Cyber Safety

सीबीएसई पाठ्यक्रम पर आधारित

कक्षा -11

द्वारा:
संजीव भदौरिया
स्नातकोत्तर शिक्षक (संगणक विज्ञान)
के० वि० बाराबंकी (लखनऊ संभाग)

परिचय

- आधुनिक जीवन हम बिना internet के सपने में भी नहीं सोच सकते हैं| जहाँ एक ओर internet ने हमें ढेर सारी सुविधाएँ मुहैया कराई हैं और बहुत से काम अत्यंत आसान बना दिए हैं |
- वहीं दूसरी ओर यदि इसको सही से इस्तेमाल न किया जाये तो सुरक्षा के लिए खतरे भी बहुत हैं |
- अतः हमारे लिए यह जानना बहुत ज़रूरी है कि internet पर क्या क्या खतरे हो सकते हैं? Internet पर काम करने के क्या क्या चुनौतियाँ और जोखिम हो सकते हैं ?
- इस अध्याय में हम इन्हीं सब के बारे में विस्तार से अध्ययन करेंगे |

Cyber Safety क्या है?

- Internet को सुरक्षित और ज़िम्मेदारी के साथ प्रयोग करना Cyber Safety कहलाता है ताकि व्यक्तिगत जानकारी(personal information) सुरक्षित रहे और किसी दूसरे की information के लिए खतरे का कारण न बने |

Web को सुरक्षित तरीके से browse करना

- आजकल web पर कार्य अत्यंत ज़रूरी हो गया है इसलिए ये जानना भी ज़रूरी है कि कितने प्रकार के खतरों का सामना करना पड़ सकता है | इसके लिए निम्न बातों का ध्यान रखना आवश्यक है -
  - क्या क्या संभावित खतरे(Possible Dangers) हैं?
  - इनको कैसे नज़रंदाज़ किया जाए ?
  - वेब ब्राउज़ करते समय आप को कैसा व्यवहार करना है?

- साथ ही ये भी ध्यान रखना है कि –
  - हर साईट सुरक्षित नहीं होती|
  - जो भी आप ऑनलाइन करते हैं वह दूसरे के द्वारा देखी जा सकती है|
  - ऑनलाइन जो भी आप देखते हैं या दिखाया जाता है, ज़रूरी नहीं की वह सही हो |
  - ऑनलाइन जाने से पहले अपने कंप्यूटर को सुरक्षित करना अत्यंत आवश्यक है |

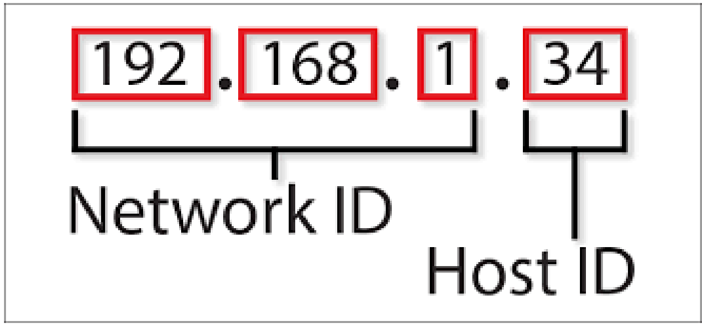
Internet प्रयोग करते समय Identity Protection

- Identity Theft एक प्रकार का छल (fraud) है जिसमे किसी दूसरे व्यक्ति की व्यक्तिगत जानकारी प्रयोग करके पैसे चुराना या कोई अन्य अनैतिक काम करना है |
- ऑनलाइन identity theft किसी की personal information चुराना है जैसे - नाम, login details इत्यादि | और इस जानकारी को ऑनलाइन प्रयोग करके कोई गलत काम करना है |
- इसका सबसे सामान्य हल है कि internet पर browsing प्राइवेट की जाये या बिना नाम (Anonymous) की जाए|
- इसके पहले हम ये देखते हैं की जब हम internet पर browse कर रहे होते हैं तब क्या क्या होता है ?

