Rashtra Sant Tukdoji Maharaj Nagpur University,Nagpur
Public Administration and Local self Government Department

Pre - PhD course work

Date 28/08/2023

Subject : Cyber security

Prof. Dr.Urmila Govind Reddy

Department of public Administration

Dayanand arts college Latur

Email ID ready.urmila 421@gmail.com

Mo.no. 8766816956

शासकीय कार्यालयामध्ये संगणकीकरणाची सुरुवात,
एन आय सी ची स्थापना
संगणकीय धोरण
मोबाईल व इंटरनेट सेवेची सुरुवात
माहिती तंत्रज्ञान कायदा २०००
राष्ट्रीय ई प्रशासन योजना
आधार कार्ड योजना
E- commerce
डीबीटी योजना
jio
डिजिटल इंडिया प्रकल्प
रोकड रहित अर्थव्यवस्था
Covid-19 पिरेड
फाईव्ह जी सेवा

ग्रामगीतेमध्ये तेराव्या अध्यायातील 103 आणि 104 ओव्यात राष्ट्रसंत तुकडोजी महाराजांनी म्हटले आहे की
"सुंदर असावी वाचनालय, नाना ग्रंथ ज्ञानमय
करावयास सुबुद्धीचा उदय गावलोकी
काय चालले जगा माजी कळावे गावी सहजासहजी
म्हणून विविध साधने असावी"
EG.I.T

सध्याचे जग हे डिजिटल आहे ते वेगाने बदलत आहे याबद्दल त्या जगाचा वेग आपल्याला पकडल्याशिवाय आज पर्याय नाही कारण नीट शिवाय आपला दिवस मावळतच नाही अन्न वस्त्र निवारा आणि मोबाईल या आपल्या गरजा बनलेल्या आहेत या सायबर युगामध्ये जगत असताना सायबर गुन्हेही तेवढा मोठ्या प्रमाणात वाढत आहेत या गुणांना आळा घ** तेवढेच महत्त्वाची आहे यासाठी सायबर सुरक्षितता व सायबर सुरक्षितता प्रबोधन करणे काळाची गरज आहे

सायबर स्पेस एखाद्याच्या सीमेपूर्ती मर्यादित नाही तर ती संपूर्ण जग वाप्ते डिजिटल तंत्रज्ञानाचा होत असलेल्या उत्क्रांतीमुळे सायबर गुन्ह्याची गतिशील स्वरूप सर्वात मोठे आव्हान आहे या आव्हानांना कमी करणे काळाची गरज आहे

सायबर अटॅक म्हणजे नक्की काय?

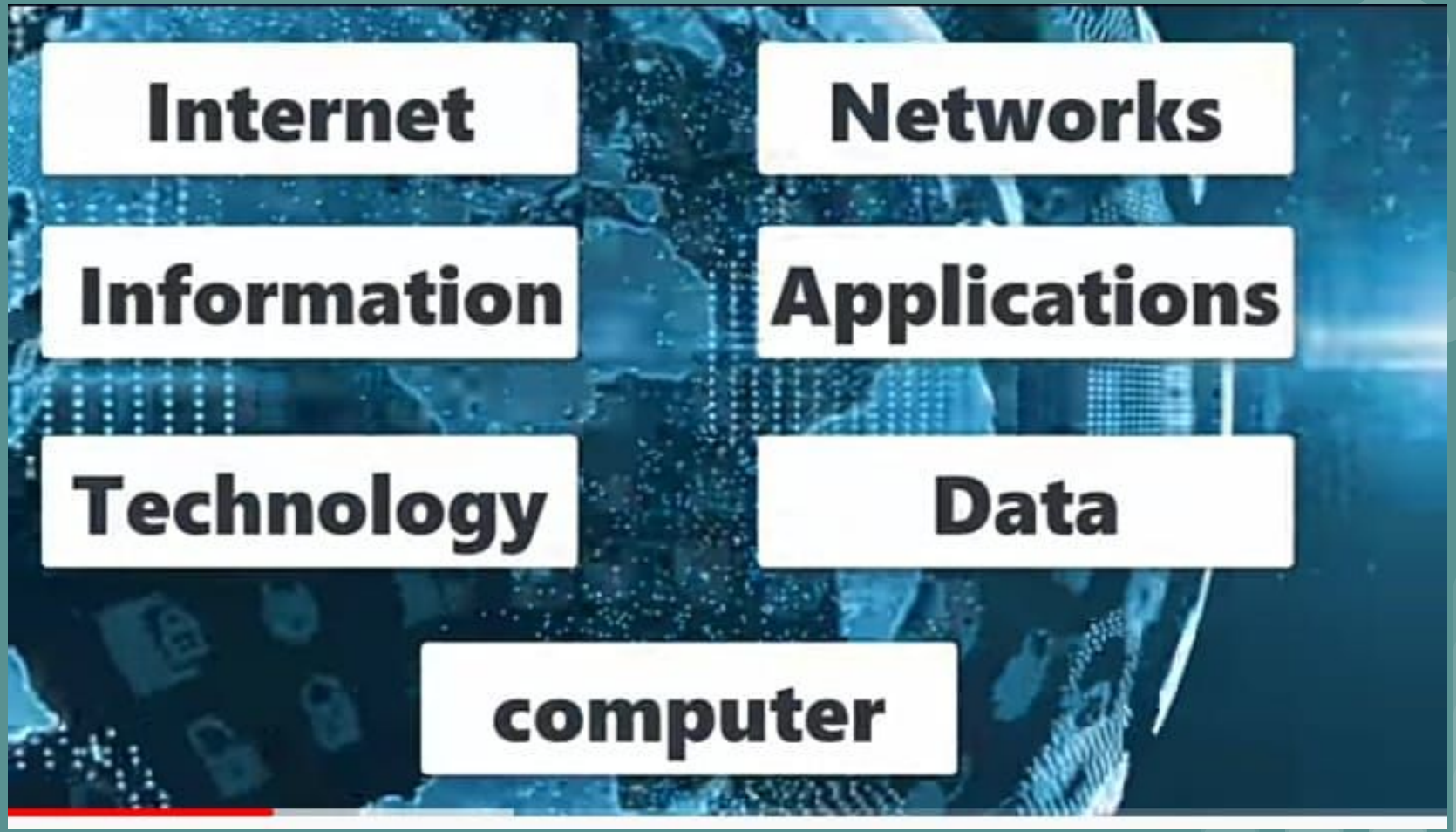
सोप्या भाषेत सायबर अटॅक म्हणजे काय हे सांगायचं झालं तर हा एक असा हल्ला आहे, जो इंटरनेटवर आणि इंटरनेटशी संबंधित गोष्टींवर केला जातो आणि जर कोणी या हल्ल्याच्या विळख्यात आला तर वापरकर्त्याचा मोबाईल किंवा कॉम्प्युटर हॅक होणे, वैयक्तिक डेटाची चोरी होणे, वापरकर्त्याची ऑनलाइन फसवणूक होणे अशा गोष्टी घडतात.

अमेरिकन सरकारची सुरक्षा सल्लागार रिचर्ड एकलारक

एका देशाच्या v व राज्याच्या
 कृती इतर देशाच्या संगणक व नेटवर्कमध्ये अनधिकृतपणे प्रवेश करून संगणक कार्यक्रमाची मोडतोड करतात याला सायबर गुन्हा असे म्हणतात
नशनल रिसर्च कौन्सिल
सायबर गुन्ह्याविषयी असे मत व्यक्त केले की सुधारित मॉडर्न चोर संगणकाच्या साह्याने इतकी मोठी हानी पोहोचू शकतात जी आणि अटल गुन्हेगार बंदुकीच्या दाखविणे देखील करू शकत नाही दहशतवादी वंपेक्षा भयानक प्रकार बसल्या ठिकाणी इलेक्ट्रॉनिक साधनांच्या आधारे केला जातो.


