्थिक, और मानसिक हानि पहुंचाना शुरू कर दिया है।

हाल ही में पूरी दुनिया भर के सरकारी संस्थाओं की websites को hackकर लिया गया था जिसके कारण बहुत सारे institutions अभी भी परेशानियां झेल रहे हैं।

Times of India
Digital arrest': How a call drop ended ...

इसका प्रमुख कारण यह भी है कि कोई भी user, और केवल एक single user ही नहीं बल्कि बड़ी-बड़ी कंपनियों और संस्थान भी Crackers का शिकार हो जाती हैं।

दरअसल इन घटनाओं के पीछे दूसरा व्यक्ति उतना जिम्मेदार नहीं होता है जितना कि हम लोग स्वयं होते हैं। हम लोग झूठे लालच में आकर अनावश्यक link को खोल देते हैं, दूसरे के संदेशों पर विश्वास करके उन पर अपना reaction देते हैं, Fack mail पर विश्वास कर लेते हैं फेक आईडी पर विश्वास कर लेते हैं अपना password share कर लेते हैं दूसरे का internet प्रयोग कर लेते हैं और इसी प्रकार की अन्य बहुत सारी कमियां होती हैं जो कि हमें internet पर गलत गतिविधियों का शिकार बना देतीहैं। Cyber bullying भी एक प्रकार का अपराध है जो की विभिन्न प्रारूपण में सामने आकर समाज में विकृति पैदा कर रहा है।

Internet के बहुत सारे खतरों में आजकल password मांगना fake OTP भेजना, screen share करना, अपना फोटो भेजना अपनी आवाज भेजना आदि बहुत सारे खतरों कहो ना एक सामान्य सी बात हो गई है। Digital arresting और AI के माध्यम से झूठी calls और चित्र बनाकर बहुत बड़ी धनराशि की मांग करना भी एक नई समस्या पैदा हो रही है।

अतः आजकल के इस समय में हम लोगों को इस बात की जानकारी होना बहुत ही जरूरी है कि हम किस प्रकार से अपने आप को cyber security से updated रखें और अपने data को safe रखें।

यह पूरा प्रोजेक्ट किसी भी user/stakeholder को cyber security पर आधारित सामान्य सी जानकारी देने से संबंधित है और अपने data को सुरक्षित रखने से संबंधित है।

समस्या: -

आजकल विभिन्न Cyber/Digital अपराधों की सूचना हमें उन्हीं OTT Platforms के माध्यम से मिलती है जिनका हम रोज प्रयोग करते हैं। समस्या उतनी बड़ी OTT platforms में नहीं है और न ही समस्या हमारे इस फोन में है, सबसे बड़ी समस्या यह है कि हम लोगों को Digital Literacy और Cyber-Security Basics की सामान्य सी समझ तक नहीं है। समस्या यह है कि हम अपने बैंक account/accounts में PIN, set करने को या फोन पर Password/Passwords डालने को ही को Digital Literacy और Cyber-Security को प्रथम और अंतिम उपाय समझ बैठे हैं। आज की इस समय में जबकि हमारे सभी प्रकार की सूचनाओं और महत्वपूर्ण आंकड़े हमारे इस फोन में संग्रहित रहते हैं तो ऐसे समय में हम लोगों को Digital Literacy को कानूनी रूप से भी समझना बहुत आवश्यक है। लेकिन समस्या यह भी है कि किसी भी बात के बीच में कानूनी रूप क्यों आ जाता है और इसका सबसे महत्वपूर्ण कारण यह है कि हमें digital ethics की समझ नहीं है।

सरल शब्दों में आजकल आजकल के digital युग में internet का प्रयोग करते समय Cyber Security और Digital literacy से संबंधित आधारभूत समझ न होने के कारण से हमारे फोन पर निम्नलिखित समस्याएं पैदा हो रही हैं।

Password चोरी करना या दूसरे को बताना या आसान Password/Passwords बनाना

- झूठी मेल का आना ।
- हमारी निजी डेटा को दूसरे व्यक्ति द्वारा हैक करना।
- वित्त संबंधी झूठ लुभाने प्रचार आना।
- फेक आईडी बन जाना।
- हमारे डॉक्यूमेंट में एडिट करके गलत जानकारी भरना।
- हमारी फोटो आदि से छेड़छाड़ करके गलत तरीके से प्रयोग करना।
- धन की मांग संबंधी झूठ संदेश आना।
- शिक्षा के क्षेत्र में TPACKS के आधार पर सूचना का सही न होना फिर भी हमको प्राप्त होती है।
- हमारे फोन पर या लैपटॉप या कंप्यूटर पर अनाधिकृत रूप से log in करना।
- हमारे Device का उपयोग अपने काम के लिए करना लेकिन इसी दौरान चोरी से डाटा चोरी कर लेना ।