Website आपको कई तरह से track करती है |

- जब भी आप किसी website को visit करते हैं आपका browser आपके device के IP address के द्वारा आपके स्थान को प्रकट कर सकता है|
- यह आपके search और browsing history को भी प्रदान कर सकता है जिसे किसी अन्य के द्वारा प्रयोग में लाया जा सकता है जैसे किसी विज्ञापन डाटा या मुजरिम के द्वारा|
- इस प्रकार website आपको track कर लेती हैं | tracking सामान्यतया advertising network के द्वारा किया जाता है ताकि आपका एक प्रोफाइल बनाया जा सके और सटीक ad-target बनाया जा सके|
- Tracking की जानकारी आपके website के प्रयोगों के pattern के अधर पर बनाया जाता है | website track करने के लिए जिन चीजों का इस्तेमाल करती हैं वे निम्न हैं –

(a) IP Address: जब आप internet प्रयोग कर रहे होते हैं तब यह आपके device का एक प्रकार का unique address होता है इसके द्वारा website आपके भौगोलिक स्थिति(geographical location) का लगभग पता लगा सकती है |



(b) Cookies और Tracking Scripts: Cookies आपके कंप्यूटर पर छोटी Text Files होती हैं जो आपकी ऑनलाइन आदतों से संबंधित जानकारी को store करती हैं | ये दो प्रकार की हो सकती हैं –

1. ***First Party Cookies:*** ये वो cookies होती हैं जो आपके login id, password, auto fill की जानकारी रखती हैं |
2. ***Third Party Cookies:*** ये आपकी search history, और web browsing history की जानकारी store करती हैं ताकि आपके interest की अनुसार ad दिखा सकें |

(c) HTTP Referrer : जब आप किसी link पर क्लिक करते हैं तो आपका web browser उस लिंक से जुड़े web page को load करता है और website को आपका पता बताता है इसे ही HTTP referrer कहते हैं |

(b) Super Cookies : ये भी एक प्रकार कीCookies ही होती हैं लेकिन ये जिद्दी और स्थायी होती हैं | ये delete किये जाने के बाद भी वापस आजाती हैं | ये कई जगहों पर अपना डाटा store करती हैं जैसे Flash Cookies, Silverlight Storage, Browsing History और HTML5 local storage इत्यादि|

(c) User Agent : आप जितनी बार website से connect होते हैं उतनी बार ब्राउज़र एक user agent भेजता है |जो website को यह बताता है कि आपके ब्राउज़र और operating system को ad की लिए और डाटा चाहिए |

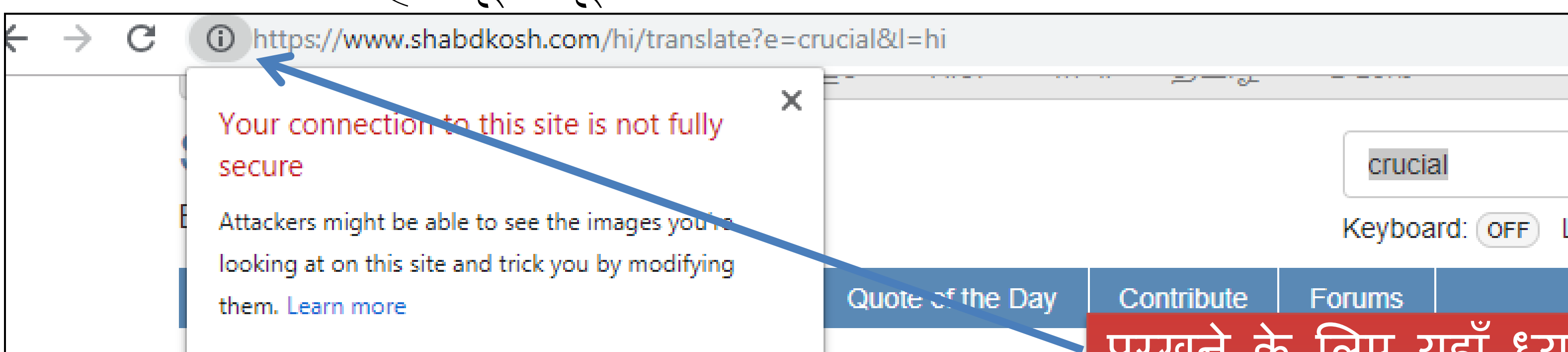
उपरोक्त सभी चीजें आपके personal डाटा को leak कर सकती हैं जिसे आपके खिलाफ प्रयोग में लाया जा सकता है | इसका हल भी वही - Private Browsing और Anonymous Browsing