HACK
THIEF
SPY
FRAUD
INFORMATION
HACKING
SAFETY
SECURE
LAPTOP
ATTACK
CRIMINAL
COMPUTER
SYSTEM
BUSINESS
BINARY
PRIVACY
ONLINE
DATA
CYBER
WEB
TECHNOLOGY
CRIME
STEALING
PROTECTION
NETWORK
SECURITY
HACKER
INTERNET
THEFT
PHISHING
DIGITAL
DANGER
CODE
STEAL
COMMUNICATION
PC
MAN
IDENTITY
VIRUS
PASSWORD

सायबर क्राईमची व्याख्या असा गुन्हा म्हणून केली जाते जिथे संगणक हा गुन्ह्याचा उद्देश असतो किंवा गुन्हा करण्यासाठी एक साधन म्हणून वापरला जातो. भारताच्या राज्यघटनेच्या सातव्या अनुसूचीनुसार सायबर गुन्हे राज्य विषयांतर्गत येतात .


Internet
Networks
Information
Applications
Technology
Data
computer


system security
Application
Network security
Information security

सायबर कायदे म्हणजे असे अदृश्य आभासी जगात ज्या घडामोडी वा व्यवहार घडतात वाघ होऊ शकतात अशा सर्व घटनांना शिस्त लावण्यासाठी जे कायदे काम बनविले जातात आणि भविष्यात बनवली जातील या सर्वांना सायबर कायदे म्हणतात

सायबर लॉ म्हणजे इंटरनेट व्यवस्थितपणे चालावी म्हणून केलेली कायदे इंटरनेटच्या सुरक्षिततेचे संबंधित प्रश्न इंटरनेटवर इंटर लेक्चर प्रॉपर्टी राइट्स आणि इंटरनेटवरील फसवेगिरीचा सामना करण्यासाठी केलेली नियम होय

एक जुलै 2015 रोजी डिजिटल इंडिया उद्घाटन प्रसंगी भारताचे पंतप्रधान नरेंद्र मोदी यांनी सायबर युद्ध विषयी चिंता व्यक्त केली जगासमोर रक्तही सायबर युद्धाचा धोका निर्माण झाला असून संपूर्ण जगाला सायबर सुरक्षित चिंता लागली आहे या संकटाला सामोरे जाण्यासाठी भारताने तोडगा काढण्यासाठी समोर यावे असे आवाहन त्यांनी केले
सायबर सुरेक्षेच्या धोक्यावर सुरक्षा ठरेल असा संशोधनात्मक आणि विश्वसनीय दुर्गा भारत देऊ शकेल असा प्रश्नही त्यांनी निर्माण केला माहिती तंत्रज्ञान सुरक्षेचा आत्मविश्वास का असायला नको संपूर्ण जगाला शांततेत नांदता यावी यासाठी भारतानेही आव्हान स्वीकारला हवी असे मोदी म्हणाले दहावी बारावी उत्तीर्ण असलेला कोणीतरी हजारो महिला अंतरावर बसून बहुतेक वर बँक खाते साफ करून टाकतो अशा परिस्थितीत मात करायला हवी असे प्रथम प्रतिपादन मोदींनी केली सुशासन प्रस्थापित करण्यासाठी सायबर सुरक्षितता महत्वपूर्ण आहे


CYBER
SECURITY

तीन एप्रिल 1973 मोटोरोला कंपनीत काम करणारे मार्टिन कपूर हे ग्रहस्थ न्यू या चार रस्त्यावर उभे होते ते सांगतात दिलेल्या आमच्या प्रतिस्पर्धी कंपनीतील जॉयल ला फोन करून मी म्हटले जोयल मी खऱ्याखोऱ्या मोबाईल फोनवरून तुला पहिला कॉल करतो आहे हा जगातला पहिला मोबाईल कॉल आज पन्नास वर्षानंतर ची अवस्था अशी जगाची लोकसंख्या आहे अंदाजे 7.95 अब्ज आणि इंटरनॅशनल टेनिस कम्युनिकेशन युनियनच्या आकडेवारीनुसार मोबाईल कनेक्शन आहेत 8.58 अब्ज थोडक्यात जागतिक लोकसंख्येपेक्षा मोबाईल जोडण्या जास्त

भारतात इंटरनेट सर्फिंग सर्वाधिक प्रमाण मोबाईलवर आहे आणि तुमचा मोबाईल नंबर ईमेल आयडी आणि तुमचे लोकेशन हे आणि कंपन्यापर्यंत सहज पोहोचलेला आहे एवढेच काय तुमच्या मोबाईल मध्ये नंबर मेसेजेस फोटोज आणि व्हिडिओ आणि कंपन्यांना सहज पाहता येतात तशी परवानगी आपण ॲप डाऊनलोड करताना दिलेली असते पण ती आपणाला माहिती नसते मोबाईल फोन वापरण्याचे बाबतीत भारत जगाचीCHINE नंतर दुसऱ्या स्थानी आहे भारताने स्वातंत्र्याच्या 75 वर्षात अनेक क्षेत्रात आघाडी घेतली आहे याचवेळी आर्थिक विकास झालेले नागरिकांच्या घरातील वस्तूंची संख्या ही वाढली देशातील तब्येत 95.5% जनतेच्या हातात मोबाईल पोहोचला आहे
2022 मध्ये भारतीयांनी ६९९ कोटी तास मोबाईलवर घालवली रोज सरासरी 4.7 तास वेळ मोबाईलवर घालवतात
एका सर्व क्षणात अशी जाणवली की ८७.८ टक्के वापर करतील लोकांना फोन जवळ नसल्यावर घबराट वाटते
73.4% लोक आपला फोन टॉयलेटमध्येही घेऊन जातात
69 टक्के लोक झोपण्याआधी पाच मिनिटे फोन चेक करतात
43.5% लोक दिवसातून कमीत कमी 50 ते 100 वेळा फोन अनलॉक करतात.
लोकांनी मोबाईल शिवाय आयुष्य जगावअसं मोबाईलचे जनक मार्टिन कपूर म्हणतात

पासवर्ड ठेवण्याची सवय करते घात बसतो फार मोठा फटका
दुबळा पासवर्ड ठेवणारी देश

कमकुवत पासवर्ड वापरण्याच्या बाबतीत महासत्ता अमेरिका पहिल्या स्थानी आहे 39 देशातील 20 उद्योगांमधील 500 कंपन्यांचा nordpasआढावा घेतला

अमेरिका 46.2%
चीन 9.6%
जपान 5.8%
India 4.2%
Britain 4.0%
France 3.8%
Canada 3.6%

कोविडदरम्यान आणि कोविडनंतर देशात ऑनलाईन सेवांमध्ये प्रचंड प्रमाणात वाढ झाली आहे. मोबाईल इंटरनेटचा वापर टाईमपासून आणि सोशल मीडियासाठी केला जायचा. तो कोविडनंतर काही व्यवहारांसाठी सोपा आणि सोयीचा देखील झाला. मात्र, दुसरीकडे सायबर क्राईमच्या घटनांमध्ये वेगाने भरमसाठ वाढ झाली आहे. याचाच अर्थ असा की, इंटरनेट माध्यम हे असे आहे सेफ टू युज अँड अन्सेफ टू मिसयुज. खूप सतर्क राहून, इंटरनेटच्या माध्यमातून पैशाचे व्यवहार अन्य गोष्टी करणे आवश्यक आहे. नाहीतर तुम्ही सायबर क्राईमला बळी पडू शकता असही ते म्हणाले आहेत.