लेकिन इन सब काम के पीछे की जो सबसे बड़ी समस्या है वह यह है कि हमें digital ethics और digital literacy की सामान्य समझ भी नहीं है।


India lags in cyber security

प्रोजेक्ट के उद्देश्य

इस प्रोजेक्ट के उद्देश्य निम्नलिखित हैं ।

1. **Cyber Security Basics: Keeping Your Data Safe** की आधारभूत समझ स्थापित करना और उसके बारे में जागरूक करना।
2. Users को Digital Ethics/Literacy/Basic Security-tools/methods/process /applications /software की जानकारी देना और इससे अवगत कराना।

3. Mails पर और विभिन्न O.T.T. PLATFORMS पर TWO WAY VERIFICATION के बारे में जागरूक करके उसका उपयोग करना सीखना।
4. Safe websites और unsafe websites की जानकारी देकर, उपयोग करवाना।
5. किसी भी websites को सर्च करते समय Enhanced Protection, Standard Protection और No Protection आदि Features की जानकारी देना।
6. अपने किसी भी account/accounts के लिए Strong Password 🔑 बनाने की जानकारी देना।
7. IT ethics की जानकारी देकर एक जिम्मेदार Netizen बनाने में सहायता करना।
8. किसी भी O.T.T. Platforms पर उपलब्ध शैक्षणिक सामग्री को 5 scaled Rubric पैमाने पर परख करके शिक्षण प्रक्रिया में लागू करना।
9. किसी भी O.T.T. platforms पर उपलब्ध शैक्षणिक सामग्री को TPACK approach पर परीक्षण करके लागू करना।
10. SAMR approach का उपयोग करके पूरे शिक्षण कार्य को redefining के स्तर तक ले जाना। धन संबंधी किसी भी प्रकार के लेनदेन में जागरूकता बरतने के लिए समझ उत्पन्न करना।
11. Creative common licence, IPR और plagiarism की सामान्य जानकारी देना।

Project/Model का विवरण का विवरण: इस प्रोटोटाइप/मॉडल में कोई भी concrete/tangible मॉडल नहीं है। विद्यार्थियों को और किसी भीstakeholder को cyber security के विभिन्न पहलुओं को समझने के लिए निम्नलिखित उपायों की जानकारी दी जाती है।

Cyber Security को अपनाकर, सुरक्षित रहने के लिए निम्नलिखित प्रमुख उपाय हैं:

- मजबूत **Password/Passwords**: हमें अपना Password/Passwords मजबूत बनाना चाहिए और प्रयास करना चाहिए कि वह कुछ अलग प्रकार का हो।
- हमें प्रयास करना चाहिए कि हम अपना Password/Passwords समय-समय पर बदलते रहे और अलग-अलग account/accounts के लिए अलग-अलग Password/Passwords रखें। Password/Passwords किसी के साथ साझा करने से बचना चाहिए।
- **Fire-wall n Antivirus**: Fireball and anti-virus हमेशा विश्वसनीय कंपनी का ही लें और उसे नियमित रूप से अपडेट करते रहें।
- **Safe websites**: हमेशा सुरक्षित websites का प्रयोग करना
    - HTTPS: सुरक्षित websites का URL HTTPS से शुरू होता है, न कि HTTP से। यह दर्शाता है कि websites का डेटा एनक्रिप्टेड है।
    - Lock Icon: सुरक्षित websites के एड्रेस बार में एक लॉक आइकन दिखाई देता है, जो दर्शाता है कि websites सुरक्षित है।
    - Vakid Certificate: सुरक्षित websites के पास एक वैध SSL सर्टिफिकेट होता है, जो websites की पहचान और सुरक्षा को प्रमाणित करता है।