Private Browsing और Anonymous Browsing

- Anonymous browsers किसी भी user को बिना personal information को शेयर किये website देखने का अवसर प्रदान करते हैं |
- इसको सरकारी, गैर-सरकारी या सुरक्षा चाहने वाले लोग इसका प्रयोग कर सकते हैं|
- इसके अलावा और भी कई रास्ते हैं जिनसे personal information शेयर नहीं होती है जैसे- Private Browsing
- **Incognito browsing** किसी ब्राउज़र का वह version होता है जो personal information खुलने नहीं देता है और आपकी activity को track नहीं करता है| ऐसा बैंक वगैरह के details आदि भरते समय लाभदायक होता है|
- **Proxy** किसी website और computer के मध्य एक बिचौलिए का कम करता है | ऐसे में website के पास जो सूचना जाती है वह उस proxy साईट की होती है|
- **Virtual Private Network (VPN)** किसी प्राइवेट या पब्लिक network में काम करने में सहायक होता है |जैसे – Wi-Fi, Hotspot इत्यादि | सिअक प्रयोग offices में आपस में डाटा शेयर करने के लिए प्रयोग में लाया जाता था | इससे sensitive information को बचाया जा सकता है |

सूचना की गोपनीयता(Confidentiality of Information)

- इसका मतलब यह है की प्राधिकृत (Authorised) व्यक्ति द्वारा sensitive और protected डाटा का access |
- ऐसा करने के लिए निम्न सावधानियां बरतनी चाहिए -
  1. जब भी संभव हो firewall का प्रयोग करें |
  2. Tracking को ब्लाक करने के लिए setting को नियंत्रित करें |
  3. जब भी संभव हो private browsing ही करें |
  4. जब भी internet पर कुछ पोस्ट करें सावधानी बरतें |
  5. जब भी अत्यंत महत्वपूर्ण सूचना website पर डालें तो safe site को परख लें |



परखने के लिए यहाँ ध्यान दें| यदि साईट सुरक्षित है तो आपको सूचना मिल जाएगी |

सूचना को गोपनीयता(Confidentiality of Information)

6. E-mails को सावधानी पूर्वक खोलें तथा भ्रामक संदेशों को नज़रंदाज़ करें | लुभावने विषय वाले mail को कतई न खोलें|
7. Wireless network पर sensitive इनफार्मेशन कतई न शेयर करें |
8. Public computers का प्रयोग करने से बचें जैसे साइबर कैफ़े के computers इत्यादि |
9. जब भी public प्लेस पर कंप्यूटर प्रयोग करें तो ब्राउज़र की history और cookies को मिटाना न भूलें |
10. बैंक आदि के user name और password डालते समय virtual keyboard का प्रयोग करें |
11. अपनी information को सेव बिल्कुल न करें |
12. जब भी sensitive information स्क्रीन पर हो तो computer के सामने से कभी न हटें |
13. Password सेव करने वाले feature को disable कर दें |