जागतिक पहिला सायबर हल्ला फ्रान्समध्ये इंटरनेट शोधाच्या आधी 1834 मध्ये झाला गुन्हेगारांनी फ्रान्सच्या टेलिग्राम प्रणालीकडे पोहोचून वित्तीय बाजाराची माहिती चोरली.
भारतात पहिला सायबर गुन्हा याहू विरुद्ध आकाश अरोराचा 1999 मध्ये झाला

सायबर युग

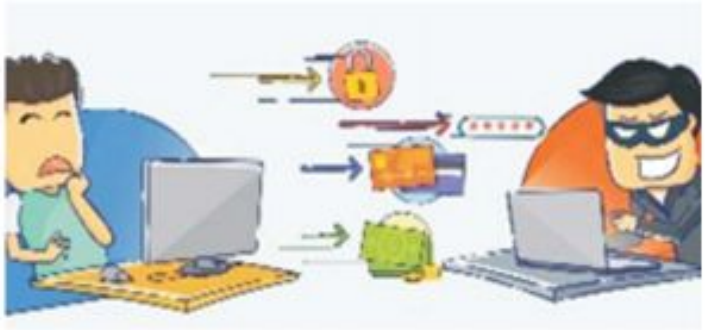
- आजच्या युगात इंटरनेट प्रत्येक व्यक्तीच्या जीवनाचा अविभाज्य भाग बनला आहे. दैनंदिन जीवनातले बरेच व्यवहार आजकाल इंटरनेटच्या माध्यमातून पार पाडले जातात. (जसे की आर्थिक व्यवहार, बँकिंग, व्यावसायिक, शैक्षणिक, वैद्यकीय व जनसंपर्क इत्यादी.)
- इंटरनेटच्या माध्यमाने मानवी जीवन सुलभ झाले आहे हे जितके खरे तितकेच याच्या अपुऱ्या माहितीने ते धोकादायक झाले आहे.
- सायबर साक्षरता ही एक महत्वाची बाब आहे जी एखाद्या व्यक्तीच्या सुरक्षिततेसाठी आवश्यक असते.
- आपण उत्तम रितीने मोबाईलचा वापर करतो पण याचा अर्थ असा नाही कि आपण सायबर साक्षर आहोत.

आपल्या दैनंदिन जीवनात येणारा इंटरनेटशी संबंध

- इंटरनेट बँकिंग
- ऑनलाईन खरेदी
- ऑनलाईन गेम्स (Games)
- मनोरंजन
- शिक्षण
- ऑनलाईन संवाद
- सोशल माध्यम

सायबर गुन्हे

- सायबर गुन्हे हे असे गुन्हे आहेत ज्यात संगणक, इंटरनेट किंवा मोबाईल तंत्रज्ञानाचा वापर करून वैयक्तिक पातळी वर किंवा संस्थांविरुद्ध कृत्य केले जाते.
- सायबर युगात सायबर गुन्हे करण्यासाठी सोशल नेटवर्किंग साइट्स, ई-मेल, चॅटरूम, पायरेटेड सॉफ्टवेअर, वेबसाइट इत्यादी सारख्या प्लॅटफॉर्मचा वापर केला जातो.
- मुले व महिला विविध प्रकारच्या सायबर क्राईमला बळी पडतात.



सायबर सुरक्षिततेची गरज

- वैयक्तिक माहितीची सुरक्षा .
- आर्थिक नुकसान टाळण्यासाठी.
- विविध प्रकारच्या ऑनलाईन सुरक्षा :
  - बँकिंग (UPI, ATM PIN, OTP, CVV No.)
  - समाज माध्यम (WhatsApp, Instagram, Facebook etc.)
  - शैक्षणिक माध्यम (Byju's, Youtube, Unacademy, Diksha etc.)
  - पेमेंट Gateways (Google Pay, PayPal, Paytm, etc.)

सायबर गुन्ह्यांचे प्रकार

- सोशल इंजिनीयरिंग
- फिशिंग
- नोकरीचे लोभ दाखवून होणारी फसवणूक.
- लग्नाचे आमिष दाखवून होणारी फसवणूक.
- बँकिंग विषयी होणारी फसवणूक इत्यादी.

अकाउंट हॅक होण्याच्या दहा पद्धती

१ अकाउंट आणि ईमेल आयडीमधून हॅकिंग

२ फिशिंग लिंक आणि पेजमधून हॅकिंग

३ डेटाबेस एक्सेस करून

४ पासवर्ड मॅनेजमेंट

५ कूकीज किंवा कॅशेतून हॅकिंग

६ इमेजच्या मदतीने

७ सेक्युरिटी सेटिंग न झाल्याने हॅकिंग

८ पर्सनल डिटेल पोस्ट केल्याने हॅकिंग,

९ पब्लिक वाय फाय वापरल्याने हॅकिंग

१० ओटीपी शेअर केल्याने हॅकिंग

सोशल इंजिनीयरिंग

- लोकांना गोपनीय माहिती उघड करण्यासाठी पटवून देण्याची कला.
- आपली गोपनीय माहिती आपल्याकडून:
  - फोन
  - ई-मेल
  - व्यक्तीश:

  इत्यादी द्वारे घेतली जाते.

फिशिंग

- फिशिंगमध्ये आपले सोशल मीडिया, बँकिंग व ATM कार्डचे डिटेल्स मिळवण्याचा प्रयत्न केला जातो.
- मूळ संकेतस्थळासारखे दिसणारे बनावट संकेतस्थळ बनवून ग्राहकांना फसवून त्यांची संवेदनशील माहिती चोरण्यात येते.
- ई-मेल किंवा फोन मेसेज वरून बनावट वेबलिंक पाठवून आपली माहिती चोरण्यात येते .

टिप : https ने सुरुवात होणाऱ्या सुरक्षित website चा वापर करावा

नोकरीचे प्रलोभन दाखवून होणारी फसवणूक

JOB SCAM

Dear Candidate, Immediate Join!

Ref: "TATA INDIA LIMITED" - DIRECT RECRUITMENT'S OFFER.

It is our good pleasure to inform you, that you are selected for one of our given requirements. The Company has urgent openings for new Plants in Delhi, Maharashtra, Gujarat, UP and Karnataka. The Company required urgent staff for Administration, IT/Computer and Production Department as Executives and Managers. Fresher's / 0-5 year of experience willing to join within 15 days or after Completion of final face to face meeting with us.

The Company Tata Motors Ltd is the best it Company in India, the Company is recruiting the candidates for our new Plants in various cities. Your interview will be held at the Company Corporate office in Delhi on 10th of June 2014, at 11.30 AM, you will be pleased to know that the 432 candidates shortlist selected by 465 candidates will be giving appointment, meaning that your Application can progress to final stage. You will have to come to the Company corporate office in Delhi, your offer letter with tickets will be sent to you by courier before date of interview. You have to come for interview with all required documents by Company HRD.

REQUIRED DOCUMENTS BY THE COMPANY HRD Fake list!

1) Photo-copies of qualification documents.
2) Photo-copies of experience certificates (if any)
3) Photo-copies of address proof Payment without proof!
4) Two Passport size photographs.

You have to deposit the (security) as an initial amount in favor of our company HR name in charges to collect your payment department for Rs. 7,200/- (Seven Thousand And Two Hundred Rupees Only) any MERCANTILE BANK, Branch from your Home City to our Company HR Name In-Charges. **(Managing Directors) A/c No. - 705710110000323, Mr. KAMAL SINGH**, this is refundable interview security. Your offer letter with Air tickets or Train tickets will be send to your Home Address by courier after receiving the confirmation of interview security deposited in any MERCANTILE BANK, and The Company will pay all the expenditure to you at the time of face-to-face meeting with you in Company. Fake promise!