- **Data Backup**: हमें अपने प्रत्येक प्रकार के डाटा को, कम से कम तीन स्थानों और प्रकारों (3-2-1 backup rule) से सुरक्षित रखना चाहिए।
- सोशल मीडिया सुरक्षा: किसी भी प्रकार के लालच के संदर्भ में दिए गए link और third-party द्वारा उपलब्ध कराए गए linkको कभी भी नहीं खोलना चाहिए। साथ ही से **Fishing n Spams** बचने के लिए संदेह से बचने के लिए Link को नहीं खोलना चाहिए।
- **Regular Update of Software**: हमें अपना प्रत्येक Device और software को समय-समय पर अपडेट करते रहना चाहिए।
- **Judicious use of Public Wi-fi**: पब्लिक वाई-फाई नेटवर्क का उपयोग करते समय सावधानी बरतें और महत्वपूर्ण जानकारी को साझा करने से बचना चाहिए।
- **Physical Safety of devices:** अपने device को लॉक करें और उन्हें सुरक्षित स्थान पर रहना चाहिए।
- **Cyber** जागरूकता: cyber सुरक्षा के बारे में जागरूक रहकर किसी भी प्रकार की धमकी से डरने के बजाय helpline no1930 पर कॉल करके समस्या के बारे में बताना चाहिए।
- **Virus** स्कैन: अपने device को नियमित रूप से virus करते रहना चाहिए।
- **Safe Mails**: सुरक्षित e mails सेवाओं का उपयोग करें और अनजान ईमेल्स को खोलने से बचना चाहिए।
- **Safe Passwords**: Password/Passwords मैनेजर का उपयोग करें और अपने Password/Passwords को सुरक्षित रखें।
- 2- way verification/Authentication: 2- way verification/Authentication का उपयोग करके हम अपने account/accounts को अतिरिक्त सुरक्षा पर प्रदान करते हैं।
- इन उपायों का पालन करके, आप अपने digital life को सुरक्षित रख सकते हैं और cyber हमलों से बच सकते हैं।

Digital Security, Digital Safety और **Cyber Security** से संबंधित सावधानियां

- काम होने के पश्चात active platform से logout हो जाएं।

YouTube
Logout from Truecaller? Sign Out From ...

Control Alt Achieve
Google Account with 2-Step Verification

- अपने प्रत्येक प्रकार की account/accounts की access गोपनीय रखनी चाहिए और यदि आवश्यक हो तो बहुत ही विश्वसनीय लोगों के साथ साझा करनी चाहिए।
- फोन पर unknown number को block करना।

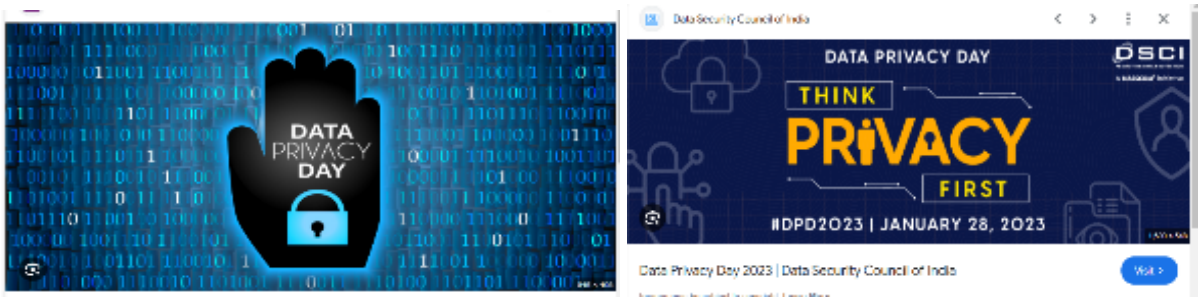
- Cybercrime/fraud आदि मामलों के पता होते ही 1903 या 100 या cyber–Crime Reporting Portal's helpline number, +91-96801 00687 आदि नंबर पर तत्काल रूप से कॉल करनी चाहिए।

Digital Ethics की सामान्य जानकारी।

Digital ethics, digital techniques के उपयोग करने से संबंधित वह नैतिक सामाजिक और व्यावहारिक मूल्य हैं जो हमारे व्यवहार को दर्शाते हैं, साथ ही यह भी दर्शाते हैं कि हम समझ में किसी भी दूसरे व्यक्ति के साथ उसको बुरा लगने वाला व्यवहार तो नहीं कर रहे हैं। Digital/Cyber Ethics के संदर्भ में हमें निम्नलिखित बिंदुओं का ध्यान रखना चाहिए।

- दूसरे की privacy का सम्मान करें। बिना दूसरे की आज्ञा के उनकी फोटो आदि ना लें।
- Plagiarism का उल्लंघन करने वाले किसी भी प्रकार का कार्य न करें।

- Creative commons नियमों का पालन करना चाहिए।
- Cyber bullying नहीं करनी चाहिए।
- किसी दूसरे व्यक्ति के ना तो device पर छेड़ना चाहिए और ना ही password को चोरी करने का प्रयास करना चाहिए।
- हमें किसी भी समाचार की विश्वसनीयता को बिना परखे हुए आगे साझा नहीं करना चाहिए।
- Clickbait news पर विश्वास नहीं करना चाहिए और ना ही उसको किसी दूसरे लोगों के साथ या समूहों के साथ साझा करना चाहिए।
- Clickbait news पर विश्वास नहीं करना चाहिए और ना ही उसको किसी दूसरे लोगों के साथ या समूहों के साथ साझा करना चाहिए।