CYBERCRIME

- Internet, कंप्यूटर, information system, electronic communication या किसी अन्य electronic device का प्रयोग करते हुए किसी अपराध को अंजाम दिया जाता है या उसमे सहभागिता की जाती है तो यह एक cybercrime है |
- कुछ सामान्य cybercrime निम्न हैं -
    1. Cyber Trolls and Bullying:
    2. Cyber Bullying
    3. Cyber Stalking (ऑनलाइन Harassment)
    4. Spreading Rumours Online (ऑनलाइन अफवाह फैलाना)
    5. Unethical hacking
    6. Stealing information etc.
- ***Reporting Cybercrime :*** cybercrime की रिपोर्ट सबसे पहले parents को, फिर school मैनेजमेंट को तथा फिर पुलिस में करनी चाहिए |
- Cybercrime की रिपोर्ट करना ठीक वैसा ही है जैसे किसी अन्य अपराध के लिए रिपोर्ट करना |
- रिपोर्ट के लिए लोकल पुलिस थाने में की जा सकती है
- कुछ राज्यों में E-FIR की सुविधा भी है |
- गृह मंत्रालय भी सी तरह के कार्यों के लिए एक website लांच करने वाला है |

COMMON **SOCIAL NETWORKING** SITES

- एक social networking site वह web application है जिसमे लोग अपनी public profile बनाकर online लोगों (ऐसे लोग जिन्होंने खुद भी उसी प्लेटफार्म पर profile बनाया हो) से जुड़ सकते हैं और communicate कर सकते हैं | ऐसे जुड़े हुए लोगों को ऑनलाइन friends कहा जाता है |
- कुछ प्रचलित social networking site निम्न हैं –
- ***Facebook***: यहाँ अपने विचार, photos, वीडियो शेयर किये जासकते है और दूसरों की पोस्ट पर प्रतिक्रिया भी दी जा सकती है |
- ***Twitter***: यह एक प्रकार की microblogging है जहाँ बहुत ही छोटे सन्देश पोस्ट किये जा सकते हैं और देखे जा सकते हैं | पहले इसमें text की लम्बाई 140 characters की थी जिसे बढाकर अब 280 कर दिया गया है |
- ***LinkedIn***: यह professionals की social साईट है | जहां लोग अपने resume इत्यादि शेयर करते हैं |
- ***Instagram***: यह ऑनलाइन फोटो शेयर करने की सबसे प्रचलित साईट है |

SOCIAL NETWORKING SITES का सही से प्रयोग

- एक social networking आजकल हर जगह है जहाँ लोग personal से लेकर professional प्रोफाइल तक बना कर रखते हैं| जिसमे anonymous रह पाना बेदह कठिन हो गया है |
- हम social media से प्रत्यक्ष या अप्रत्यक्ष रूप से प्रभावित होते ही रहते हैं|
- आप ऑनलाइन जो भी करते हैं उसका एक स्थाई foot print रह जाता है और वह सालों तक सेव रहता है जिसे digital foot print भी कहते हैं |
- एक बार जो पोस्ट कर दिया उसके बाद वह पोस्ट public डोमेन में आजाती है और फिर ये सबको दिख सकती है |
- अतः पोस्ट करने से पहले अत्यंत सावधानी बरतनी चाहिए | ताकि बाद में इसका खामियाजा न भुगतना पड़े |
- Social media पर कम करते समय कुछ सावधानियां और नियमों का पालन करना चाहिए ताकि आगे आने वाली असुविधाओं से बचा जा सके |
- Social media में privacy सेटिंग ज़रूर करनी चाहिए ताकि बिना आपके जान पहचान वाला user आपकी प्रोफाइल न देख सके |

SOCIAL NETWORKING SITES पर क्या करना चाहिए?

- Social media पर आपको ज़िम्मेदारी के साथ काम करना चाहिए ताकि आप social media का सही मायने में आनंद और लाभ ले सकें |
- जिसके लिए social media के कुछ rules आपको अपनाने चाहिए -
- अपनी identity के प्रति इमानदार रहें और authentic रहें |
- Disclaimer का प्रयोग करें|
- Online झगडे न करें |
- फर्जी व गलत नामों का प्रयोग न करें |
- अपनी पहचान सुरक्षित करें |
- जब भी कुछ पोस्ट करें तो publicity टेस्ट अवश्य करें |
- अपने audience का सम्मान करें |
- दूसरे की भावनाओं का सम्मान करें |
- Comments को मॉनिटर करते रहें |

धन्यवाद

और अधिक पाठ्य-सामग्री हेतु निम्न लिंक पर क्लिक करें -

www.pythontrends.wordpress.com