The Job profile, salary offer, and date-time of interview will be mentioned in your offer letter. Your

अर्जंट जॉईन करण्या बाबत

खोटी यादी

Payment ची मागणी, पुरावा न घेता

खोटी आश्वासने

नोकरीचे/लॉटरीचे प्रलोभन दाखवून होणारी फसवणूक

- आपल्याला अज्ञात संकेतस्थळांकडून नोकरीची ऑफर मिळाल्यास प्रथम त्याची सत्यता पडताळून पहा.
- आपल्याला लॉटरीच्या ऑफर प्राप्त झाल्यास सावधगिरी बाळगा.
- लॉटरीची रक्कम मिळविण्यासाठी ऍडव्हान्स पैसे भरू नका.
- अज्ञात ईमेलमधील संलग्न फाईल किंवा लिंक उघडताना खबरदारी घ्या.

लग्नाचे आमिष दाखवून होणारी फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी

- विवाहविषयक संकेतस्थळावर फसवणुकीच्या उद्देशाने गुन्हेगार खोट्या आकर्षक प्रोफाईल बनवतात.
- लग्न करण्याचे आमिष दाखवून त्या व्यक्तीशी जवळीक साधली जाते.
- पिडीत व्यक्तीला पैशांची मागणी किंवा एखादे गैरकृत्य करण्यास भाग पाडतात.

लग्नाचे आमिष दाखवून होणारी फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी

- सोशल मीडियावरून मैत्री करताना सावधानता बाळगा.
- आपली संवेदनशील वैयक्तिक माहिती अज्ञात व्यक्तीला सांगू नका.
- सोशल मीडियावरील समोरच्या व्यक्तीचे प्रोफाइल तपासून बघावे.
- समोरच्या व्यक्तीचे प्रोफाइल तपासल्यावरच मैत्री करावी व खात्री केल्याशिवाय अशा माणसांना उधारीने पैसे देऊ नका.
- अज्ञात व्यक्तींबरोबर वैयक्तिक फोटो Share करू नका.

लग्नाचे आमिष दाखवून होणारी फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी

- सोशल मीडियावरून मैत्री करताना सावधानता बाळगा.
- आपली संवेदनशील वैयक्तिक माहिती अज्ञात व्यक्तीला सांगू नका.
- सोशल मीडियावरील समोरच्या व्यक्तीचे प्रोफाइल तपासून बघावे.
- समोरच्या व्यक्तीचे प्रोफाइल तपासल्यावरच मैत्री करावी व खात्री केल्याशिवाय अशा माणसांना उधारीने पैसे देऊ नका.
- अज्ञात व्यक्तींबरोबर वैयक्तिक फोटो Share करू नका.

बँक विषयक फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी

- आपल्या डेबिट / क्रेडिट कार्ड ची माहिती, १६ अंकी नंबर, पिन , ओटीपी क्रमांक इ. कोणालाही देऊ नका.
- लक्षात ठेवा! अशा माहितीसाठी बँक कधीही कॉल करत नाही.
- आपला पिन क्रमांक ए.टी.एम. किंवा इतर ठिकाणी प्रविष्ट करताना सावधानता बाळगा.
- एटीएमच्या वापरानंतर आपल्या एटीएम पावत्या नष्ट करा
- जर तुम्हाला काही संशयित मेसेज आले तर त्वरित तुमच्या बँकेत संपर्क साधा.

IDENTITY THEFT

- सार्वजनिक प्लॅटफॉर्मवर वैयक्तिक माहिती (जन्मतारीख, जन्मस्थान, पूर्वीचे नाव, कौटुंबिक तपशील, पत्ता, फोन नंबर) देऊ नका
- इंटरनेटचा वापर करताना आपल्या ओळख पत्रांची माहिती (आधार, पॅन, ड्रायव्हिंग लायसन्स) अनोळखी माणसांना किंवा सार्वजनिक प्लॅटफॉर्मवर देऊ नका.
- आपली वैयक्तिक माहिती मिळवून तो इतरांना आपण आहोत असे भासवून त्यांच्याशी चुकीच्या पद्धतीने संवाद साधू शकतो
- गुन्हेगार हा ई-मेल, मेसेज किंवा फोनद्वारे व्यक्तीची वैयक्तिक ओळख चोरी करतो.
- तुमचे ओळखपत्र सबमिट करताना त्यावर नेहमी कारण ,तारीख व स्वाक्षरी करावी.
- लकी ड्रॉ कुपन किंवा कोणताही फॉर्म भरताना काळजी घ्या!

Free Wi-Fi usage theme

- संवेदनशील खाजगी माहितीचा वापर करताना सार्वजनिक वाय-फाय चा वापर टाळा.
- सार्वजनिक वाय फाय वापरताना व्हर्च्युअल प्रायव्हेट नेटवर्क(VPN) वापरा.
- सुरक्षित ब्राउझिंगसाठी HTTPS वेबसाइट वापरा.
- स्मार्टफोनवरील स्वयंचलित (Automatic) वाय-फाय लॉग-इन बंद करा
- वाय-फाय साठी साइन अप करण्यासाठी संवेदनशील खाजगी माहिती देताना सावधगिरी बाळगा.

Passwords / Anti-virus

- नेहमीच एक सशक्त पासवर्ड वापरा जेणेकरून तो कोणाच्याही लक्षात येणार नाही.
- पासवर्ड नियमितपणे बदलत राहावे.
- आपला पासवर्ड कोणालाही सांगू नका.
- प्रत्येक अकाउंटसाठी वेगळा पासवर्ड वापरा.
- आपल्या कॉम्प्यूटरसाठी अँटीव्हायरस आणि फायरवॉलचा वापर करा.

महिला व बालकांसंदर्भात होणाऱ्या गुन्ह्यांचे प्रकार

चाईल्ड पोर्नोग्राफी

- १८ वर्षाखालील बालकांवर होणारा लैंगिक अत्याचार व त्याचे चित्रीकरण याला चाईल्ड पोर्नोग्राफी असे म्हणतात.
- लहान बालकांवर खाऊ, खेळणी इत्यादीचे आमिष दाखवून लैंगिक अत्याचार केले जातात.

सायबर ग्रुमिंग

- सोशल मिडिया किंवा मेसेजिंग प्लॅटफॉर्मद्वारे मुलांचे लैंगिक शोषण किंवा कोणत्याही प्रकारे शोषण करण्याच्या उद्देशाने जवळीक निर्माण केली जाते.
- सायबर ग्रुमर आपल्याला भेटवस्तू, प्रशंसा, मॉडेलिंग जॉबची ऑफर देतात आणि नंतर ते अश्लिल संदेश, छायाचित्रे किंवा व्हिडिओ पाठवू लागतात आणि आपल्या बरोबर लैंगिक सुस्पष्ट प्रतिमा किंवा व्हिडिओ पाठविण्यास सांगतात.

सायबर बुलींग

- सायबर बुलींग मध्ये स्त्रियांना व मुलांना धमकी देऊन त्यांना मानसिक त्रास दिला जातो.
- अश्लिल किंवा हानिकारक संदेश, टिप्पण्या आणि प्रतिमा / व्हिडिओ पाठवून एखाद्याला त्रास देण्यासाठी इंटरनेट किंवा मोबाईल तंत्रज्ञानाचा वापर केला जातो.
- सायबर गुन्हे करणारी व्यक्ती मजकुर संदेश, ई-मेल, सोशल मिडिया प्लॅटफॉर्म, वेबपृष्ठे, चॅटरूम्स इत्यादीचा वापर करतात.
- यामुळे विद्यार्थ्यांच्या शारीरिक, भावनिक, सामाजिक आणि मानसिक जीवनात गंभीर परीणाम होतात.