Cyber Security and Digital Security की उचित समझ न होने से हमारे दैनिक जीवन में प्रभावित होने वाले क्षेत्र

1. धन के लेनदेन से संबंधित क्षेत्र।
2. निजी जानकारी से संबंधित विभिन्न प्रकार के सरकारी दस्तावेज।
3. अपनी निजी फोटो या कोई निजी जानकारी।
4. किसी भी सरकारी आंकड़े से संबंधित जानकारी।
5. विभिन्न प्रकार की ऑडियो रिकॉर्डिंग।
6. विभिन्न प्रकार की वीडियो रिकॉर्डिंग।

YouTube
Logout from Truecaller? Sign Out From ...

Control Alt Achieve
Google Account with 2-Step Verification

AI integration with Cyber Security Basics: Keeping our Data Safe एक सामान्य से user के लिए जो कि android phone से अपने दैनिक जीवन के काम को आसान बनाना चाहता हो, AI की समझ रखने बड़ा मुश्किल हो जाता है। या फिर सामान्य सी परिस्थितियों में भी किसी भी User को Coding आदि सीखने को कहा जाता है जो विभिन्न संसाधनों के अभाव में और अन्य कारणों से बड़ा मुश्किल होता है । एक विद्यार्थी के लिए ही नहीं, वरन एक आम आदमी के लिए जिसके पास कोई सामान्य सा Android Phone है, WhatsApp पर Meta AI के feature का प्रयोग करके दैनिक जीवन की बहुत सारी समस्याओं के संबंध में सूचना प्राप्त करके उसका समाधान कर सकता है। एक शिक्षार्थी के लिए तो यह सूचना बहुत ही जरूरी है और Meta AI के प्रयोग से वह अपनी दैनिक जीवन में AI का Integration बहुत आसानी से कर सकता है।

प्रभाव एवं उपयोगिता: इस प्रोजेक्ट के माध्यम से प्रयास किया गया है कि हर एक Digital Device User, उसके द्वारा प्रयोग किए जाने वाले Digital Devices, IoTs, hardware, software के अपने दैनिक जीवन में प्रयोग करते समय **Cyber Security Basics: Keeping Data Safe** विषय के विभिन्न बिंदुओं और संदर्भों में जागरूक हो जाए। साथ ही वह इन hardware/software के संबंध में Ethics की पूरी समझी विकसित करके अपने आप तो सुरक्षित (Cyber Security) बन ही सके साथ ही एक पूरे समाज में एक आदर्श Netizens का समूह स्थापित कर सके।

सारांश: इस प्रोजेक्ट में दी गई जानकारी और समझ के आधार पर कोई भी User या stakeholder, digital literacy और Cyber Security Basics के बारे में जानकारी रख करके न केवल स्वयं को विभिन्न प्रकार के digital अपराधों से बचा सकता है बल्कि पूरे समाज को भी इस प्रकार से होने वाले खतरों से भी बचा सकता है।

भविष्य की रूपरेखा: मेरा प्रस्ताव है कि विद्यालयों में सामान्य विषयों की तरह digital literacy और cyber security जैसे महत्वपूर्ण विषय को पाठ्यक्रम का अनिवार्य भाग बना दिया जाना चाहिए साथ ही इसमें IT Act 2000/2008 को भी जोड़ा जाना चाहिए। आप में से जो लोग digital literacy और Cyber Security Basics के संदर्भ में IIT-Banglore के माध्यम से Cyber security basics पर 6 महीने का एक कोर्स करना चाहते हैं तो उनके लिए यह सूचना भी जरूरी है।

Credits n links of information/images—TOI, Dainak Jagran JOSH, YOU TUBE, F.B., Various OTT sources, paper cuttings of various News Papers. https://images.app.goo.gl/TE5hwGR1CEG3XXHo6, https://images.app.goo.gl/WKH7aVM2witvzLTHA, https://images.app.goo.gl/kNPwaLue87i1hQ9K7 https://images.app.goo.gl/VrEEosbH3cRZM5tE9 https://images.app.goo.gl/didQtm1wmzJAaCX36, https://images.app.goo.gl/K6bTKVHpCDAkkmCM8 https://images.app.goo.gl/MLxszHwLH2bB5srv8 https://images.app.goo.gl/ky1JVsvRR6Vksp1W7 …

Thanks