मॉर्फिंग

- मॉर्फिंग मध्ये एखाद्या व्यक्तीचे मूळ चित्र बदलले जाते.
- महिलांचे मूळ चित्र वेबसाईट वरून डाउनलोड करून, मॉर्फिंग करून, पुन्हा ते वेबसाईट वर रिपोस्ट/अपलोड करून फेक प्रोफाईल बनवली जाते.

सायबर डिफेमेशन [बदनामी]

- सायबर डिफेमेशन मध्ये एखाद्या व्यक्ती बाबत चुकीचे विधान करून त्याच्या सामाजिक प्रतिष्ठेला हानी पोहचवली जाते.
- उदा: एखाद्या व्यक्तीच्या सामाजिक प्रतिष्ठेला हानी पोहचविण्याच्या उद्धेशाने केलेले ई-मेल किंवा केलेली पोस्ट.

सायबर स्टॉकिंग

- एखाद्या व्यक्तीच्या online हालचालींचा पाठलाग करणे, त्यांच्यावर सतत लक्ष ठेवणे व त्याची वैयक्तिक माहिती गोळा करून ती सोशल मीडिया वर पोस्ट करणे.
- अशी संवेदशील माहिती गोळा करून सायबर स्टॉकर खालील प्रकारे दुरुपयोग करू शकतात जसे की नाव, कौटुंबिक पार्श्वभूमी, Mobile नंबर आणि पिडीतेच्या दैनंदिन व्यवहारामध्ये प्रवेश करुन, स्टॉकर पिडीतेच्या नावाने डेटिंग सेवांशी संबंधित वेबसाइटवर पोस्ट करतो.

ऑनलाईन गेमिंग

- मुले मोबाईल, संगणक, पोर्टेबल गेमिंग डिव्हाइसचा वापर करून सोशल नेटवर्क वर ऑनलाईन गेम खेळतात .

  उदा. BlueWhale, Momo challenge, Pub G.

- ऑनलाईन गेमिंगचा आतिरेक केल्यामुळे मुले चोरी, आत्महत्या यासारख्या गुन्ह्यांना बळी पडतात.

सायबर गुन्हेगारीवर प्रतिबंधक उपाय (१/२)

- ❑ आपल्या कॉम्प्युटर कडे कधीही दुर्लक्ष करू नये. तुम्ही जागेवर नसताना कॉम्प्युटरची स्क्रीन लॉक्ड् असली पाहिजे.
- ❑ सॉफ्टवेअर Update ठेवले पाहिजे.
- ❑ महत्वाच्या फाईल्स साठी पासवर्डचा वापर करावा.
- ❑ Password कधीही Share करू नका.
- ❑ कॉम्प्युटरला/ Device ला एक मजबूत Password ठेवा आणि त्याला 2-Factor Authentication करा.
- ❑ महत्वाच्या फाईल्सचा बॅकअप घ्यावा.
- ❑ WhatsApp, Facebook, Instagram आदी समाज माध्यमांव्दारे स्वत:चे व कुटुंबियांचे सध्याचे लोकेशन Share करणे टाळा.

सायबर गुन्हेगारीवर प्रतिबंधक उपाय (२/२)

- ❑ पायरेटेड सिनेमा/गाणी डाउनलोड करू नका.
- ❑ वेबकॅम / मायक्रोफोन काम नसताना बंद ठेवा.
- ❑ वैयक्तिक डेटा Online share करू नका.
- ❑ आपल्या संगणकामध्ये Anti-Virus टाका.
- ❑ आपली Operating System वारंवार चेक करून त्याला Updated ठेवा.
- ❑ सिस्टिमचा फायरवॉल चालू ठेवा.
- ❑ Online भेटलेल्या अनोळखी व्यक्तीला प्रत्यक्षात भेटु नका/ संपर्क साधू नका.

इट्स नॉट युवर फॉल्ट !!!

- घर आणि कामाच्या ठिकाणी केले जाणारे शोषण.
- इंटरनेट आणि मोबाइल फोनच्या वापराबाबत साक्षरतेचा अभाव.
- गैरवर्तन सहन करणे.
- समाजामध्ये बदनामीची भीती.

मुले व महिलांची सुरक्षा (१/२)

- लहान मुलांची पोर्नोग्राफी (Pornography) हा गंभीर स्वरूपाचा गुन्हा आहे व कठोर कारवाईस पात्र आहे.
- लहान मुलांच्या अश्लील चित्रफिती बनवणे, बाळगणे आणि त्याचे वितरण करणे हे कायद्याने गुन्हा आहे.
- जर तुम्ही मुलाचे किंवा स्त्रियांचे अत्याचार (Child /Woman Abuse) किंवा गैरवर्तनाने (Harassment)पिडीत असाल तर जवळच्या पोलीस ठाण्यात त्वरित तक्रार दाखल करा.
- आक्षेपार्ह मेसेज रिसिव्ह झाल्यास डिलिट करू नका, त्याचा वापर पोलिसांना पुरावा (Evidence) म्हणून होऊ शकतो.
- मुलांना सायबर सुरक्षेबाबत योग्य ते शिक्षण /माहिती द्या.

मुले व महिलांची सुरक्षा (२/२)

- ❑ पॅरेंटल कंट्रोल सॉफ्टवेअर वापरा.
- ❑ रात्री उशिरा मोबाईल किंवा लॅपटॉप वापरण्यावर मर्यादा ठेवा.
- ❑ मुले इंटरनेटवर कोणाच्या संपर्कात आहेत याचा मागोवा ठेवा.
- ❑ आपल्या मुलाची इंटरनेट Activity तपासा.
- ❑ आपली मुले ऑनलाईन Surfing करत असताना त्यामध्ये सहभागी व्हा.
- ❑ मुलांशी त्याच्या दैनंदिन Activity बाबत संभाषण करा.
- ❑ शाळा आणि महाविद्यालयांमध्ये विद्यार्थी व पालकांसाठी कार्यशाळा आयोजित केली पाहिजे.

मोबाईल फोन टिप्स

- ❑ नेहमीच एक सशक्त पासवर्ड वापरा.
- ❑ विश्वसनीय संकेत स्थळावरूनच ॲप डाउनलोड करावे.
- ❑ एकापेक्षा जास्त प्रमाणीकरण (मल्टिपल ऑथेंटिकेशन/ 2-Factor Authentication) असावे.
- ❑ बँक किंवा इतर महत्वाच्या ॲप्सला ॲप-लॉक वापरावे.
- ❑ आपले पासवर्ड मोबाईल मध्ये स्टोअर करू नये.
- ❑ विविध ॲप्सला देण्यात आलेल्या परवानग्या नियमितपणे तपासा.

सोशल मीडिया

- नवीन डिव्हाईस मधून लॉग-इन (Log-in) केले असल्यास वापर झाल्यावर नेहमी लॉग-आऊट (Log-out) करा.
- सोशल मीडियावरती तुमचे स्थान व इतर गोष्टी (Activity) शेयर करू नका.
- वाईट किंवा चुकीची पोस्ट अपलोड, शेअर आणि लाइक करू नका.
- आपल्या खात्याची गोपनीयता आणि सुरक्षिततेबाबत (Privacy and Security) काय दक्षता घ्यावी ह्याची माहिती ठेवा.

माहिती तंत्रज्ञान कायदा 2000

गुन्हा	कलम
संगणकातील कोड किंवा प्रोग्राम या मध्ये फेरफार करणे	कलम ६६
चोरलेली संगणक साधनसामुग्री अप्रामाणिकपणे वापरणे.	कलम ६६ब
ओळखदर्शक गोष्टींची (Identity Theft) चोरी केल्यास	कलम ६६ क
खाजगीपणाचे उल्लंघन केल्यास	कलम ६६ इ
सायबर दहशतवाद पसरविल्यास	कलम ६६ फ

माहिती तंत्रज्ञान कायदा 2000

गुन्हा	कलम
अश्लील मजकूर इलेक्ट्रॉनिक स्वरुपात प्रसिद्ध केल्यास किंवा पाठविल्यास	कलम ६७
लैंगिक भावना उत्तेजीत करणारे साहित्य इलेक्ट्रॉनिक स्वरुपात प्रसिद्ध केल्यास	कलम ६७ अ
कामवासना उत्तेजीत करणारी कृती इत्यादीमध्ये लहान मुलांचे चित्रण केलेले साहित्य इलेक्ट्रॉनिक स्वरुपात प्रसिद्ध केल्यास (Child Pornography)	कलम ६७ ब
मध्यस्थाद्वारे माहितीचे जतन केल्यास व धारण केल्यास (Man in the Middle Attack)	कलम ६७ क

लैंगिक अपराधांपासून बालकांचे संरक्षण अधिनियम, (POCSO) २०१२

- लैंगिक हमला, लैंगिक सतवणूक व संभोगचित्रण अशा अपराधांपासून बालकांचे संरक्षण करण्यासाठी लैंगिक अपराधांपासून बालकांचे संरक्षण अधिनियम, (POCSO) २०१२ हा कायदा अमलात आलेला आहे.
- वाढता बाल लैंगिक अत्याचार अपराध रोखण्यासाठी २०१९ ला कायदामध्ये सरकारने शिक्षेत वाढ केली आहे.

उदा:

Section 4 मध्ये तुरुंगवासाची शिक्षा ७ वर्षा ऐवजी १० वर्ष केली आहे.

ऑनलाइन फ्राड पासून मुक्ती

जमाना ऑनलाइनच आहे खरेदी विक्री पैशाची देवाण-घेवाण आधी सह अनेक कामे ऑनलाईन होतात अनेकदा नागरिकांना ऑनलाइन व्यवहार करताना नेमकी कोणती काळजी घ्यावी याची माहिती नसते आधार पॅन कार्ड द्यावा की नाही हेही ठाऊक नसते पिन नंबर देणे आणि क्यू आर कोड स्कॅन करणे किती धोक्यात आहेत ही अनेकांना ठाऊक नसते या सर्व लक्षात येईपर्यंत चोरट्याने तुमचे बँक खाते रिकामी केलेली असते टेक्नॉलॉजी आपलीशी करताना अमृत काळात डिजिटल शिक्षणावर मोठ्या प्रमाणावर काम करावे लागणार आहे

१)फिशिंग लिंक पाठवून लुबाड
२) ऑफरच्या नावे लुबाडणूक
३) ऑनलाइन विक्रीतून गंडा
४) क्रेडिट कार्ड फीमाफी
५) एटीएम कार्ड स्किमिंग
६) सिम कार्ड क्लोनिंग खाते साप
७) क्यू आर कोडणेपैशांचा अपहार
८) सोशल मीडियातील तोतियागिरी
९) चार्जिंग केबलने डेटा चोरी
१०) लॉटरी लागण्याची बतावणी
११) जॉब ऑफरचा बहाना
१२) लसीकरणाची आमिष
१३) लोन रिकवरी एजंट बनून चोरी
१४) चेन मार्केटिंग मधून झटपट पैसे
१५) अनुदानाच्या अपेक्षाची लुबाडणूक
१६) ऑनलाइन सुट्ट्याच्या जाळ्यात
१७) मेसेज द्वारे पैशाची लुबाणूक
१८) फेक विमा पॉलिसीची विक्री

साभार परत उपक्रम : सामाजिक माध्यमांवर पोलिसांचे लक्ष

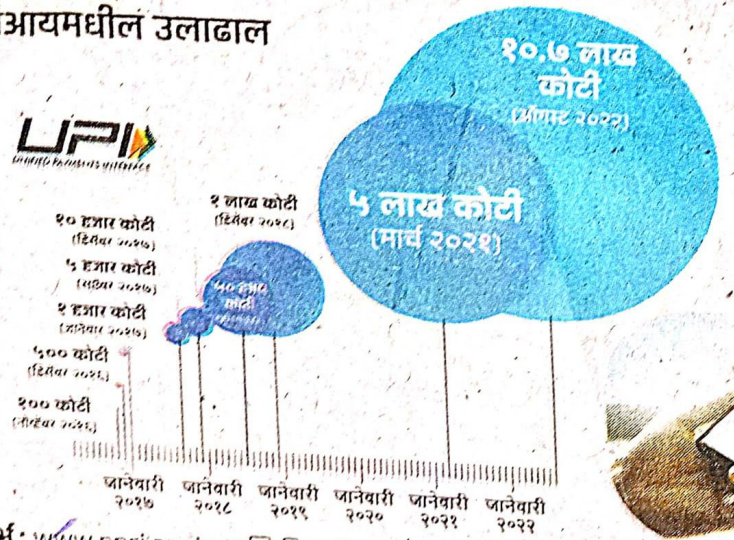
सोशल मीडियातील अशा अपप्रवृत्तींना आळा घालण्यासाठी लातूर पोलिस दलाने सोशल मीडिया मॉनिटरिंग सेलची स्थापना केली आहे. या सेलद्वारे फेसबूक, व्हॉटसॲप, इन्स्टाग्राम, ट्विटर आणि रिल हे सोशल मीडिया बारकाईने तपासले जात आहेत. सोशल मीडियाच्या ज्या पोस्टमध्ये हत्यार अथवा आक्षेपार्ह मजकूर दिसत आहे, त्याचा शोध घेऊन कारवाई केली जात आहे. गेल्या चार महिन्यांत तिघांवर असे गुन्हे दाखल झाले आहेत.

सोशल मीडियावर आक्षेपार्ह पोस्ट करणारे अल्पवयीन मुलेही असतात. त्यांचे भविष्य उद्ध्वस्त होऊ नये, म्हणून सोशल मीडिया मॉनिटरिंग सेलच्या माध्यमातून साभार परत हा उपक्रम राबविला जात आहे. त्यात अल्पवयीन मुलगा व त्याच्या पालकांचा शोध घेऊन त्यांना बोलावून समुपदेशन केले जाते. त्यानंतर त्यांना साभार प्रमाणपत्र देऊन पालकांच्या ताब्यात दिले जाते. आजवर दीडशे अल्पवयीन मुलांचा शोध घेऊन त्यांच्या पालकांना साभार प्रमाणपत्र दिले आहे.


ICICI Bank
BACHOGE
YA PHASOGE?
#BeatTheCheats
40 MILLION+
VIEWS

UPI -१०० कोटींवरून १० लाख कोटींवर!

सहा वर्षांत वाढत गेलेली यूपीआयमधील उलाढाल



संदर्भ : www.npci.org.in आणि फिनशॉट्स

वीस रुपयांच्या मिरची, कोथिंबिरीपासून, तीनेक हजारांच्या किराणा खरेदीपासून ते महत्त्वाच्या व्यवहारांपर्यंत सर्वत्र वापरली जाणारी यूपीआय (युनिफाईड पेमेंट सिस्टीम) म्हणजेच आपल्या ओळखीचे फोन पे, गुगल पे किंवा भीमसारखी ॲप्स यांचा शिरकाव आपल्या आयुष्यात फार वेगाने झाला आणि आपल्या आर्थिक व्यवहारांची रीतच बदलून गेली. सुरुवातीला फोनच्या स्क्रीनवरून पैसे पाठवायला दचकणारे लोकही त्यातल्या सोपेपणामुळे आता स्कॅन करण्यासाठी क्यूआर कोड कुठे आहे, असे भाजीवाल्यालाही सहज विचारतात. भारतात यूपीआयची चाचणी झाली एप्रिल २०१६ मध्ये नोव्हेंबर २०१६ मध्ये या प्रणालीतून १०० कोटी रुपयांच्या व्यवहाराचा टप्पा गाठला गेला. ऑगस्ट २०२२ मध्ये हा आकडा कितीवर पोहोचला असेल? - १० लाख ७० हजार कोटी रुपये!

कर्नाटकातील बेंगळुरू येथे सायबर गुन्ह्यांसाठी भारतातील पहिल्या पोलीस स्टेशनचे उद्घाटन करण्यात आले. सायबर गुन्ह्यांसाठी भारतातील पहिले पोलीस स्टेशन 2001 मध्ये सुरू झाले.

महाराष्ट्र राज्यात अत्याधुनिक सायबर सुरक्षा प्लॅटफॉर्म तयार करणार उपमुख्यमंत्री फडणवीस यांनी सांगितले

सायबर सुरक्षा धोरण 2013
दोन जुलै 2013 रोजी भारताने सायबर सुरक्षा किंवा माहिती तंत्रज्ञान सुरक्षिततेचा विचार करून स्वतंत्र धोरण आखली आहे या धोरणाचा मुख्य उद्देश नागरिक उद्योग प्रशासन यांना माहिती तंत्रज्ञानाची सुरक्षितता प्राप्त करून देणे हा आहे या धोरणाची रूपरेषा इलेक्ट्रॉनिक आणि माहिती तंत्रज्ञान विभाग भारत सरकारने केली आहे हे धोरण यूएस नॅशनल सिक्युरिटी एजन्सीच्या धरतीवर अवलंबलेले आहे

सायबर विश्वात लोकांच्या वैयक्तिक माहितीला मोठा धोका असतो तुमची माहिती कोण कशी वापरली याचं काही निर्णय त्यामुळे लोकांच्या प्रायव्हसीला सुरक्षित ठेवण्यासाठी बहुप्रतिक्षित डेटा प्रोटेक्शन विधेयकाला केंद्रीय मंत्रिमंडळाने नुकतीच मंजुरी दिली
प्रायव्हसी संबंधी नियमांची उल्लंघन केल्यास 500 कोटी रुपयांपर्यंत उठवण्यात येईल असे सांगण्यात आली लोकसभेत डिजिटल वैयक्तिक डेटा संरक्षण विधेयक मंजूर करण्यात आली

भारतातील सर्वात मोठा सायबर हल्ला

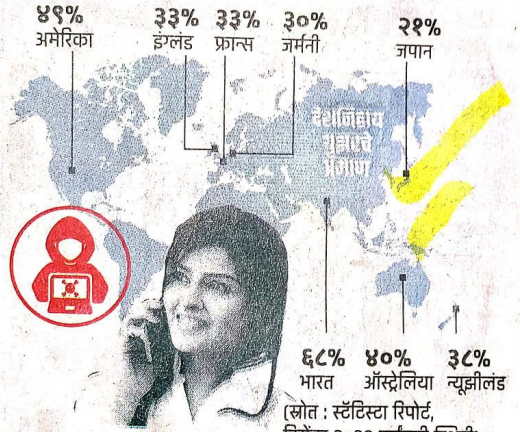
कॉसमॉस बँकेवर १३ ऑगस्ट २०१८ रोजी सायबर दरोडा पडला एकाच वेळी तब्बल 28 देशांमधून व्यवहार करून हॅकर्स मी तब्बल 94 कोटी रुपये लुटले या घटनेमुळे सर्वसामान्य नागरिकांच्या डिजिटल विश्वासाला थोडा थोडा गेला

देशात ६८ टक्के युझर ठरले गुन्ह्यांचे बळी

सायबर क्राइममध्ये भारत जगात 'नंबर वन'

महेश घोराळे
लोकमत न्यूज नेटवर्क

मुंबई : नोटाबंदी तसेच कोविडनंतर देशात ऑनलाइन सेवांमध्ये मोठ्या प्रमाणात वाढ झाली. मोबाइल इंटरनेटचा वापर चेनीबरोबरच सोयीचाही झाला. मात्र, दुसरीकडे सायबर क्राइमच्या घटनांमध्ये भरमसाठ वाढ झाली. चिंतेची बाब म्हणजे सायबर क्राइम आणि त्याला बळी पडलेल्यांमध्ये जगात भारतीयांचे प्रमाण सर्वाधिक आहे. भारतात ६८% युझरनी डिसेंबर २०२२ पर्यंत कोणत्या ना कोणत्या सायबर गुन्ह्याचा अनुभव घेतला आहे. नोव्हेंबर ते डिसेंबर २०२२ दरम्यानच्या एका सर्वेक्षणातून ही आकडेवारी ('संमिश्र'वर)



(स्रोत : स्टॅटिस्टा रिपोर्ट, डिसेंबर २०२२ पर्यंतची स्थिती)

अमेरिका अशा घटनांमध्ये दुसऱ्या क्रमांकावर आहे. तेथे ४९% लोकांना सायबर क्राइमचा वाईट अनुभव आहे.

१२ हजार सरकारी वेबसाइटस् धोक्यात

केंद्राचा इशारा; हॅक्टिव्हिस्ट इंडोनेशियाने जाहीर केली यादीं

नवी दिल्ली : भारतातील केंद्र व राज्य सरकारांच्या १२ हजार वेबसाइटस्ची यादी हॅक्टिव्हिस्ट इंडोनेशिया या गटाने जारी केली आहे. या वेबसाइटवर त्या गटाकडून नजीकच्या काळात सायबर हल्ला होण्याचा मोठा धोका आहे. त्यामुळे केंद्र, राज्य सरकारांची विविध खाती, तसेच अन्य यंत्रणांना अतिशय सतर्क राहण्याचा इशारा केंद्रीय गृह खात्याने दिला आहे.

सायबर हल्ले चढविणाऱ्या प्रवृत्ती देश किंवा विदेशातून सक्रिय असू शकतात. भारत व अन्य देशांतील वेबसाइट हॅक्टिव्हिस्ट इंडोनेशिया या गटाने याआधी हॅक केल्या आहेत. त्या गटाने भारतातील १२ हजार वेबसाइटची यादी जारी केल्याची माहिती सर्वांत प्रथम केंद्रीय इलेक्ट्रॉनिक्स व माहिती मंत्रालयाच्या अखत्यारीतील कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीमने केंद्र सरकारला दिली. विविध राज्ये सरकारांच्या वेबसाइटवर हल्ले होण्याचा मोठा धोका असल्याचेही या टीमने कळविले. त्यानंतर सर्व राज्यांना याची तातडीने माहिती देण्यात आली. (वृत्तसंस्था)

- या गटाकडून चीन, तसेच युक्रेनच्या वेबसाइटवरही हल्ला होऊ शकतो, असे केंद्र सरकारच्या सूत्रांनी सांगितले.
- हॅक्टिव्हिस्ट इंडोनेशिया भारतातील सरकारी व अन्य वेबसाइटवर सायबर हल्ला करण्याची अशी शक्यता गेल्या वर्षापासून वर्तविण्यात येत होती.

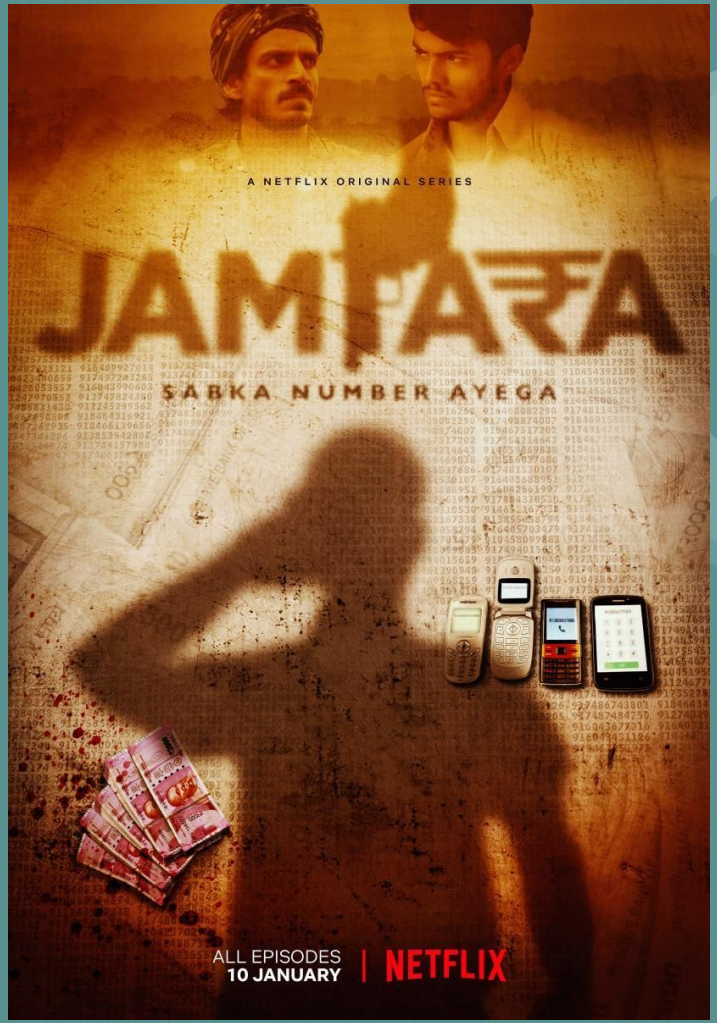
कोण आहे हॅक्टिव्हिस्ट?

- हॅक्टिव्हिस्ट इंडोनेशिया असे नाव असले तरी हा गट इंडोनेशियातीलच आहे असे खात्रीलायकरीत्या सांगता येत नाही.
- सायबर हल्ले करणारा हा गट मलेशिया किंवा अन्य इस्लामी देशांतूनही कारवाया करत असण्याची शक्यता नाकारता येत नाही. तशा हल्ल्यांचे काही प्रयत्नही झाले होते; पण आता त्या गटाने भारतातील सरकारी वेबसाइटची यादीच जाहीर केल्याने या प्रकरणाला गंभीर वळण लागले आहे.

गुजरातच्या वेबसाइटवर गेल्या वर्षी हल्ले

या गटाने गेल्या वर्षी गुजरात सरकारच्या वेबसाइटवर हल्ले केले होते. वेबसाइटचे कामकाज स्लोडाउन व्हावे, देण्यात येणाऱ्या सेवांचा लोप कोणालाही घेता येऊ नये, असे प्रयत्न गटाने केले होते. डिजिटल्युवेद डिनायल ऑफ सर्व्हिस प्रणालीचा वापर करून सायबर हल्लेखोर सरकार किंवा खासगी वेबसाइटवर आपले नियंत्रण प्रस्थापित करतात, असा काही प्रकार घडल्यास त्याची माहिती सरकारी यंत्रणा cybercrime.gov.in या वेबसाइटवर त्वरित देऊ शकतात असे केंद्र सरकारने म्हटले आहे.

देशभरात सर्वाधिक प्रकरणे महाराष्ट्रात : चिंतेची बाब म्हणजे सायबर क्राइम आणि त्याला बळी पडलेल्यांमध्ये जगात भारतीयांचे प्रमाण सर्वाधिक आहे. भारतात 68 टक्के यूझर्स डिसेंबर 2022 पर्यंत वेगवेगळ्या कारणांनी सायबर गुन्ह्याला बळी पडले आहेत. नोव्हेंबर ते डिसेंबर 2022 दरम्यानच्या स्टॅटिस्टाच्या सर्वेक्षणातून ही आकडेवारी समोर आली आहे. सायबर वर्ल्डद्वारे होणारा पाठलाग अर्थात सायबर स्टॉकिंगमध्ये महाराष्ट्र (2021)मध्ये देशात पहिल्या क्रमांकावर होता. देशभरात सर्वाधिक प्रकरणे महाराष्ट्रातून उघडकीस आली होती. त्याचबरोबर भारतामागोमाग अमेरिकेत 49 टक्के सायबर क्राईमचे प्रमाण आहे. तर, जपानमध्ये 21 टक्के, जर्मनीत 30टक्के, इंग्लंड आणि फ्रान्समध्ये 33 टक्के आणि न्युझीलँडमध्ये 38 टक्के इतके सायबर क्राईमचे प्रमाण आहे असही ते म्हणाले आहेत.


A NETFLIX ORIGINAL SERIES
JAMTARA
SABKA NUMBER AYEGA
ALL EPISODES
10 JANUARY
NETFLIX


A NETFLIX
ORIGINAL
JAMTARA
NETFLIX

सायबर साक्षर होणे काळाची गरज आहे

सायबर क्राईम म्हणजे काय सायबर क्राईम चे प्रकार कोणते आहेत प्रत्येक नागरिकाला याची माहिती करून देणे आज आवश्यक आहे यासाठी प्रत्येक नागरिकांनी सायबर साक्षर होणे महत्त्वाचे आहे
अनोळखी व्यक्तीला मोबाईल वरून कॉल आल्यास ओटीपी किंवा बँक माहिती युपी आयडी कोणाशी शेअर करू नये ऑनलाइन फोन किंवा कोणत्याही ॲपच्या माध्यमातून दाखवल्या जाणाऱ्या अमिषाला बळी पडू नये आपली प्रोफाईल लॉक करून ठेवावे मोबाईल मध्ये अनोळखी लोकांनी पाठवलेल्या कोणत्याही लिंक वर क्लिक करू नये अनोळखी नंबरचा व्हिडिओ कॉल आल्यास कॉल उचलु नये मी मोबाइलयावर अनोळखी स्त्री किंवा पुरुष व्यक्तीची फ्रेंड रिक्वेस्ट अजिबात स्वीकारू नये
सुंदर आवाजात व सुंदर चेहऱ्यात दिसणारी स्त्री ही स्त्री असते तसं नाही

रिपोर्टिंग पोर्टल

- आपल्याला बँकिंग किंवा संवेदनशील वैयक्तिक माहिती विचारणारे कोणतेही फसवे एसएमएस, ई-मेल, फोन कॉल प्राप्त झाल्यास, महाराष्ट्र सायबरच्या **www.reportphishing.in** या पोर्टलवर तात्काळ रिपोर्ट करा.
- सायबर गुन्हे नोंद करण्यासाठी, **https://cybercrime.gov.in** या संकेत स्थळावर तक्रार नोंदवा.
- आपला मोबाईल चोरी झाल्यास किंवा हरवल्यास मोबाईलचा IMEI क्रमांक ब्लॉक करण्यासाठी, **www.ceir.gov.in** या संकेतस्थळावर रिपोर्ट करा.
- आपल्या मोबाईलचा १५ अंकी IMEI क्रमांक ***#06#** डायल करून नोंद करून ठेवा
- महिला आणि बालकांसाठी सायबर गुन्ह्यांच्या तक्रारी करीता Toll Free Helpline Number **155260**


THANK YOU